THALES
Building a future we can all trust

Cyber Threat Handbook

2022

Contents


Cyber threats in a nutshell
Attackers groups
Targeted sectors
Geographical zones
Editorial
References
Index

Index

_EDITORIAL p.7

_WORLDWIDE CYBER THREATS IN A NUTSHELL p.11

_GEOGRAPHICAL ZONES : p.12

_Zone Europe p.12
_Zone Commonwealth of Independent State p.18
_Zone Africa p.24
_Zone North America p.30
_Zone South America p.38
_Zone Western Asia p.44
_Zone East Asia p.52
_Zone South Asia p.58
_Zone Oceania p.64

_ATTACKERS GROUPS : p.71

_**ATK1**, DragonFish, Lotus Blossom. p.72
_**ATK103**, Gold Tahoe, Graceful Spider. p.76
_**ATK104**, Mummy Spider, Mealybug. p.80
_**ATK11**, APT-C-09, Chinastrats. p.84
_**ATK112**, APT-C-38, ZooPark. p.88
_**ATK113**, FIN8. . . .. p.92
_**ATK116**, Cloud Atlas, Inception group. p.96
_**ATK117**, APT 38, Bluenoroff. p.100
_**ATK120**, Cobalt Lyceum, HEXANE. p.104
_**ATK128**, OurMine. p.108
_**ATK13**, Group 88, Hippo Team. p.1112
_**ATK132**, Deadeye Jackal, SEA. p.116
_**ATK133**, UCC, United Cyber Caliphate. p.120
_**ATK14**, Black Energy, ELECTRUM. p.124
_**ATK15**, APT27, Bronze Union. p.128
_**ATK168**, PINCHY SPIDER, REvil Ransomware Gang. p.132
_**ATK17**, APT-32, APT-C-00. . . .. p.136
_**ATK2**, APT 17, APT 41. . . .. p.140
_**ATK23**, Dagger Panda, Ice Fog, Icefog. p.144
_**ATK233**, HAFNIUM. p.148
_**ATK234**, SPIRAL. p.152
_**ATK236**, GOLD CABIN, Shathak, TA551. . . .. p.156
_**ATK237**, Grandoreiro Operator, Guildma / Astaroth Operator. p.160
_**ATK241**, Agrius. p.164
_**ATK27**, Dark Caracal, TAG-CT3. . . .. p.166
_**ATK29**, APT 40, BRONZE MOHAWK. p.170
_**ATK3**, COVELLITE, Hidden Cobra. p.174
_**ATK32**, FIN7, GOLD NIAGARA. p.180
_**ATK33**, PLATINUM, TwoForOne. p.184
_**ATK35**, APT33, COBALT TRINITY. p.188
_**ATK4**, APT37, Dark Seoul. p.192
_**ATK40**, APT34, CHRYSENE. p.196
_**ATK41**, APT10, BRONZE RIVERSIDE. p.200
_**ATK5**, APT28, Fancy Bear. p.204
_**ATK51**, MERCURY, MobhaM. p.210
_**ATK52**, APT-C-06, DUBNIUM. p.214
_**ATK6**, CrouchingYeti, DYMALLOY. p.218
_**ATK64**, APT36, C-Major. p.222
_**ATK66**, APT-C-23, Arid Viper. p.224
_**ATK7**, APT29, Cozer. p.228
_**ATK73**, TAG-CR4, TDO. p.232
_**ATK78**, Thrip. p.236
_**ATK8**, Animal Farm, SNOWGLOBE. p.240
_**ATK80**, APT-C-27, Golden RAT. p.244
_**ATK86**, Silence, Silence APT group. p.248
_**ATK88**, FIN6, ITG08. . . .. p.252
_**ATK89**, Extreme Jackal, Gaza Hackers Team. p.256
_**ATK91**, TEMP.Veles, TRITON group. p.260
_**ATK92**, Gorgon group, Subaat. p.266

_TARGETED SECTORS : p.270

_Automotive p.274
_Aviation p.276
_Communication p.278
_Civil Society p.280
_Education p.282
_Energy p.286
_Financial p.292
_Government p.294
_Health p.296
_Information Technology p.298
_Legal p.300
_Manufacturing p.302
_Maritime p.304
_Media and Entertainment p.306
_Retail p.308
_Space p.312
_Transportation p.316

_OUR EXPERTS p.320

_REFERENCES p.324

Editorial

Cyber threats no longer have borders and we are now facing increasingly organized and international groups. The networks of attackers have professionalized and today target government organizations such as large companies or even the smallest ones.
In recent years, recent health and geopolitical crises have further increased the tensions of the Cyber World and we now observe attacks targeting all sectors of activity whether for lucrative purpose as ransomware attacks, espionage or even, data theft.
The first weapon in the face of this threat is to be able to understand our opponents, their techniques, tactics and procedures of attackers in order to ensure to protect the critical assets of our clients and government partners.
As the European leader in cyber security and the worldwide leader in data protection, Thales addresses the entire information security lifecycle, the cornerstone of digital trust. Thales helps secure the digital transformation of the most demanding government bodies, private firms and critical infrastructure providers.
Capitalising on our teams worldwide, with more than 11 consultancy teams and 6 Security Operation Centres, we can leverage our international threats expertise to ensure cyber protection to our customers from space to the ground and from information systems to operational technologies.
Our Cyber Threat Intelligence expert team is screening on a daily basis a rich database and multiple cyber threat sources around the world, which we have been monitoring for several decades in order to ensure actionable strategies for critical companies or governments. It relies among other things, on collaboration and transparency between organizations to ensure the right sharing of information.
Today, we want to provide as many expertise and solutions as possible for a cybersecurity that only makes sense if it is collective. It is with this objective that we wanted to broaden the scope of our Cyber Threat Atlas named “Cyber threat Hitmap” and provide it, for the first time, in a digital format opened to everyone.
Our Thales Cyber Threat Atlas will open-source to everyone a detailed knowledge of the cyber threat ecosystem by contextualizing the activity of attacker groups.
For this, we have selected a sample of 50 preliminary attacker groups that we believe are particularly important in today’s cyber threat landscape. The knowledge of these attackers, their nature, their motivations, their tools and their operating methods served as a basis for the construction of this Atlas.
This work, which comes from both geographical and sectoral angles, offers several complementary reading grids. Our analysis shows a breakdown into fourteen sectors of activity, allying the most traditional sectors (transportation, energy, education and research, telecommunications, health, government, legal, finance, manufacturing, retail) to innovative industries (automotive, space, maritime, aviation) which by the strategic nature of their activity are of interest to advanced threat actors.
Thales uses directly this information to feed its Cybels offer of tools and services and provide high added value actions to ensure a better protection for everyone.
Understanding the geostrategic frameworks as well as main targeted sectors threats is key to the relevance of Cyber detection and protection. Combined, they provide much better understanding state of the threat.
I am sure that you will be able to make good use of this book for your detection and protection needs and I wish you a good read and regular browsing on http://cyberthreat.thalesgroup.com/ for live updates!

Pierre-Yves Jolivet,
Vice-President Cyber Defence Solutions, Thales

For more informations:
cyberthreat.thalesgroup.com

Geographical zones

Worldwide Cyber Threats in a Nutshell*

_Most targeted sectors**

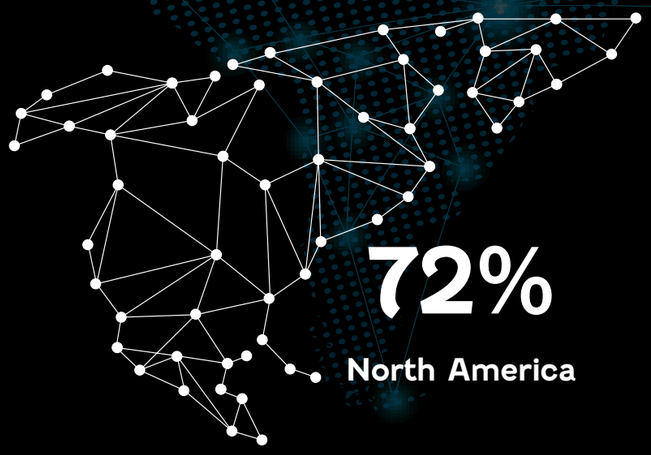
72% Defence and administration

62% Communications

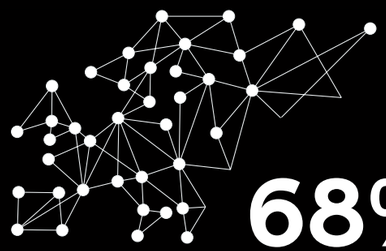
48% High technologies

40% Finance

_Most targeted areas



72% North America



68% Europe

*Analysis of the past two years
**As part of the website panel

+30%
Increase in attacks between 2020 and 2021, in the Europe area.

_The most significant attacks in recent years

Early 2022

Since January/February 2022, Ukraine underwent numerous attempts of destructive attacks (wiper)

Since the beginning of the conflict in Ukraine, the cyber community has observed the appearance and often the use of malware designed to destroy/erase the target's systems.
We can mention: WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AcidRain and to some extent Industroyer 2.0.

Mid 2021

Kaseya Supply Chain attack with REvil ransomware

In July 2021, several Managed Service Providers (MSPs) have been targeted by the Revil group. The threat group exploited a flaw in Kaseya VSA (a cloud-based MSP patch management and monitoring platform) to spread the Revil ransomware.

End of 2020

SolarWinds supply chain attack

In December 2020, FireEye uncovered a widespread espionage campaign that targeted numerous public and private organizations around the world since Spring 2020. The threat actor gained access to victims via trojanized updates to SolarWind's Orion IT monitoring and management software (affected versions are 2019.4 through 2020.2.1 HF1).

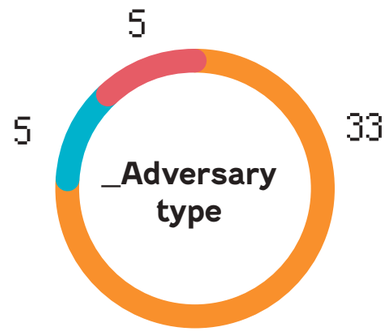
Zone Europe_

Albania
Andorra
Austria
Belarus
Belgium
Bosnia-Herzegovina
Bulgaria
Croatia
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Ireland
Italy
Kosovo
Latvia
Liechtenstein
Lithuania
Luxembourg
Northern Macedonia
Malta
Moldova
Monaco
Montenegro
Netherlands
Norway
Poland
Portugal
Romania
San Marino
Serbia
Slovakia
Slovenia
Spain
Sweden
Switzerland
Ukraine
United Kingdom
Vatican Republic

65 ATKS (Attackers)
targeted European countries

_Adversary Type

- _Terrorists
- _State-Sponsored
- _Cyber Criminal



_Top 3 attacked sectors

Energy
Education
Manufacturing

- _Energy
- _Manufacturing
- _Communication
- _Transportation
- _Education
- _Aviation
- _Retail

Contextual analysis of Europe and geocyber risks

Europe today is an incredibly complex geopolitical space — the result of centuries of history marked by a constant oscillation between strife and union. It is composed of over 40 different countries and cultures with a great diversity of national and regional languages.
Geographically, Europe comprises a highly developed Western Europe, which has long been open to globalisation and its Atlantic interface; a Southern Europe with a Mediterranean culture and outlook; an Eastern Europe observing Western Europe on one side and Russia on the other; and a Northern Europe around the Baltic. Modern Europe continues to reflect this history and geography.
Despite these geostrategic and cultural differences, a European cooperation has been built around the European Union, the euro zone[1] and bilateral and/or multilateral agreements. The European continent is a privileged territory for the development of cyber threats: the size of the attack surface (governmental structures, enterprises) provides opportunities for cybercriminals, and different motivations can come into play, as Europe is both the cradle of companies willing to pay ransoms and a powerful symbol of the western world - justifying ideology-based attacks.

TERRITORY AND IDENTITY: THE RISK OF CYBER DESTABILISATION

One of the greatest geocyber risks that Europe faces is destabilisation. The purpose of Europe as a combined entity is to be unified in order to ensure a shared development and a place on the international stage. This can lead to attempts to weaken it from abroad. One striking example is Brexit, which has marked a profound geopolitical reconfiguration in Europe. This shift has been exploited by threat actors to weaken political entities such as the European Union and the United Kingdom itself.

_BREXIT EXPLOITED AS A WAY TO TARGET GOVERNMENT AGENCIES IN THE UK AND WESTERN EUROPE

In 2018, the ATK5 (APT28, Sofacy) group, known for its involvement on the 2016 U.S presidential election campaign and its allegedly close ties to Russian intelligence, conducted a phishing scheme targeting Western Europe and the United Kingdom in particular.

Fake Brexit-related document containing the Zebrocy malware were sent to multiple specific targets, enabling ATK5 to break into the computer networks of European government agencies. Most importantly, this attack displays the ability of attacker groups to leverage sensitive political issues and turn them into potential attack vectors. Zebrocy acted as a first-stage backdoor and was used to perform system reconnaissance, create or modify files, execute commands, take screenshots and create Windows scheduled tasks[2].

_PLAYING ON THE WEST'S FEARS: THE EXAMPLE OF THE ATTACK ON TV5MONDE

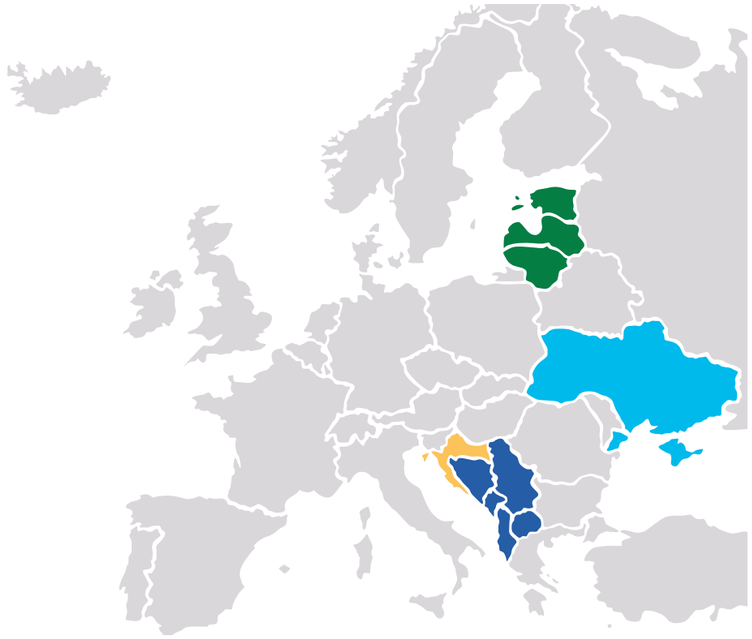
Some attacks also take advantage of internal crisis in certain countries to destabilise public opinion. On 8 April 2015, a hacker group took control of the TV5Monde website and its social media accounts and caused television programmes to be interrupted for several hours. We now know that this attack was carried out by ATK5 (APT28), although it has not been directly attributed to the group. A hacker group calling itself the Cyber Caliphate, linked to so-called Islamic State, first claimed responsibility. To shed light on the attack and identify the real perpetrators, TV5Monde called in technical experts from ANSSI, France's national agency for information system security, who restored service and conducted a forensic investigation to search for clues. As their investigation progressed, suspicions began to point to ATK5 (APT28). The evidence gathered by the experts looked similar to a modus operandi already used by the group. As reflected in this attack, it should be noted that groups such as ATK5 (APT28) use visceral issues of contention between or within European countries to destabilise and weaken them[3]. Interestingly enough, the main destabilising agent is not the attacks itself but rather its erroneous attribution to an entity close to ISIS, creating an alliance of circumstance between an ideological opponent wishing to undermine European influence and a civilizational adversary who uses the claim to instil fear within the population.

_TERRITORY AND DEVELOPMENT: CYBERCRIME RISK AND INDUSTRIAL ESPIONAGE

Europe has many large corporations and SMEs (Small to medium-sized enterprises) that are interdependent at continental level. They are also part of the global economy. This European financial, industrial and innovation ecosystem inevitably attracts the attention of large cybercriminal groups as well as actors motivated by industrial espionage.

_THE ERA OF CYBER-EXTORTION AND THE RISK OF GLOBAL SUPPLY CHAIN ATTACKS

On 30 January 2020, French contractor Bouygues Construction was the victim of an attack claimed by the group of attackers behind the Maze ransomware[4]. The operators demanded a ransom of €10 million from the French group in exchange for a decryption key and the guarantee that its sensitive data would not be leaked. On 21 October 2020, Sopra Steria announced that it had fallen victim to the Ryuk ransomware[5]. A month later, in November 2020, Italy-based international energy group Enel announced that it had become the victim of the Netwalker ransomware and that its operators were demanding a payment of some €14 million[6]. Most European companies are closely integrated into the market economy and are therefore especially vulnerable to supply chain attacks. During the REvil ransomware attack on IT management software company Kaseya in July 2021, over 1,000 other organizations were impacted, mostly in Europe[7]. Swedish supermarket franchise Coop had to close 800 stores because they were unable to use their cash registers[8]. This supply chain attack culminated in a record ransom demand of $70 million in return for a universal decryption key.



_AIRBUS VICTIM OF INDUSTRIAL ESPIONAGE AND THE RISK OF GLOBAL ATTACKS VIA THE SUPPLY CHAIN

Supply chain attacks on European industrial or financial groups are not only motivated by financial gain but also by technological catch-up. As a result, industrial espionage against major European corporations is now a significant threat. In 2019, Airbus was hit by a supply chain attack designed to steal information about the A350 airliner and the A400M military transport plane[9]. The attack was initially attributed to the Chinese hacker group ATK41 (APT10), then to the ATK146 group (Avivore)[10]. It should be noted that it is difficult to determine the exact origin of this attack, mainly because Chinese espionage groups tend to share their infrastructure and attack tools. This sophisticated attack demonstrated the strategic adaptability of certain groups and the advanced threat posed by supply chain attacks. For the attackers, the impossibility of a frontal attack on the Airbus group was circumvented by compromising suppliers of the aircraft manufacturer such as Rolls-Royce or Expleo, laying the ground for actors with basic capabilities to attack high value targets[11].

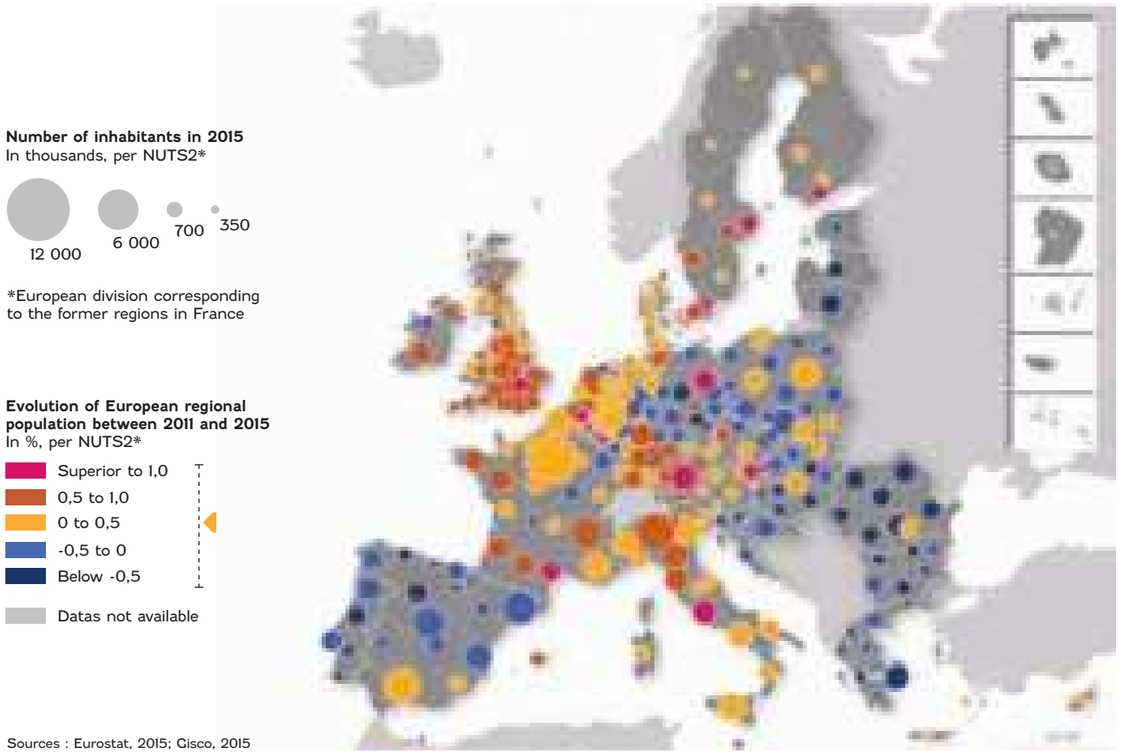
_TERRITORIES AND POLITICAL MODELS: RISK OF STRATEGIC INCIDENTS

Europe, as we explained earlier, is a geopolitical space with a diverse array of identities, territories, political orientations and societies, which can lead to conflicts.

_AREAS OF INSTABILITY

UKRAINE
On the edge of Europe, in Ukraine, an armed conflict between Ukrainian government forces and Russian separatist militias has been ongoing since 2014. It is the result of the annexation of Crimea by Russia, which provoked an open war in eastern Ukraine. In 2014 and 2015, Germany, France, Ukraine and Russia ratified two different versions of the Minsk agreements to settle the conflict and end the fighting in the industrialized regions of Donetsk and Luhansk. These agreements were never implemented and the conflict was prolonged, taking the form of a trench war along the front line. The conflict has escalated in December 2021 with Russia moving troops near the border, making western governments fear a military attack of Ukraine[12].

French regions that largely contribute to European demographic growth



Sources : Eurostat, 2015; Gisco, 2015

_CYBERATTACKS AGAINST UKRAINE AMID TENSIONS WITH RUSSIA

The ongoing armed conflict between the Ukrainian military and pro-Russian troops has sparked an intense cyber activity in the region, targeting especially the Ukrainian territory.
The ATK14 hacker group (BlackEnergy) has long been known for targeting companies in Europe's energy sector. Starting in early 2015, the group infiltrated a large number of Ukrainian electricity distribution companies in order to install the BlackEnergy malware and access their OT/SCADA infrastructure. On 23 December 2015, hackers successfully compromised the SCADA systems of three Ukrainian energy companies and shut down their substations. They used the KillDisk plugin to destroy files on workstations. The group also launched a more conventional DDoS attack on the call centres of the three companies to make them unavailable to customers. The attack left about 230,000 people without power for nearly six hours in the Ivano-Frankivsk, Chernivtsi and Kiev oblasts (regions). This attack is one of the first cases of cyber sabotage directed at a power grid and demonstrates the determination and skill of the attackers. It is still not known whether the malware caused the power outage, or simply allowed its operators to do it manually.
On June 2017, a major cyberattack hit Ukrainian companies. The malware used is a new version of Petya, a family of ransomware uncovered in 2016, which had been infecting Windows-based systems. This attack dubbed NotPetya, initially targeting Ukrainian infrastructures spread globally and is still considered as one of the most destructive cyberattack ever achieved. The attackers leveraged the EternalBlue vulnerability and used unpatched computers to propagate across entire networks. The UK government, through its National Cyber Security Centre asserted with a high degree of confidence that the Russian military had carried out the NotPetya cyberattack, whose objective was to disrupt energy companies and government institutions in Ukraine13. The estimated cost for the global economy reaches 10 billion dollars.
On the night of January 13-14, 2022, a cyberattack named "Operation Bleeding Bear" affected several Ukrainian government sites, rendering the computer structure of state-owned sites temporarily inoperable. This low-complexity attack consisted of the defacement of the targeted sites with the replacement of the homepage with a propaganda message in Ukrainian. It seems that the attacker exploited a known vulnerability in a content management system (CMS). Besides, a dozen of systems (Windows and Linux) were also destroyed by a wiper malware. This attack comes in a context of escalating tensions due to the failure of negotiations and the massive presence of pro-Russian forces stationed at the border. If Ukraine points the finger at the group of hackers known as UNC1151, affiliated with the Belarusian secret service, the low level of technicality of the attacker opens up a wide range of possibilities in terms of its origin, from individual hackers to state-sponsored groups. This attack is indicative of the use of non-traditional fields including cyber in the pursuit of political objectives. In this case, the destabilization of the Ukrainian government as well as the loss of confidence of the Ukrainian population towards its institutions seem to be the objectives pursued.

WESTERN BALKANS
The Western Balkan is a region composed of several eastern European countries, namely Bosnia-Herzegovina, Croatia, Kosovo, Northern Macedonia, Montenegro, Serbia and Slovenia. In this region, where ethnic and religious tensions still exist between Kosovo and Serbia, and within Bosnia-Herzegovina itself, the European Union is trying to bring political stability through agreements pending eventual integration[14]. The issue remains complex because Russia also exerts an influence in the region, which can exacerbate geopolitical destabilisation and lead to cyberattacks.

BALTIC STATES
The Baltic states are a region where the homogenisation four dimensions — identity, society, politics and territory — is proving difficult. These countries, which declared independence in 1990 after the collapse of the Soviet Union, quickly sought to distance themselves from Russia's sphere of influence by refusing to be integrated into the Commonwealth of Independent States (CIS) and instead joining the EU and NATO in 2004. Since the 2016 Warsaw Summit., they have benefited from NATO airspace and on the ground protection. While the region may seem well protected, it remains surrounded by Russian influence to the east and south (Kaliningrad enclave and Russian forces in Belarus) and lies in part alongside Russia's access route to the Baltic Sea. It should also be noted that there are significant Russian minorities in these countries (26.5% in Estonia, 26% in Latvia and 5.8% in Lithuania)[15].

_MASSIVE CYBERATTACKS IN ESTONIA

In April 2007, dozens of Estonian organisations — Parliament, banks, government ministries, newspapers, etc. — were simultaneously targeted by a DDoS attack. In this large-scale campaign, one of the malwares used was none other than BlackEnergy from the ATK14 group (BlackEnergy). As a result of these significant and destructive attacks, NATO decided to set up its Cooperative Cyber Defence Centre of Excellence, which is based in Estonia.

_A POWER SPACE AT RISK FROM STRATEGIC ESPIONAGE

In addition to these attacks, which are exceptional in terms of their consequences, European countries are regularly under threat from strategic espionage campaigns by foreign groups.

CONTINUOUS ESPIONAGE
In November 2019, ANSSI, France's national agency for information system security, reported cyberattacks against service providers and design offices. The hackers used the PlugX malware to infiltrate their systems, steal data and, almost certainly, access the networks of their clients. In July 2021, it was discovered that the Pegasus spyware was being used on a massive scale — a reminder of the strategic nature of certain types of cyberattacks. More recently, in September 2021, the German authorities announced that German politicians had been spied on in the run-up to the federal elections by the Ghostwriter gang, an APT group known for its alleged close ties with Russian military service GRU. This is not the first time Germany has been at the center of an espionage-motivated attack campaign, as between 2017 and 2018 its government agencies were reportedly targeted by ATK56 (APT28), another group linked to Russia. During this incident, the hackers managed to gain access to the network of several German ministries (foreign affairs, defence) as well as the German's Chancellery and the Federal Court of Auditors. German interests are also closely scrutinized by other countries, most notably Iran and China. The activity of Iranian attack groups on German targets has intensified recently with the rise of tensions in the Gulf and the maintenance of financial sanctions. A report by the Dutch intelligence services even pointed to the Iranian strategy of using cyber espionage as a tool in the quest to acquire European military technology. This strategy even extends to the political domain with the surveillance of its expatriate population in the Netherlands and the monitoring of the criticism addressed to the Iranian regime[16].

Conclusion

As we have seen, Europe is a complex geopolitical space where multiple spheres of power and various models are at play, chief among them the European Union, NATO and Russia.
These models sometimes clash, leading to crises that are conducive to the emergence of cyberthreats — as in Ukraine, the Baltic countries and the Western Balkans.
Europe is the product of permanent oscillation between unity and plurality of identities, with political aspirations that can provoke societal, economic, political and territorial crises, and that can be utilised as levers of destabilisation by cyberattacker groups.
Europe is also highly integrated into the globalisation process, with industrial and financial champions, but also thanks to a myriad of SMEs, which are permanent targets of organised cybercrime and even industrial espionage.

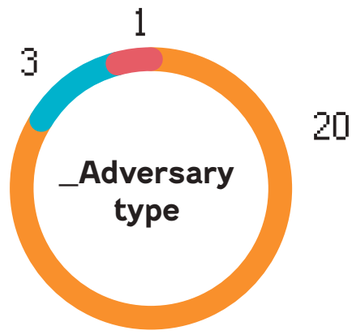
Zone Commonwealth of Independent States_

Armenia
Azerbaijan
Belarus
Georgia
Kazakhstan
Kyrgyzstan
Moldova
Russia
Tajikistan
Turkmenistan
Uzbekistan

12 ATKS (Attackers)
targeted European countries

_Adversary Type

_Terrorists _State-Sponsored _Cyber Criminal



_Top 3 attacked sectors

Energy
Transportation
Manufacturing

- _Energy
- _Manufacturing
- _Communication
- _Transportation
- _Education
- _Aviation

Contextual analysis of CIS and geocyber risks

On 8 December 1991, just before the USSR officially collapsed, Russia, Ukraine and Belarus signed the Minsk Treaty. This treaty established the Commonwealth of Independent States (CIS), which was intended to guarantee a form of multilateral consistency between the former Soviet republics, despite the overall disintegration.

On 21 December, Armenia, Azerbaijan, Turkmenistan, Kazakhstan, Kyrgyzstan, Uzbekistan, Moldova and Tajikistan joined the CIS. Two years later, in 1993, Georgia joined the group. It should be noted that the Baltic States, former soviet socialist republics, never joined the CIS.
This organisation, built on the historic foundations of the Eastern Bloc, is made up of a set of complex, intertwined dynamics, a Soviet Union centred on Moscow and the influences of new powers in a multipolar world.
This confrontation leads to the emergence of regional tensions that justify the use of cyber as a vector of influence.

_CAUCASUS: A STRATEGIC CROSSROADS

The Caucasus is a strategic zone in several respects. First, geographically, it serves as a buffer zone between two continents: Europe and Asia. North of the Greater Caucasus mountain range, on the Georgian and Azerbaijani borders, lies Russia, the former heart of the Soviet Union. To the south is Turkey, with its Sunni nationalist culture, and Iran, which has a Shiite Islamic culture. The three countries are geographically intertwined and bordered to the east by the Caspian Sea and the west by the Black Sea.
This particular geography and topography makes the Caucasus a narrow corridor and a crossroads of cultures and identities. This crossroads is also strategic and lead certain nearby powers — such as the European Union (with NATO), Turkey, Iran and Russia — to assert their influence in the region

_SEPARATISM, NATIONALISM AND JIHADISM IN GEORGIA

After the fall of the USSR, many internal conflicts broke out. In Georgia, a civil war (1991-1993) pitted the secessionist provinces of Abkhazia and South Ossetia against the central government in Tbilisi[1].
Geographically, the Caucasus extends into Russian territory, with the North Caucasus. It was in the North Caucasus that the First Chechen War erupted in 1994. This conflict — as in Abkhazia and South Ossetia — was the scene of confrontation between independence movements and a former Soviet republic, in this case Russia.

The regional consequences of the Russo-Chechen conflicts are significant and make terrorism even more entrenched. For example, the Pankisi Gorge crisis from 2002 to 2003 saw Georgia clash with Chechen rebels and members of Al-Qaeda.
The 2000's were also marked by the appearance of colour revolutions in former Soviet republics, in Georgia in 2003 (Rose Revolution), in Ukraine in 2004 (Orange Revolution) and in Belarus in 2005 (Jeans Revolution). Characterized by popular, peaceful demonstrations, these revolutions highlight the confrontation between Western influence and Russia's desire to control its near abroad. The democratic aspirations of the people and the spectre of the emergence of pro-Western civil societies in the region motivate Russian interference, particularly through disinformation campaigns as a part of a more global hybrid warfare strategy.

In 2008, a war broke out between Georgia and South Ossetia, supported by Russia, Abkhazia and the CIS armed forces. This conflict, which Georgia lost, allowed to leave the CIS. This conflict signals the resurgence of Moscow's influence, which is posing as the protector of secessions.
In 2007 and 2008, around the time of the Russo-Georgian War and the widespread attacks in Estonia, the ATK5 group (APT28) really began to structure its attack campaigns. From 2007 to 2014, ATK5 (APT28) massively targeted Georgian government agencies, including the Ministry of the Interior and Ministry of Defence, as well as civilians. The ATK14 group (BlackEnergy) also launched massive DDoS attacks against Georgia and later began to target Estonia as well. The source code of the malware was sold at that time, which increased the number of attacks on Georgia. From 2011 to 2013, another ATK14 malware called Potao was used to target Armenia and Georgia. In late 2013, it began to be deployed in Ukraine, with several samples used to target this country. From September 2014, the victims of this malware included Ukrainian government agencies and the armed forces.
In spring 2010, the ATK7 group (APT10) conducted actions across the entire Caucasus and Central Asia, with continued campaigns using PinchDuke against Turkey and Georgia as well as numerous campaigns against other members of the Commonwealth of Independent States, such as Kazakhstan, Kyrgyzstan, Azerbaijan and Uzbekistan. This same malware was identified in Chechnya in 2008. In 2015, ATK7 (APT29) also targeted Georgian entities with the CosmicDuke malware and a file attachment with a name in Georgian that translates "NATO consolidates control of Black Sea. docx".

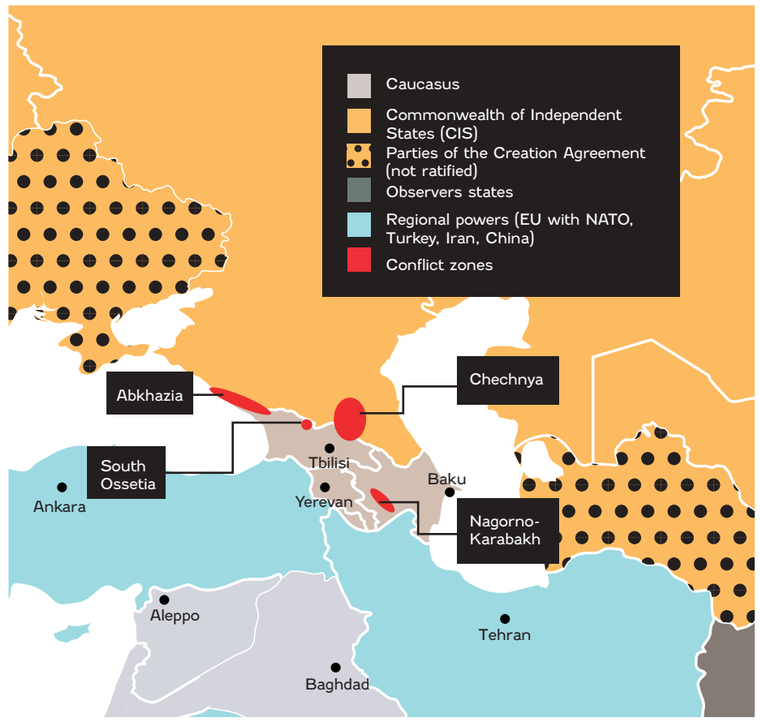
_CONFLICT BETWEEN ARMENIA AND AZERBAIJAN LINKED TO THE QUESTION OF NAGORNO-KARABAKH

The path to the independence of Armenia from Azerbaijan was made in the throes of a war (1988-1994) between these two former Soviet republics. In 2020, a second war broke out between Nagorno-Karabakh, supported by Armenia, and Azerbaijan and the Syrian National Army, backed by Turkey. In November 2020, a ceasefire was jointly announced by the belligerents. Azerbaijan regained possession of the Agdam, Kalbajar and Lachin districts. Tensions are still extremely high in the region and animosity between Armenia and Azerbaijan remains significant.
The 2020 conflict in Nagorno-Karabakh was also the theatre of a lot of cyber activity. The ATK116 group (Inception, Cloud Atlas) was active in October and November 2020 with an espionage campaign based on use of an article entitled: "Armenia transfers YPG/PKK terrorists to occupied area to train militias against Azerbaijan". Both sides were targeted in this campaign. Threat actors also conducted attacks against Armenian targets using Zero Days via Chrome and Internet Explorer. Azerbaijan was targeted by the ATK178 and ATK228 groups and the PoetRAT malware. The targets were highly specific and appeared to be mainly Azerbaijani public and private sector organisations, especially ICS (Import Control System) and SCADA (Supervisory Control and Data Acquisition) systems in the energy sector. The number and variety of tools they used indicate that the attacks were carefully planned. The ATK228 group's main objective was to compromise the wind power companies that produce Azerbaijan's electricity. On 5 August 2020, ATK5 (APT28) also launched an attack campaign using the Zebrocy malware against several NATO member governments, Middle Eastern governments and the Azerbaijan government, which cooperates with NATO. This attack campaign came just days after the clashes between Azerbaijan and Armenia and less than two months before the conflict began on 27 September.

_CENTRAL ASIA AT THE HEART OF INTERNAL TENSIONS AND EXTERNAL INFLUENCES

_CENTRAL ASIA, WITNESS TO RECONFIGURATIONS OF POWER UNDER CHINESE INFLUENCE

The Central Asia region partly corresponds to historic Turkestan.
This region, which is as large as the European Union, is made up of five countries: Kazakhstan in the north, Kyrgyzstan in the east, Tajikistan in the southeast, Turkmenistan in the southwest and Uzbekistan, which is landlocked between these four countries. The Great Steppe covers the north and the South mainly correspond to desert regions.
These five countries, which became independent from the Soviet Union in 1991, are surrounded by Russia to the north and west, China to the east and Iran to the south.
Chinese influence in the region was strengthened with the launch in the fall of 2013 of the «Silk Road Economic Belt.»
It is one of the priorities set by the Chinese government for the years



ahead. An extensive network of transport, pipeline and telecommunication infrastructure will form the physical skeleton of a future Eurasian "economic corridor". This network will link China to Western Europe by land via Central Asia, Asia Minor, the Persian Gulf, the Caucasus and the Balkans. It will also link them by sea via the South China Sea, the Indian Ocean and the Persian Gulf through to the Mediterranean.

The $50 billion Asian Infrastructure Investment Bank (AIIB) and the $40 billion Silk Road Fund were set up by Xi Jinping to inject investment into regional infrastructure. Despite the altruistic rhetoric, Beijing is responding to national priorities and serving primarily Chinese economic, political and strategic interests. While based on the historic aura of the ancient road that linked the Chinese and Roman empires, the objectives of these "new silk roads" are adapted to serve contemporary geopolitical needs.

Central Asia is a key part of the original New Silk Roads project, which aimed to promote the construction of transport infrastructure between China and Europe. Xi Jinping's speech announcing the launch of the Silk Road Economic Belt was made in Astana (renamed Nur-Sultan on 23 March 2019), Kazakhstan. The imagery of the Silk Roads is especially resonant in this part of the world, which was at the heart of the trade flows between Europe, the Middle East and the Chinese Empire prior to the 15th century. Of the six "economic corridors" in the new Belt and Road Initiative (BRI), two directly concern Central Asia: the New Eurasian Land Bridge (China, Kazakhstan, Russia, Belarus, Poland, Germany) and the China-Central Asia-West Asia Economic Corridor (China, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, Turkmenistan, Iran, Turkey).

In spite of having become the first trading partner for central Asia countries, China's interest in its neighbouring region to the west is not only based on an economic vision. For the Chinese central government, helping stabilise and develop the countries on its western front is a way to avoid instability at the gates of its western Xinjiang region. This region, considered unstable by Beijing, is mainly populated by ethnic Uyghurs[2]. Security cooperation between China and Central Asia is largely centred around the Uyghur question and the fight against the "three scourges" identified by the Shanghai Cooperation Organisation (SCO): terrorism, separatism and religious extremism.

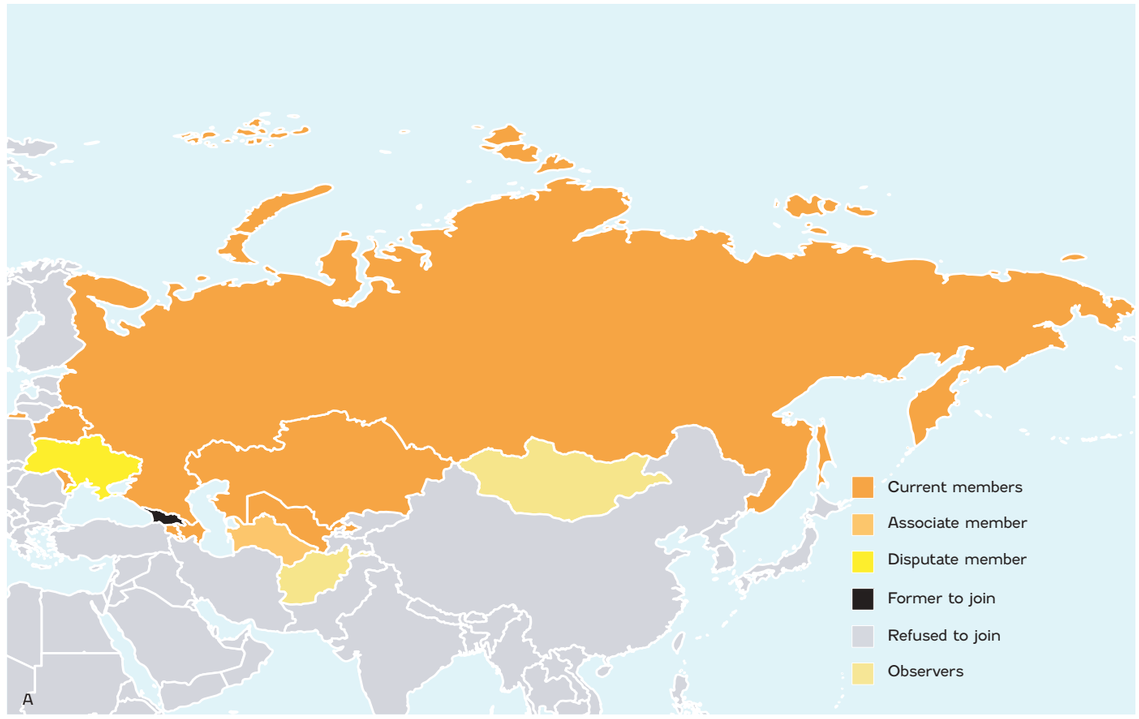
In the years ahead, Russia's reactions to China's growing presence in its historic area of influence will be closely watched. For Russia, the BRI certainly comes with advantages, such as investment capacities that it cannot offer its partners and that will help improve infrastructures and make trade within the EAEU more seamless. Launched in 2015, it does not challenge Russia's monopoly on political-security issues in Central Asia — at least for now — and it supports institutional recognition of the EAEU as a credible and legitimate regional organisation[3]. Nonetheless, China's security presence could be strengthened in the medium or long term with the expansion of Chinese economic interests in the zone, as can be seen in Tajikistan[4].

_LOOKING AT THE MAJOR ATTACKERS WHO HAVE TARGETED THE REGION, WE QUICKLY SEE THAT THE GEOPOLITICAL CONTEXT HAS A SIGNIFICANT IMPACT ON THE NATURE AND STRUCTURE OF THE CYBERTHREAT.

The cyber continuity of the Chinese Silk Road initiative is rendered essential by the need to secure sea and land routes. Among the 360 cyberattack campaigns observed since the birth of the project, one can notice the presence of high-intensity actors with allegedly close ties to Chinese authorities. The ATK15 (Emissary Panda) group launched campaigns between fall 2017 and March 2018 targeting a Central Asian data center. The use of a compromised router (RouterOS Mikrokit) allowed the attacker group to access government resources. While the beginnings of ATK 15 date back to 2009, its recent activity reflects China's need to secure land and sea routes to Europe. Nevertheless, while Central Asian countries and Russia seem relatively unaffected by the massive and repeated attacks that other countries in the region (India in particular) may suffer, several indicators tend to show a reversal of this logic with the spectre of direct attacks on strategic infrastructures in Central Asia or Russia.

Other active hackers in the region such as ATK23 (Icefog) and ATK147 (Poison Carp) have targeted Uyghur and Tibetan minorities in particular.

Commonwealth of Independant States



Conclusion

We have observed that the countries of the Commonwealth of Independent States, which were formerly Soviet republics[5], share two main characteristics. First, they have a high risk of internal instability (within each country and across the broader regions), notably due to the emergence of separatist movements in the Caucasus.

In addition, they are strategically important, because their geographic location fuel the geopolitical appetites of neighbouring powers. The Caucasus is an interface between Continental Europe and East Asia. Central Asia, the heart of Eurasia, is at the crossroads of Russian, Chinese, Iranian and Western (NATO) influences.

This second feature, shared by the two zones and their respective countries, is leading the world's major powers to project their influence on these territories, even if it means taking advantage of or stirring up potential internally destabilising factors

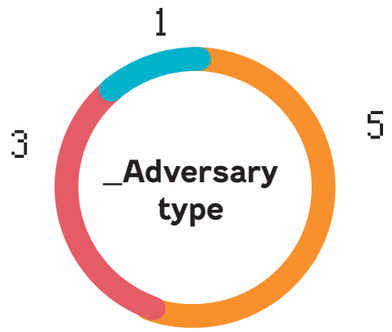
Zone Africa_

Algeria
Angola
Benin
Botswana
Burkina Faso
Burundi
Cape Verde
Cameroon
Central African Rep.
Chad
Comoros
Congo
Congo (Dem. Rep.)
Cote d'Ivoire
Djibouti
Egypt
Equatorial Guinea
Eritrea
Eswatini
Ethiopia
Gabon
Gambia
Ghana
Guinea
Guinea-Bissau
Kenya
Lesotho
Liberia
Libya
Madagascar
Malawi
Mali
Mauritania
Mauritius
Mayotte (FR)
Morocco
Mozambique
Namibia
Niger
Nigeria
Reunion (FR)
Rwanda
Saint Helena (UK)
Sao Tome & Principe
Senegal
Seychelles
Sierra Leone
Somalia
South Africa
South Sudan
Sudan
Tanzania
Togo
Tunisia
Uganda
Western Sahara
Zambia
Zimbabwe

33 ATKS (Attackers)
targeted European countries

_Adversary Type

_Terrorists
_State-Sponsored
_Cyber Criminal



_Top 3 attacked sectors

Energy
Education
Aviation

_Energy	● ●
_Communication	●
_Transportation	●
_Education	● ●
_Aviation	● ●
_Retail	●

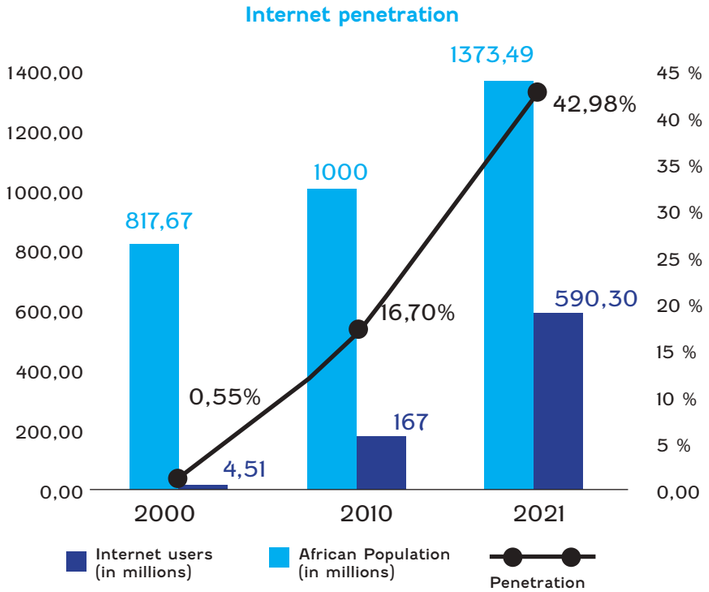
Contextual analysis of Africa and geocyber risks

The cyberthreat on the African continent is complex because the digital transition and cybersecurity are developing at different rates.
This equation is a combination of various strong and rapid dynamics. They include the exponential growth of Internet access and the very young profile of the population, with different uses of technology to other parts of the world. Other factors include weak cybersecurity and cyberdefence infrastructure and culture and almost no visibility of security incidents in most countries.
Added to these issues is the real and/or feared influence of foreign powers.

_MAJOR TRENDS

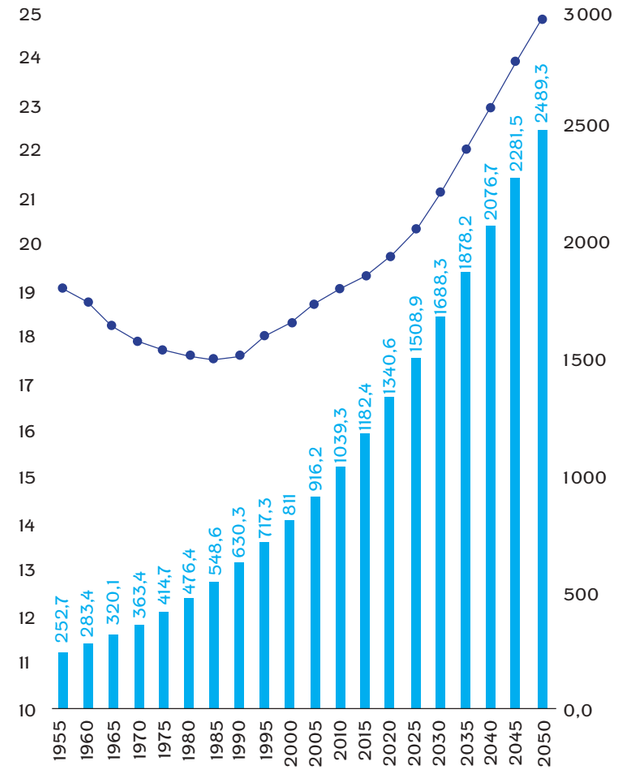
_INTERNET PENETRATION

To understand the cyberthreat in Africa, one of the most significant contextual trends is the exponential growth of Internet penetration in the various countries.
From 2000 to 2021, the African population increased by almost 68%, from 817.67 million in 2000 to 1,373.49 million in 2021. Over the same period, the number of Internet users rose from 4.51 million to 590.3 million, an increase of 12,988.7% [1,2,3,4,5].
In 2021, Internet penetration in Africa extended to 43% of the population, or almost one in two people. This figure is 78 times higher than 20 years ago. Africa today is modern and connected.



_DEMOGRAPHIC STRUCTURE

Added to this hugely important factor, the population is very young and receptive to digital tools, especially mobile devices. According to United Nations forecasts, Africa's median age is expected to rise by five years by 2050 and the population is expected to grow by almost 1.15 billion[6].
In 30 years, Africa will be home to 1.2 billion people under the age of 25, which means that the use of digital tools will continue to grow at an even faster rate. In addition, the increase in the median age by just over five years, coupled with the increase in per capita living standards by 2050, will also lead to a diversification and increase in the use of digital media.
Inevitably, the higher Internet penetration rate will spell an upsurge in the number of interconnections and, as a result, a greater vulnerability and threat surface.
The implication in terms of cyberthreats is directly apparent, but it is probably still underestimated. On the issue of mobile phones, for example, Symantec observed in 2016[7] a considerable growth in the number of malwares directed at the Android operating system, which represents 89% of the smartphone market in Africa. In Nigeria alone, one smartphone in seven was infected by malware in 2016, and by 2019 they were 184.6 million mobile subscribers in the country[8].



African population and median age

African Population (in millions)

Median age of the African population

Mobile Economy Sub-Saharan Africa

Unique mobile subscribers
2019-2025 CAGR: 4.3%
2019 477m
2025 614m
Penetration Rate (% of population)
45% 50%

Mobile internet users
2019-2025 CAGR: 9.7%
2019 272m
2025 475m
Penetration Rate (% of population)
26% 39%

Sim Connection
Excluding licensed cellular iot
2019-2025 CAGR: 4.3%
2019 816m
2025 1.05bn
Penetration Rate (% of population)
77% 86%

Operation revenues and investment
2019 $44.3bn
2025 $48.7bn

Smartphone
% of total connections
2019 45%
2025 65%

4G
of total connections Excluding licensed cellular iot
2019 9%
2025 27%

5G
2025 30m connections
3% % of total connections Excluding licensed cellular iot

Mobile industry contribution to GDP
2019 $155bn
2024 $184bn
9% of GDP

Public funding
2019 $17bn
Mobile ecosystem contribution to public funding

Employment
2019 650,000
Jobs formaly supported by to the mobile ecosystem
+ 1.4m informal jobs

_BY EXTENSION, GSMA ESTIMATES THAT 615 MILLION PEOPLE IN SUB-SAHARAN AFRICA WILL HAVE SUBSCRIBED TO MOBILE SERVICES BY 2025, WITH 64% OF THEM SMARTPHONE SUBSCRIPTIONS[9]. RISKS AND THREATS

This dual dynamic of a rapidly expanding vulnerability surface and the persistence of critical cybersecurity and cyberdefence issues has an impact on the level of cyberthreat observed across the African continent.

_EXAMPLE OF LIBERIA IN 2016

In October 2016, Liberia suffered a massive DDoS (distributed denial of service) attack, which caused all banking transactions to be suspended for half the country[10]. Over half a million security cameras around the world simultaneously attempted to connect to the servers used by Lonestar Cell MTN,[11] the country's largest telecommunications company, leading to an extended service outage.

_EXAMPLE OF SOUTH AFRICA IN 2019

In July 2019, the City of Johannesburg fell victim to a devastating ransomware attack[12]. The operators of the malware, the Shadow Kill Hackers, targeted City Power, the city's main power company, forcing the authorities to shut down the city's website, e-services platform and billing system[13]. Electricity was also cut off for several hours in the city.

_EXAMPLE OF ETHIOPIA IN 2020

In June 2020, 13 official Ethiopian government websites were affected by a cyberattack by the Cyber_Horus Group. The hackers, whose Egyptian origin seems to be established, left several nationalist messages denouncing the filling of the Renaissance Dam on the Nile, reflecting the significant geopolitical tension between Egypt and Ethiopia[14].

_OPPORTUNITIES AND CHALLENGES

The contextual issue for understanding the cyberthreat in Africa is not simply the exponential increase in digital technology across the continent. In reality, the problem also lies in the imbalance between this increase and the status of cybersecurity and cyberdefence in the societies concerned.

_LACK OF CYBER EXPERTS

This imbalance is mainly due to three co-constituent factors. First, it is a human problem, which does not only concern the African continent. In Africa, an additional 100,000 cybersecurity experts are needed in order to respond to the current challenges[15]. And the trends we have discussed will further increase this need.

_POOR VISIBILITY OF THE NUMBER OF SECURITY INCIDENTS

There is also a cultural issue in cybersecurity in terms of reporting and fixing security incidents. Some 96%[16] of incidents are not reported or resolved, which means that the level of cyberthreat in Africa is likely to be much higher than we know.

_LEGAL AND STRATEGIC ARMOURY UNDER CONSTRUCTION

Most African countries have not yet, or have not sufficiently, structured their legal armoury to deal with the cyberthreat. In 2016, it was estimated that over 40 countries across the entire continent had not or had only partially implemented specific legal provisions to address the challenges of cybercrime and oversee the gathering of electronic evidence[17]. It should also be noted that only 15 African countries have a national cybersecurity strategy in place[18].

Conclusion

Africa is destined to become one of the geographic parts of the world where the cyber issue will be the most decisive factor for the future of societies and organisations.
Already, the continent's colossal trends are fuelling a strategically important yet unsuspected cyberthreat. These trends include the exponentially increasing Internet penetration across society and industry (up 12,988.7% in 20 years), the demographic structure of these societies (1.2 billion people under 25 by 2050) and the rapidly growing popularity of digital tools.
At the same time, 96% of security incidents are unknown or unreported and decisive attacks are already affecting the continent, as we have seen in Ethiopia, South Africa and Liberia.
These trends will obviously continue to create huge issues and challenges, yet a mismatch is already apparent when we consider the structure of cybersecurity and cyberdefence across the continent. Three challenges need to be met, namely the training of the population to create cyber experts, the visibility of incidents and a clearly defined legal and strategic framework to address the cyberthreat.

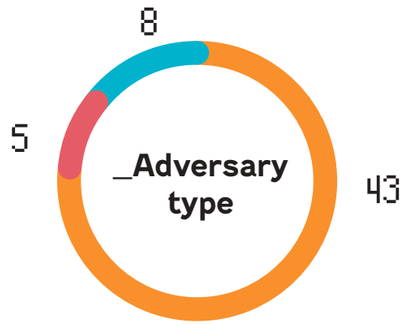
Zone North America _

United States
Canada
Mexico

29 ATKS (Attackers)
targeted the aera

_Adversary Type

_Terrorists _State-Sponsored _Cyber Criminal



_Top 3 attacked sectors

Energy
Education
Manufacturing

- _Energy
- _Manufacturing
- _Communication
- _Transportation
- _Education
- _Aviation
- _Information Technology
- _Retail

Contextual analysis of North America and geocyber risks

The Americas can be divided into three geographic regions: North America, which includes the United States, Canada and Mexico; Central America; and South America. This hemisphere is marked by its cultural contrasts and, in particular, by its economic diversity.
The United States and Canada are rich and developed, while other countries in the region are considered to be emergent or low-income economies. The Americas are beset by many geopolitical tensions taking the form of border conflicts between countries or even social conflicts within them. The role of the United States, sometimes described as dominant, is often cited as the cause.
More accurately, dominance on the continent can be described as being shared between the United States and Canada, the region's two most developed nations. This creates a geoeconomic contrast on the continent as a whole, as these two countries constitute one of the three major poles of the world economy. Indeed, in 2015, the GDP of the United States was $18,036 billion, the highest in the world. Canada's was $1,550 billion, placing it in tenth. These countries have diversified economies that are extremely well-integrated into global trade. The United States is home to many of the largest multinational corporations and several global cities, chief among which is New York.
However, such disparities and issues of hegemony can exacerbate international tensions, fostering an environment of heightened geopolitical cyberthreats.

_ONGOING INTERNATIONAL TENSIONS IN NORTH AMERICA

Since the end of the Second World War – and, more to the point, since the Bretton Woods agreement in 1944 – the United States has remained at the top of the international order.

_THE US AND CHANGING FOREIGN POLICIES IN THE ERA OF "AMERICA FIRST"

Canada, Mexico and the rest of the world have had to significantly amend their foreign policies over the last several years, under pressure during Donald Trump's term as President of the United States from 2017 to 2021.

FOREIGN RELATIONS OF NORTH AMERICAN NATIONS

The leaders of Canada and Mexico, along with foreign ministries from other nations around the world, have adjusted their foreign policies either in the US's favour or to turn away from it. For example, Canadian Prime Minister Justin Trudeau and Mexican President Enrique Peña Nieto have frequently remarked on their disagreements with President Trump, while remaining clear that they wish to continue their cooperation with the world's leading economy.
During his term, President Trump oriented its foreign policy towards a strengthening of bilateral relationships with Russia, Iran, and even China.

RUSSIA–US RELATIONS

The power balance between the United States and these three nations was a touchstone of Trump's tenure, and continues to be so under Biden, albeit with less emphasis on Russia.
On Russia specifically, some observers of Russia–US relations, particularly pro-Kremlin Europeans, have claimed that Vladimir Putin is an "ideal" or "useful" enemy for America. They imply that the US is almost entirely responsible for its tense, fragile relationship with Putin's Russia, or even that it benefits from the hostility that exists between the two countries. However, the US hardly revels in the ongoing tensions, and does not appear to profit from them, not least because as Russia grows more distant from other European countries and US, it is becoming increasingly dependent on its relations with China and less inclined towards mitigating the increasing asymmetry between these powers.

IRAN–US RELATIONS

Relations between the US and Iran have become yet more precarious. Indeed, the recent spike in tensions starting in early 2019 is part of a broader trend of escalating diplomatic disagreements between the two countries. Already fraught after the US's withdrawal from the Iran nuclear deal (JCPOA) in May 2018, Iran–US relations have degraded even further, especially since the Trump administration added the Revolutionary Guards to its list of terrorist organisations in April 2019 and tightened its sanctions against Tehran the following month. In 2020, relations between these two countries were aggravated yet further with the killing of the Iranian General Qassem Soleimani, the Islamic Republic's representative in Iraq and head of the Quds Force, in an American raid in Baghdad on 3 January 2020. Despite an Iranian retaliation in the form of several missile strikes on US bases in Iraq, tensions have begun to soften as the two sides seek some level of stability.

CHINA–US RELATIONS

In recent years, relations between China and the United States have been beset by several geopolitical events that have strained the limits of diplomacy between the two countries.
For example, in 2020, the US accused China at length of data theft and widespread espionage, leading to the closure of the Chinese consulate in Houston, Texas. The US Secretary of State justified these steps as being for the protection of US intellectual property and the personal information of individual Americans. Mike Pompeo also described the Chinese consulate in Houston as having been a hub for espionage. Moreover, two Chinese nationals were charged by a US court with computer hacking offences for allegedly stealing data from a company working on a Covid-19 vaccine.
However, the closure of the Houston consulate in particular was all the more symbolic as it was the PRC's first in the United States, having opened in 1979 with the reestablishment of diplomatic relations between the two powers. China viewed the closure as a step too far, declaring it an outrageous, unjustified and unilateral provocation by the US. Beijing retaliated by ordering the closure of the US consulate in Chengdu, in central China, on 24 July 2020. In a press release, the Chinese foreign minister described this as a "legitimate and necessary response to the unreasonable measures taken by the United States".

_US FOREIGN POLICY HAVE HAD SIGNIFICANT CONSEQUENCES ON THE CYBER-THREAT LANDSCAPE.

The threat represented by Russia has been compounded by a marked increase in the number and severity of attacks since 2019. In cyberespionage, the SolarWinds attack (December 2020) demonstrated the danger posed by attacks from state-sponsored groups. This supply chain breach had a particularly serious impact because, rather than directly targeting the federal government or a private company's network, the perpetrators attacked a third-party software supplier serving these entities. The target was an IT management platform called Orion, a product of Texas-based company SolarWinds. More than 33,000 businesses used Orion. According to SolarWinds, 18,000 of its clients were affected, including 425 Fortune 500 companies.
This heightened threat is also exemplified by the ransomware attack conducted by ATK168 using REvil, also known as Sodinokibi. The attack on software company Kaseya by the REvil ransomware operation is considered the largest ever such attack by a cybercriminal group. While 2017's three ransomware attacks (WannaCry, NotPetya and Bad Rabbit) were larger, they were linked to state-sponsored actors rather than groups with financial motives. According to cybersecurity researchers at Symantec, some vague indications point to political motives behind the attack. The US has not explicitly linked the REvil attacks to the Kremlin, but President Joe Biden has nevertheless warned his Russian counterpart that the latter's government must act against such criminal organisations, and that US authorities would do so if necessary. In January 2021, several members of REvil were arrested by Russian authorities obeying to a US demand. While it may appear as the reinforcement of collaboration between the two countries, the timing of this announcement raises questions as several Ukrainian government sites

were targeted by a cyberattack and Russian troops are massed at the border.
Likewise, the largest oil pipeline of the US, Colonial Pipeline, fell victim to the RaaS (Ransomware-as-a-Service), forcing the company to temporarily shut down its activity. The incident, which happened on May 7, 2021, affected the delivery of gas in Southern states, provoking shortages at gas pumps.
Former US President Donald Trump was also the target of several influence campaigns. These attacks appeared to originate from groups operating in China, including ATK213 (also known as APT31). This group carried out more than 150 breaches over the course of six months. In 2020, Trump called for the social media platform Tik Tok to be banned in the United States, on the basis that the data collected through the app was disseminated to the Chinese government. This ban provoked many Chinese actors to carry out influence campaigns aimed at destabilising the US elections by sowing disinformation about the President to sway voters.

_THREATS ARE ALSO EMERGING FROM OUTSIDE OF CHINA.

After months of heightened tensions between the US and Iran, there were fears that this could have been used as justification for an attempt to destabilise the US election. After Trump withdrew the US from the JCPoA in May 2018 and Iranian general Qassem Soleimani was killed on Iraqi soil in January 2019, the risk of cyberespionage or more conventional attacks (such as phishing or ransomware campaigns) aiming to destabilise the then-US President became markedly more significant. In May and June 2020, this fear was realised in the form of an attack by the group Phosphorus, which gained access to several accounts belonging to members of the administration, Trump campaign staff and others involved in the 2020 presidential election.
Twitter announced that it had deleted around 130 Iran-based accounts that had disrupted the public conversation on the platform during the first campaign debate between Biden and Trump. This also illustrated a shift in technique as attackers targeted the two candidates directly and the electoral process itself. It is becoming more and more difficult to predict this type of real-time attack and proactively analyse the threat landscape to prevent them.

_CANADA AND TRANSATLANTIC RELATIONS

In recent years, countries have strengthened their diplomatic and economic links with Canada as, since 2017, the US has drifted further towards protectionism. The US's decision to heavily tax steel and aluminium imports had been extremely damaging to Canada and the member states of the European Union. The move even provoked threats of retaliation from the EU, Canada and Mexico. In May 2018, Canadian Prime Minister Justin Trudeau publicly declared his disapproval and, along with policymakers in European countries, claimed that the President's invocation of the national security defence, referring to WTO regulations, did not hold water.
It is therefore unsurprising to see Canada looking to the nations of the Old Continent for less protectionist economic partners, more open to diplomatic relations.
This transition took a significant step forward with the signing of the Comprehensive Economic and Trade Agreement (CETA) between Canada and the EU in autumn 2016. The goal of this agreement was to ease the export of Canadian products to the European market by almost completely eliminating tariff and non-tariff barriers, while creating a more stable investment context for Canadian and European businesses.
Prime Minister Trudeau and French President Emmanuel Macron portrayed this bolstered Canada–France relationship as favouring a just, fair and rules-based international order. Canada and France have instituted structural frameworks for their joint activities, particularly in the areas of culture, the environment, development aid, sustainable development, artificial intelligence and defence. The two countries have committed to a joint meeting of their cabinets with the goal of building further institutional ties.

_IN CANADA, THE CYBERTHREAT ENVIRONMENT IS CONSTANTLY CHANGING AS BAD ACTORS CONTINUE TO ADJUST THEIR STRATEGIES.

As Canadians adopt new technologies and Internet-connected devices, it is certain that new threats will arise. Furthermore, Canada's rapprochement with Europe may create a major risk from adversary foreign powers.
The Covid-19 pandemic has had a significant impact on the cyberthreat landscape in Canada. In 2019, the medical laboratory company LifeLabs fell victim to a cyberattack which compromised the personal and medical data of 15 million Canadians. The company finally paid the ransom to recover this data.
Geopolitical events such as the warming of relations between Canada and the EU can also make cyberattacks more likely. For instance, activists such as environmentalists might aim to weaken CETA, as the agreement eases the process of importing polluting fuels and GMO foodstuffs. This was observed in 2017 and 2019 when Twitter data revealed that Russian and Iranian trolls had been posting to the site using fraudulent accounts. The purpose of this activity was to exacerbate divisions among Canadians and provoke conflict by widening the reach of inflammatory content on political issues like terrorism, climate change, pipeline construction, immigration policy and refugees.
Many of these disinformation campaigns have responded to significant events such as the January 2017 massacre at a Quebec City mosque or the June 2019 approval of the Trans Mountain pipeline.

_MEXICO

Although Mexico is a multiparty democracy, power remains concentrated in the hands of the Institutional Revolutionary Party (PRI), which controlled both chambers of Congress and the presidency continuously from the Second World War until 2018. Despite persistent inequalities, the country's industrial sector has seen a meteoric rise since the war.
Large oil reserves, exploited by a state-owned corporation, have contributed to Mexico's economic stability, which had been shaken by plummeting prices during the 1980s.
However, Mexico's ambition to become a major power on the international stage (and within North America in particular) is hampered by several factors, including crime and immigration, which remains an issue to this day.

_CRIME IN MEXICO

Mexican drug-trafficking cartels are among the most developed organised crime rings in the world. While fragmentation has reduced the number of such groups with large international operations, those which remain have access to networks covering most of the Americas, even extending into Europe and Asia.
These international cartels interact with foreign actors but generally lack a strong grounding in Mexico. Their activities more often take the form of joint ventures with other Mexican groups. These organisations focus on international drug trafficking, which brings in millions of dollars in revenue every year, but also engage in other activities such as oil theft, illegal logging, human trafficking, kidnapping and extortion.
Mexican drug cartels have access to firearms, including military-grade weapons, and conflict between rival groups and security forces is com-

mon. Drug cartels control large tracts of territory throughout Mexico, supplanting government authority by means of bribery and intimidation to facilitate illicit activities and skew the democratic process. Politicians are frequently assassinated or threatened by organised crime groups, who ensure that public positions are filled by cooperative individuals.

In addition, the fragmentation of cartels has produced smaller offshoot groups with no permanent power structure, which pose a security threat as turf wars become more common and localised. These groups generally lack access to the necessary resources to manage transnational drug trafficking networks and favour activities such as extortion, kidnapping, vehicle theft, oil smuggling, human trafficking and smuggling, wholesale drug dealing and illegal mining. They play a key role in the drug trafficking supply chain, handling local transport and security within wider networks.

While state actors do not control criminal markets, corruption within the government and agencies responsible for law enforcement enables criminal networks and shapes illicit activities, constituting a stream of income for high-ranking public officials.

_ORGANISED CYBERCRIME IN MEXICO POSES A GROWING THREAT TO CIVILIANS AS WELL AS PUBLIC AND PRIVATE ORGANISATIONS

As crime increases, the eyes of the cybersecurity world have turned towards the country. In fact, Mexico has suffered more cyberattacks than any other Latin American country besides Brazil. In both countries, emails containing links to malicious websites are fairly common. Some of these websites are believed to be among the most prolific generators of spam in the world.

Symantec placed Mexico among the 10 countries most affected by email phishing scams. Mexico was ranked seventh, after Ireland, Australia, New Zealand, Brazil, Norway and the UK.

The last few years have seen many criminal cyberattacks hit the country. For example, sites belonging to the Lotería Nacional y Pronósticos, the national lottery, were rendered inaccessible to visitors outside of Mexico after being targeted using Avaddon ransomware.

Avaddon is found throughout the world and spreads using emails styled as love letters. It appears to have been distributed by the botnet Trik (also known as Phorpiex) since early June 2020. Avaddon's operators launched a data leak site to extort victims in August of that year. In conducting their activities, the group observed the so-called 5×5 rule, wherein the starting price in negotiations is placed at 5% of the victim's annual revenue, which is estimated at a fifth of total revenue. Cybersecurity researchers at Advanced Intel estimate Avaddon's total revenue at $87 million before it ceased operations in June 2021.

Furthermore, attackers are increasingly using malware capable of paralysing a whole set of systems, including supply chains, manufacturing and payments, removing the malware only after receiving substantial sums of money.

One notable example was the case of Pemex, the Mexican state oil company, which was targeted using the ransomware Ryuk. Ryuk generally targets businesses with revenue between $500 million and $1 billion. Although operations appeared to continue as normal and petroleum production and storage were not affected, this attack against critical infrastructure demonstrates the severity of the cyberthreat facing Mexico.

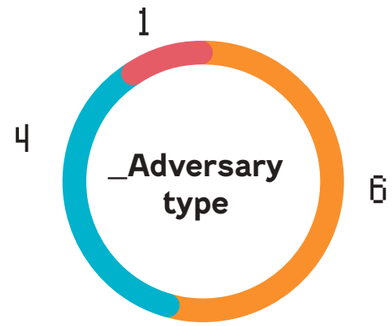
Zone South America _

Argentina
Bolivia
Brazil
Chile
Colombia
Costa Rica
Cuba
Guatemala
French Guiana
Honduras
Nicaragua
Panama
Paraguay
Peru
Uruguay
Venezuela
Ecuador

30 ATKS (Attackers)
targeted the aera

_Adversary Type

_Terrorists _State-Sponsored _Cyber Criminal



_Top 3 attacked sectors

Energy
Education
Manufacturing

_Energy	
_Manufacturing	
_Transportation	
_Education	
_Retail	

Contextual analysis of Latin America and geocyber risks

17 July 1979 remains a pivotal date in the history of South American geopolitics. A military junta seized power in Managua, Nicaragua's capital, triggering a civil war that engulfed the country. The so-called Sandinista revolution marked the start of more than 10 years of civil war in Latin America.
Geopolitical tensions abound in the Americas, fuelled by border conflicts between countries or social conflicts within them, as well as the dominant role of the United States.
Central and South America are regions beset by perennial and long-standing conflicts. In Central America, the Sandinista revolution against the US-backed dictatorship in Nicaragua in the 1970s marked the beginning of a decade of strife.
In South America, some tensions are rooted in national borders drawn during the post-colonial period. The wounds of the War of the Pacific, in which Bolivia lost its only province with access to the sea to Chile, remain raw for many Bolivians.
The repercussions of this animosity are still being felt as Bolivia refuses to provide energy resources to Chile. Since the end of the 2000s, there have also been significant tensions between Colombia and Venezuela.
Despite these ongoing strains, the continent is becoming more and more integrated. Human and capital flows are on the rise, albeit oriented towards the US. In North America, the USMCA (United-States, Mexico, Canada Agree has established an area where capital and goods circulate freely. Its equivalent in the South is MERCOSUR.
The region's troubled internal relations may give rise to groups of attackers aiming to take advantage of its geopolitical instability and set off an explosion of cybercrime within the region and beyond.

_DEEP-ROOTED TENSIONS IN CENTRAL AND SOUTH AMERICA

In recent decades, urban conflicts have erupted throughout Latin America in response to several phenomena including poverty and rising inequality. As for international clashes, several Central and South American countries have been in conflict for many years. Meanwhile, the same countries are often plagued by internal tensions, as populations searching for a new socio-economic order make their grievances known through a variety of protest movements.

_ECONOMIC MODELS IN LATIN AMERICAN COUNTRIES

Boosted by growth in the early 2000s thanks to sluggishness in the US, South America has seen some economic success. Brazil, for example, is one of the five emergent economies known as the BRICS countries.
However, since 2011, this growth has been merely relative, and most Latin American countries have slid into recession.
In fact, after a "golden decade" between 2003 and 2013, during which economies boomed and inequalities narrowed, Latin America's GDP (Gross Domestic Products) per capita had collapsed to 2010 levels by the end of 2020. The price of exported primary commodities has weighed heavily on countries' financial capacities as well as their economic growth. The fossil fuels sector has also been a factor in this crisis: in 2014, oil prices plummeted in Argentina, Brazil and Venezuela.

_REGIONAL DIVISIONS STOKING BORDER CONFLICTS

Border conflicts in this region are nothing new. For hundreds of years, Latin America has been the setting for several international conflicts, with some still ongoing that stretch back to the 19th century.
Today, political disagreements between countries continue for a variety of reasons, including various permutations of nationalism and conflicts of economic interest. These battles are fought in the raw materials sector, particularly oil and gas, as well as within the framework of increasingly fragile regional alliances.
On 1 May 2006, Evo Morales nationalised Bolivia's oil wells, hitting Brazilian company Petrobras (a third of whose shares are owned by the Brazilian government) particularly hard and impacting other foreign companies including Spain's Repsol. In response to objections by Brazil, backed by Argentina, Bolivia gained the support of Venezuela, resulting in a temporary schism between the region's left-wing governments.
Furthermore, more than ten years after its founding treaty was signed, the Union of South American Nations (UNASUR) is now moribund. In 2018, six of its 12 members announced their temporary withdrawal from the union and suspended their financial contributions in response to the organisation's collective inability to designate a new secretary general to succeed the former president of Colombia.
This institutional breakdown is the result of these countries' shift towards nationalism and prioritisation of their own economic interests, which has aggravated regional divisions and conflicts between countries.
Their inward turn is hardly surprising, as many of them had endured or continue to endure deep economic, political and social crises. These situations dampen the driving force that motivates earnest cooperation and regional projection, instead favouring policy focused on the internal welfare of the nation.

_FOREIGN POWERS CAN TAKE ADVANTAGE OF DETERIORATING REGIONAL UNITY THROUGH ESPIONAGE ACTIVITIES

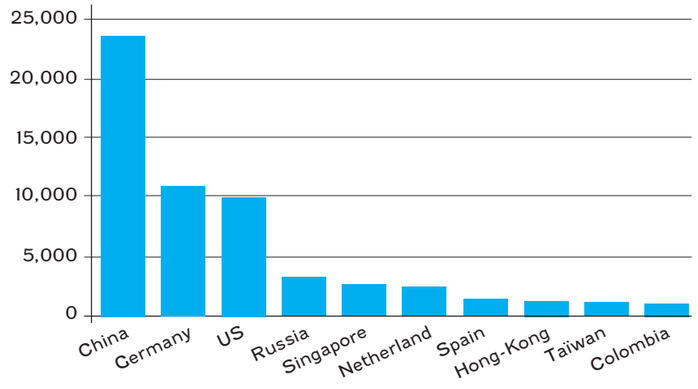
This was the case with ATK97, known as "El Machete", a cyberespionage group that has been active since 2010. Its agents usually target the governmental and military sectors in Latin America as well as the US, Korea and several European countries. The source code of the group's malware, which it usually deploys in sophisticated spear phishing attacks, suggest that the developers are Spanish speakers. The question of potential sponsorship of the attacking group by a foreign power remains unresolved. Most of the victims of the group's 2010 campaign of attacks were in countries such as Venezuela, Ecuador, Colombia, Peru and Cuba.
Finally, it is interesting to note the large number of countries around the world that target this region with cyberattacks. In February 2021, of the ten main countries from which attacks targeting Brazil, Chile, Colombia and Panama originated, China was the source of 23,583 attacks, Germany 10,847 and the US 10,019.

_INTERNAL CONFLICTS

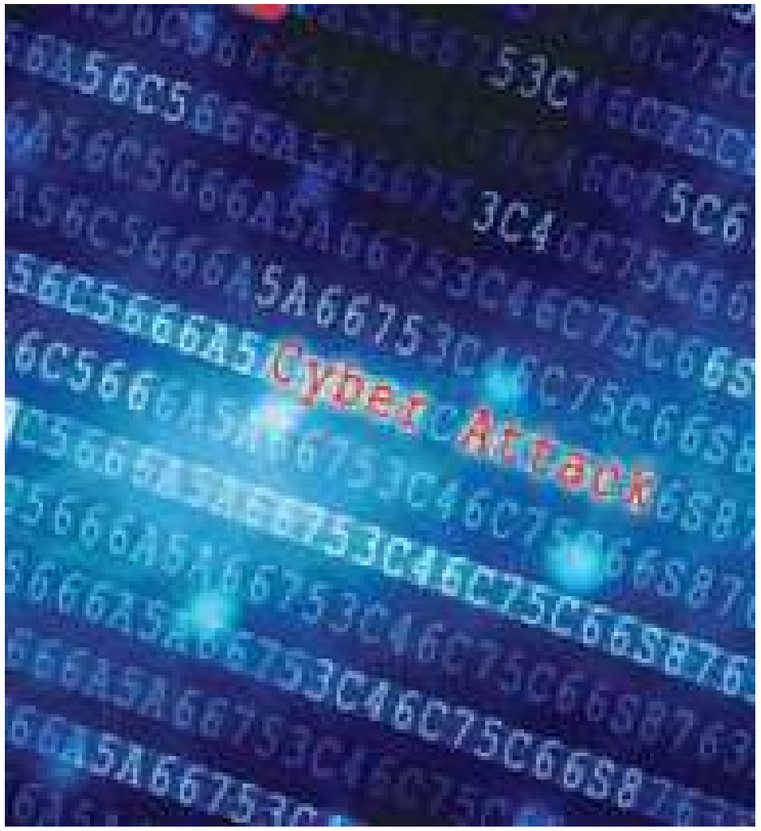
The social and political consequences of the economic crisis of the 2020s have weakened Latin American societies. The OECD has expressed concern at deteriorating social cohesion and growing alienation between citizens and public institutions in all countries in the region.
With the exception of Venezuela, where political and economic crises have triggered a humanitarian crisis, the resultant turbulence has manifested internally in other South American countries. Massive protests erupted in Paraguay in opposition to a decision by President Mario Abdo to sign an agreement with Brazil, considered disadvantageous to the small country, concerning the Itaipu hydroelectric power station.
Political tensions were particularly marked in countries such as Peru, where President Martín Vizcarra dissolved Congress, triggering new legislative elections. His actions led to protests throughout the country. In one case, protesters blocked ac-

Areas of tension in the South American region

Suspected origin of attackers targeting this region



cess to a copper mine and forced it to halt production.
In most countries, protests were caused by political decisions that may seem insignificant. However, such decisions can exacerbate inequalities, increase tension in society and sometimes result in a violent backlash by the population. This was the case in Chile, in 2019, where a political decision was made to increase ticket prices on the Santiago Metro.
This was merely a catalyst for a much broader protest movement challenging the Chilean economic model and spotlighting the



country's inequalities. Surging poverty and inequality, deteriorating public services and wage stagnation, combined with ever-increasing precarity and unemployment, have laid bare widespread dissatisfaction and defiance towards elites and governments.
In addition, corruption scandals continue to come to light in a majority of countries, gradually undermining the legitimacy of political systems and institutions as the public discovers their extent. The Odebrecht case embodies the current situation with regard to corruption. Some 10 countries have been impacted by the scandal, which led to the downfall of Peruvian president Pedro Pablo Kuczynski.
All of these factors have coalesced to breed discontentment within Latin American societies and foster a feeling of insecurity. Rising crime, whether tangible or virtual, has made the region one of the most dangerous in the world.
Latin America is home to 40 of the 44 cities where criminal activity poses the most severe threat. For instance, El Salvador, Honduras and Guatemala have the highest homicide rates in the world. Much of this urban violence is perpetrated by gangs, specialized in drug trafficking. Indeed, due to its geography, Latin America is an active participant in the drug trade, notably providing the US with cocaine. Figures show that 80% of cocaine arriving in the country transits through Central America. This lucrative and straightforward business has led to the formation of thousands of small, violent gangs across the region (including maras, Mexican cartels and Brazilian mafia organisations). Law enforcement and politicians are often powerless to stop them, and the rot is often worsened by corruption and public officials accepting bribes.

_LATIN AMERICA'S INSTABILITY HAS LED TO WIDESPREAD PRECARITY, OPENING THE DOOR FOR CYBERCRIMINALS TO CONDUCT VARIOUS TYPES OF ATTACK CAMPAIGNS BOTH WITHIN THE REGION AND AROUND THE WORLD

These groups include ATK237, also known as the Tetrade. This malware family, of Brazilian origin, is characteristic of the country's cybercrime landscape. Until 2011, it primarily targeted Brazilian victims, before expanding its focus worldwide. It comprises four malware families called GUILDMA (aka Astaroth), GRANDOREIRO, JAVALI (aka Osaban) and MELCOZ. Cybersecurity researchers from Kaspersky Lab identified this series of malware as being responsible for attacks on financial institutions in Brazil, other Latin American countries and Europe. The Brazilian cybercriminal underground is known to be particularly geared towards the development and sale of banking trojans.
Finally, the group ATK243 (aka Carbanak or Anunak) is worth highlighting in order to demonstrate cybercrime's important place in this part of the world. The ATK243 label was assigned to resolve confusion between the aliases FIN7 and Carbanak/Anunak, two groups which are tracked as a united operation. Their common feature is the use of the malware Carbanak. Note that, despite its shared interests with ATK32, ATK243 is a separate group.
ATK243 was first identified in 2013. Since then, they have attempted to attack up to 100 banks, electronic payment systems and other financial institutions in around 30 countries, including Brazil. According to data from Kaspersky Lab, Cabarnak's targets include financial institutions in Russia, the US, Germany, China, Ukraine, Canada, Hong Kong, Taiwan, Romania, France, Spain, Norway, India, the UK, Poland, Pakistan, Nepal, Morocco, Iceland, Ireland, the Czech Republic, Switzerland, Brazil, Bulgaria and Australia.

_LATIN AMERICA AND COVID-19

Covid-19 has caused over 1.5 million deaths in Latin America and the Caribbean, according to an AFP study of official figures.
The early stages of the epidemic were characterised by uncertainty, as the region was initially only marginally affected. However, Latin America quickly became the hardest-hit region in the world (and remained so until October 2020, when the changing seasons put Europe back in the lead), representing more than a quarter of the planet's cases and a third of its deaths with just 9% of its population.
The Covid death toll in Brazil has exceeded 600,000, making it the country with the second-most deaths after the United States. Mexico, Peru, Colombia and Argentina had the highest mortality rates after Brazil.
In October 2021, Brazil was continuing to suffer heavily, with the highest daily number of cases in the region.

Despite improvement, epidemics have afflicted Latin America for decades, and the region accounts for a disproportionate share of health and economic costs as a result. These challenges are compounded by rising hunger, economic hardship, widening inequalities and a rapidly approaching hurricane season. Hunger and food insecurity have the potential to generate widespread conflict, provoke political turbulence and force vulnerable families to flee.

Consequently, several indicators have shown that Latin America is on the verge of a major economic crisis due to Covid-19 in the medium term. Countries in the region lack resources, continue to fall deeper into debt and remain dependent on raw materials exports to regions in crisis, currently including China and Europe.
The Economic Commission for Latin America and the Caribbean estimates that the pandemic will cause the region's economy to shrink by 5.3%, with 29 million falling into poverty. South America will not return to its already poor pre-Covid status quo until 2023 at best, and possibly not until 2030.

_THE INSTABILITY CAUSED BY COVID-19 IS EXPECTED TO LEAD TO MANY ATTACK CAMPAIGNS AGAINST LATIN AMERICAN COUNTRIES, PARTICULARLY BRAZIL

Cybersecurity company Fortinet recorded more than 2.6 billion cyberattack attempts in Brazil between January and June 2020, out of a total of 15 billion attempts in Latin America and the Caribbean.
COVID has also led to an increase in the use of phishing techniques by attackers. Cybercriminals would share messages on WhatsApp aiming to steal the victim's personal data for use in future attacks or trick the victim into downloading legitimate applications in order to collect payment from affiliate programmes.
Many elements of critical infrastructure in Brazil have been targeted since the start of the Covid-19 pandemic. In 2020, the country saw a rise in brute force attacks due to the increase in remote working. For instance, the infamous ransomware REvil, also known as Sodinokibi, was one of the first to take advantage of the pandemic to launch attack campaigns. In July 2020, REvil's operators (ATK168) demanded a ransom of $14 million from Brazilian electricity provider Light SA. In 2021, Centrais Eletricas Brasileiras (Eletrobras) and the Companhia Paranaense de Energia (Copel), two major public electricity providers, announced that they had suffered ransomware attacks in the last week. In Copel's case, the attack was the work of the Darkside ransomware gang, who claim to have stolen more than 1,000GB of data including sensitive infrastructure access information and the personal details of top management and customers. The attack on Eletrobras affected servers on the company's administrative network and had no impact on the operations of nuclear power stations Angra 1 and Angra 2.

Zone Western Asia_

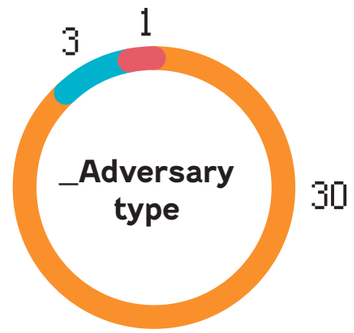
Turkey
Syria
Lebanon
Jordan
Israel
Palestinian Territories
Yemen
Saudi Arabia

Kuwait
Afghanistan
Oman
Qatar
United Arab
Emirates
Bahrain

38 ATKS (Attackers)
targeted the aera

_Adversary Type

_Terrorists _State-Sponsored _Cyber Criminal



_Top 3 attacked sectors

Energy
Education
Manufacturing

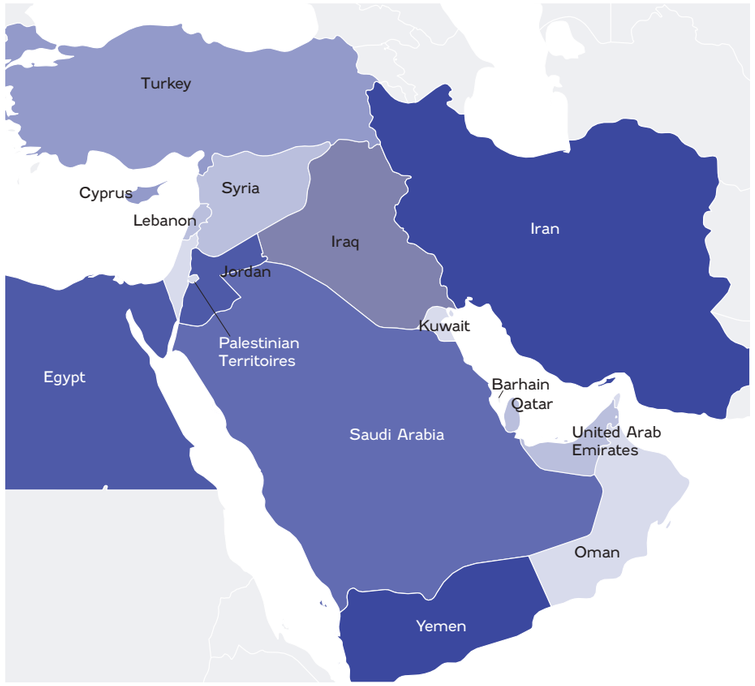
_Energy	● ● ● ● ● ● ● ● ● ● ●
_Manufacturing	● ● ● ● ● ●
_Communication	● ● ●
_Transportation	● ● ● ●
_Education	● ● ● ● ● ●
_Aviation	● ● ● ●

Contextual analysis of Western Asia and geocyber risks

The Middle East is a region geographically and culturally diverse. It comprises the Anatolian zone with present-day Turkey, the Levant zone, which includes Syria, Lebanon, Jordan, Israel and the Palestinian Territories, the Arabian Peninsula and the Iraq-Iran zone. Geographically, the Middle East is rich in natural resources and especially in oil and gas. Culturally, the region is home to the major monotheistic religions: Islam and its various branches (Sunnism, Shiism, etc.), Christianity (Druze, Coptic, Maronite) and Judaism.

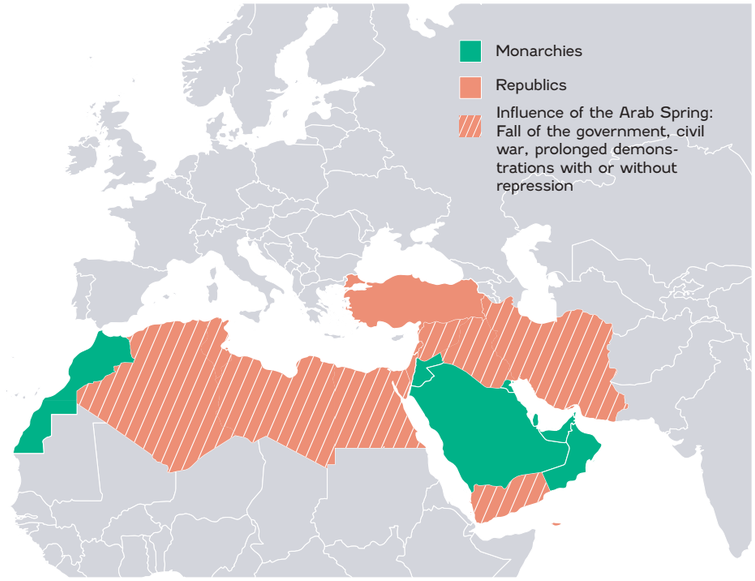
_THE ARAB SPRING AND ITS IMPACT ON THE MIDDLE EAST

In 2011, a wave of democratic protests swept across various countries in the Arab world. From Tunisia, the desire of the North African peoples for democracy spread to Western Asia, leading to radical responses, severe repression (Kuwait) and even civil wars (Syria, Yemen).
Initially, these protests took the form of peaceful demonstrations, where people expressed their disagreement with the political and institutional systems, which they deemed obsolete and corrupt. The Middle Eastern region is built around two types of political models: absolute or constitutional monarchies and republics. Many of the most important uprisings were in the Arab republics and have continued to this day in the form of civil wars, most notably in Syria and Yemen. The countries of the Arabian Peninsula, most of which are rentier states, have effectively established an unspoken social contract by offering a high standard of living for their populations.



_SECURITY AND TERRORISM IN THE REGION

Since the late 1980s, the Western Asia region has seen the emergence of terrorist groups advocating radical Islam and encouraging its political manifestation in the form of a violent jihad. Jihad has experienced several mutations. It was theorized as a violent struggle against the near enemy, which refers to the apostate regimes of the Middle Eastern peninsula. The first mutation appeared with Al-Qaeda. The group exported jihad across regional border and started to target the “far enemy”. Al-Qaeda first appeared in Afghanistan in 1987 and has carried out numerous terrorist acts, claiming responsibility for the attack on the twin towers of the World Trade Center in New York in September 2001. The group is still active in various parts of North Africa and the Middle East, with the presence of Al-Qaeda in the Islamic Maghreb (AQIM), the Arabian Peninsula (AQAP) and the Indian subcontinent (AQIS).
The second major mutation happened with Daech. The terrorist group created a horizontal structure, relying on the masses. Formed in response to America’s intervention in Afghanistan in 2003, it is mainly present in Iraq, where it has its organisational core. It is also present in North Africa, the Caucasus, Somalia, Southeast Asia and the Indian subcontinent. In 2014, Abu Bakr al-Baghdadi proclaimed the creation of an Islamic State in Iraq. The Islamic State group took part in the Syrian conflict in 2013, fighting both Kurdish militias and Syrian regime forces, with the aim of establishing an Islamic caliphate. Building on an existing terrorist group in the region, the Al-Nusra Front, Islamic State became the Islamic State in Iraq and the Levant (ISIL).



_ON 4 APRIL 2016, THE CYBER CALIPHATE ARMY (CCA), ISIS’S MAIN HACKING UNIT, AND OTHER PRO-ISIS GROUPS LIKE THE SONS CALIPHATE ARMY (SCA) AND KALACNIKOV.TN (KTN) MERGED TO FORM THE UNITED CYBER CALIPHATE (UCC). UCC GROUPS INCLUDE:

- ***The Cyber Caliphate, or Cyber Caliphate Army (CCA), which was created shortly after Islamic State was formed. The key person in this organisation was Junaid Hussain (Abu Hussain al-Britani), or TriCk. CCA’s most significant cyber terrorist attack was in January 2015, when the Twitter and YouTube accounts of US Central Command and later the Twitter accounts of Newsweek magazine were hacked.***
- ***The Sons Caliphate Army (SCA) was formed in 2016 as a subgroup of the Cyber Caliphate. It is mostly known for disrupting social media traffic on Facebook and Twitter. SCA claimed to have hacked into 10,000 Facebook accounts, over 150 Facebook groups and more than 5,000 Twitter profiles.***
- ***Kalashnikov E-Security Team was initiated in 2016. This group focuses on technology security consulting for ISIS jihadists. It has uploaded ISIS-related jihadist literature, shared posts from cyber jihadist groups, reported successful attacks on websites or Facebook pages and published various web hacking techniques. Over time, the hackers began to carry out or take part in website hacking.***

While we have not identified any ATK133 attacks in almost two years, it is highly likely that group members have been redeployed to new operations within other terrorist groups as a result of ISIS movements.

_CIVIL WAR IN SYRIA AND YEMEN

When Yemeni President Ali Abdullah Saleh was forced to accept the terms of the revolutionaries under the mediation of the Gulf Monarchies in 2011, no one thought the country would collapse. However, the now former President allied with Shiite Houthi rebels, backed by Iran, in order to regain power. The country was plunged into a conflict that became international in 2015 with the intervention of a Saudi-led Arab coalition.
In Syria, the democratic aspirations of 2011 quickly degenerated into a civil war sparked by the killing of children in Daraa by Bashar al-Assad’s regime. As with Yemen, the conflict became international when Islamic State got involved in 2013. What began as a national conflict quickly turned into a regional and international conflict in which Russia, Iran and Turkey have taken part. Russia and Iran have sent militias to support President Assad’s regime and its strategic interests in the region. Turkey sent in its armed forces in late 2019 after the US withdrawal from the region, officially to protect its borders and fight jihadists. Unofficially, Turkey has also been fighting the Kurds, with whom it is in conflict within its borders. This Kurdish population, present today in northern Syria but also in Turkey, Iraq and Iran, claims a territory in Syria’s north. The Kurds, a minority which has suffered for many years under the Assad clan, were spread over a territory straddling Iran, Iraq, Turkey and Syria, before the borders of these countries were defined at the end of World War II.

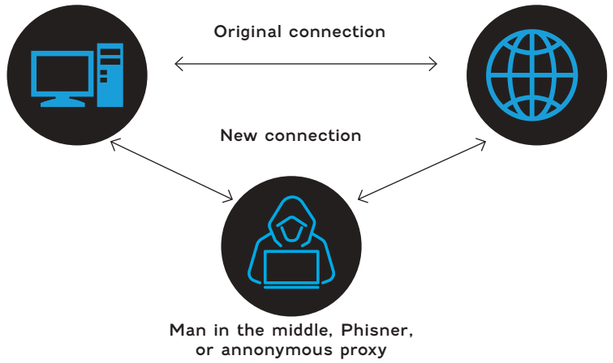
_USE OF CYBER WEAPONS IN THESE CONFLICTS: THE EXAMPLE OF SYRIA

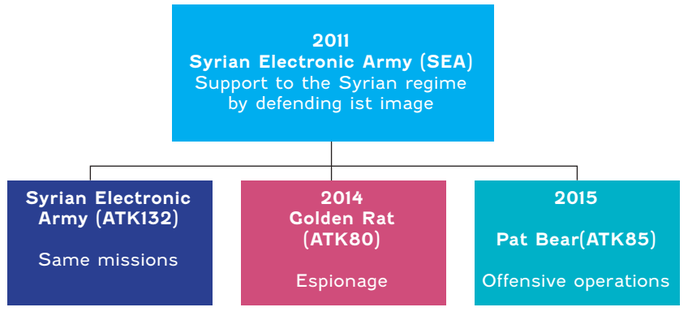
These conflicts also have a dimension that is much less reported in the media because it is less visible: cyber confrontations. In this respect, the Syrian conflict demonstrates the importance of the cyber weapon and its use by the regime of Bashar al Assad.
Firstly, the cyber tool allows the regime to carry out missions to spy on the opposition. The technique known as «man in the middle» allows the interception of communications between two stations without either operator being aware of it. Infowar Monitor reported in May 2011 that this type of attack was used in Syria on a secure version of Facebook, allowing the attacker to access the victim’s private conversations. Still with the objective of espionage, the Syrian government has used RATs (Remote Administration Tools), pro-

grams that allow full remote control of a computer from another device. DarkComet is a French-made RAT that has been modified to spy on Syrian revolutionary forces.
Secondly, the Damascus regime uses the cyber tool to destabilize its opponents. For example, the Syrian government regularly cuts off the country's communications to interfere with the rebels' exchanges. In addition to cutting off the Internet and GSM networks at strategic times, it may send a large number of connection requests in order to saturate the network.
The Syrian leaders regularly mobilise hacker groups, such as ATK132 (Syrian Electronic Army) which carry out DDoS (distributed denial of service) or defacement attacks. Certain Arabic media outlets are regularly targeted by the Syrian Electronic Army (SEA). For example, the website of the Qatar-based Al Jazeera news channel was hacked by the SEA in April 2012. At the same time, the Twitter account of Al Arabiya, a Saudi Arabian television news outlet, posted bogus messages about an explosion at a Qatar gas facility, the replacement of Qatar's Prime Minister and Foreign Affairs Minister and the arrest of the Prime Minister's daughter in London. The SEA was almost certainly seeking to exacerbate the tensions between Qatar and Saudi Arabia in order to undermine their partnership on the Syrian issue. In January 2013, the Syrian Electronic Army announced that it had several documents detailing the role played by Turkey, Saudi Arabia and Qatar in the Arab world for nearly two years. This information was later published on the website of Al Akhbar, a Lebanese newspaper that is reputedly pro-Hezbollah. This type of initiative is frequent and the countries targeted are always those that take an official position against Bashar al-Assad and that are accused by the Syrian government of militarily supporting the opposition.

_STRUCTURE OF THE CYBER-THREAT GENERATED BY THE ASSAD REGIME

The Pat Bear group (ATK85) should not be confused with the SEA, though it is related to it. The SEA emerged in 2011 to support the Assad government in the civil war, then the regional war. Its objective was to support the President's image and positions in a context of dissent and violence against civilians. Logically, the group uses website defacement, spam, phishing and DoS techniques, especially against opponents of the regime. In 2014, the Golden Rat group (ATK80) appeared. This group also came out of the SEA, but it does not have the same missions. It specialises in espionage and mainly directs its actions at the national level. Pat Bear emerged in 2015 with the objective of launching cyber offensive operations against the Syrian regime's enemies, including the opposition and Islamic State.





_THE IRAN-SAUDI RELATIONSHIP

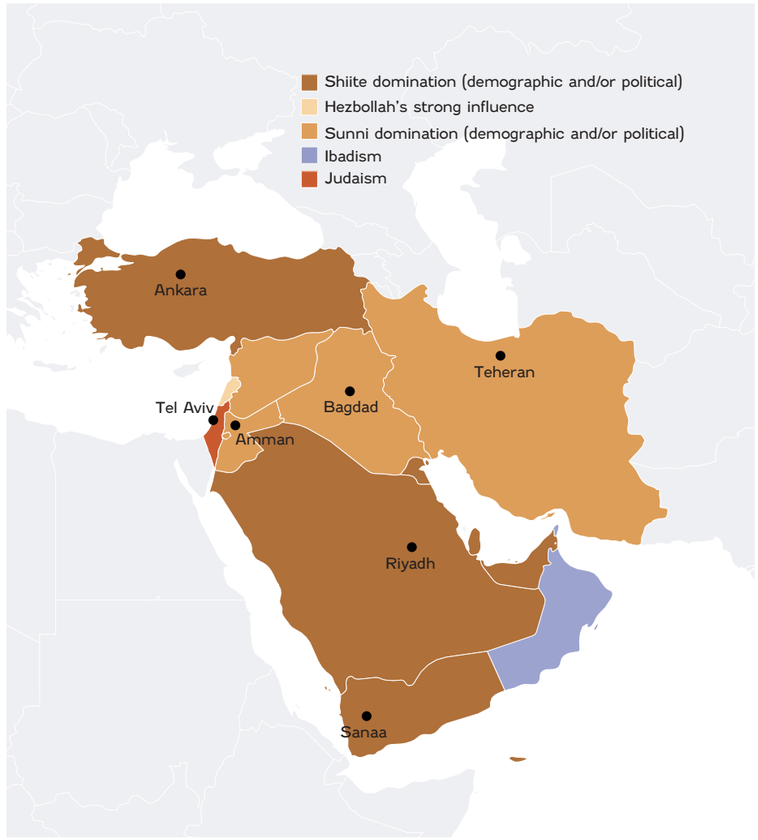
Iran and Saudi Arabia are two major regional powers whose fundamental mutual opposition tends to shape tensions in the region. A regional Cold War type scenario has become established in the last few years around two diametrically opposed models. These two models, in the form of blocs, indirectly confront each other in the region (Syria, Yemen, etc.). This opposition is also evident in the realm of cyberthreats.

_A BIPOLAR CONFIGURATION REFLECTED IN CYBERSPACE

IIt appears that the Saudi bloc is partly supported by the ATK144 group (DarkMatter, Project Raven). Project Raven is a threat group that has been conducting targeted spyware attack campaignsagainst Emirati journalists, militants, activists and dissidents since at least 2012. Circumstantial evidence suggests that there could be a link between this group and the United Arab Emirates (UAE) government. Project Raven is the offensive and operational division of the National Electronic Security Authority (NESA), the UAE equivalent of the NSA. In 2016, this project was moved to DarkMatter and began targeting America. Raven's targets include militants in Yemen, foreign adversaries such as Iran, Qatar and Turkey, as well as specific individuals.
The opposition to the Saudi bloc has been structured around groups that are certainly Iranian in origin, such as ATK40 (Oilrig), ATK26 (Rocket Kitten), ATK35 (Magnallium), ATK19 (Cutting Kitten), ATK30 (Copy Kitten), ATK51 (MuddyWater) and ATK50 (Shamoon). These groups have specialised in destructive wiper malware attacks such as Zerocleare and Shamoon. These are regularly directed against vital Saudi organisations.

_THE 2017 QATAR CRISIS: A SYMPTOM OF A BIPOLAR STRUCTURE

From the 1990's, Qatar gradually broke away from the Saudi "bloc" to demonstrate its independence and moved closer to Iran. In June 2017, after some comments allegedly made by the Emir of Qatar in which he praised Iran, Hezbollah and the Muslim Brotherhood, the petro-monarchies of the gulf severed diplomatic ties with Qatar.
On 16 July 2017, the Washington Post claimed, based on sources from the US Secret Service, that the statement from the Emir originated from a computer hack perpetrated by the UAE. The objective of destabilizing the Qatari emirate and asserting Saudi power in the region has proven to be counterproductive, as witnessed by the rapprochement between Qatar and Iran.
Above all, this crisis reveals the fragmentation of the Middle East around the opposition between Sunni Wahhabi Saudi Arabia and Shiite Iran. This confrontation is not simply religious, with Sunnism and Shiism, or cultural through Arab or Persian influences, but geopolitical with a desire for power and influence in the Western Asia zone. As during the Cold War, the neighbouring civil wars in Syria, Yemen and to a lesser extent Libya are turning into theatres of indirect confrontation between the two blocs.



_JERUSALEM AND THE ISRAELI-PALESTINIAN CONFLICT

This diversity of religions lies at the heart of the ancient problem in the city of Jerusalem, which is the cradle of the three monotheistic religions (Islam, Judaism and Christianity). Long contested because of its religious significance, Jerusalem today is the capital of both Israel and Palestine.
In 1948, the declaration of independence of the Jewish State in Palestine, which then became Israel, led the member countries of the Arab League to contest and take armed action against it. Numerous confrontations between Arabs and Jews ensued in the second half of the 20th century, and countries outside the conflict took a position. What the Arab League contests is Israel's policy of expansion, which it considers illegitimate. The Palestinians do not hesitate to protest against this policy, and various terrorist movements have been born out of this conflict. One example is Hamas, which carried out suicide attacks until 2005 and now focuses on attacks on Israeli cities. In response, Israel has stepped up its militarisation and accelerated the process of expansion into the Palestinian territories. In early 2021, clashes in Gaza, under Israeli control, flared up again like a recurring theme. They serve as a reminder that the issue of territory that divides Israel and Palestine is as contentious as ever, many decades after the conflict began. The conflict has given rise to several hacker groups, which structure their actions around this issue.

_ATK89 (MOLERATS, GAZA CYBERGANG) IS A POLITICALLY MOTIVATED GROUP. IT IS ACTIVE WORLDWIDE, INCLUDING IN EUROPE AND THE UNITED STATES, BUT MAINLY IN THE MIDDLE EAST AND NORTH AFRICA (MENA) AND PALESTINE. THE GROUP IS COMPOSED OF THREE SUB-GROUPS:

- *Gaza Cybergang Group 1 (aka MoleRATs). Its aim is to infect its victims with a RAT, often via text sharing platforms such as PasteBin, github.com, upload.cat and others.*
- *Gaza Cybergang Group 2 (aka Desert Falcons). This subgroup uses homemade malware tools and techniques. Victims are often in-*

fected by social engineering methods such as fake websites claiming to publish censored political information, spear phishing emails or social network messages.

- *Gaza Cybergang Group 3 (aka Operation Parliament). It focuses on espionage and targets executive and judicial bodies around the world, but mostly in the MENA region, especially Palestine. The group has used malware with CMD/PowerShell commands for its attacks.*

Each group is different in its TTPs (tactics, techniques and procedures), but they all use the same tools after taking control of their victims. ATK89 seems to still be active. In late 2020, it added two new backdoors (DropBook and SharpStage) to its arsenal as well as a downloader (MoleNet) in order to target Israel in particular.
ATK66 (APT-C-23) is commonly regarded as an APT group linked to the ruling Hamas organisation in the Gaza Strip. The group was reportedly formed in 2011, but it became active in 2014, when the first attacks were detected in the wild. By examining its victims and TTPs, it is apparent that the group mainly attacks targets related to the Palestinian Authority. APT-C-23 members are native Arabic speakers in or from the Middle East. One of the most recent ATK66 campaigns began in Palestine in late 2020 and targeted people in the same region, including government officials, members of the Fatah political party, student groups and security forces.

_FINANCIAL RETURNS FROM HYDROCARBONS AS A POLITICAL DRUG

The region is also rich in hydrocarbons (oil and uranium), which ensures that the countries of the Persian Gulf and Arabian Peninsula benefit from significant financial returns. As a result, these countries satisfy the primary needs of their populations, such as medical care and social infrastructure (universities, etc.) and even exempt them from taxes.
Hydrocarbons are like a drug in the Middle East. Internally, the rentier countries enjoy the satisfaction of substantial and continuous income streams. However, this income is dependent on world prices, which can create a kind of "withdrawal" effect. This serves as a geopolitical lever in the region, especially in the context of the Iran-Saudi Arabia proxy conflict.
Riyadh and Tehran are among the best supplied with hydrocarbons and the largest producers in the region. In 1960, they helped create the Organisation of the Petroleum Exporting Countries (OPEC) but soon began to display doctrinal divergences, especially at the Caracas summit in 1977, where the members aligned around Saudi Arabia's productivist vision. Since the 1980s, Saudi Arabia has increased its production in order to bring down the price per barrel and put financial pressure on Iran. The Iranian economy, which was not diversified at the time, was quickly hit by American sanctions in the 1990s.
In the future, this energy lever could pose a significant risk of geopolitical destabilisation and lead to an increase in the level of cyberthreat.

Current OPEC members

Conclusion

As we have seen, the Middle Eastern cyberthreat landscape is shaped by several geopolitical factors. The region is highly polarised around a fundamental divergence between Saudi Arabia and Iran. This polarisation takes the form of a subregional Cold War with a "bloc" logic that is often reduced to a simple opposition between Sunnis and Shiites, but which in reality is much more complex. These two blocs confront each other indirectly in war zones such as Syria and Yemen, as well as through militia or Islamist intermediaries.
Ultimately, this complexity is transposed into cyberspace with an array of hacker groups and a sustained level of activity.

Zone East Asia _

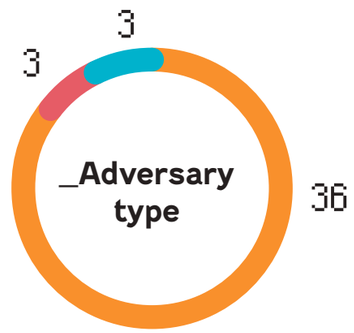
Burma
Brunei
Cambodia
Indonesia
Laos
Malaysia
Philippines
Singapore
Thailand
East Timor

Vietnam
China
Japan
North Korea
South Korea
Taiwan
Mongolia

70 ATKS (Attackers)
targeted the aera

_Adversary Type

_Terrorists
_State-Sponsored
_Cyber Criminal



_Top 3 attacked sectors

Energy
Education
Manufacturing

_Energy	● ● ● ● ● ● ● ● ● ●
_Manufacturing	● ● ● ● ● ● ● ● ● ●
_Communication	● ● ● ● ●
_Transportation	● ● ● ● ● ●
_Education	● ● ● ● ● ● ● ● ● ●
_Aviation	● ● ●

Contextual analysis of East Asia and geocyber risks

The Far East is a vast area that comprises two naturally connected sub-areas: East Asia and Southeast Asia.

_THE FAR EAST AND CHINESE POWER

Over the last decade, the cyber-threat landscape in this region has been greatly impacted by the growing influence of China as an economic, political and cultural player. China has sought to structure its presence by creating international organisations in the region and using them to exert its influence.
Furthermore, the New Silk Roads project launched by Chinese President Xi Jinping in 2013 directly serves Chinese foreign policy. This project is supported by organisations with significant funds, such as the Asian Infrastructure Investment Bank (AIIB).
Today, China is a key player in the region and has been competing with the Western powers for the last decade. The growth of China as a focal point has prompted the other Far Eastern countries to adopt a cautious posture with respect to Beijing.
For the main countries of the zone, two objectives are emerging: that of creating counterweigts to Chinese influence with the aim of strategic rebalancing, and that of maintaining a peaceful relationship with Beijing in order to preserve the economic ties.
Within the Association of Southeast Asian Nations (ASEAN), for example, trade between China and its southern interface has created a strong interdependence, so much so that China has become the largest trading partner in the zone[1].

In turn, Japan has established trade with the various countries in the region and has maintained relations with China, despite a difficult shared history and China's claim to certain islands in the archipelago. Tensions between the two countries are ongoing in the East China Sea over the delimitation of their exclusive economic zones (EEZs).
North Korea is heavily reliant on China, which accounted for 90% of its trade before the Covid-19 crisis[2]. In addition, North Korea remains the only country with which China has signed a defence treaty[3].
Seoul remains relatively close to Beijing, with regular bilateral talks, which began to normalise in late 2019. Trade between the two countries is extremely limited, however, since China introduced economic sanctions against South Korea in 2017. These sanctions follow South Korea's agreement to host America's Terminal High Altitude Area Defense (THAAD) anti-ballistic missile defence system[4]. On the other hand, relations between ASEAN, Japan and the two Koreas remain cordial.
The Far East appears as a breeding ground for cyber threats. At the regional level, a decisively important game is clearly being played out, fuelled by China's desire to influence the zone and the responses of the other countries. Agendas are also being played out in smaller arenas, as we will see with the Korean question.

_A REGIONAL STRUGGLE FOR INFLUENCE REFLECTED IN CYBERSPACE

From a geostrategic viewpoint, Chinese domination is often presented as overwhelming and hard to contest. Yet the cyber tool creates a discrepancy in this logic of seemingly one-way domination. Indeed, the level of discretion and military effectiveness of this weapon allows for a strategic rebalancing. This creates opportunities for other players to assert themselves in the region. This is evidenced by the activity of several APT groups seeking to be counterweights to Chinese influence.

_SIGNIFICANT ACTIVITY BY GROUPS OF CHINESE ORIGIN

There are no less than 45 ATK groups, known under more than 200 aliases, which appear to originate in China.

_THESE GROUPS SHARE A LOT OF TOOLS AND MALWARE WITH EACH OTHER, WHICH MAKES IT DIFFICULT TO DELINEATE THEIR ACTIVITIES

In 2014, the ATK34 group (Goblin Panda) aided by the 1937CN group[5], launched cyber-espionage operations on Vietnam's oil sector. In 2016, the same two groups carried out sabotage operations on the country's transportation sector, then in August 2017 attacked its political institutions. This attack came a few days after the re-emergence of tensions around control of the South China Sea between China and Vietnam, which is set against the backdrop of historic discord over the Paracel Islands[6]. On 5 August 2017, the meeting of foreign ministers of ASEAN countries in Manila had resulted in a resurgence of tensions provoked by Vietnam against China.
In addition to the ATK34 group, of which Goblin Panda is a part, the ATK1 group (Lotus Blossom) regularly attacks the region. Before 2013, one of the group's hackers called Elise installed backdoors on Southeast Asian networks, focusing especially on electronics manufacturers and telecommunication companies, which enabled attackers to penetrate the systems[7]. In 2015, ATK1 conducted massive espionage campaigns aimed at government and military organisations across Southeast Asia[8]. These campaigns, whose objective was to weaken political organizations and spy on group members, are still ongoing. The most prominent example is the ASEAN, which suffered from a cyber espionage attack operated by ATK1 in January 2018[9].
Other groups, considered less prolific, appear to be more responsive to a political agenda. ATK34's campaign of attacks on Vietnamese institutions in August 2017, for one, reflects intensifying tensions with China. The ATK29 (TEMP.Periscope) group has also demonstrated its ability to exploit local contexts and leverage them into cyber attack opportunities. ATK29's campaign in Cambodia in July 2018 during the legislative elections is indicative of this trend. ATK29 group is interesting because the first evidence of its activity dates from the start of the Silk Roads project in 2013.
Initially focusing on the maritime domain, its range of targets was later extended to the defence, transportation, engineering and space sectors. In recent campaigns, it has directed its attacks at the countries involved in the Silk Roads project, reflecting a shift in targets and paradigm. Its activities have turned more particularly to industrial espionage and destabilisation. It was to this end that ATK29 targeted Cambodia in July 2018. From September 2017, the country had been plunged into significant political stagnation, making the attack all the easier. The leader of the Cambodia National Rescue Party (CNRP) had been charged with treason and spying by Prime Minister Hun Sen[10]. He had also dissolved the CNRP, the only opposition party, ahead of the July 2018 legislative elections, which is when the attack occurred. This created an opportunity for the Chinese actor to leverage its cyber arsenal to gain high visibility on Cambodian politics and the actions under consideration by the government.

A similar scenario happened in the Philippines in 2015. China refused to take part in an arbitration procedure with the Philippines at the Permanent Court of Arbitration (PCA) in The Hague to settle territorial issues in the Philippine Sea. In the same year, Barack Obama raised the issue of control of the South China Sea at the Asia Pacific Economic Cooperation (APEC) Summit, which was endorsed by the host country, the Philippines[11]. Shortly after, ATK29 (NanHaiShu) attacked the Philippine Department of Justice[12].

_VIETNAM AND THE ATK17 GROUP (APT32)

VIETNAM ALSO MAINTAINS THIS STANCE OF NON-SUBMISSION TO ITS GIANT NORTHERLY NEIGHBOUR

Relying on a highly successful group called ATK17 (APT32), Vietnam conducts almost continuous espionage campaigns against diverse but well-defined targets. The techniques implemented by ATK17 include the use of decoy documents that allow for initial access to multiple platforms (Windows and MacOS in particular). The group was thus able to achieve its objectives by carrying out numerous attacks against Chinese interests.

SOUTH KOREA IS ALSO RESPONDING TO CHINESE PRESSURE. KOREAN-SPEAKING GROUP ATK52 (DARKHOTEL) IS VERY ACTIVE AGAINST CHINA

While some experts link this threat actor to North Korea, especially given the overlap between it and ATK4 (APT37), the consensus is that it is

actually linked to South Korea. It targets government entities, especially in the areas of diplomacy, defence and justice. Its activity is focused in particular around the Sea of Japan and the East China Sea. Its purpose is to spy on specific people, especially Chinese individuals. The group leverages its cryptographic skills to produce fake certificates and use zero-day. It also has access to an extensive and reliable network infrastructure, which enables it to maintain long-term access to its targets.

_THE PHILIPPINES AND THE NATIONAL BRANCH OF THE LULZSEC MOVEMENT

TK129 (Pinoy LulzSec) is the Philippine branch of the international LulzSec movement, embracing its anarchist ideology. According to statements by its members, ATK129 has been active since 2012, with a surge of its activity in 2017 and 2018.
In April 2019, the Philippine government and its defence institutions and industry were the victims of an April Fools' targeted campaign. The hackers conducted dozens of attacks during these campaigns, mainly website defacement and theft of data, which was then leaked on online file sharing platforms. The hackers primarily attacked government-related targets, but they also targeted the education sector.
These campaigns against the Philippine government came after President Duterte signalled a rapprochement with China. More recently, the group's attacks have directly targeted the People's Republic, with the idea to pursue efforts to defend the country's sovereignty against Chinese influence.

_TAIWAN AND THE ATK153 GROUP (APT-C-01)

Taiwan, with Hong Kong, is one of the states most subject to Chinese pressure and cyberattacks by groups believed to be based in China.

However, the island state is supported by ATK153 (APT-C-01), an APT group that has been conducting cyber-espionage campaigns against key Chinese units and departments such as government, national defence, science and technology, education and maritime agencies for 11 years. The group mainly targets the defence industry in connection with strategic issues such as Chinese-US relations, Cross-Strait relations and maritime-related issues. This 11-year series of cyber-espionage campaigns in China includes no less than 15 major attacks on Chinese strategic interests.

_THE KOREAN CHESSBOARD

Contrary to appearances, the Asian chessboard is not only structured around China as the focal point. The Korean conflict is ongoing and is guided and shaped independently according to its own logics. On July 27, 2021, the two Koreas decided to re-establish communication channels, witnessing a rapprochement. Diplomatic ties had been cut a year earlier, as a result of the stalled discussions. This resumption of dialogue comes at a time when North Korea is going through a crisis related to the decline of its agricultural production, causing food shortages in the country.
The history between the two countries is complex and periods of escalation have followed periods of relaxation. The rapprochement, initiated in the late 1990s around economic assistance, ended in 2008 with the arrival in power of the conservative Lee Muyung-bak. The dispute over the disputed maritime zone regularly results in deaths on both sides and the escalation of tensions often lead to surges in cyber-activity from both sides.

_THE MANY KNOWN ATTACKS TO DATE ARE STRUCTURES AROUND TWO EMBLEMATIC GROUPS

On the South side, ATK52 (DarkHotel), regularly targets North Korean interests, reinforcing the hypothesis of a South Korean origin. In the North, the People's Democratic Republic relies on the Lazarus nebula to carry out espionage and destabilization missions on its southern neighbour and attack it. Lazarus comprises several known entities. ATK117 (APT38, Bluenoroff) specialises in recovering funds for the country and is believed to be the source of the Wannacry attack in 2017. ATK4 (APT37) appears to be a more independent group, specialising in cyber espionage of foreign interests, especially in South Korea.[13]

Conclusion

Contextually, the cyber-threat in the Far East is primarily driven by the rise of Chinese influence.
For over a decade, this geopolitical focal point has prompted threat groups in the region to step up their activities in support of the national interests of their respective countries.
However, the cyber-threat is not only driven by these regional factors. Certain geopolitical spaces have specific features linked to their historic context, as is the case with the Korean peninsula.

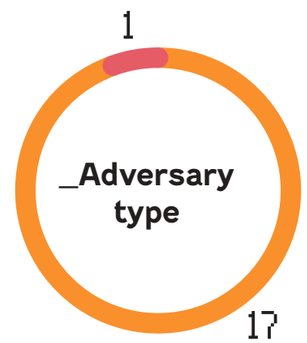
Zone South Asia_

India
Pakistan
Afghanistan
Bangladesh
Bhutan
Maldives
Nepal
Sri Lanka

38 ATKS (Attackers)
targeted the aera

_Adversary Type

_Terrorists _State-Sponsored _Cyber Criminal



_Top 3 attacked sectors

Energy
manufacturing
Transportation

_Energy	● ● ● ● ● ● ●
_Manufacturing	● ● ● ●
_Transportation	● ● ●
_Education	● ● ●
_Retail	●

Contextual analysis of South Asia and geocyber risks

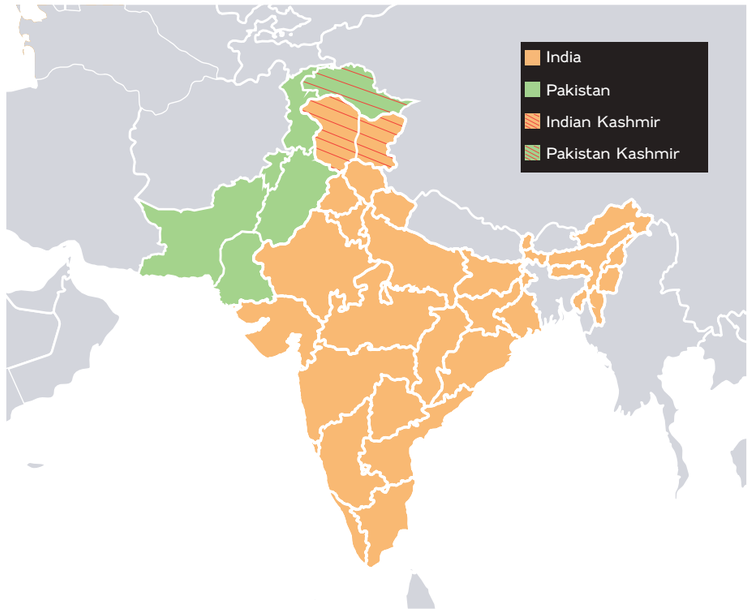
South Asia is a geographic and geopolitical zone that is still fragmented due to current and historic tensions and conflicts.

_TENSIONS AND REGIONAL INTEGRATION PROJECTS

South Asia is shaped by significant regional tensions, most notably between the three giants, namely India, Pakistan and Afghanistan, but also by a desire for rapprochement and integration in order to protect from the influence of neighbouring powers.

_INDO-PAKISTANI TENSIONS AND KASHMIR

The conflict between India and Pakistan began in 1947, when the two countries gained independence and the British Raj was split in two. Pakistan is a predominantly Muslim country that was formed as the Islamic Republic of Pakistan. India, conversely, is a secular state that inherited much of the territory of the Raj.
Shortly after independence, the First Indo-Pakistani war took place in Kashmir. The Kashmir region, independent since 1947, spans territories claimed by India, Pakistan and China. Pakistan and India lay claim to all of these territories. Reflecting this complex heritage, the population of Kashmir is now predominantly Muslim, but it is ruled by a Hindu Maharaja.
This first war ended in 1949 after the United Nations brokered a ceasefire agreement based on a future Line of Control (LoC). Since the LoC was established, Kashmir has been a region in two parts: Indian Kashmir and Pakistani Kashmir. The Line of Control has become a militarised zone, with the Indian and Pakistani armies facing



off across the divide. The Indo-Pakistani conflict remains crystallized on the Kashmir issue. Today, the border between India and Pakistan is considered one of the most dangerous in the world.
On 14 February 2019, tensions between Pakistan and India reignited when a suicide attack claimed by Pakistan-based Islamist group Jaish-e-Mohammed (JeM) killed 41 Indian soldiers. The attacker was a 20-year-old Kashmiri rebel, whose act led to a resurgence of military activism in the region. Narendra Modi, Prime Minister of India since 2014, condemned the attack and announced that there would be a response.
On 18 February, in retaliation, India conducted an armed raid in the area where the attack had taken place. Nine people were killed in the town of Balakot, where a JeM training camp is located. The resurgence of terrorist attacks in the region is worrisome for the Indian government, which is using all possible means to protect against them. Since both countries are nuclear powers, and the border between them is one of the most militarised in the world, an open conflict would be devastating for the region.

_FOR THIS REASON, THE CYBER LEVER APPEARS THE BEST WAY FOR EACH SIDE TO ASSERT ITS CLAIMS

Indo-Pakistani tension is mostly latent, with no open and direct confrontation since 1971. Nonetheless, current tensions are high, and groups of cyberattackers, suspected to be from both countries, regularly conduct operations against each other's security forces. After the February 2019 suicide attack, the number of cyberattacks increased.
On the Pakistan side, ATK64 (alias Mythic Leopard) is a Pakistan-based group whose operations are most likely conducted from Karachi. It uses social engineering and spear phishing to target Indian military and defence entities.
On the Indian side, ATK11 (alias Patchwork) is a cyber espionage group active since at least 2010. One of its specific techniques is the use of code copied and pasted from multiple online forums combined with high-quality social engineering. It began with Operation Hangover, the purpose of which seemed to be surveillance of targets of national security interest to India, such as Pakistan and the Nagaland movement. The group was also involved in the Monsoon campaign, which targeted various sectors in India's neighbouring countries.

_AFGHANISTAN: THE UNSTABLE STATE

India and Pakistan have different relationships with Afghanistan. Historically, each country's bilateral relations with its Afghan neighbour have oscillated between long-term support projects and containment actions linked to the presence of the Taliban.
India was the only South Asian country to recognise the Soviet-backed Democratic Republic of Afghanistan in the 1980s. In turn, Pakistan suffered destabilisation attempts perpetrated by the Soviets and implemented by the Afghan government with the objective of arming Pakistan's Pashtun independence fighters so they could overthrow the regime of the time. Since then, Pakistan has continued to treat its westerly neighbour with suspicion.
With the rise of the Taliban movement, both countries have maintained their course of action. India supported the then regime, helping overthrow the Taliban, while Pakistan has been regularly accused by Afghanistan of funding the mujahideen through its Inter-Services Intelligence (ISI).
Before the Taliban came to power, India provided Afghanistan with substantial aid (it was the fifth largest contributor in 2017 with $3 billion) and maintained its stance toward the Taliban. However, the summer 2021 was marked by a formal meeting between Taliban leaders and an Indian delegation in Qatar.
Relations between Pakistan and the Taliban are more complex, especially since the Taliban announced that it does not recognise the Durand Line, which marks the border between the two countries. Furthermore, Pakistan, like Afghanistan, has suffered Taliban attacks on its soil, which has prompted the two countries to cooperate more closely in recent years.
Despite Afghanistan's instability and this historic context, both India and Pakistan are trying to cooperate with their neighbour. Notably, Pakistan has reached a Memorandum of Understanding with Afghanistan for the establishment of the Afghanistan-Pakistan Transit Trade Agreement (APTTA) and the construction of a rail link between the two countries. This cooperation may extend to joint defence and intelligence sharing operations.
In turn, India, which historically has a stronger relationship with Afghanistan, has set up agricultural development projects on Afghan territory and, in the last decade, several hundred Afghan soldiers have been trained at Indian institutions.

_DESPITE THESE PARALLEL BILATERAL COOPERATIONS, WHICH REMAIN IN PLACE TODAY, CYBER OPERATIONS ARE STILL BEING CONDUCTED

For example, the ATK64 group (Transparent Tribe, APT36), suspected of being sponsored by Pakistan, has repeatedly targeted Afghanistan in espionage operations. The most recent attacks were in July 2021[1].

Another attacker group known as SideCopy APT, affiliated with Pakistan, has led attack campaigns against public and private organizations in South Asia, including ministries in India and Afghanistan. In 2021, some of the most notorious victims included Afghanistan's ministries of finance and foreign affairs, the administrative office of the Afghan president, and a computer containing the credentials of the Indian government and education departments. In the case of the attacks against Afghanistan, the attacker was able to exfiltrate numerous personal documents including diplomatic visas as well as the IDs of Afghan government officials. SideCopy APT uses fake documents as well as Trojan Horses distributed via spear-phishing techniques[2].

_COMMITMENT TO REGIONAL INTEGRATION

_SOUTH ASIAN ASSOCIATION FOR REGIONAL COOPERATION

At the regional scale, the eight South Asian countries created the South Asian Association for Regional Cooperation (SAARC) in 1985 to promote cooperation between member states and drive economic development.
This regional organisation has permanent links with the United Nations as an observer. It has also developed ties with other regional organisations such as the European Union. In 2006, SAARC created the South Asian Free Trade Area (SAFTA) encompassing 1.6 billion people.
At the local level, cooperation projects are emerging. In 2015, the gas pipeline project linking four South Asian countries, namely Turkmenistan, Afghanistan, Pakistan and India, was born. This project, which allows the countries to achieve greater energy autonomy, strengthens the ties between the South Asian states.
These various cooperation projects, aimed at better regional integration and economic development, are also intended to give the countries in the region greater autonomy with respect to neighbouring powers.
The region is surrounded by China to the north and east and by Iran to the west. It should also be noted that Russia, further north, has a historic influence in the region. This influence has been achieved by cyberthreat actors suspected of being sponsored by these neighbouring powers.

A COMPLEX SINO-INDIAN RELATIONSHIP, SOURCE OF POLITICAL TENSIONS AND CYBER OPERATIONS

China and India are states that share many similarities. Formerly under colonial rule, both countries have experienced exceptional economic and demographic growth that has allowed them to assert themselves as major powers at the regional and global levels. The two governments maintain close relations, particularly at the economic level, marked by bilateral partnerships and their leading role in the Shanghai Cooperation Organization (SCO). In spite of this collaboration, tensions remain between the two political regimes as they clash over their common frontier as well as over the trade routes developed in recent years.

CONFLICT AROUND THE SINO-INDIAN BORDER ZONE

June 15, 2020 is an important date in the evolution of the border conflict between the two countries. For the first time in 45 years, the frontier zone was the scene of violent clashes leading to the death of Indian and Chinese soldiers in the mountainous Galwan River valley. This historic conflict is based on divergent views between the two regimes, with India considering the frontier region to be nearly 3500 km long, compared to an estimate repeated by the Chinese media of around 2000 km. While the likelihood of an open conflict between India and China remains low, the intensification of tensions related to the frontier regions could lead both sides to resort more frequently to the cyber tool.

SILK ROAD AND FREEDOM ROAD: A SYMBOL OF SINO-INDIAN RIVALRY

In 2013, Xi Jinping gave a speech in Astana in which he unveiled the comprehensive project to build infrastructure along the ancient Silk Roads. This project called «The New Silk Roads» shows the Chinese hegemonic ambition to create a new strategic paradigm along land and sea routes. In order to compete with this ambition, India and Japan have developed an infrastructure and transport project that is supposed to revitalize the trade routes between the Asian and African continents: the «Freedom Road». The rivalry between both projects tends to intensify tensions between Beijing and New Delhi. The port of Gwadar, a symbol of the «New Silk Roads», has to face competition from the port of Chabahar, inaugurated in 2017 by an Indo-Iranian alliance wishing to challenge the grip of Chinese influence in Central Asia.

THE RISE IN SINO-INDIAN TENSIONS HAS LED TO A SHARP INCREASE IN CYBER ESPIONAGE ACTIVITIES BY CHINESE-BASED ATTACKER GROUPS ON INDIAN TERRITORY

The energy sector has been particularly affected, as have port facilities. TTPs analysis seems to correlate these actions to the activity of Chinese attacker groups, including APT41, Tonto Team or even RedEcho.

In 2013, India announced its desire to compete with the «New Silk Roads.» That same year, a group known as Wet Panda, operating since 2010 launched massive campaigns against the country. The government, the Indian Informatic Centre, the defence industry, telecom providers and even NCOs were targeted. An IP address of one of the attackers was associated with a university based in Chengdu, China. The same targets were attacked in 2018 by operations attributed to ATK2 (Wicked Panda). This campaign appears to be related to the inauguration of the port of Chabahar, Iran, a competitor to Gwadar, a few months earlier.

SEVERAL GROUPS POTENTIALLY SUPPORTED BY CHINA HAVE TARGETED THE REGION. *They include ATK2 (APT17), ATK13 (Turla), ATK23 (Icefog), ATK34 (APT30) and ATK41 (APT10).*

Among the groups suspected of being linked to Russia are ATK5 (APT28) and ATK116 (CloudAtlas).

Lastly, groups believed to be of Iranian origin, such as ATK19 (RocketKitten), ATK51 (MuddyWater) and ATK229 (APT-C-50), have also targeted countries in the region.

Conclusion

South Asia is a geographic region that tends to move towards closer unity despite the dissensions and diversities.

It is physically permeated by contradictory geopolitical issues, culturally shaped by beliefs, which are hard to reconcile, and historically marked by a heritage of conflict. Tensions between India and Pakistan, the instability of Afghanistan and the great difference in development and wealth between the countries make regional integration unlikely. This is reflected in the many cyberattacks between groups in these countries.

However, the states in question are trying to overcome the difficulties through development projects, bilateral and multilateral cooperation and the creation of a free trade area.

These challenging attempts are motivated by an awareness of a broader contextual dimension. Regional integration, albeit imperfect, should help the countries in the region protect from neighbouring influences and gain significance on the international stage in an autonomous manner.

As we have seen, cyberattacks from neighbouring countries occur regularly and often focus on destabilisation and espionage by exploiting these historic, cultural and physical animosities.

Zone Oceania_

Melanesia
(Solomon Islands, Fiji, Vanuatu)
Micronesia
(Mariana Islands, Marshall Islands, Caroline Islands, Nauru and Guam)
Islands of Polynesia (Hawaii, Easter Island)
New Zealand and Australia

10 ATKS (Attackers)
targeted the aera

_Adversary Type

_Terrorists _State-Sponsored _Cyber Criminal

_Top 3 attacked sectors

Energy
Education
Transportation

_Energy	
_Manufacturing	
_Communication	
_Transportation	
_Education	
_Aviation	

Contextual analysis of Oceania and geocyber risks

Oceania extends over a vast area of the Pacific Ocean, and encompasses different sub-regions made up of island states and island groups, including Melanesia (the Solomon Islands, Fiji and Vanuatu), Micronesia (Mariana Islands, Marshall Islands, Caroline Islands, Nauru and Guam), and the islands of Polynesia (Hawaii and Easter Island). It also includes New Zealand and Australia, larger countries which are more economically developed than the island states.

The region's dynamics play out at Pacific-wide, sub-regional, and island levels. While Australia and New Zealand stand out as key countries thanks to their demographic and economic importance, the island states of Oceania are still over-dependent on other countries, leading to the development of a "north-south" divide in the region.

Largely ignored in the history of international relations, Oceania has emerged as a zone of significant strategic interest in the post-war period. Australia and New Zealand are seeking extensive US engagement in Oceania, while affirming their position as regional powers.

The decolonisation process has also focused attention on the challenges and vulnerabilities of small states in the region. The economic and political emergence of Asian powers has driven the development of closer links with Asia, and a stronger sense of belonging to the Asia-Pacific region.

While retaining ties with the UK and with their European heritage, Australia and New Zealand are also turning to the United States as a key security ally, evidenced notably in the AUKUS alliance in 2021, associated with the nuclear submarines scandal.

_AUSTRALIA AND NEW ZEALAND EXPERIENCE INCREASING TENSION IN RELATIONS WITH CHINA

_TENSIONS BETWEEN CHINA AND AUSTRALIA

Australia and China have adopted a more confrontational approach to each other.
In 2018, bilateral relations between Australia and China appeared to be at their lowest ebb for a decade when Australia ruled out Chinese telecom giant Huawei from building its 5G network on national security grounds. Over the year 2020, however, the relationship between the two countries has deteriorated even further, at a critical time for the region.
The ongoing degradation of relations between Canberra and Beijing throughout 2020 had unprecedented consequences for trade and economic links. On April 19, 2020, Scott Morrison's government upped the stakes even further with its proposal for a global inquiry into China's handling of the Covid-19 epidemic in Wuhan, thereby suggesting that China might be responsible for the global pandemic, and leading to an immediate response from the Chinese government.
Australia and China subsequently became embroiled in an escalation of trade disputes. Starting in May 2020, for example, China introduced a series of commercial sanctions against Australian products. The sanctions resulted in higher tariffs and stricter quotas being imposed on Australian products such as wine or barley.
In parallel with these commercial tensions, diplomatic disputes between the two countries also intensified. In May 2020, the Morrison government used its veto power to cancel Chinese investments that were to expand the New Silk Roads to the Oceanic continent, in the state of Victoria.
In July 2020, Canberra promise to offer a safe haven to residents of Hong Kong after China rolled out its national security law to the city.
The Chinese embassy in Australia responded by accusing Canberra of political interference in China's internal affairs.
In November 2020, Chinese Foreign Ministry spokesperson Zhao Lijian tweeted – via his official Twitter account – a controversial fake image depicting an Australian soldier holding a bloodied knife over the throat of an Afghan child. Canberra requested that China apologise for this attack on the conduct of Australian soldiers in Afghanistan, but received no reply.
This series of diplomatic incidents between the two countries must be viewed within the context of Australia's broader security concerns about Chinese growth presenting a threat to the Asia-Pacific region. In response to the issue, Australia has consolidated its collaboration with allies and regional partners, such as the United States, the United Kingdom, Canada, New Zealand, Japan and India.

_ESCALATING ECONOMIC AND DIPLOMATIC TENSIONS IN 2020 BETWEEN CHINA AND AUSTRALIA HAVE ENCOURAGED OFFENSIVES BY CHINESE ATTACK GROUPS AGAINST AUSTRALIAN TARGETS, NOTABLY NATIONAL UTILITIES AND HOSPITALS

In June 2020, the Australian government issued an advisory on increased cyber activity by a state actor against networks belonging to its agencies and companies in the country.
According to the Australian's government, the attack was operated by a state-sponsored actor that relied on an exploit code which had been slightly modified for past vulnerabilities. Unofficially, China was blamed. The actor targeted public-facing infrastructure through the use of remote code execution vulnerabilities. This was the fourth warning in a year from the Australian Cyber Security Centre (ACSC) about threat actors exploiting critical vulnerabilities in Telerik UI (CVE-2019-18935, CVE-2017-9248, CVE-2017-11317, CVE-2017-11357). Exploit code had been publicly available for a while. If they failed to gain initial access by leveraging these flaws, the attacker turned to spear phishing to harvest credentials, deliver malware, and steal Office 365 OAuth tokens.
A link to China is provided by the threat actor's use of malware – such as PlugX – that has been associated with Chinese hacker groups, some believed to work on behalf of the government. Several actors, all connected to China and engaged in espionage activities, have PlugX in their toolset (ATK2, ATK37, ATK220, ATK41, and ATK15).

_NEW ZEALAND'S POSITION IN THE OCEANIA REGION

The intensification of tensions between China and Australia raises questions about New Zealand's strategic positioning in this new context. On the one hand, the country is a historical ally of Australia and the trans-Tasman relationship was built around a common British colonial heritage. The two countries are part of the Commonwealth of Nations, the Five Eyes for strategic intelligence sharing, and have developed economic collaboration around the Closer Economic Relations (CER) free trade agreement. On the other hand, China accounts for nearly 30% of Australia's exports and maintaining a peaceful bilateral relationship is critical to the sale of Australian dairy products overseas.
In May 2020, the Five Eyes alliance (Canada, the United States, the United Kingdom, Australia and New Zealand) decided to broaden its pre-

rogatives to allow for the display of a unique posture on issues related to democracy and fundamental human rights. In November 2020, this new role took shape when the alliance condemned China's intervention in Hong Kong and called for the reinstatement of the members of the Legislative Council who had been suspended by Beijing. This declaration also denounced the treatment of the Uighur population.
While New Zealand Prime Minister Jacinda Ardern spoke of the difficulty of «reconciling» differences between the two countries, Foreign Minister Nanaia Mahuta refused to join the Five Eyes alliance's condemnation of the treatment of the Uighur minority in Xinjiang province.
This statement, in addition to jeopardizing the alliance's political project, shows the fragility of New Zealand's diplomatic position, torn between preserving its relationship with Australia and its economic well-being. The progressive militarization in the South China Sea and Chinese interference in Hong Kong could lead New Zealand to adopt a clearer strategic line in the future. Depending on the positioning chosen, New Zealand could become a breeding ground for offensive activity by Chinese cyber attackers.

_AUSTRALIA AND THE NEW AUKUS ALLIANCE IN THE INDO-PACIFIC REGION

AUKUS (an acronym based on the country names Australia, United Kingdom and United States) is a new trilateral strategic defence alliance. It was initially created for the purpose of constructing a class of nuclear-powered submarines, collaborating in the Indo-Pacific region (where the rise of China is viewed as a growing threat), and developing more advanced technologies. The agreement led Australia to terminate the contract awarded to France in 2016 for the construction of 12 diesel-electric submarines to replace its ageing fleet of Collins-class submarines. Australia decided in November 2021 to engage alongside its American and British allies.
Aside from the United Kingdom, this is the first time that the United States has shared nuclear propulsion technology with an ally. Consequently, many observers believe that Australia, the United Kingdom and the United States have entered into a historic nuclear defence and security agreement which will have consequences in the Indo-Pacific region for decades to come. The agreement will enable Australia to build a fleet of at least eight nuclear attack submarines in order to counter Chinese influence.
However, it is also interesting to note that the AUKUS agreement will include artificial intelligence as well as other technologies, such as cybersecurity. AUKUS could therefore be one of the most important defence and cooperation alliances for decades.
According to the associated press release, the partnership is a historic opportunity for the three nations to protect their shared values, and contribute to the stability and prosperity of the Indo-Pacific region, together with friends and partners who share the same ideas.

The decision to involve Australia in the longstanding cooperation between the US and the UK reflects the West's growing concern about Beijing's military expansion, debt diplomacy and cyber-intimidation.

_THE AUKUS ALLIANCE GOES WELL BEYOND JUST SUBMARINES

Attention has focused on French and Australian diesel/nuclear submarines, and military hardware is certainly a key component, in view of the geopolitical issues at stake. However, the agreement also covers other forms of conflict. The AUKUS alliance attaches particular importance to cyberspace.
At the press conference announcing the agreement, US president Joe Biden said that a cybersecurity component would be included, in addition to submarine technology. Although President Biden did not specify this during the press conference, it appears probable that the United States and the UK would support Australia in the deployment of cyber-defence, and potentially also cyber-attack, capabilities.
In recent years, Australia has been the target of several major cyber-attacks, one of the most striking of which took place in June 2020. Australian Prime Minister Scott Morrison went on the record to officially state that the country had been the subject of a sophisticated state-sponsored cyber-attack.
Suspecting that China was responsible, Mr Morrison said that he had talked to British Prime Minister Boris Johnson about the incident, although it is uncertain whether the United Kingdom had provided cyber-expertise to Australia.

Attackers Groups

Threat Actor_

ATK1
Lotus Blossom, Spring Dragon, DragonFish is a state sponsored (China) first seen in 2012.
_Type of attacker: State Sponsored

Alias_

_DragonFish
_Lotus Blossom
_ST Group
_Spring Dragon

Targeted Sectors_

_Universities
_Telecommunication
_Satellites and Telecommunications
_Military
_High-Tech
_Government and administration agencies
_Financial Services
_Education
_Communication

Motivations_

_Information theft
_Espionage

Targeted Areas_

NORTH AMERICA
Canada
United States Of America

WESTERN EUROPE
France

SOUTH EAST ASIA
Vietnam
Thailand
Singapore
Philippines
Myanmar
Malaysia
Indonesia
Cambodia
Lao People's Democratic Republic

EASTERN ASIA
Japan
Hong Kong
Taiwan

Suspected origin of the attacker_

China

_DESCRIPTION

ATK1 aka - The group focuses mainly on the territories bordering its country of origin (South China Sea); The group primarily targets government institutions and political parties; Educational establishments such as universities, as well as companies in the telecommunications sector are not spared.
They notably used the Elise malware, it was intended to spy on many government organizations, mainly in Southeast Asia. We can think that this campaign was intended to support the Silk Roads project by securing the maritime side of the latter.
At the end of 2015, its "Emissary" malware received numerous updates, probably to avoid being detected by security products. After a very active period, the group remained discreet until the beginning of 2017.
Other campaigns were carried out sporadically until 2018, still using Elise as the main attack vector, and sometimes using new exploits, such as CVE-2017-11882. ATK1 is capable of performing very large operations over a long period of time, while developing its specific arsenal.
These targets are extremely precise and the group rarely deviates from them.
Examination of the group targets reveals that they correspond to the preferred geographic areas followed by offices 2 and 6 (units 61398 and 61726), which are the United States / Canada and South Asia / Taiwan areas, respectively. These offices are part of the Network System Department (NSD), which reports directly to the Strategic Support Force (SSF), which is part of the PLA Staff Department of the Central Military Commission. The information gathered through these espionage campaigns therefore has an undeniable strategic dimension for the Chinese military administration.

_USED MALWARES

- Catchamas
- Elise
- Emissary
- Hannotog
- Mimikatz
- Rikamanu
- Sagerunex
- Spedear
- Syndicasec

_USED TOOLS

- Living off the Land
- PsExec
- gpresult

USED VULNERABILITIES

- CVE-2009-0927
- CVE-2012-0158
- CVE-2014-4114
- CVE-2014-6332
- CVE-2017-11882

_ATTACKS HAPPENED ON

> **Attack against military and governement targets in Vietnam - Philippines - Hong Kong - Taiwan and Indonesia**
Happened on: 2012-01-08

> **Phishing campaign using a PDF document containing an invitation to a defence event**
Happened on: 2012-09-08

> **Attack against Taiwan United States - Canada and some other countries**
Happened on: 2013-07-08

> **Emissary Malware used against French Ministry of Foreign Affairs**
Happened on: 2015-01-08

> **Elise campaign against its traditionnal targets in Southeast Asia**
Happened on: 2017-01-08

2012
2012-01-08
Attack against military and governement targets in Vietnam - Philippines - Hong Kong - Taiwan and Indonesia

2013
2012-09-08
Phishing campaign using a PDF document containing an invitation to a defence event

2014
2013-07-08
Attack against Taiwan United States - Canada and some other countries

2015
2015-01-08
Emissary Malware used against French Ministry of Foreign Affairs

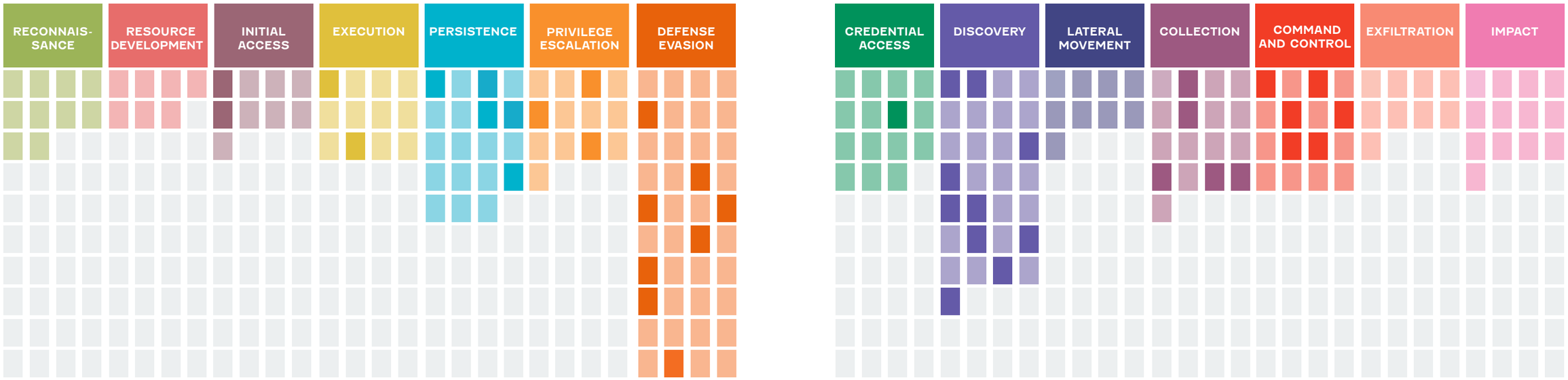
2016

2017
2017-01-08
Elise campaign against its traditionnal targets in Southeast Asia

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1007 - System Service Discovery
T1010 - Application Window Discovery
T1016 - System Network Configuration Discovery
T1027 - Obfuscated Files or Information
T1027.001 - Binary Padding
T1027.002 - Software Packing
T1036 - Masquerading
T1571 - Non-Standart Port
T1046 - Network Service Scanning
T1055 - Process Injection
T1055.001 - Dynamic-link Library Injection
T1056 - Input Capture
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.003 - Windows Command Shell
T1069 - Permission Groups Discovery
T1069.001 - Local Groups
T1070.004 - File Deletion
T1070.006 - Timestomp
T1071 - Application Layer Protocol
T1074 - Data Staged
T1082 - System Information Discovery
T1087 - Account Discovery
T1095 - Non-Application Layer Protocol
T1098 - Account Manipulation
T1105 - Ingress Tool Transfer
T1112 - Modify Registry
T1113 - Screen Capture
T1115 - Clipboard Data
T1132 - Data Encoding
T1135 - Network Share Discovery
T1136 - Create Account
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1218.011 - Rundll32
T1497 - Virtualization/Sandbox Evasion
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1569.002 - Service Execution
T1573 - Encrypted Channel
T1573.001 - Symmetric Cryptography

_CYBER ATTACK PHASES



Threat Actor_

ATK103

This threat actor is active since at least 2014, responsible of the largest malicious spam campaigns.

_Type of attacker: Cyber Criminal

Alias_

_Gold Tahoe
_Graceful Spider
_Hive0065
_SectorJ04
_SectorJ04 Group
_TA505

Targeted Sectors_

- _Media
- _Manufacturing
- _Healthcare
- _Financial Services
- _Energy
- _Education

Languages_

_Russian

Motivations_

_Financial Gain

Targeted Areas_

NORTH AMERICA
Canada
United States Of America

CENTRAL AMERICA
Mexico

SOUTH AMERICA
Chile

NORTHERN EUROPE
Sweden
Netherlands

WESTERN EUROPE
Italy

EASTERN EUROPE
Lithuania
Greece

MIDDLE EAST/ WESTERN ASIA
United Arab Emirates
Georgia

SOUTH EAST ASIA
Singapore

EASTERN ASIA
China
Korea
Taiwan

_DESCRIPTION

ATK103 - (aka: TA505). It is a significant part of the email threat landscape and is responsible for the largest malicious spam campaigns Proofpoint have ever observed, distributing instances of the Dridex banking trojan, Locky ransomware, Jaff ransomware, the Trick banking trojan, and several others in very high volumes. ATK103 use Necurs botnet to drive massive spam campaigns. ATK103 seems to be motivated by financial gains. It is hightly adaptable, often changes its malwares and techniques, uses off-the-shelf malwares and operates on a massive scale. It doesn't seem to be trying to stay stealthy. Since March 2018, ATK103 was observed using FlawedAmmyy RAT, a variant of the leaked AmmyyAdmin 3 (Remote Administration Tool). The use of these tools can make us think that this actor wants to switch from big spam campaigns to more targeted attacks. In July 2018, ATK103 has been seen using the SettingContent-ms files in their decoy documents. This technique has been described by Matt N. and in early June 2018, MSRC responded with a note that the severity of the issue is below the bar for servicing and that the case will be closed. Some of these malwares were signed with a COMODO SECURE certificate. ATK103 seems to be a Russian speaking group.

ATK103 (TA505) AS KEY PLAYER IN THE CYBERCRIME ECOSYSTEM

- As mentioned in ATK104's description, ATK103 has a more or less tenuous relationship with ATK104, as shown by the identical nature of certain functions developed in the Emotet and Trickbot download software (which is an adaptation of the original TrickBot malware created by ATK82 (Wizard Spider).
- However, this relationship is not limited to ATK104. We know that the ATK86 group (Silence group), which specializes in targeting large banks and their ATMs, and the ATK88 group (FIN6), which specializes in attacking points of sale and stealing credit card data, have already used the FlawdAmmyy remote administration tool developed by ATK103 (TA505).

_USED MALWARES

- Amadey
- Clop Ransomware
- FlawedAmmyy
- FlawedGrace
- Get2
- GlobeImposter
- MINEBRIDGE
- SDBbot
- ServHelper
- SnatchLoader
- TinyMet

_USED TOOLS

- Living off the Land
- Necurs
- TinyMet

_ATTACKS HAPPENED ON

> **TrickBot spread by Necurs Botnet adds Nordic Countries to its Targets**
Happened on: 2017-06-09

> **Locky campaign New invoice**
Happened on: 2017-08-28

> **Globeimposter Ransomware Campaign**
Happened on: 2017-11-30

> **TA505 targets the US retail industry with personalized attachments**
Happened on: 2018-12-06

> **New campaign of the Russian group TA505 directed to Chile and Argentina**
Happened on: 2019-04-22

> **Malicious documents spreading Ransomware**
Happened on: 2019-05-29

> **TA505 is Expanding its Operations**
Happened on: 2019-05-29

> **Breaking Down TA505 Groups Use of HTML and RATs**
Happened on: 2019-06-12

> **TA05 using new malware Gelup and Flowerpipi**
Happened on: 2019-07-04

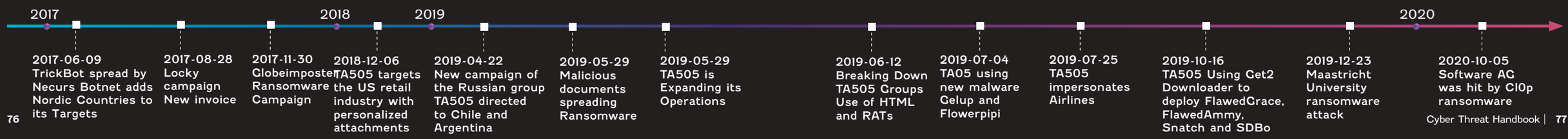
> **TA505 impersonates Airlines**
Happened on: 2019-07-25

> **TA505 Using Get2 Downloader to deploy FlawedGrace, FlawedAmmy, Snatch and SDBot**
Happened on: 2019-10-16

> **Maastricht University ransomware attack**
Happened on: 2019-12-23

> **October 5, 2020 - October 31, 2020 : Software AG was hit by Cl0p ransomware**
Happened on: 2020-10-05

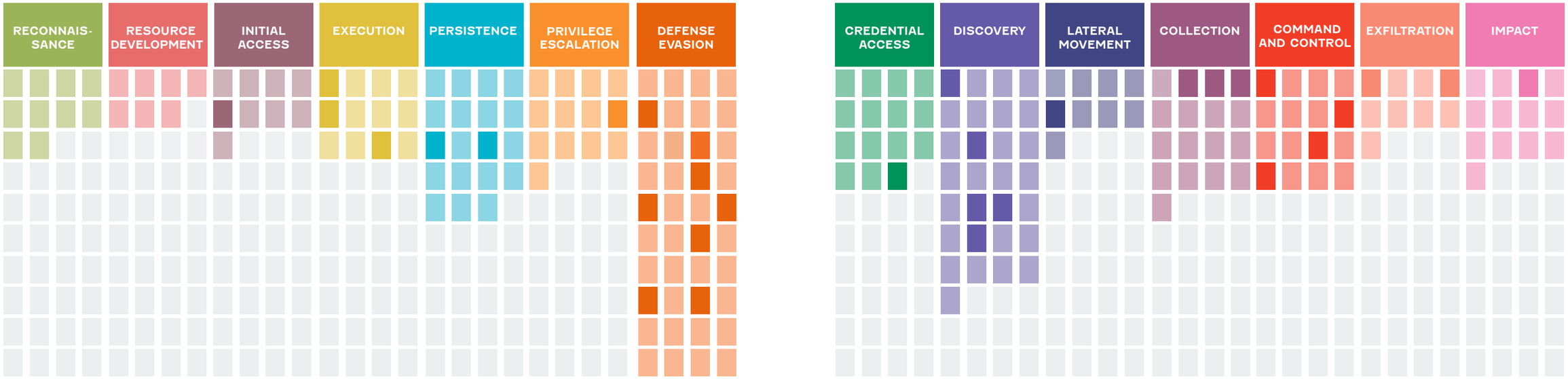
> **Explosive New MirrorBlast Campaign Targets Financial Companies**
The Morphisec Labs team tracked a MirrorBlast campaign that started in early September 2021. This campaign uses phishing emails as its entry point, containing malicious links leading to a malicious Excel document. This document has a near-0 detection rate on VirusTotal due to its lightweight and obfuscated macro.
Happened on: 2021-09



_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1012 - Query Registry
T1020 - Automated Exfiltration
T1021 - Remote Services
T1021.001 - Remote Desktop Protocol
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1041 - Exfiltration Over C2 Channel
T1571 - Non-Standart Port
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1087 - Account Discovery
T1090 - Proxy
T1105 - Ingress Tool Transfer
T1112 - Modify Registry
T1119 - Automated Collection
T1123 - Audio Capture
T1140 - Deobfuscate/Decode Files or Information
T1204 - User Execution
T1218 - Signed Binary Proxy Execution
T1218.011 - Rundll32
T1222 - File and Directory Permissions Modification
T1486 - Data Encrypted for Impact
T1546.011 - Application Shimming
T1552.001 - Credentials In Files
T1553.002 - Code Signing
T1559.002 - Dynamic Data Exchange
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link

_CYBER ATTACK PHASES



Threat Actor_

ATK104
(aka: Mummy Spider) is a criminal entity linked to the core development of the malware most commonly known as Emotet or Geodo.
_Type of attacker: Cyber Criminal

Alias_

_Mummy Spider
_Mealybug
_TA542

Targeted Sectors_

_Cyber-security

Motivations_

_Financial Gain

Targeted Areas_

Suspected origin of the attacker_

Ukraine

_DESCRIPTION

ATK104 - First observed in mid-2014, this malware shared code with the Bugat (aka Feodo) banking Trojan. However, Mummy Spider swiftly developed the malware capabilities to include an RSA key exchange for command and control communication and a modular architecture.
Mummy Spider does not follow typical criminal behavioral patterns. In particular, Mummy Spider usually conducts attacks for a few months before ceasing operations for a period of between three and 12 months, before returning with a new variant or version. After a 10 month hiatus, Mummy Spider returned Emotet to operation in December 2016 but the latest variant is not deploying a banking Trojan module with web injects, it is currently acting as a loader delivering other malware packages. The primary modules perform reconnaissance on victim machines, drop freeware tools for credential collection from web browsers and mail clients and a spam plugin for self-propagation. The malware is also issuing commands to download and execute other malware families such as the banking Trojans Dridex and Qakbot.
Mummy Spider advertised Emotet on underground forums until 2015, at which time it became private. Therefore, it is highly likely that Emotet is operated solely for use by Mummy Spider or with a small trusted group of customers.
The group is composed of competent personnel, and Emotet is regularly considered as one of the most threatening malware for businesses.
The group seems to have an interesting interaction with the ATK103 (TA505). TA505 is a financially motivated group that is active since 2014, seemingly of Russian origin. It is a significant part of the email threat landscape and is responsible of large malicious spam campaigns, mostly to distribute the Dridex and Trickbot banking trojan, the Locky and Jaff ransomwares, among others. TA505 use Necurs botnet to drive these campaigns. It is highly adaptable, often change its malwares and techniques, regularly use off-the-shelf malwares and operate on a massive scale.
Since March 2018, ATK103 was observed using FlawedAmmyy RAT, a variant of the leaked AmmyyAdmin 3 (Remote Administration Tool). The use of these tools can make us think that this actor is willing to switch from big spam campaigns to more targeted attacks.
First, TrickBot is probably the most distributed malware by Emotet, and has been distributed nearly every day since September 2018. The links were rather tenuous however, and TrickBot was just another malware dropped by Emotet until September 2019. In the beginning of June 2019, the group took a break until September 16, 2019. The group, as previously mentioned, came back with a new infrastructure zone (Epoch 3).
Since this day, every time that a TrickBot malware is deployed via Emotet (currently, nearly every day) its tag (an identifier that is added to every build of TrickBot) follows a specific pattern, while previous distribution tags were seemingly random. This hints to a bigger cooperation between the ATK103 group and Emotet. Moreover, on September 18, 2019 the group introduced a new loader. This loader, that is bigger, shares some code with the TrickBot loader.
This might mean that the group used the summer break they took to strengthen their relationships with ATK103. Indeed, deploying the group malware in a privileged way is one thing, but potentially sharing code is another.
On 27 January 2021 Europol announced that the infrastructure of the Emotet network had been neutralised through a multilateral police operation.

_USED MALWARES :

- Emotet

_ATTACKS HAPPENED ON

> **Emotet long-running campaigns**
Happened on: 2014-05-01

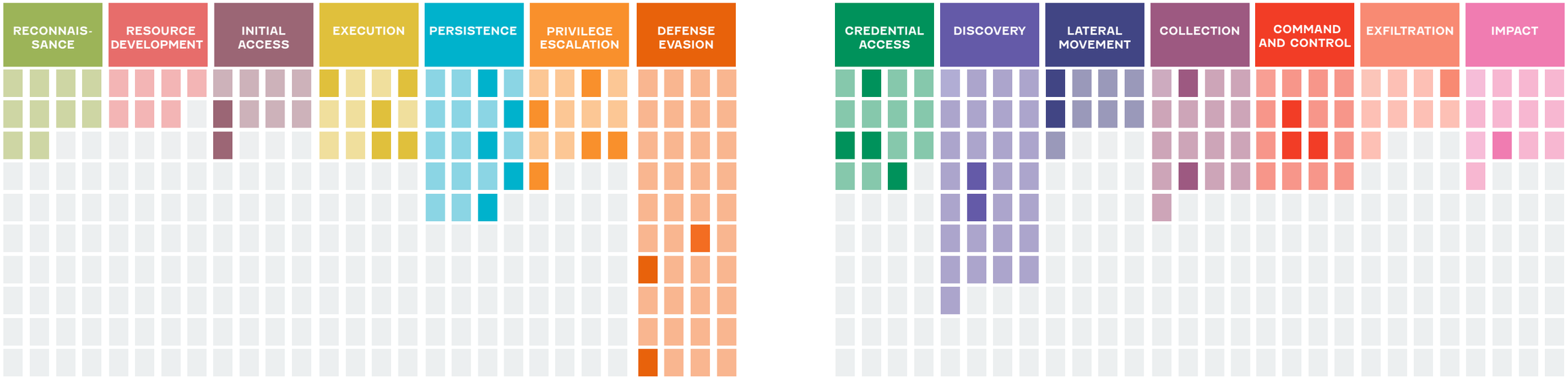
> **October 2019 - External SOCs used as lures by Emotet**
Happened on: 2019-10-14

> **2021 - Delta Variant Malspam Campaign**
Proofpoint researchers observed an increase in COVID-19 related threats since late June 2021. As TA542 first began using COVID-19 in email threats in January 2020, some of this activity might be related to this group.
Happened on: 2021-06

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1021.002 - SMB/Windows Admin Shares
T1027 - Obfuscated Files or Information
T1027.002 - Software Packing
T1040 - Network Sniffing
T1041 - Exfiltration Over C2 Channel
T1047 - Windows Management Instrumentation
T1053 - Scheduled Task/Job
T1055 - Process Injection
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1078 - Valid Accounts
T1095 - Non-Application Layer Protocol
T1110 - Brute Force
T1114 - Email Collection
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1210 - Exploitation of Remote Services
T1498 - Network Denial of Service
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1552.001 - Credentials In Files
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1571 - Non-Standard Port
T1573 - Encrypted Channel

_CYBER ATTACK PHASES



Threat Actor_

ATK11
(aka: Patchwork) is a cyber espionage group active since at least 2010. One of its specificity is the use of code copy-pasted from multiple online forums combined with high quality social engineering.
_Type of attacker: State Sponsored

Alias_

_APT-C-09
_Chinastrats
_Dropping Elephant
_Monsoon
_Operation Hangover
_Patchwork
_Quilted Tiger
_Sarit

Targeted Sectors_

_Software
_Public Services
_Political Organizations
_Pharmacy and drug manufacturing
_Non-governmental organizations
_Military
_Government and administration agencies
_Financial services
_Energy
_Embassies
_Aviation

Languages_

_ English

Motivations_

_Information theft
_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
United Kingdom Of Great Britain and Northern Ireland

MIDDLE EAST/ WESTERN ASIA
Israel

SOUTHERN ASIA
Sri Lanka
Pakistan
Bangladesh

EASTERN ASIA
Korea
Japan
China

Suspected origin of the attacker_

India

_DESCRIPTION

ATK11 - It started by the Operation Hangover which goal seemed to be the surveillance of targets of national security interests for India such as Pakistan or the Nagaland movement. This group was involved in the Monsoon campaign targeting multiple Indian neighbours in various sectors.
Patchwork used actuality/sector related themes in lure documents exploiting known vulnerabilities in Microsoft Office software send via email with links to websites customized for the intended target. The group is continuously adding new exploit in their arsenal.
Patchwork uses different web services as C2 channel like RSS feeds, Github, forums, blogs or dynamic DNS hosts. These channels can be difficult to detect in legitimate traffic.
Some RTF files used by this group were linked with C2 servers which were compromised and defanced by Cyber Gangsters which is an anti-Pakistan group. By following the alias Fortinet managed to get his identity in their article of April 2017. Nevertheless, Fortinet says if it is really linked to the Badnews malware or if it is a coincidence.
Multiple articles showed similarities between Patchwork behaviors and other Confucius, Bahamut, Donot Team or Bitter Apt, but there is no definitive conclusion as to whether these groups are the same or not.

_USED MALWARES

- Badnews
- Backconfig
- Enfourks
- NDiskMonitor
- QuasarRAT
- SocksBot
- Tinytyphon
- Taskhost Stealer
- Unkown Logger Public
- Wintel Stealer

_USED TOOLS

- BITSAdmin
- QuasarRAT
- schtasks

_USED VULNERABILITIES

- CVE-2012-0158
- CVE-2012-0422
- CVE-2012-1856
- CVE-2012-4792
- CVE-2014-1761
- CVE-2014-4114
- CVE-2014-6352
- CVE-2015-1641
- CVE-2015-2545
- CVE-2016-0034
- CVE-2016-4171
- CVE-2017-0199
- CVE-2017-0261
- CVE-2017-11882
- CVE-2017-12824
- CVE-2017-8570

_ATTACKS HAPPENED ON

> **2010: Operation Hangover**
Happened on: 2010-01-01

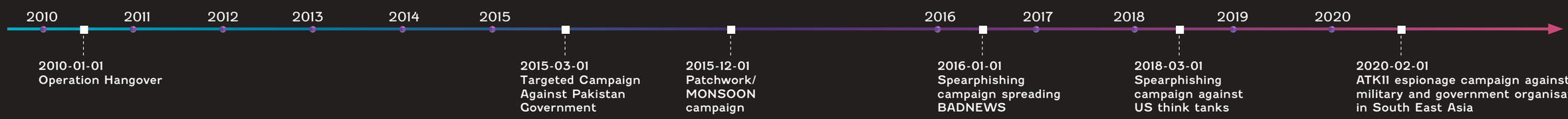
> **March - May 2015: Targeted Campaign Against Pakistan Government**
Happened on: 2015-03-01

> **December 2015 - July 2016: Patchwork/MONSOON campaign**
Happened on: 2015-12-01

> **2016 - 2017: Spearphishing campaign spreading BADNEWS**
Happened on: 2016-01-01

> **March - April 2018: Spearphishing campaign against US think tanks**
Happened on: 2018-03-01

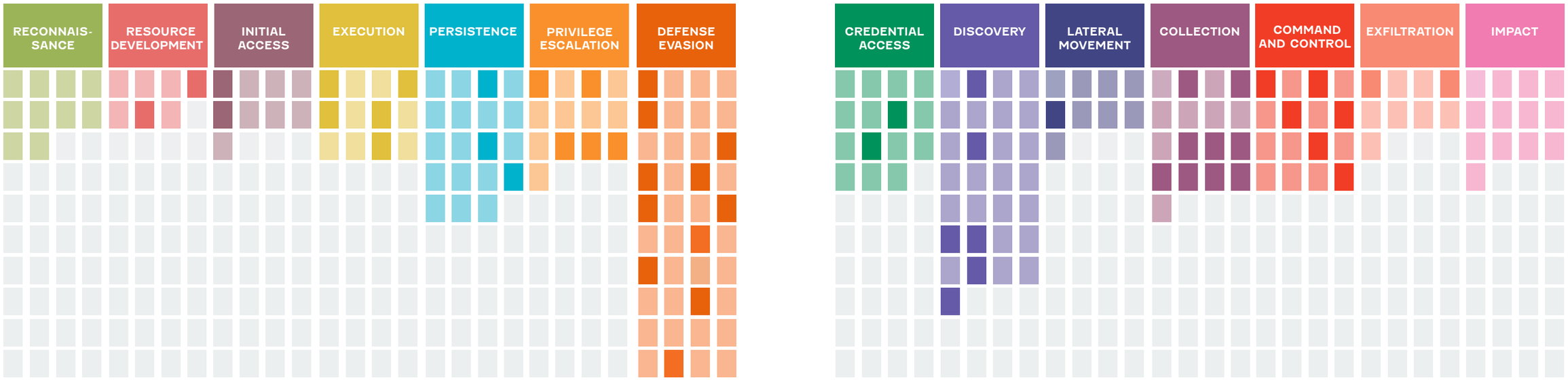
> **February - May 2020: ATK11 espionage campaign against military and government organisations in South East Asia**
Happened on: 2020-02-01



_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1005 - Data from Local System
T1010 - Application Window Discovery
T1020 - Automated Exfiltration
T1021.001 - Remote Desktop Protocol
T1025 - Data from Removable Media
T1027 - Obfuscated Files or Information
T1027.001 - Binary Padding
T1027.002 - Software Packing
T1027.005 - Indicator Removal from Tools
T1033 - System Owner/User Discovery
T1036 - Masquerading
T1039 - Data from Network Shared Drive
T1041 - Exfiltration Over C2 Channel
T1571 - Non-Standart Port
T1053 - Scheduled Task/Job
T1055.012 - Process Hollowing
T1056 - Input Capture
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1074 - Data Staged
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1102 - Web Service
T1105 - Ingress Tool Transfer
T1112 - Modify Registry
T1113 - Screen Capture
T1114 - Email Collection
T1119 - Automated Collection
T1132 - Data Encoding
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1497 - Virtualization/Sandbox Evasion
T1518.001 - Security Software Discovery
T1547.001 - Registry Run Keys / Startup Folder
T1548.002 - Bypass User Account Control
T1553.002 - Code Signing
T1559.002 - Dynamic Data Exchange
T1560 - Archive Collected Data
T1564.001 - Hidden Files and Directories
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1573 - Encrypted Channel
T1574.002 - DLL Side-Loading
T1587.001 - Malware
T1588.001 - Malware
T1588.002 - Tool

_CYBER ATTACK PHASES



Threat Actor_

ATK112
(aka: ZooPark by Kaspersky)
is a group that mostly uses
an Android Malware, “UnitMM”,
which saw multiple iterations.
_Type of attacker: State Sponsored

Alias_

_APT-C-38
_ZooPark

Targeted Sectors_

_Political Organizations
_Media
_International Organizations

Motivations_

_Information theft
_Espionage

Targeted Areas_

AFRICA
Morocco
Egypt

MIDDLE EAST/WESTERN ASIA
Lebanon
Kuwait
Jordan
Iraq
Iran

2015

2015-01-08
APT-C-38 targets Middle East since 2015

_DESCRIPTION

ATK112 - This group was first noticed in June 2015, and is still active to 2018.

The group mostly focuses on espionage, and has seen technical progresses since its debuts: While it first used forked commercial software in order to accomplish its deeds, the group extended it and brought it to a fully-fledged espionage platform.
According to 360 Beaconlab however, the group purchases its malicious software from a commercial development group, nicknamed “Apasec”.

Hackers mainly used waterhole attacks as infection vector, the experts discovered several news websites that have been compromised to redirect visitors to a downloading site that delivered the final malware.

The group deploys its tools through multiple main vectors: Telegram channels and watering holes.
Indeed, it regularly uses compromised websites in order to gain access its targets.

The group also started using an exclusive Windows malware, nicknamed “SpecialSaber”.

_USED MALWARES

- SpecialSaber
- UnitMM

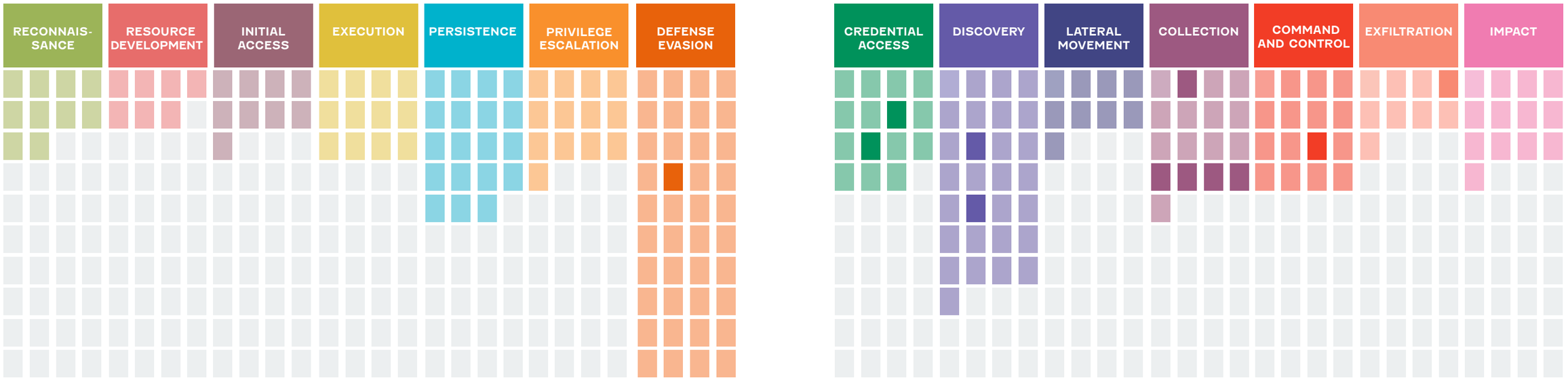
_ATTACKS HAPPENED ON

> **APT-C-38 targets Middle East since 2015**
Happened on: 2015-01-08

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1041 - Exfiltration Over C2 Channel
T1571 - Non-Standart Port
T1056 - Input Capture
T1057 - Process Discovery
T1074 - Data Staged
T1083 - File and Directory Discovery
T1113 - Screen Capture
T1114 - Email Collection
T1560 - Archive Collected Data
T1562.001 - Disable or Modify Tools

_CYBER ATTACK PHASES



Threat Actor_

ATK113
(aka: FIN8) is a financially motivated group targeting the retail, hospitality and entertainment industries.
_Type of attacker: Cyber Criminal

Alias_

_FIN8

Targeted Sectors_

_Retail
_Hospitality
_Healthcare
_Food and Agriculture
_Entertainment
_Banking

Motivations_

_Financial Gain

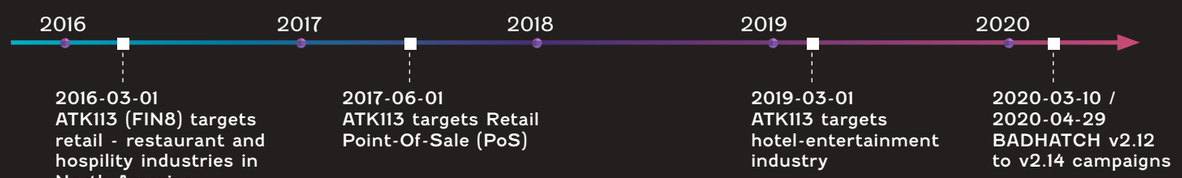
Targeted Areas_

NORTH AMERICA
United States Of America
Canada

SOUTH AMERICA
Panama

WESTERN EUROPE
Italy

AFRICA
South Africa



_DESCRIPTION

ATK113 - The actor had previously conducted several tailored spear-phishing campaigns using the downloader PUNCHBUGGY and POS malware PUNCHTRACK.

_USED MALWARES

- BADHATCH
- PUNCHBUGGY
- PUNCHTRACK
- PoSlurp
- Sardonic

_USED TOOLS

- Net
- dsquery

_USED VULNERABILITIES

- CVE-2016-0167

_ATTACKS HAPPENED ON

> **ATK113 (FIN8) targets retail - restaurant and hospility industries in North America**
Happened on: 2016-03-01

> **ATK113 targets Retail Point-Of-Sale (PoS)**
Happened on: 2017-06-01

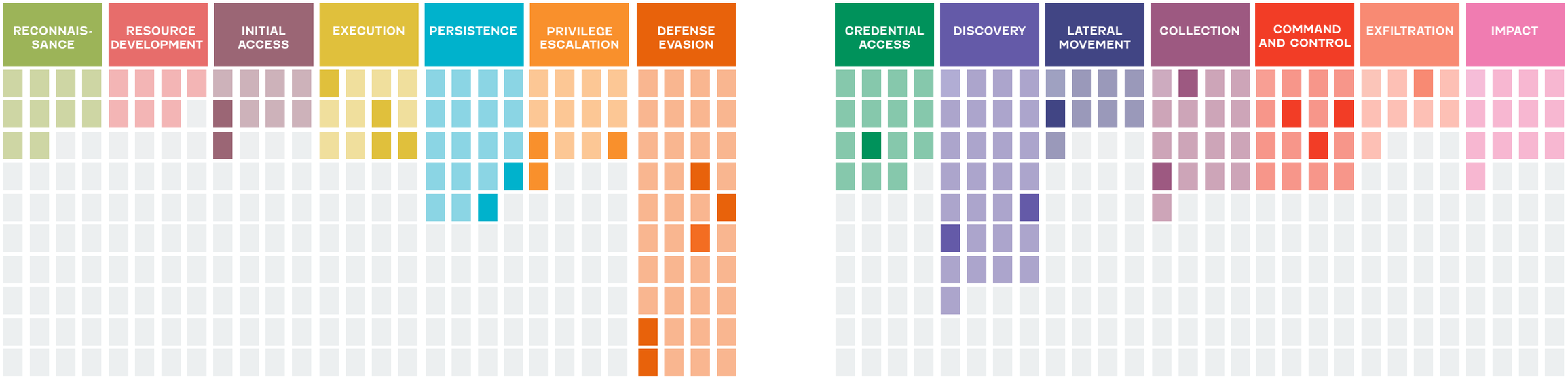
> **ATK113 targets hotel-entertainment industry**
Happened on: 2019-03-01

> **2020 - BADHATCH v2.12 to v2.14 campaigns**
The BitDefender team observed the evolution of the BADHATCH toolkit used by FIN8 between April 29 and March 10, tracking its evolution. The latest version, v2.14, was still in use at the time of the whitepaper publication.
Happened on: 2020-04-29

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1003.001 - LSASS Memory
T1018 - Remote System Discovery
T1021.001 - Remote Desktop Protocol
T1021.002 - SMB/Windows Admin Shares
T1027 - Obfuscated Files or Information
T1571 - Non-Standart Port
T1047 - Windows Management Instrumentation
T1048 - Exfiltration Over Alternative Protocol
T1048.003 - Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
T1053 - Scheduled Task/Job
T1053.005 - Scheduled Task
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1068 - Exploitation for Privilege Escalation
T1070 - Indicator Removal on Host
T1070.001 - Clear Windows Event Logs
T1070.004 - File Deletion
T1074 - Data Staged
T1074.002 - Remote Data Staging
T1078 - Valid Accounts
T1105 - Ingress Tool Transfer
T1112 - Modify Registry
T1204 - User Execution
T1204.001 - Malicious Link
T1204.002 - Malicious File
T1518.001 - Security Software Discovery
T1560 - Archive Collected Data
T1560.001 - Archive via Utility
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1573 - Encrypted Channel
T1573.002 - Asymmetric Cryptography

_CYBER ATTACK PHASES



Threat Actor_

ATK116
A cyber espionage group active since at least 2007, focusing on governmental agencies around the world.

Alias_

_Cloud Atlas
_Inception group

Targeted Sectors_

_Research
_Military
_Government and administration agencies
_Energy
_Aerospace

Languages_

_Russian

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
Italy
France
Belgium
United Kingdom Of Great Britain And Northern Ireland

EASTERN EUROPE
Ukraine
Slovenia
Belarus
Greece

AFRICA
Morocco
Uganda

MIDDLE EAST/ WESTERN ASIA
Azerbaijan
Armenia
Iran
Saudi Arabia
Turkey
United Arab Emirates
Iran

CENTRAL ASIA
Kazakhstan
Turkmenistan

SOUTHERN ASIA
India
Pakistan
Afghanistan

SOUTH EAST ASIA
Vietnam

RUSSIA
Russian Federation

_DESCRIPTION

ATK116 - This group is known for the Operation Red October targeting governmantal agencies (embassies), research, energy, aerospace and military in a wide range of countries, mostly in Russia, Western and Eastern Europe, Central Asia, South America and Africa. This group seems to have Russian-speaking origins.

This group used a large CnC network of infected machines and dozens of domain names working as a chain of proxies to hide the attacker's location. Cloud Atlas is able to target mobile devices, network equipment and removable disk drives increasing the quantity of sensitive data accessible. They use multiples exploits but not 0-days which can be interpreted as a lack of ressources.

Cloud Atlas created the Inception framework. A sophisticated framework able to launch multiple modules allowing the group to adapt to its target. This framework is still used in 2019.

After the Kaspersky disclosure in 2013, the group hid and then reappeared in 2014 with the Cloud Atlas malware. This behaviour will be repeated thereafter in 2014 after the publication of Symantec. The group improved its C2 infrastructure in 2014 by using cloud services which have the advantage of not being blacklisted and use encrypted communication protocols. They can also use compromised router as proxies to hide their origin.

According to DomainTools the ATK116 group (Inception, Cloud Atlas) was active in October-November 2020 in the conflict between Azerbaijan and Armenia in Nagorno-Karabakh with an espionage campaign based on the use of a decoy article entitled: Armenia transfers YPG/PKK terrorists to occupied area to train militias against Azerbaijan.

_USED MALWARES

- Inception framework
- POWERSHOWER
- VBShower

_USED VULNERABILITIES

- CVE-2009-3129
- CVE-2010-3333
- CVE-2011-3544
- CVE-2012-0158
- CVE-2012-1856
- CVE-2014-1761
- CVE-2017-11882
- CVE-2018-0802

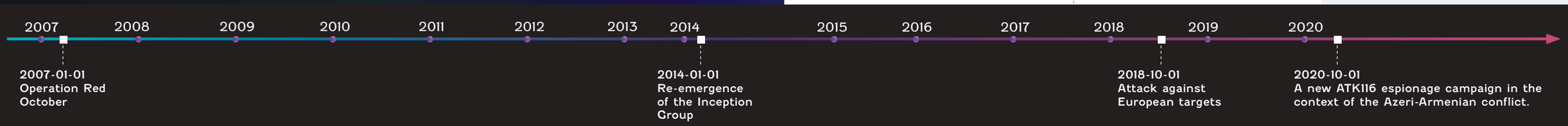
_ATTACKS HAPPENED ON

> **2007 - 2013: Operation Red October**
Happened on: 2007-01-01

> **2014 - 2017: Re-emergence of the Inception Group**
Happened on: 2014-01-01

> **October 2018: Attack against European targets**
Happened on: 2018-10-01

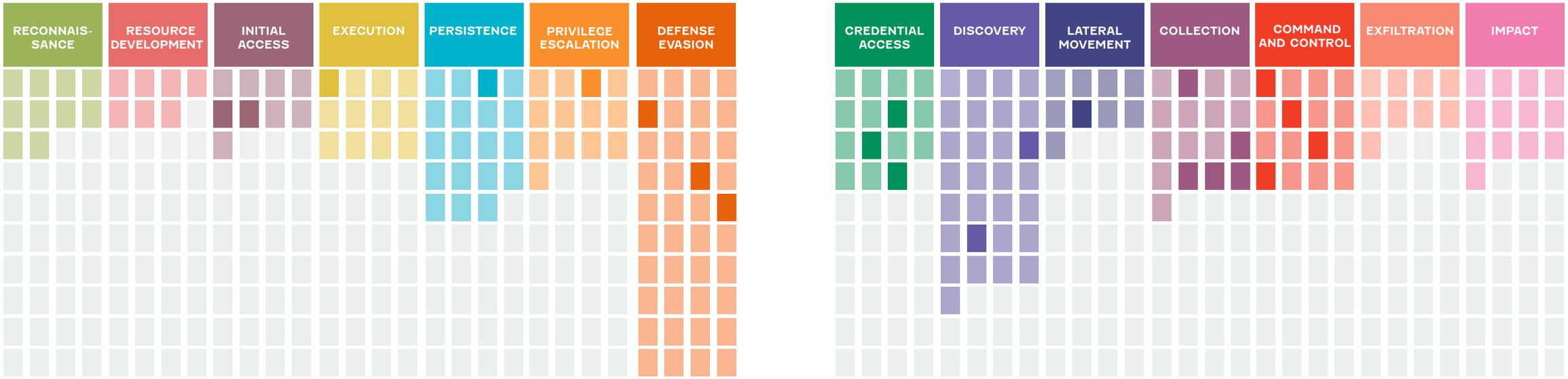
> **October 2020: A new espionage campaign in the context of the Azeri-Armenian conflict.**
Happened on: 2020-10-01



_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1025 - Data from Removable Media
T1046 - Network Service Scanning
T1056 - Input Capture
T1059.001 - PowerShell
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1082 - System Information Discovery
T1090.003 - Multi-hop Proxy
T1091 - Replication Through Removable Media
T1112 - Modify Registry
T1113 - Screen Capture
T1114 - mail Collection
T1140 - Deobfuscate/Decode Files or Information
T1547.001 - Registry Run Keys / Startup Folder
T1552.002 - Credentials in Registry
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1571 - Non-Standard Port
T1573 - Encrypted Channel

_CYBER ATTACK PHASES



Threat Actor_

ATK117

Apparently a North Korean state-sponsored cyberthreat actor with prerogatives similar to those of Unit 180 of the North Korean Army's General Reconnaissance Bureau.

_Type of attacker: State Sponsored

Alias_

_APT 38
_APT38
_Bluenoroff
_Stardust Chollima
_Subgroup: Bluenoroff

Targeted Sectors_

- Media
- Manufacturing
- Healthcare
- Financial Services
- Energy
- Aerospace

Motivations_

_Financial Gain

Targeted Areas_

NORTH AMERICA
United States Of America

CENTRAL AMERICA
Mexico

SOUTH AMERICA
Uruguay
Chile
Brazil

EASTERN EUROPE
Poland

MIDDLE EAST/ WESTERN ASIA
Turkey

SOUTHERN ASIA
Bangladesh

SOUTH EAST ASIA
Vietnam
Philippines
Malaysia

EASTERN ASIA
Taiwan

RUSSIA
Russian Federation

Suspected origin of the attacker_

North Korea

_DESCRIPTION

ATK117 - This North Korean state-sponsored cyberthreat actor has similar prerogatives to those of Unit 180 of the North Korean Army's General Reconnaissance Bureau. The Unit 180 is the North Korean Unit in charge of obtaining funds for the cyber activity and for the Noth Korean regime. This activity exists since at least 2014 and seems to have been increasing since North Korea has been subject to severe financial sanctions due to the development of new weapons. The economic pressure on Pyongyang leads the North Korean government to find new ways to obtain funding.

APT38 is a North Korean financially motivated threat group who developed multiple ways to steal money from the targeted attacks on banks and cryptocurrency exchanges to the spreading of ransomwares. This group seems to be learning about financial transaction in 2014 and developed a SWIFT malware in 2015. From 2014 to 2017 they mostly targeted organizations from Southeast Asia and expand to South America and Africa in mid-2016. They also targeted Europe and North America from October 2016 to October 2017.

APT38 has a complete arsenal of malwares and tools using defense evasion techniques and false flags (use of some poorly translated Russian language in some malwares, re-useage of known malwares). It is possible that these malwares were developed by another Unit (such as Unit 31), these techniques could be used by other North Korean groups. Despite this arsenal, APT38 uses Live-of-the-Land tools when it is possible. They put an effort into discovert the targeted environment and maintain access as long as possible while staying undetected unitil they reach their goal. FireEye estimates that they stay in a victim network approximately 155 days.
Since 2018 the group has gone from stealthy to noisy using the destructive KillDisk malware as a distraction tactic while they are targeting the SWIFT network to initiate malicious transactions.
We suspect the Unit 180 to be source of the WannaCry ransomware in 2017.
The report from the UN Security Council said that North Korea is carrying out "widespread and increasingly sophisticated" cyberattacks and estimates that North Korea has generated $2 billon.

_USED MALWARES

- DYEPACK
- DarkComet
- HERMES
- HOTWAX
- JspSpy
- KEYLIME
- KillDisk
- MAPMAKER
- NACHOCHEESE
- NESTEGG
- QUICKCAFE
- QUICKRIDE
- RATANKBAPOS
- RAWHIDE
- REDSHAWL
- SCRUBBRUSH
- SHADYCAT
- SLIMDOWN
- SMOOTHRIDE
- SORRYBRUTE
- WHITEOUT
- WORMHOLE
- WannaCry

_USED TOOLS

- Net
- Sysmon

_USED VULNERABILITIES

- CVE-2015-8651
- CVE-2016-1019
- CVE-2016-4119

_ATTACKS HAPPENED ON

> **February 2014: Attack of the Southeast Asian bank**
Happened on: 2014-02-01

> **December 2015: Attempted heist at TPBank**
Happened on: 2015-12-01

> **January 2016: Multiple international bank heist**
Happened on: 2016-01-01

> **February 2016: Bangladesh bank heist**
Happened on: 2016-02-01

> **October 2016: Watering hole attacks on government and media sites**
Happened on: 2016-10-01

> **May 2017: WannaCry**
Happened on: 2017-05-12

> **October 2017: Far Eastern International Bank heist**
Happened on: 2017-10-01

> **January 2018: Attempted heist at Bancomext**
Happened on: 2018-01-01

> **Arpil 2018: Attack on three Mexico banks**
Happened on: 2018-04-01

> **May 2018: Heist at Banco de Chile**
Happened on: 2018-05-01

> **June - August 2019: «Movie Coin» campaign focuses on Korean Bitcoin traders**
Happened on: 2019-06-01

>**TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies**
Happened on: 2022

2014
- 2014-02-01 Attack of the Southeast Asian bank

2015
- 2015-12-01 Attempted heist at TPBank

2016
- 2016-01-01 Multiple international bank heist
- 2016-02-01 Bangladesh bank heist
- 2016-10-01 Watering hole attacks on government and media sites

2017
- 2017-05-12 WannaCry
- 2017-10-01 Far Eastern International Bank heist

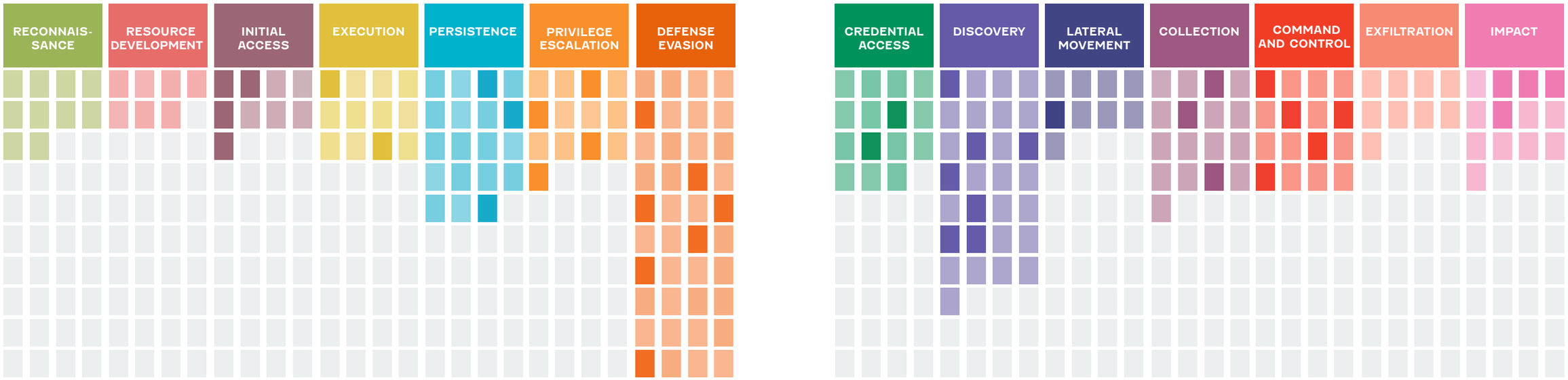
2018
- 2018-01-01 Attempted heist at Bancomext
- 2018-04-01 Attack on three Mexico banks
- 2018-05-01 Heist at Banco de Chile

2019
- 2019-06-01 Movie Coin» campaign focuses on Korean Bitcoin traders

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1021.001 - Remote Desktop Protocol
T1027 - Obfuscated Files or Information
T1027.002 - Software Packing
T1036 - Masquerading
T1046 - Network Service Scanning
T1055 - Process Injection
T1056 - Input Capture
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1070 - Indicator Removal on Host
T1070.004 - File Deletion
T1070.006 - Timestomp
T1071 - Application Layer Protocol
T1078 - Valid Accounts
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1087 - Account Discovery
T1090 - Proxy
T1105 - Ingress Tool Transfer
T1112 - Modify Registry
T1115 - Clipboard Data
T1123 - Audio Capture
T1135 - Network Share Discovery
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1190 - Exploit Public-Facing Application
T1204 - User Execution
T1485 - Data Destruction
T1486 - Data Encrypted for Impact
T1518.001 - Security Software Discovery
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1547.010 - Port Monitors
T1561.002 - Disk Structure Wipe
T1565.001 - Stored Data Manipulation
T1565.002 - Transmitted Data Manipulation
T1565.003 - Runtime Data Manipulation
T1566.001 - Spearphishing Attachment
T1571 - Non-Standard Port
T1573 - Encrypted Channel

_CYBER ATTACK PHASES



Threat Actor_

ATK120
(aka: Lyceum, Hexane)
This threat group targets organizations in sectors of strategic national importance, including oil and gas and possibly telecommunications.

Alias_

_Cobalt Lyceum
_HEXANE

Targeted Sectors_

_Energy

Motivations_

_Sabotage

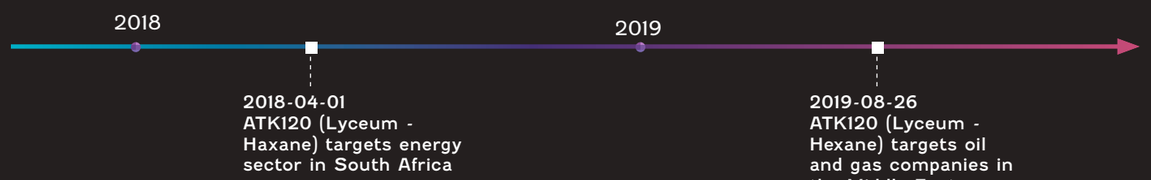
Targeted Areas_

AFRICA
South Africa

MIDDLE EAST/ WESTERN ASIA
Kuwait

Suspected origin of the attacker_

Unknown



_DESCRIPTION

ATK120 - LYCEUM may have been active as early as April 2018. Domain registrations suggest that a campaign in mid 2018 focused on South African targets has been conducted by ATK120. In May 2019, the threat group launched a campaign against oil and gas organizations in the Middle East. This campaign followed a sharp uptick in development and testing of their toolkit against a public multi-vendor malware scanning service in February 2019. Its target core is very similar to that of the APT Xenotime (ATK91), and some similarities can be found with Magnallium and Chrysene. No definitive links can be established.

_USED MALWARES

- DanBot
- DanDrop

_USED TOOLS

- Decrypt-RDCMan.ps1
- Get-LAPSP.ps1
- kl.ps1

_ATTACKS HAPPENED ON

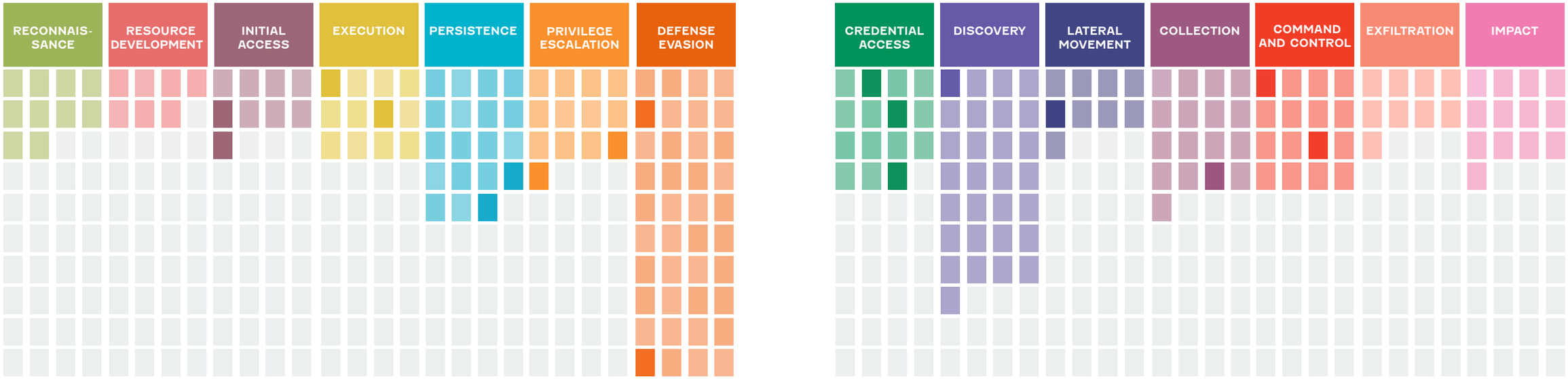
> **ATK120 (Lyceum - Haxane) targets energy sector in South Africa**
Happened on: 2018-04-01

> **ATK120 (Lyceum - Hexane) targets oil and gas companies in the Middle East.**
Happened on: 2019-08-26

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1021.001 - Remote Desktop Protocol
T1571 - Non-Standart Port
T1053 - Scheduled Task/Job
T1056 - Input Capture
T1059.001 - PowerShell
T1071 - Application Layer Protocol
T1078 - Valid Accounts
T1087 - Account Discovery
T1110 - Brute Force
T1140 - Deobfuscate/Decode Files or Information
T1552.001 - Credentials In Files
T1566.001 - Spearphishing Attachment

_CYBER ATTACK PHASES



Threat Actor_

ATK128
(aka: OurMine) is a hacking group active since mid 2016 that has been identified for being from Saudi Arabia.

_Type of attacker: Hacktivist, Cyber Criminal

Alias_

_OurMine

Targeted Sectors_

_High-Tech
_Communication
_Casino & Gaming

Languages_

_English

Motivations_

_Revenge
_Personal Satisfaction
_Financial Gain
_Dominance
_Coercion

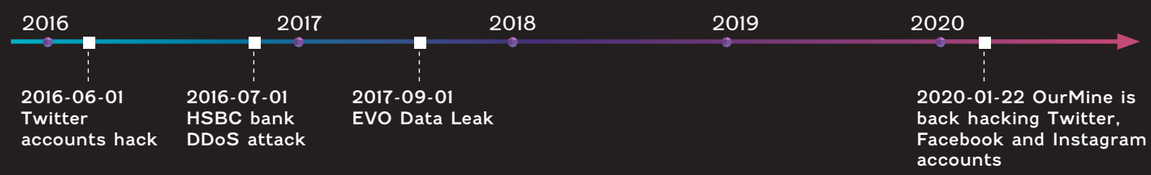
Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland

Suspected origin of the attacker_

Saudi Arabia



_DESCRIPTION

ATK128 is mostly known for taking over Twitter accounts of high ranked personnel such as CEOs of large cooperations and more, and Twitter accounts of organizations themselves. In most cases they claimed that they took over the account to show its owner its low level of security, while requesting them to contact the group directly to solve this problem. This shows that the group presents itself as a kind of a grey-hat group who looks for vulnerabilities and security issues in order to receive money from the companies in which these issues were found. This was also the case with the two DDoS attacks they launched against HSBC bank and Pokemon Go (in 2016 and 2017 respectively), allegedly to enhance the level of security of those companies. However, even though OurMine tried to show themselves as a group that enhances cyber security of companies, some of their attacks were done as a revenge. For example, they took over a media website after publishing an article that allegedly revealed the real identity of the threat actor behind the group, a teen from Saudi Arabia. Another example was when they leaked information of a company that did not contact them about security issues they found in its servers. Furthermore, in some cases they tried to brag about their capabilities when they were challenged to hack the website of WikiLeaks in 2017. Overall, the group did not launch very sophisticated attacks, and all the attacks were detected very quickly. Of note, since mid 2017, the group is not active, and their website seems to be under maintenance.

On January 22, 2020, the group started to target social medias account (Twitter, Facebook, Instagram) which combined have tens of millions of followers. they published the message “Hi, we’re OurMine group. We are here for 2 things: 1) Announce that we are back 2) Show people that everything is hackable. To improve your accounts security contact us: contact@ourmine.org”.

_ATTACKS HAPPENED ON

> **June-2016 Twitter accounts hack**
Happened on: 2016-06-01

> **July 2016 HSBC bank DDoS attack**
Happened on: 2016-07-01

> **August 2016 - Jimmy Wales Twitter account hack**
Happened on: 2016-08-01

> **October 2016 BuzzFeed hack**
Happened on: 2016-10-01

> **21 December 2016 - NFL, Netflix and Marvel’s Twitter accounts hack**
Happened on: 2016-12-21

> **July 2017 - Pokemon Go DDoS attack**
Happened on: 2017-07-01

> **July 2017 - TechCrunch Hack**
Happened on: 2017-07-01

> **August 2017 - WikiLeaks Hack**
Happened on: 2017-08-01

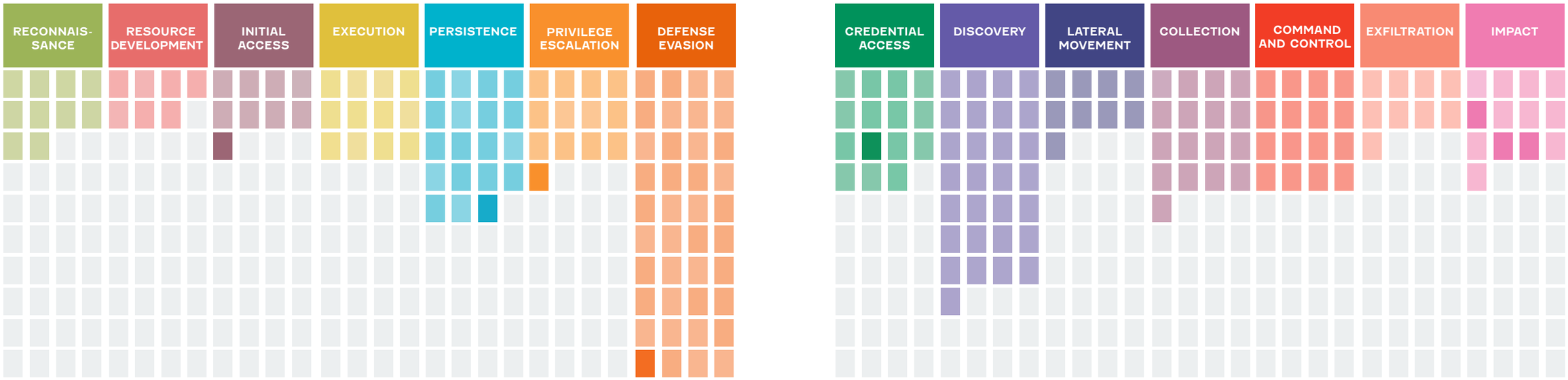
> **August 2017 - Game of Thrones Twitter account hack**
Happened on: 2017-08-01
September 2017 VEVO Data Leak
Happened on: 2017-09-01

> **January 2020 - OurMine is back hacking Twitter, Facebook and Instagram accounts**
Happened on: 2020-01-22

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1078 - Valid Accounts
T1491 - Defacement
T1496 - Resource Hijacking
T1498 - Network Denial of Service

_CYBER ATTACK PHASES



Threat Actor_

ATK13
(aka: Turla, Uroburos, Waterbug, Venomous Bear) is a cyber espionage threat actor active since at least 2008, when it breached the US Department of Defense.
_Type of attacker: State Sponsored

Alias_

_Group 88
_Hippo Team
_Iron Hunter
_KRYPTON
_MAKERSMARK
_Pacifier APT
_Pfinet
_Popeye
_SIG23
_Snake
_TAG_0530
_Turla
_Turla Group
_Turla Team
_Uroburos
_VENOMOUS Bear
_WRAITH
_Waterbug
_WhiteBear

Targeted Sectors_

_Research
_Political Organizations
_Military
_International Organizations
_High-Tech
_Government and administration agencies
_Education
_Defence
_Aerospace

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

NORTHERN EUROPE
Finland
Netherlands

WESTERN EUROPE
Italy
France
Belgium
United Kingdom Of Great Britain And Northern Ireland
Germany

EASTERN EUROPE
Poland
Romania
Belarus

MIDDLE EAST/ WESTERN ASIA
Saudi Arabia
Jordan
Iran
Iraq

CENTRAL ASIA
Uzbekistan
Tajikistan
Kazakhstan

SOUTHERN ASIA
India

RUSSIA
Russian Federation

Suspected origin of the attacker_

Russia

_DESCRIPTION

ATK13 is a Russian-speaking group widely believed to be a Russian state-sponsored organization.

In 2015, Kaspersky described ATK13 as one of the "several elite APT groups that have been using — and abusing — satellite links to manage their operations — most often, their Command & Control (C&C) infrastructure". Indeed, while APT C&C servers are regularly taken down by authorities, satellite connections hides the exact location of the servers. Satellite-based Internet receivers can be located anywhere within the area covered by a satellite, and this is generally quite large. To do that, the attacker needs to pay an expensive connections (full duplex satellite links can be very expensive: a simple duplex 1Mbit up/down satellite link may cost up to $7000 per week) or hijack the network traffic between the victim and the satellite operator that requires either exploitation of the satellite provider itself, or of another ISP on the way. The oldest sample found by Kaspersky that used a satellite connections has been compiled in November 2007.

During 2018 and 2019, ATK13 continued to target governments and international organizations in multiple waves of attacks and continued to improve its tools. The most recent attack targeted an Iranian APT group called OilRig.

Turla's attack on one of Iran's most successful groups combines opportunism and international interests. It should be recalled that since 2014 and the annexation of the Crimea, Western pressures and the fall of the oil price have plunged Russia into recession. For this reason, Russia has moved closer to Saudi Arabia, whose alliance with the United States had weakened under the Obama era in the alder of the Iranian nuclear agreement, supported by the former US President. It seems that the change in American diplomatic line since the election of Donald Trump has not diverted Saudi Arabia from this alliance. This rapprochement of interests is denounced by Iran, most recently at the OPEC meeting in Vienna in July 2019. The reason for the tension is also economic as both countries are positioning themselves to address the European gas market.

_USED MALWARES

- Agent.btz
- Carbon
- ComRAT
- Crutch
- Epic
- Gazer
- Kazuar
- KopiLuwak
- Mimikatz
- Mosquito
- Neptun
- Tinyturla
- Turla Outlook backdoor
- Uroburos

_USED TOOLS

- Arp
- Empire
- Living off the Land
- Meterpreter
- Mimikatz
- Net
- Reg
- Systeminfo
- Tasklist
- gpresult
- nbtstat
- netstat

_USED VULNERABILITIES

- CVE-2009-3129
- CVE-2012-1723
- CVE-2012-4681
- CVE-2013-2729
- CVE-2013-3346
- CVE-2013-5065

_ATTACKS HAPPENED ON

> **2005 - 2014 : The Snake campaign**
Happened on: 2005-01-01

> **November 2008: Cyber-attack on US Defense Department computers**
Happened on: 2008-11-21

> **Turla has targeted government institutions - military - education - research and pharmaceutical companies in more than 45 countries**
Happened on: 2011-01-08

> **Governments and Defense contractors compromised**
Happened on: 2013-01-08

> **Turla attacks a Swiss company**
Happened on: 2014-01-08

> **Turla conducted a watering hole campaigns by targeting embassy websites**
Happened on: 2014-01-08

> **Turla used a designed Adobe Flash fake installer and used a web app hosted on Google Apps Script as a CnC server**
Happened on: 2018-01-08

> **Turla attacked OilRig**
Happened on: 2018-01-08

> **2021 since 2020 - ATK13's new discreet but effective malware - TinyTurla**
Happened on: 2020-03-28

> **2020 — Attacks on Armenian websites**
Happened on: 2021-09-13

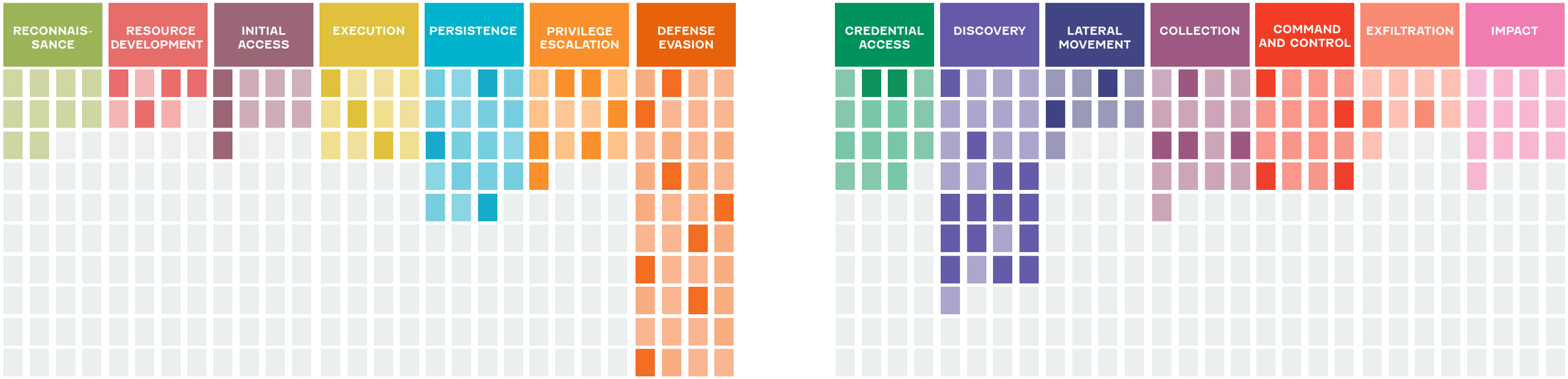
2005 2006 2007 2008 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021

2005-01-01 The Snake campaign
2008-11-21 Cyber-attack on US Defense Department computers
2011-01-08 Turla has targeted government institutions - military - education - research and pharmaceutical companies in more than 45 countries
2013-01-08 Governments and Defense contractors compromised
2014-01-08 Turla attacks a Swiss company
2014-01-08 Turla conducted a watering hole campaigns by targeting embassy websites
2018-01-08 Turla used a designed Adobe Flash fake installer and used a web app hosted on Google Apps Script as a CnC server
2018-01-08 Turla attacked OilRig
2020-03-28 2021 since 2020 - ATK13's new discreet but effective malware - TinyTurla
2021-09-13 Attacks on Armenian websites

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1005 - Data from Local System
T1007 - System Service Discovery
T1011 - Exfiltration Over Other Network Medium
T1012 - Query Registry
T1016 - System Network Configuration Discovery
T1016.001 - Internet Connection Discovery
T1018 - Remote System Discovery
T1021.002 - SMB/Windows Admin Shares
T1025 - Data from Removable Media
T1027 - Obfuscated Files or Information
T1027.005 - Indicator Removal from Tools
T1049 - System Network Connections Discovery
T1055 - Process Injection
T1055.001 - Dynamic-link Library Injection
T1057 - Process Discovery
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1059.005 - Visual Basic
T1059.006 - Python
T1059.007 - JavaScript
T1068 - Exploitation for Privilege Escalation
T1069.001 - Local Groups
T1069.002 - Domain Groups
T1071 - Application Layer Protocol
T1071.001 - Web Protocols
T1071.003 - Mail Protocols
T1078.003 - Local Accounts
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1087.001 - Local Account
T1087.002 - Domain Account
T1090 - Proxy
T1102 - Web Service
T1102.002 - Bidirectional Communication
T1105 - Ingress Tool Transfer
T1106 - Native API
T1110 - Brute Force
T1112 - Modify Registry
T1120 - Peripheral Device Discovery
T1124 - System Time Discovery
T1134.002 - Create Process with Token
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1201 - Password Policy Discovery
T1204 - User Execution
T1204.001 - Malicious Link
T1213 - Data from Information Repositories
T1518.001 - Security Software Discovery
T1546.003 - Windows Management Instrumentation Event Subscription
T1546.013 - PowerShell Profile
T1547.001 - Registry Run Keys / Startup Folder
T1547.004 - Winlogon Helper DLL
T1553.006 - Code Signing Policy Modification
T1555.004 - Windows Credential Manager
T1560.001 - Archive via Utility
T1562.001 - Disable or Modify Tools
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1567.002 - Exfiltration to Cloud Storage
T1570 - Lateral Tool Transfer
T1583.006 - Web Services
T1584.003 - Virtual Private Server
T1584.004 - Server
T1584.006 - Web Services
T1587.001 - Malware
T1588.001 - Malware
T1588.002 - Tool

_CYBER ATTACK PHASES



Threat Actor_

ATK132
(aka Syrian Electronic Army) is a hacking group active since the beginning of the Syrian Civil War in 2011.
_Type of attacker: Cyber Terrorist

Alias_

_Deadeye Jackal
_SEA
_Syria Malware Team
_Syrian Electronic Army

Targeted Sectors_

_Retail
_Political Organizations
_Military
_Media
_High-Tech
_Government and administration agencies
_Defence
_Communication

Languages_

_English
_Arabic

Motivations_

_Revenge
_Organizational Gain
_Notoriety
_Ideology
_Dominance
_Coercion

Targeted Areas_

NORTH AMERICA
United States Of America
Canada

WESTERN EUROPE
France
United Kingdom Of Great Britain And Northern Ireland

Suspected origin of the attacker_

Syria

_DESCRIPTION

ATK132 - (aka: Syrian Electronic Army) is a hacking group active since the beginning of the Syrian Civil War in 2011. The group supports the current regime of Bashar Al-Assad, and according to several reports, it is actually part of it. In the hight of the civil war, the group launched many cyber-attacks, usually against online platforms of media outlets, in order to deface them and spread their pro-Syrian regime agenda. The attacks and defacements were not just against the official websites of the media outlets, but also against their social media accounts and even their registrar. In addtion, the group is known to use different types of malware, usually against groups and individuals that oppose Al-Assad's regime. These malware are of various types and usually have advanced capabilities. In addtion, they usually used spear-phishing as their attack vector, but also other techniques such as watering holes. All of this indicates on the high professional level of its members and their capabilities. Their attacks were occasionally launched by affiliated groups and hackers of the SEA, such as Syrian Malware team, who share infrastructure and personnel with the SEA. Of note, in recent years, cyber-attacks affiliated with the group have become more and more rare.
In October 2021, Facebook's threat disruption team took action against hackers in Pakistan and Syria. They specifically removed 3 Syrian hackers networks from the platform, namely the SEA (APT-C-27, aka. ATK132), APT-C-37 (aka. ATK85) and a government-backed group that targeted minority groups, activists, opposition, Kurdish journalists, activists, members of the People's Protection Units (YPG), Syria Civil Defense and the White Helmets. Note: SEA's activity was linked by Facebook to Syria's Air Force Intelligence in their latest campaign.

According to 360 Core Security, the group features two distinct branches, tracked as Golden Rat (ATK80) and Pat Bear (ATK85).

_USED MALWARES

- SilverHawk

_ATTACKS HAPPENED ON

> **July 2013 - Tango and Viber attack**
Happened on: 2013-07-01

> **End of 2013 - 2015 - Phishing attacks against the Syrian opposition**
Happened on: 2013-11-01

> **February 2014 - Changing Facebook's WHOIS information**
Happened on: 2014-02-01

> **April 2014 - Reuters attack**
Happened on: 2014-04-01

> **July 2014 - BlackWorm campaign**
Happened on: 2014-07-01

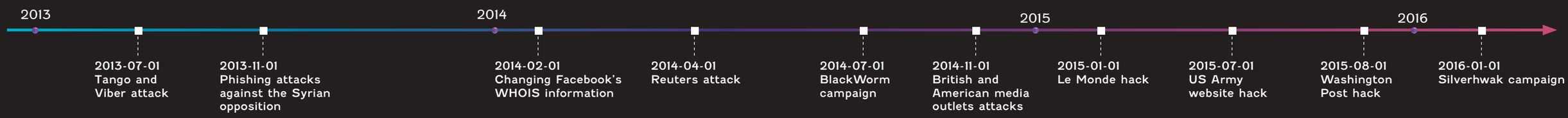
> **November 2014 - British and American media outlets attacks**
Happened on: 2014-11-01

> **January 2015 - Le Monde hack**
Happened on: 2015-01-01

> **July 2015 US Army website hack**
Happened on: 2015-07-01

> **August 2015 - Washington Post hack**
Happened on: 2015-08-01

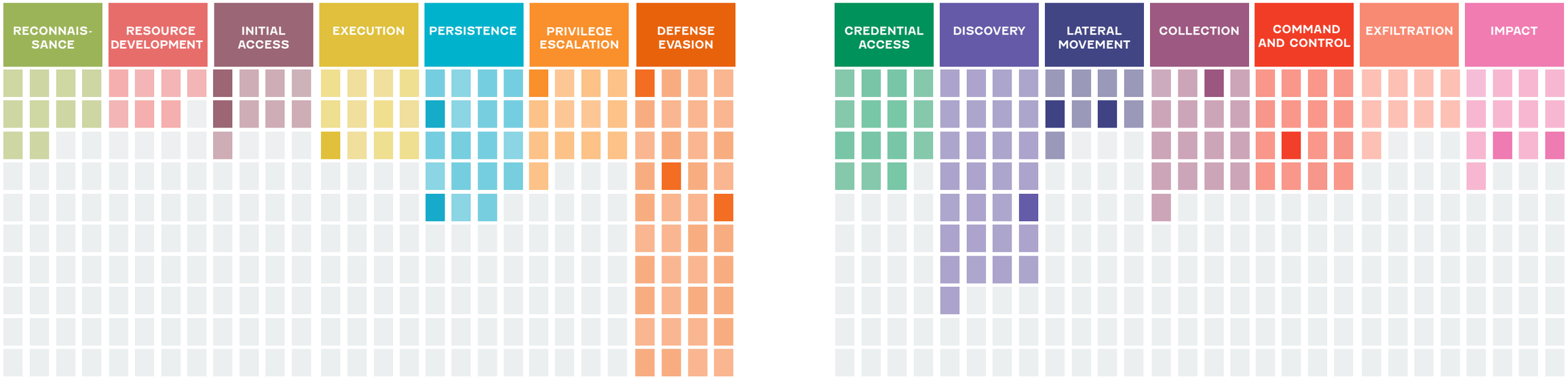
> **2016 - 2018 Silverhwak campaign**
Happened on: 2016-01-01



_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1018 - Remote System Discovery
T1021 - Remote Services
T1072 - Software Deployment Tools
T1095 - Non-Application Layer Protocol
T1112 - Modify Registry
T1123 - Audio Capture
T1176 - Browser Extensions
T1189 - Drive-by Compromise
T1489 - Service Stop
T1498 - Network Denial of Service
T1505.003 - Web Shell
T1548.002 - Bypass User Account Control
T1562.001 - Disable ora Modify Tools
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link

_CYBER ATTACK PHASES



Threat Actor_

ATK133

Member of the United Cyber Caliphate (UCC) or Islamic State Hacking Division, the name of an umbrella for several hacking groups working for the Islamic State of Iraq and Levant (ISIS or ISIL) terrorist organization.

_Type of attacker: Cyber Terrorist

Alias_

_UCC
_United Cyber Caliphate

Targeted Sectors_

_Political Organizations
_Naval
_Military
_Media
_Government and administration agencies
_Education
_Defence
_Aviation

Languages_

_English
_Arabic

Motivations_

_Revenge
_Organizational Gain
_Notoriety

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
France
United Kingdom Of Great Britain And Northern Ireland

AFRICA
Egypt

SOUTH EAST ASIA
Malaysia

OCEANIA
Australia

Suspected origin of the attacker_

Worldwide

_DESCRIPTION

ATK133 - The organization emerged in April 2016. Mostly known for its campaign against US military and governmental personal.

On April 4, 2016, the Cyber Caliphate Army (CCA), the principal ISIS hacking unit, and other pro-ISIS groups like the Sons Caliphate Army (SCA) and Kalacnikov. TN (KTN) merged and formed The United Cyber Caliphate (UCC). UCC groups include the: - Cyber Caliphate, or Cyber Caliphate Army (CCA) was established shortly after the establishment of the Islamic State. The Key person behind the group was Junaid Hussain (Abu Hussain al Britani), or TriCK.

The most important cyber-terrorist attack of the CCA occurred on January 2015 when the Twitter and YouTube accounts of U.S Central Command and later on the Twitter accounts of the magazine Newsweek were hacked. The Sons Caliphate Army (SCA) was established in 2016, as a sub group of Cyber Caliphate.

Mostly known for disrupting social media traffic on Facebook and Twitter. SCA Claimed to have hacked 10,000 Facebook accounts, more than 150 Facebook groups and over 5,000 Twitter profiles. Kalashnikov E-Security Team was established in 2016. This group is focused on tech security advisory for ISIS Jihadists. It also uploaded ISIS-related jihadi literature, sharing posts from cyber jihadi groups, reporting successful attacks on websites and Facebook pages and publishing various web-hacking techniques. Gradually, the hackers started to conduct or assist in defacing hacks.
Although we have not seen any attacks by this group for almost two years, it is worth noting that members of the group may have reoriented themselves to new operations in other terrorist groups following the movements of ISIS.

_USED TOOLS

- Ancalog Exploit Builder
- Caliphate Cannon
- Multy BruteForce Facebook
- Telegram
- WhatsApp

_ATTACKS HAPPENED ON

> **January 2015 The Albuquerque Journal and Maryland's WBOC Hacking**
Happened on: 2015-01-01

> **January 2015 - Malaysia Airlines Website Attack**
Happened on: 2015-01-01

> **February 2015 - Newsweek magazine Twitter account hijacked**
Happened on: 2015-02-01

> **September 2015 - UK Government Email Hacking**
Happened on: 2015-09-01

> **April 2016 - Australian Websites Hacking**
Happened on: 2016-04-01

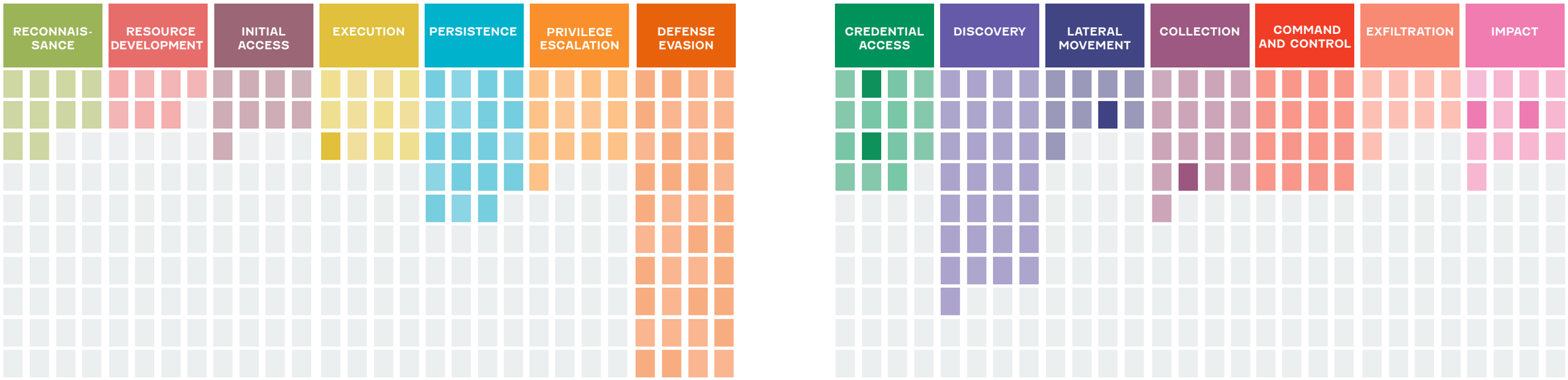
> **April 2017 - 8K Kill List Release**
Happened on: 2017-04-01

> **October 2018 - ISIS Launch Cracking Software**
Happened on : 2018-10-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1072 - Software Deployment Tools
T1110 - Brute Force
T1114 - Email Collection
T1491 - Defacement
T1499 - Endpoint Denial of Service

_CYBER ATTACK PHASES



Threat Actor_

ATK14
(aka: BlackEnergy, Sandworm) is an attacker group of Russian origins, active since at least 2008.

Alias_

_Black Energy
_BlackEnergy
_ELECTRUM
_GreyEnergy
_Iron Viking
_Quedagh
_Sandworm
_Sandworm Team
_TEMP.Noble
_TeleBots
_Voodoo Bear

Targeted Sectors_

_Transportation
_Media
_Government and administration agencies
_Energy

Motivations_

_Sabotage
_Espionage

Targeted Areas_

WESTERN EUROPE
France

EASTERN EUROPE
Estonia
Ukraine
Poland

MIDDLE EAST/ WESTERN ASIA
Georgia

RUSSIA
Russian Federation

Suspected origin of the attacker_

Russia

_DESCRIPTION

ATK14 - (aka BlackEnergy, Sandworm) is a group of attackers of Russian origin, active since at least 2008. This attacker is extremely active and skilled, and is well known for the BlackEnergy campaign as well as the NotPetya campaign. This group appears to correspond to unit 74455 (Main Center for Special Technologies).
In early 2022, the group appears to be responsible for the attack attempt against a Ukrainian energy provider using Industroyer2.

ORIGINS OF THE GROUP
The malware BlackEnergy is a malware, allegedly created in 2006-2007. This malware was used to launch DDoS attacks against machines. It was used against Georgia and Estonia in large campaigns, taking down governmental and banking websites. The attacker reportedly sold the source code for $700. Several actors did use this malware, continuing DDoS attacks against Georgia. Around 2014, a group created SCADA and ICS plugins for BlackEnergy, in order to target manufacturing and the energy sector worldwide. This is the group named ATK14.

_ORIGINS OF THE GROUP

The malware BlackEnergy is a malware, allegedly created in 2006-2007. This malware was used to launch DDoS attacks against machines. It was used against Georgia and Estonia in large campaigns, taking down governmental and banking websites. The attacker reportedly sold the source code for $700. Several actors did use this malware, continuing DDoS attacks against Georgia. Around 2014, a group created SCADA and ICS plugins for BlackEnergy, in order to target manufacturing and the energy sector worldwide. This is the group named ATK14.

_USED MALWARES

- BCS-Server
- BlackEnergy
- GCat
- GreyEnergy
- Mimikatz
- Potao
- Telebot
- WSO
- c99shell

_USED TOOLS

- 3proxy
- Dante
- Dropbear SSH
- Living off the Land
- Nmap
- Plink
- PsExec

_USED VULNERABILITIES

- CVE-2010-3333
- CVE-2014-1761
- CVE-2017-0143
- CVE-2017-0144
- CVE-2017-0146
- CVE-2017-0147

_ATTACKS HAPPENED ON

> **2011 - 2015 Operation Potao**
Happened on: 2011-01-01

> **2013 - 2014: BlackEnergy Lite**
Happened on: 2013-01-01

> **2015: Evolution of BlackEnergy - KillDisk**
Happened on: 2015-01-01

> **December 2015: Power outage in Ukraine**
Happened on: 2015-12-23

> **2016: Continuing interest in energy and renewal of the group arsenal**
Happened on: 2016-01-01

> **December 2016: Second attack against Ukraine power grid**
Happened on: 2016-12-17

> **June 2017: NotPetya outbreak**
Happened on: 2017-06-27

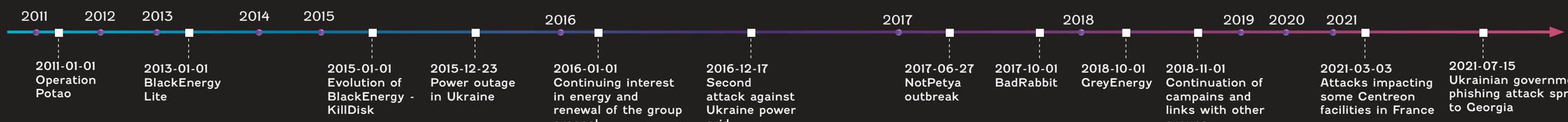
> **October 2017: BadRabbit**
Happened on: 2017-10-01

> **October 2018: GreyEnergy**
Happened on: 2018-10-01

> **2018 - 2019: Continuation of campains and links with other groups**
Happened on: 2018-11-01

> **2021 March - Attacks impacting some Centreon facilities in France**
Happened on: 2021-03-03

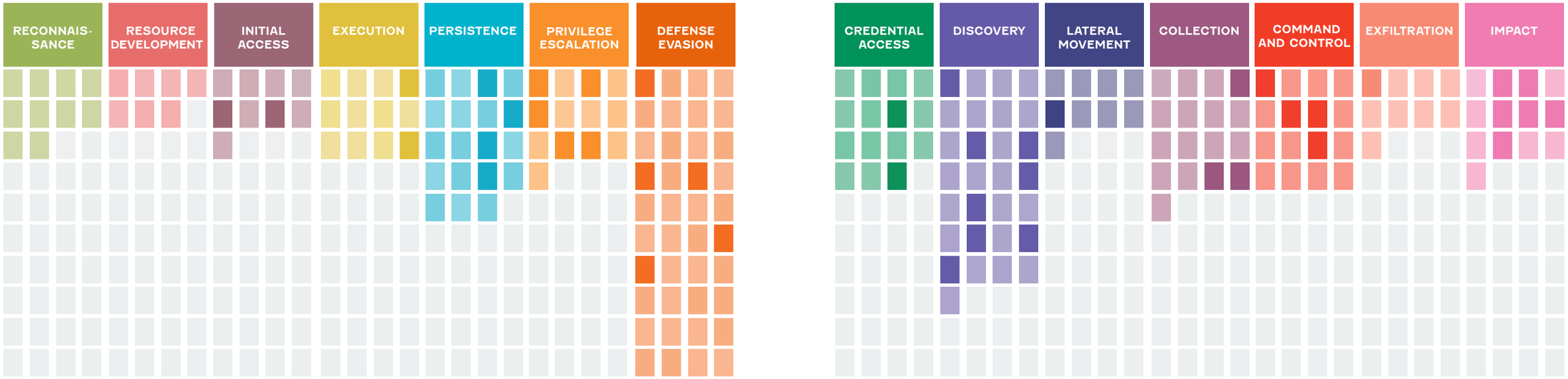
> **2021 July - Ukrainian government phishing attack spreads to Georgia**
Happened on: 2021-07-15



_MITRE ATTCK® TECHNIQUES USED BY THIS ATTACKERS GROUP:

T1008 - Fallback Channels
T1016 - System Network Configuration Discovery
T1020 - Automated Exfiltration
T1021.002 - SMB/Windows Admin Shares
T1571 - Non-Standart Port
T1046 - Network Service Scanning
T1047 - Windows Management Instrumentation
T1049 - System Network Connections Discovery
T1055 - Process Injection
T1056 - Input Capture
T1057 - Process Discovery
T1070 - Indicator Removal on Host
T1071 - Application Layer Protocol
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1087 - Account Discovery
T1113 - Screen Capture
T1119 - Automated Collection
T1120 - Peripheral Device Discovery
T1195 - Supply Chain Compromise
T1203 - Exploitation for Client Execution
T1485 - Data Destruction
T1486 - Data Encrypted for Impact
T1495 - Firmware Corruption
T1498 - Network Denial of Service
T1499 - Endpoint Denial of Service
T1542.003 - Bootkit
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1548.002 - Bypass User Account Control
T1552.001 - Credentials In Files
T1552.004 - Private Keys
T1561.001 - Disk Content Wipe
T1561.002 - Disk Structure Wipe
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1573 - Encrypted Channel
T1574.010 - Services File Permissions Weakness

_CYBER ATTACK PHASES



Threat Actor_

ATK15
(Aka Emissary Panda) is a cyber espionage group active since at least 2009 (first spearphishing spotted by TrendMicro on November 25, 2009), likely based in the Republic of China.

Alias_

_APT 27
_APT27
_Bronze Union
_Emissary Panda
_Group 35
_HIPPOTeam
_Iron Tiger
_Iron Tiger APT
_Lucky Mouse
_LuckyMouse
_Operation Iron Tiger
_TEMP.Hippo
_TG-3390
_Threat Group 3390
_Threat Group-3390
_ZipToken

Targeted Sectors_

_Political Organizations
_Naval
_Manufacturing
_High-Tech
_Government and administration agencies
_Education
_Defence
_Communication
_Aerospace

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland
Spain

MIDDLE EAST/ WESTERN ASIA
Turkey

SOUTH EAST ASIA
Philippines

EASTERN ASIA
China
Hong-Kong

Suspected origin of the attacker_

China

_DESCRIPTION

ATK15 - The group has a preference for leveraging strategic web compromise (SWC) and scan-and-exploit techniques to compromise target systems.
The cyber-spies also used proprietary remote access tools in attacks observed since 2016, including SysUpdate and HyperBro. A multi-stage malware, SysUpdate is used exclusively by the group, being delivered via multiple methods, including malicious Word documents leveraging Dynamic Data Exchange (DDE), manual deployment via stolen credentials, or via a redirect from a strategic web compromise (SWC).
Access to government resources are abused to conduct their campaign attacks. The tools HyperBro and shikata_ga_nai compressor have been used in their recent campaigns. This group is known for their strategic web compromises, relying on whitelist to deliver payloads. The group also has tendency to compromise Microsoft exchange servers.

_MALWARE & TOOLS

Tools used by multiple threat groups:
- PlugX
- HttpBrowser
- ChinaChopper web shell
- Hunter
- Wrapikatz

Tools that appear to be exclusive to ATK15:
- OwaAuth web shell
- ASPXTool
- Rcmd

Publicly available tools:
- Windows Credential Editor (WCE): obtains passwords from memory
- gsecdump: obtains passwords from memory
- winrar compresses data for exfiltration
- Nbtscan: scans NetBIOS name servers
- Netview: host-enumeration tool that presents details about IP addresses, network shares, remote sessions, and logged-on users
- Kekeo: toolset to manipulate the Kerberos authentication protocol
- Metasploit
- BeEF

_USED MALWARES

- ASPXSpy
- Antak
- HTTPBrowser
- OwaAuth
- ZXShell

_USED TOOLS

- Living off the Land
- Windows Credential Editor
- gsecdump

_USED VULNERABILITIES

- CVE-2017-11882

_ATTACKS HAPPENED ON

> **APT27 Spear Phishing**
Happened on: 2009-11-25

> **Iron Tiger operation**
Happened on: 2010-08-08

> **APT27 Spear Phishing with corrupted documents related to Taiwan**
Happened on: 2013-04-23

> **New spear phishing campaign from APT27**
Happened on: 2014-05-09
Spear-phishing on telecommunication an technology companies
Happened on: 2014-09-05

> **APT27 conducted a strategic web compromise (SWC)**
Happened on: 2016-01-08

> **Operation PZChao**
Happened on: 2017-01-08

> **APT27 targets a national data center in the Central Asia**
Happened on: 2017-10-08

> **ATK15 (UNC215) espionage campaign against Israeli companies**
Happened on: 2019-01-01

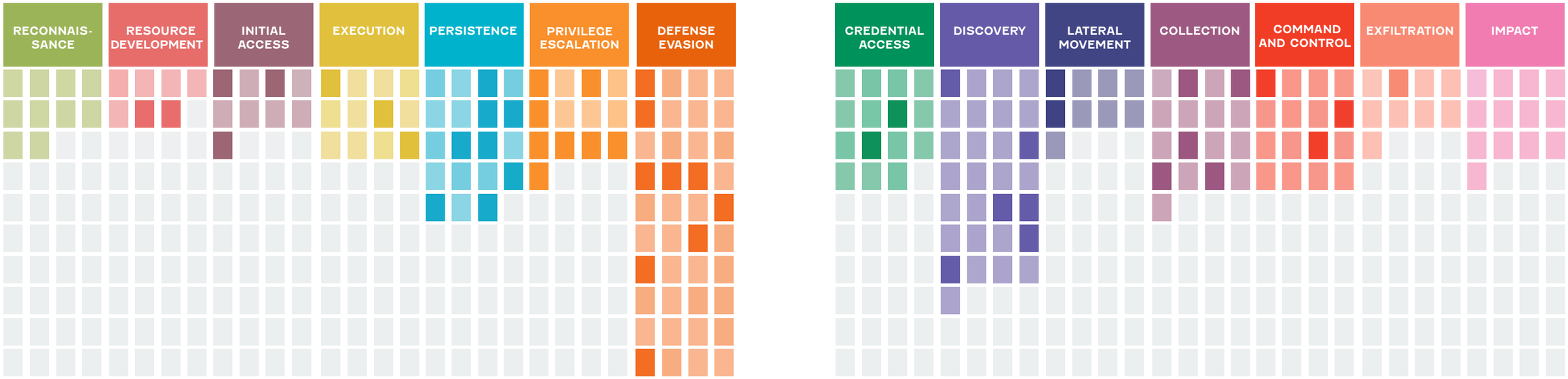
2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019

2009-11-25 APT27 Spear Phishing
2010-08-08 Iron Tiger operation
2013-04-23 Spear Phishing with corrupted documents related to Taiwan
2014-05-09 New spear phishing campaign from APT27
2014-09-05 Spear-phishing on telecommunication an technology companies
2016-01-08 APT27 conducted a strategic web compromise (SWC)
2017-01-08 Operation PZChao
2017-10-08 APT27 targets a national data center in the Central Asia
2019-01-01 ATK15 (UNC215) espionage campaign against Israeli companies

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1003.001 - LSASS Memory
T1003.002 - Security Account Manager
T1003.004 - LSA Secrets
T1005 - Data from Local System
T1012 - Query Registry
T1016 - System Network Configuration Discovery
T1018 - Remote System Discovery
T1021.006 - Windows Remote Management
T1027 - Obfuscated Files or Information
T1030 - Data Transfer Size Limits
T1571 - Non-Standart Portt
T1046 - Network Service Scanning
T1047 - Windows Management Instrumentation
T1049 - System Network Connections Discovery
T1053 - Scheduled Task/Job
T1053.002 - At (Windows)
T1055 - Process Injection
T1055.012 - Process Hollowing
T1056 - Input Capture
T1056.001 - Keylogging
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1068 - Exploitation for Privilege Escalation
T1070.004 - File Deletion
T1070.005 - Network Share Connection Removal
T1071 - Application Layer Protocol
T1071.001 - Web Protocols
T1074 - Data Staged
T1074.001 - Local Data Staging
T1074.002 - Remote Data Staging
T1078 - Valid Accounts
T1087 - Account Discovery
T1087.001 - Local Account
T1105 - Ingress Tool Transfer
T1136 - Create Account
T1112 - Modify Registry
T1119 - Automated Collection
T1133 - External Remote Services
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1210 - Exploitation of Remote Services
T1505.003 - Web Shell
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1548.002 - Bypass User Account Control
T1560 - Archive Collected Data
T1560.002 - Archive via Library
T1562.001 - Disable or Modify Tools
T1562.002 - Disable Windows Event Logging
T1574.001 - DLL Search Order Hijacking
T1574.002 - DLL Side-Loading
T1588.002 - Tool
T1608.002 - Upload Tool
T1608.004 - Drive-by Target

_CYBER ATTACK PHASES



Threat Actor_

ATK168
(aka Pinchy Spider by Crowdstrike, Sodinokibi, Revil Ramsomware Gang or Gold Southfield by Mitre Att&ck) is motivated by financial gains.

_Type of attacker: Cyber Criminal

Alias_

_PINCHY SPIDER
_REvil Ransomware Gang

Targeted Sectors_

_Telecommunication
_Pharmacy
_Drug manufacturing
_High-Tech
_Computers and software development

Motivations_

_Financial Gain

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
France

SOUTH EAST ASIA
Taiwan

2020

2020-04-01
Continuous campaign using the Sodinokibi ransomwareespionage campaign against Israeli companies

_DESCRIPTION

ATK168 - The group behind the CandCrab ransomware was selling access for use in a program partnership with a limited number of accounts. In May 2019, the group announced their retirement, which coincided with the first appearance of Revil / Sodinokibi in April of the same year.

Revil is a *Ransomware as a service* ; (RaaS). In 2020, it is the ransomware most often involved in attacks. These not only consist of encrypting the data that the victim can only recover for a ransom, but in addition, the cybercriminals blackmail the distribution of this data.

The main infection vector is a phishing email that invites you to download a compressed file, but other techniques have been used (such as in June 2021 a software vulnerability of the company Kaseya). Several elements indicate a Russian origin of this malware: the program is instructed to suspend its activity if it detects that the system language is Russian, and it is for sale on Russian-speaking forums.

On 13 July 2021, REvil websites and other infrastructure vanished from the internet.

This group has been the source of tensions between the newly elected US President Joe Biden and Vladimir Putin, following the numerous attacks suffered by the US from Russia. Following the closure of the group's infrastructure, senior officials do not rule out the possibility that the Russian government put pressure on the group.

_USED MALWARES

- GandCrab
- Sodinokibi

_USED VULNERABILITIES

- CVE-2019-11510

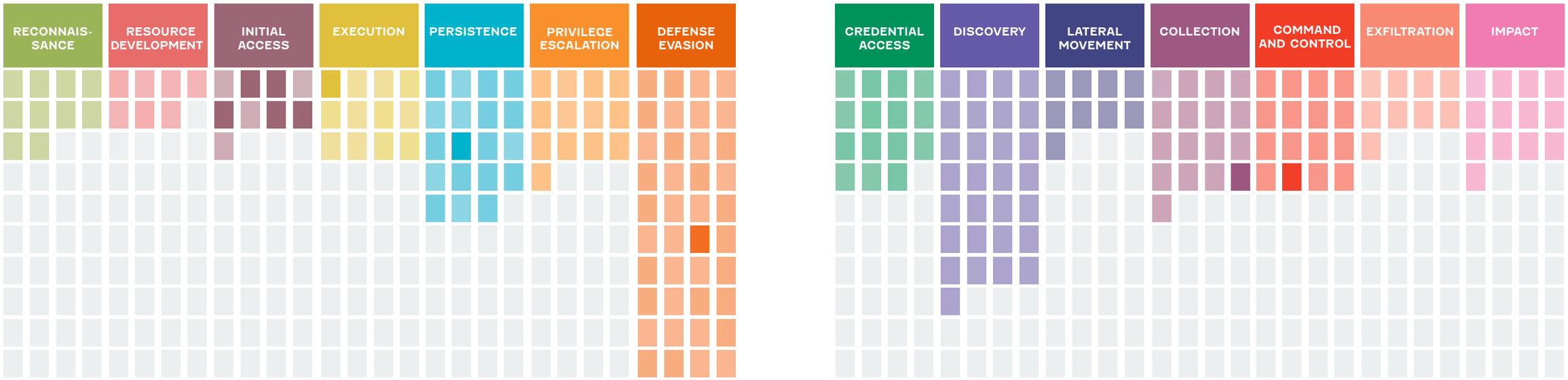
_ATTACKS HAPPENED ON

> **Continuous campaign using the Sodinokibi ransomware espionage campaign against Israeli companies**
Happened on: 2020-04-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1027 - Obfuscated Files or Information
T1059.001 - PowerShell
T1113 - Screen Capture
T1133 - External Remote Services
T1190 - Exploit Public-Facing Application
T1195.002 - Compromise Software Supply Chain
T1199 - Trusted Relationship
T1219 - Remote Access Software
T1566 - Phishing

_CYBER ATTACK PHASES



Threat Actor_

ATK17
(aka: APT32, SeaLotus, OceanLotus, APT-C-00) is a Vietnamese group that leverages a nearly continuous espionage campaign against various but well-defined targets while maintaining a developed arsenal of tools.

_Type of attacker: State Sponsored

Alias_

_APT 32
_APT-32
_APT-C-00
_APT32
_Cobalt Kitty
_Ocean Buffalo
_Ocean Lotus
_OceanLotus
_OceanLotus Group
_POND LOACH
_Sea Lotus
_SeaLotus
_SectorF01
_TIN WOODLAWN

Targeted Sectors_

_Transportation
_Research
_Naval
_Military
_Media
_Manufacturing
_Legal Services
_International Organizations
_High-Tech
_Government and administration agencies
_Financial Services
_Education
_Dissidents
_Defence
_Communication

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
Germany

SOUTH EAST ASIA
Vietnam
Philippines

EASTERN ASIA
China

OCEANIA
Australia

Suspected origin of the attacker_

Vietnam

Motivations_

_Espionage

_DESCRIPTION

ATK17 - This group is known for the diversity of the lures that it uses in order to target its victims. ATK17 is targeting foreign corporations with a vested interest in Vietnam manufacturing, consumer products, and hospitality sectors. Furthermore, there are indications that ATK17 actors are targeting peripheral network security and technology infrastructure corporations. Furthermore to focused targeting of the private sector with ties to Vietnam, ATK17 has also targeted foreign governments, as well as Vietnamese dissidents and journalists since at least 2013. For instance, in 2017, social engineering content in lures used by the actor provided evidence that they were likely used to target members of the Vietnam diaspora in Australia as well as government employees in the Philippines.

It is an active group, with diverse tools on multiple platforms (Windows and MacOS). This group is dangerous because of its unusual adaptablability even when discovered and has used multiple CVEs in order to reach its goals.

_USED MALWARES

- Custom ATK17 netcat
- Denis
- Goopy
- Horsum
- JEShell
- KOMPROGO
- METALJACK
- MacOS Trojan
- PHOREAL
- ROLAND
- Rizzo
- SOUNDBITE
- Unnamed Outlook Backdoor
- WINDSHIELD
- rastls

_USED TOOLS

- CamCapture Plugin
- Cobalt Strike
- Custom IP check tool
- Customized Outlook Credentials Dumper
- Customized Windows Credentials Dumper
- Don't-Kill-My-Cat
- GetPassword_x64
- HookPasswordChange
- KerrDown
- Mimikatz
- PowerShell
- Remy
- Splinter

_USED VULNERABILITIES

- CVE-2016-7255
- CVE-2017-0144
- CVE-2017-11882
- CVE-2018-20250
- CVE-2020-0688

_ATTACKS HAPPENED ON

> **2010: First mention of APT32**
Happened at: 2010-01-09

> **2013 - 2014 Evolution of the group to an Advanced Persistent Threat (APT) group.**
Happened at: 2013-09-09

> **2014-2017: Widening of APT32's scope.**
Happened at: 2014-01-09

> **2014: APT32 targets manufacturing sector in Germany**
Happened on: 2014-08-29

> **2014: APT32 targets dissidents in Vietnamese Southeast Asian diaspora**
Happened on: 2014-08-29

> **2014: APT32 targets Network Security in Vietnam**
Happened on: 2014-08-29

> **2015: APT32 targets China**
Happened on: 2015-08-29

> **2015: APT32 targets Vietnamese media**
Happened on: 2015-08-29

> **2016 - 2017: New techniques for selecting APT32 victims.**
Happened at: 2016-01-09

> **2016: APT32 targets consumer products sector in Philippines**
Happened on: 2016-08-29

> **2016: APT32 targets IT sector in Philippines**
Happened on: 2016-08-29

> **2016: APT32 targets consumer products sector in the USA**
Happened on: 2016-08-29

> **2016: APT32 targets banking sector of Vietnam**
Happened on: 2016-08-29

> **2016: APT32 targets media sector of Vietnam**
Happened on: 2016-08-29

> **2017 - Operation Cobalt Kitty**
Happened on: 2017-01-01

> **2017: APT32 targets dissidents in Vietnamese Australian diaspora**
Happened on: 2017-08-29

> **2017: APT32 targets government employees of Philippines**
Happened on: 2017-08-29

> **2018 - APT32 changes its delivery method.**
Happened at: 2018-01-09

> **2019 - Massive campaign in the Indochinese Peninsula**
Happened at: 2018-01-09

> **2019 - OceanLotus Campaigns against car manufacturers**
Happened on: 2019-03-24

2014
- 2014-08-29 APT32 targets manufacturing sector in Germany
- 2014-08-29 APT32 targets Network Security in Vietnam

2015
- 2015-08-29 APT32 targets China

2016
- 2016-08-29 APT32 targets consumer products sector in the USA

2017

2018
- 2018-01-09 Massive campaign in the Indochinese Peninsula

2019
- 2019-03-24 OceanLotus Campaigns against car manufacturers

2020
- 2020-01-01 ATK17 campaigns against Wuhan and the Chinese Ministry of Emergency Management
- 2020-06-01 New APT32 attack campaign's in the aim to target Cambodian Government

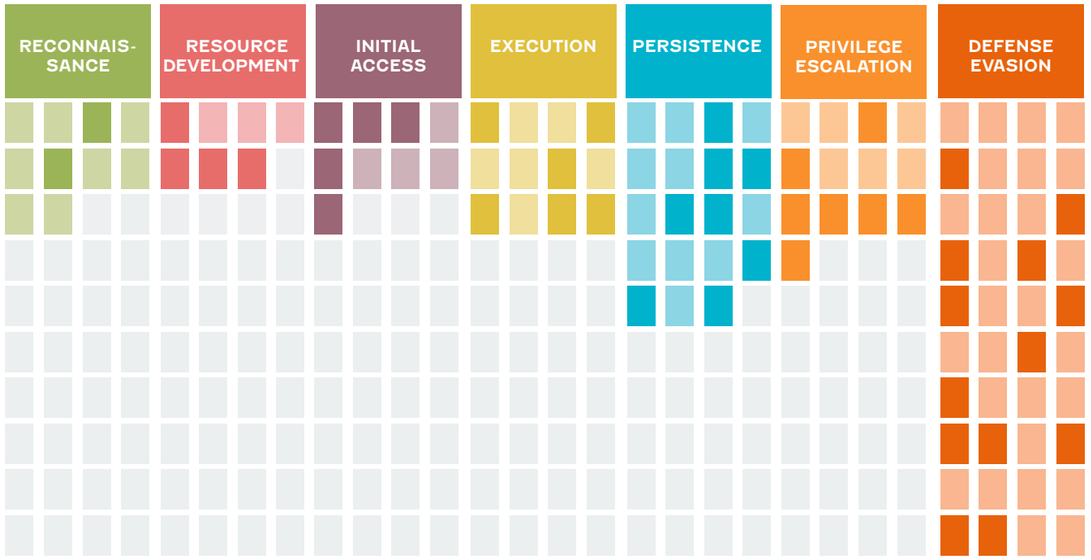
> **2020 - ATK17 campaigns against Wuhan and the Chinese Ministry of Emergency Management**
Happened on: 2020-01-01

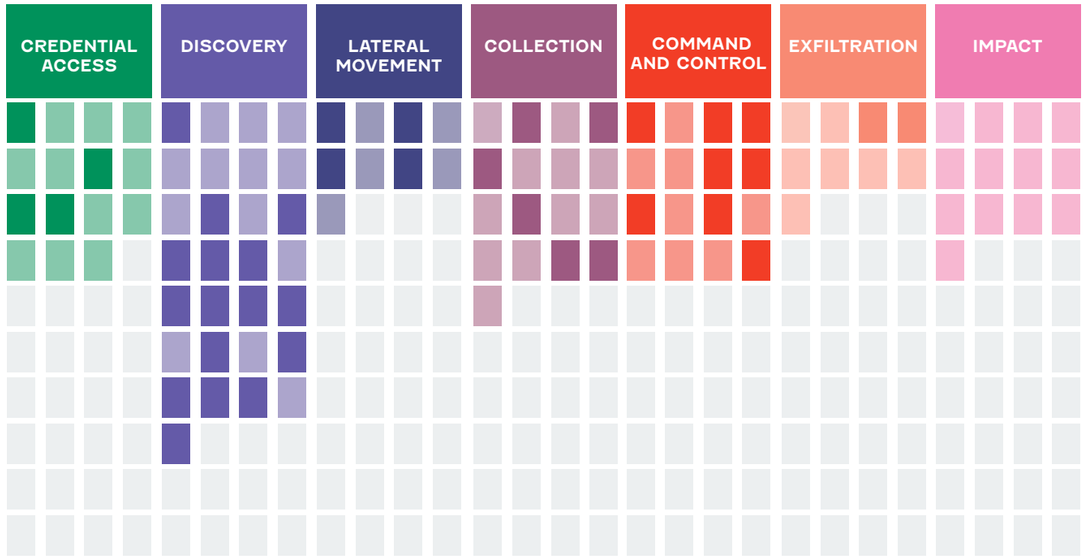
> **2020 - New APT32 attack campaign's in the aim to target Cambodian Government**
Happened on: 2020-06-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1003 - OS Credential Dumping
T1003.001 - LSASS Memory
T1005 - Data from Local System
T1007 - System Service Discovery
T1008 - Fallback Channels
T1012 - Query Registry
T1016 - System Network Configuration Discovery
T1018 - Remote System Discovery
T1021 - Remote Services
T1021.002 - SMB/Windows Admin Shares
T1027 - Obfuscated Files or Information
T1027.001 - Binary Padding
T1033 - System Owner/User Discovery
T1036 - Masquerading
T1036.003 - Rename System Utilities
T1036.004 - Masquerade Task or Service
T1036.005 - Match Legitimate Name or Location
T1040 - Network Sniffing
T1041 - Exfiltration Over C2 Channel
T1046 - Network Service Scanning
T1047 - Windows Management Instrumentation
T1048 - Exfiltration Over Alternative Protocol
T1048.003 - Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
T1049 - System Network Connections Discovery
T1053.005 - Scheduled Task
T1055 - Process Injection
T1056 - Input Capture
T1056.001 - Keylogging
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1059.005 - Visual Basic
T1059.007 - JavaScript
T1068 - Exploitation for Privilege Escalation
T1069 - Permission Groups Discovery
T1070 - Indicator Removal on Host
T1070.001 - Clear Windows Event Logs
T1070.004 - File Deletion
T1070.006 - Timestomp
T1071.001 - Web Protocols
T1071.003 - Mail Protocols
T1072 - Software Deployment Tools
T1078 - Valid Accounts
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1087 - Account Discovery
T1087.001 - Local Account
T1102 - Web Service
T1104 - Multi-Stage Channels
T1105 - Ingress Tool Transfer
T1136 - Redundant Access
T1110 - Brute Force
T1112 - Modify Registry
T1113 - Screen Capture
T1119 - Automated Collection
T1132 - Data Encoding
T1133 - External Remote Services
T1135 - Network Share Discovery
T1137 - Office Application Startup
T1140 - Deobfuscate/Decode Files or Information
T1185 - Man in the Browser
T1189 - Drive-by Compromise
T1190 - Exploit Public-Facing Application
T1201 - Password Policy Discovery
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1210 - Exploitation of Remote Services
T1216 - Signed Script Proxy Execution
T1216.001 - PubPrn
T1218.005 - Mshta
T1218.010 - Regsvr32
T1218.011 - Rundll32
T1221 - Template Injection
T1497 - Virtualization/Sandbox Evasion
T1505.003 - Web Shell
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1560 - Archive Collected Data
T1564.001 - Hidden Files and Directories
T1564.003 - Hidden Window
T1564.004 - NTFS File Attributes
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1570 - Lateral Tool Transfer
T1571 - Non-Standard Port
T1574.002 - DLL Side-Loading
T1583.001 - Domains
T1583.006 - Web Services
T1585.001 - Social Media Accounts
T1588.002 - Tool
T1589 - Gather Victim Identity Information
T1589.002 - Email Addresses
T1598.003 - Spearphishing Link
T1608.001 - Upload Malware
T1608.004 - Drive-by Target

_CYBER ATTACK PHASES





Threat Actor_

ATK2
(aka: Aurora Panda) group has been in operation since at least 2009 and is most likely a professional organization that offers a “hackers for hire” service.

_Type of attacker: State Sponsored

Alias_

_APT 17
_APT 41
_APT17
_APT41
_Aurora Panda
_Axiom
_BRONZE ATLAS
_BRONZE EXPORT
_Barium
_Blackfly
_Deputy Dog
_DeputyDog
_Dogfish
_Group 72
_Group 8
_Group72
_Hidden Lynx
_Lead
_Ragebeast
_Suckfly
_Tailgater
_Tailgater Team
_Wicked Panda
_Wicked Spider
_WinNTI
_Winnti Group
_Winnti Umbrella

Targeted Sectors_

_Transportation
_Media
_Manufacturing / industry
_High-Tech
_Healthcare
_Government and administration agencies
_Financial Services
_Education
_Defence
_Aerospace

Targeted Areas_

NORTH AMERICA
United States Of America
Canada

WESTERN EUROPE
France
United Kingdom Of Great Britain And Northern Ireland
Germany

SOUTHERN ASIA
India

SOUTH EAST ASIA
Singapore

EASTERN ASIA
Taiwan
Korea
Japan
Hong-Kong
China

RUSSIA
Russian Federation

OCEANIA
Australia

Suspected origin of the attacker_

China

Motivations_

_Espionage

_DESCRIPTION

ATK2 - They have the capability to attack many organizations with concurrently running campaigns. They operate efficiently and move quickly and methodically. Based on these factors, the group would need to be a sizeable organization made up of between 50 and 100 individuals.

The members of this group are experts at breaching systems. They engage in a two-pronged strategy of mass exploitation and pay-to-order targeted attacks for intellectual property using two Trojans designed specifically for each purpose:

_Team Moudoor distributes Backdoor. Moudoor, a customized version of “Ch0st RAT”, for large-scale campaigns across several industries. The distribution of Moudoor requires a sizeable number of people to both breach targets and retrieve the information from the compromised networks.
_Team Naid distributes Trojan. Naid, the Trojan found during the Bit9 incident, which appears to be reserved for more limited attacks against high value targets. This Trojan was leveraged for a special operation during the VOHO campaign and is probably used by a specific team of highly skilled attackers within the group. This Trojan was also found as part of “Operation Aurora” in 2009.

Much of the attack infrastructure and tools used during these campaigns originate from network infrastructure in China. The ATK2 group makes regular use of zero-day exploits and has the ability to rework and customize exploits quickly. They are methodical in their approach and they display a skillset far in advance of some other attack groups also operating in that region, such as the Comment Crew (also known as APT1). The ATK2 group is an advanced persistent threat that has been in operation for at least four years and is breaking into some of the best-protected organizations in the world. With a zero-day attack already under their belt in 2013, they continue to operate at the leading edge of targeted attacks.

Between January and March 2020, APT41 launched a large scan attempting to exploit vulnerabilities in Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central on a large number of companies in many sectors and countries. During these exploitation attempt, APT41 only used publicly available malware such as Cobalt Strike and Meterpreter. These tools were propably used as reconnaissance step before useing more advanced custom malwares. This campaign shows that the group is ressourceful and can quickly leverage newly disclosed vulnerabilities.

_USED MALWARES

- BLACKCOFFEE
- Briba
- CrossWark
- Darkmoon
- Derusbi
- Hydraq
- Linfo
- Naid
- Nerex
- Pasam
- PoisonIvy
- Vasport
- Wiarp
- ZXShell
- gh0st RAT
- StealthVector
- StealthMutant
- ScrambleCross

_USED TOOLS

- Living off the Land
- Meterpreter

_USED VULNERABILITIES

- CVE-2010-0249
- CVE-2011-0609
- CVE-2011-0611
- CVE-2011-2110
- CVE-2012-0779
- CVE-2012-1535
- CVE-2012-1875
- CVE-2012-1889
- CVE-2012-4792
- CVE-2013-1347
- CVE-2013-1493
- CVE-2013-3893
- CVE-2014-0322
- CVE-2018-0802

_ATTACKS HAPPENED ON

> **June to December 2009 - Operation Aurora**
Happened on: 2010-01-01

> **November 2011 - EASYUPDATE campaign**
Happened on: 2011-11-02

> **June to July 2012 - VOHO Campaign**
Happened on: 2012-06-02

> **February to March 2013 - FINSHO Campaign**
Happened on: 2013-02-02

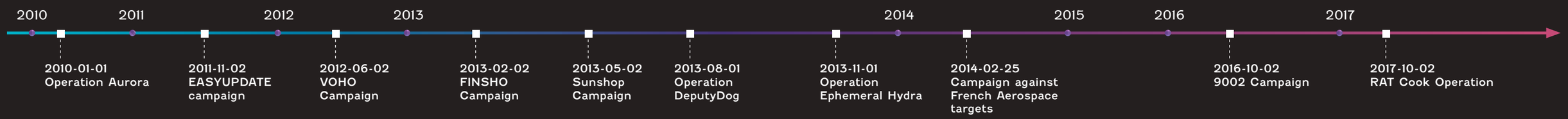
> **May 2013 - Sunshop Campaign**
Happened on: 2013-05-02

> **August 2013 - Operation DeputyDog**
Happened on: 2013-08-01

> **November 2013 - Operation Ephemeral Hydra**
Happened on: 2013-11-01

> **Beginning of 2014 - Campaign against French Aerospace targets**
Happened on: 2014-02-25

> **2016 - 9002 Campaign**
Happened on: 2016-10-02



> **2017 - RAT Cook Operation**
Happened on: 2017-10-02

> **Phishing campaign**
The campaign took place between March 20 and March 28, 2018 and used Google's shortening link service.
Happened on: 2018-03

> **APT41 Initiates Global Intrusion Campaign Using Multiple Exploits**
Happened on: 2021

> **2021 - ColumnTK campaign (SITA Breach)**
Happened on: 2021

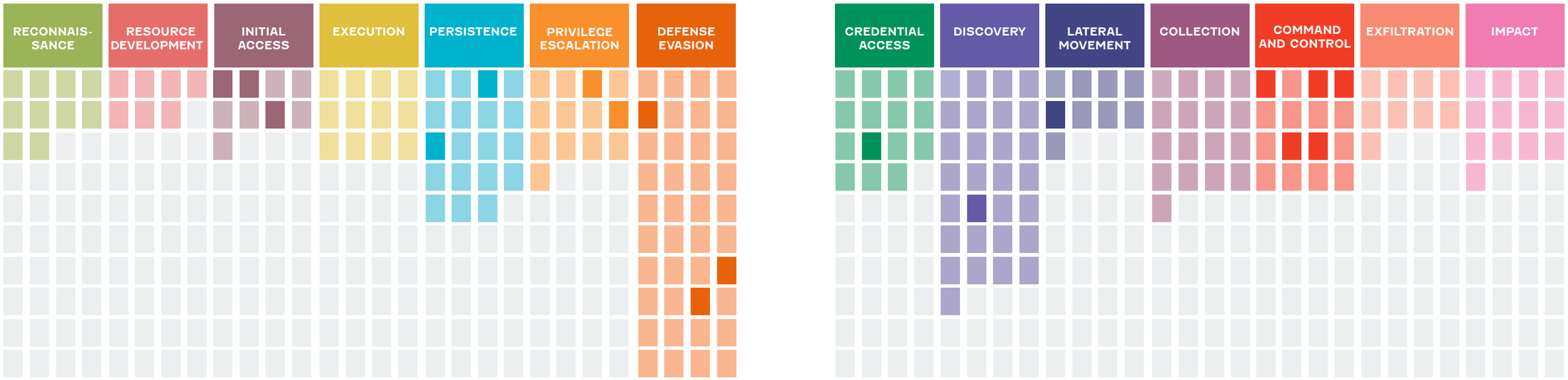
> **Earth Baku Returns**
Happened on: 2021-08-24

> **2021 - APT41 U.S. State Governments campaign**
Happened on: 2021

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1003 - OS Credential Dumping
T1014 - Rootkit
T1021.001 - Remote Desktop Protocol
T1571- Non-Standard Port
T1057 - Process Discovery
T1071 - Application Layer Protocol
T1095 - Non-Application Layer Protocol
T1132 - Data Encoding
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1190 - Exploit Public-Facing Application
T1195 - Supply Chain Compromise
T1546.008 - Accessibility Features
T1547.001 - Registry Run Keys / Startup Folder
T1553.002 - Code Signing

_CYBER ATTACK PHASES



Threat Actor_

ATK23
(aka: Icefog) is an Chinese cyber espionange group active since at least 2011.

_Type of attacker: State Sponsored

Alias_

_Dagger Panda
_Ice Fog
_Icefog

Targeted Sectors_

_Water distribution and supply
_Naval
_Military
_Media
_Maritime Compagnies
_High-Tech
_Government and administration agencies
_Energy
_Defence
_Aerospace

Languages_

_Chinese

Motivations_

_Espionage

Suspected origin of the attacker_

China

Targeted Areas_

NORTH AMERICA
United States Of America
Canada

NORTHERN EUROPE
Netherlands

WESTERN EUROPE
France
United Kingdom Of Great Britain And Northern Ireland
Germany
Italy
Austria

EASTERN EUROPE
Belarus

MIDDLE EAST/ WESTERN ASIA
Turkey

CENTRAL ASIA
Kazakhstan
Uzbekistan
Tajikistan

SOUTHERN ASIA
India
Sri Lanka
Pakistan

SOUTH EAST ASIA
Singapore
Philippines
Malaysia

EASTERN ASIA
Taiwan
Korea
Japan
Hong-Kong
China
Mongolia

OCEANIA
Australia

RUSSIA
Russian Federation

2010

2011-01-01
Ice Fog campaign against Japan, South Korea and Taiwan between 2011 to 2013

_DESCRIPTION

ATK23 - This group is described as a group having a relative lack of complexity but they sucessfully compromised their targets which are mostly the defence contractors, industrial campanies, shipbuilding companies, telecommunication operators and medias in Japan, Taiwan and South Korea. This group used spearphishing emails exploiting CVE-2012-0158 and CVE-2012-1856 or contains a web link to Oracle Java exploits CVE-2013-0422 and CVE-2012-1723. It uses already known and patched vulnerabilities. Its lure Word documents contains pictures of a woman or are related to political actuality. This group also used HLP files abusing Windows features to drop its malwares.

After the initial access, the group list folder on the disk, IP configuration and information about the victim network. If the victim is interesting it deploys additional softwares such as backdoor and lateral movement tools to dump password from Windows, IE or Outlook and a legitimage RAR compressing tool. It also try tool steal Windows address books (.WAB files) and XSL, DOC or HWP documents. The stolen document are compressed and split into multiple parts using WinRAR or CABARC to be transfered to the C2 server.

The lateral movement is done using multiple tools to dump credential from browsers or Outlook.

The C2 servers are hosted on shared hosting plateforms and dedicated hosting. Their C2 infrastructure is very ephemeral. Icefog seems to use a hit and run strategy. They infects their victims, steal the data and the C2 infrastructure expires in a few months. This strategy indicates that they knew what they are looking for. They did not maintain a persistent presence on the compromised network when their goal is reached.

After the Kaspersky reports from September 2013 and January 2014, the group desapeared. In 2015 after nearly a year of silence, new variants of the ICEFOG (ICEFOG-M and ICEFOF-P) have been found, used during campaign which targets do not match with previously seen campaign.

NB: According to the researcher Chi-en Shen from FireEye, the new variants of the ICEFOG backdoor are used by multiple Chinese groups (APT9, APT15, Goblin Panda and another group name Temp Group A which can actually be the original Icefog group). The conclusion is that the ICEFOG backdoor cannot be used to attribute a campaign.

_USED MALWARES

- 8.t Dropper
- ICEFOG
- JavaFog
- MacFog

_USED TOOLS

- CABARC
- WinRAR

_USED VULNERABILITIES

- CVE-2012-0158
- CVE-2012-1723
- CVE-2012-1856
- CVE-2013-0422

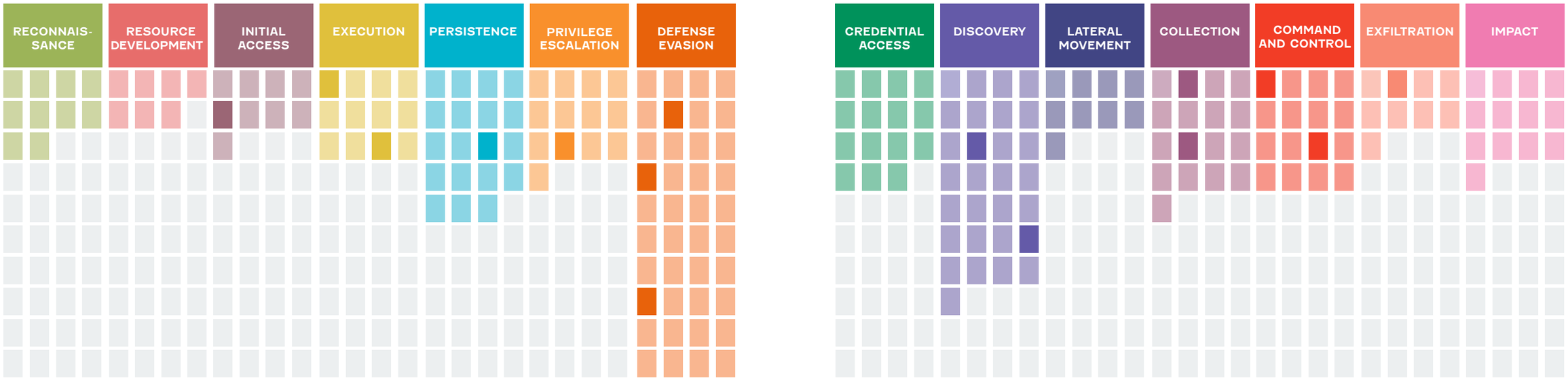
_ATTACKS HAPPENED ON

> **Ice Fog campaign against Japan, South Korea and Taiwan between 2011 to 2013**
Happened on: 2011-01-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1005 - Data from Local System
T1016 - System Network Configuration Discovery
T1030 - Data Transfer Size Limits
T1059 - Command and Scripting Interpreter
T1071 - Application Layer Protocol
T1083 - File and Directory Discovery
T1140 - Deobfuscate/Decode Files or Information
T1204 - User Execution
T1218.001 - Compiled HTML File
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1571 - Non-Standard Port
T1574.001 - DLL Search Order Hijacking

_CYBER ATTACK PHASES



Threat Actor_

ATK233
(aka HAFNIUM by Microsoft) is the group designated as responsible for the Microsoft Exchange server data breach in 2021.
It is mainly based in China and uses servers based in United States.

_Type of attacker: State Sponsored

Alias_

_HAFNIUM

Targeted Sectors_

_Universities
_Scientific Research and Consulting
_Political
_Non-governmental organizations
_Healthcare
_Defence contractors

Motivations_

_Cyber Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

Suspected origin of the attacker_

China

2021 — 2022

2021-01-01ATK233 Exchange Vulnerability scanning in USA

2022 - HAFNIUM August 2021 to February 2022 Campaign

_DESCRIPTION

ATK233 - The group is suspected to be state sponsored and operating out of China.

According to the investigative results of Microsotf (the main informant on this group), they are based in China but mainly use virtual private servers based in the United States.

Their target during this campaign will have been infectious disease researchers, law firms, higher education institutions, defense entrepreneurs, policy think tanks and NGOs.

In July 2021, British Foreign Secretary Dominic Raab said the attack was carried out by “Chinese state-backed groups” linked to the Ministry of State Security (MSS). The Chinese government has denied responsibility for the Microsoft breach in 2021.

The group is described as “highly skilled and sophisticated”.

_USED MALWARES

- Tarrask

_USED TOOLS

- Covenant
- ProcDump

_USED VULNERABILITIES

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

_ATTACKS HAPPENED ON

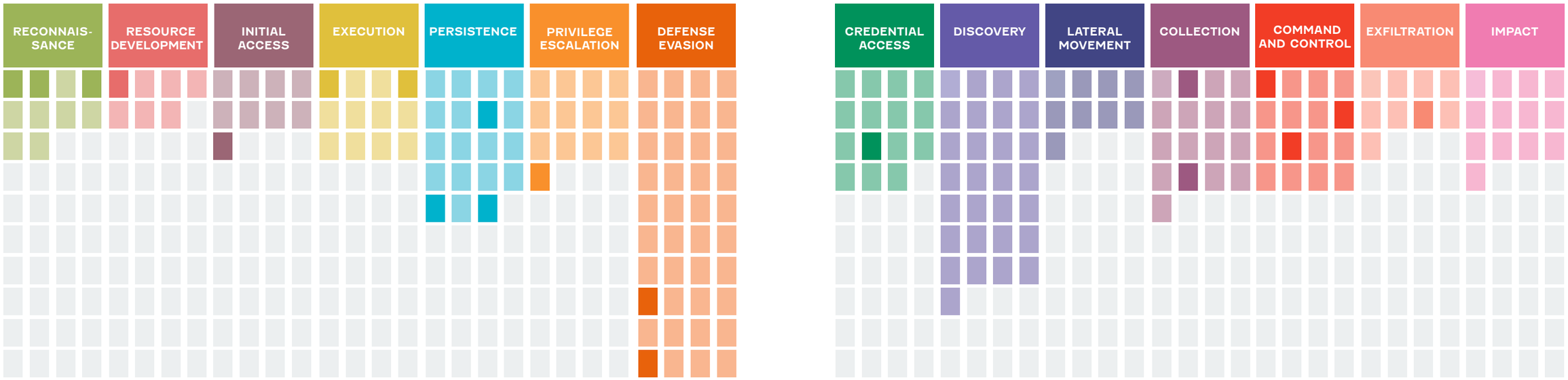
> **2021 JAN - ATK233 Exchange Vulnerability scanning in USA**
Happened on: 2021-01-01

> **2022 - HAFNIUM August 2021 to February 2022 Campaign**
Happened on: 2022-02

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003.001 - LSASS Memory
T1003.003 - NTDS
T1059.001 - PowerShell
T1071.001 - Web Protocols
T1078.003 - Local Accounts
T1095 - Non-Application Layer Protocol
T1105 - Ingress Tool Transfer
T1114.002 - Remote Email Collection
T1136.002 - Domain Account
T1203 - Exploitation for Client Execution
T1218.011 - Rundll32
T1505.003 - Web Shell
T1560.001 - Archive via Utility
T1567.002 - Exfiltration to Cloud Storage
T1583.003 - Virtual Private Server
T1583.006 - Web Services
T1590 - Gather Victim Network Information
T1590.005 - IP Addresses
T1592.002 - Software
T1595.002 - Vulnerability Scanning

_CYBER ATTACK PHASES



Threat Actor_

ATK234
(Aka SPRIRAL) is a Chinese state sponsored hacker group.
_Type of attacker: State Sponsored

Alias_

_SPIRAL

Targeted Sectors_

_Information Technology
_Government and administration agencies

Targeted Areas_

NORTH AMERICA
United States Of America

Suspected origin of the attacker_

China

_DESCRIPTION

ATK234 - Their latest SUPERNOVA attack was discovered at the same time as the Russian SUNBURST on SOLARWINDS 'ORION platform. Although this attack is less sophisticated than the one of the Russians and went under the radar. It is nonetheless important. The Chinese group had already used these techniques against ZOHO MAIL.

_USED MALWARES

- SUPERNOVA

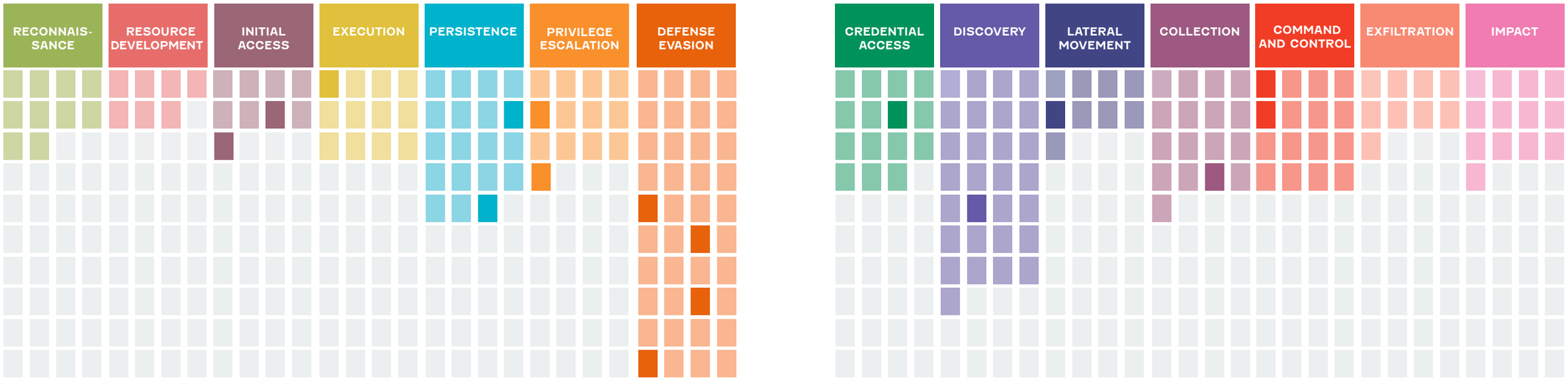
_ATTACKS HAPPENED ON

> **2021 march - ATK234 deploys Supernova on Solarwinds**
Happened on: 2021-03-08

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1021 - Remote Services
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1056 - Input Capture
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1071 - Application Layer Protocol
T1078 - Valid Accounts
T1195 - Supply Chain Compromise
T1543.003 - Windows Service
T1553 - Subvert Trust Controls
T1568.002 - Domain Generation Algorithms

_CYBER ATTACK PHASES



Threat Actor_

ATK236
(aka TA551, GOLD CABIN, Shathak) is a financially-motivated threat group that uses large-scale phishing campaigns to deliver additional malware payloads.
_Type of attacker: Cyber Criminal

Alias_

_GOLD CABIN
_Shathak
_TA551

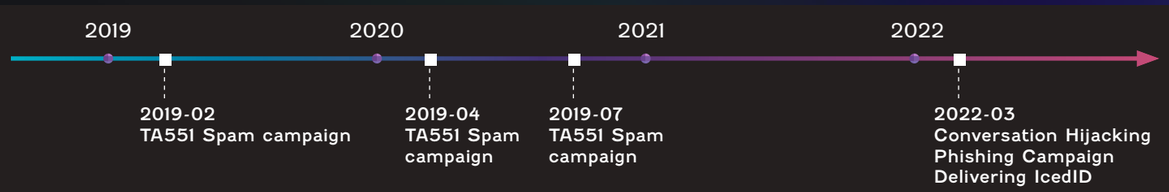
Motivations_

_Financial Gain

Targeted Areas_

WESTERN EUROPE
Italy
Germany

EASTERN ASIA
Japan



_DESCRIPTION

ATK236 - (aka: TA551, GOLD CABIN, Shathak) is a financially-motivated threat group that has been active since at least 2018 that uses large-scale phishing campaigns to deliver additional malware payloads. IcedID and Valak were the predominant payloads we observed with TA551 phishing campaigns in 2020. The group has distributed different malware families over time, but consistently used password-protected ZIP archives containing macro-enabled Office documents.
The group has primarily targeted English, German, Italian, and Japanese speakers through email-based malware distribution campaigns.
In September 2021, the group was observed pushing Trickbot to the infected hosts, which, in turns, delivered DarkVNC and Cobalt Strike beacons.

_USED MALWARES

- Gozi-Isfb
- IcedID
- QakBot
- Ursnif
- Valak

_ATTACKS HAPPENED ON

> **TA551 Spam campaign**
Happened on: 2019-02

> **April 2020 to July 2020 - TA551 Spam campaign**
Happened on: 2020-04

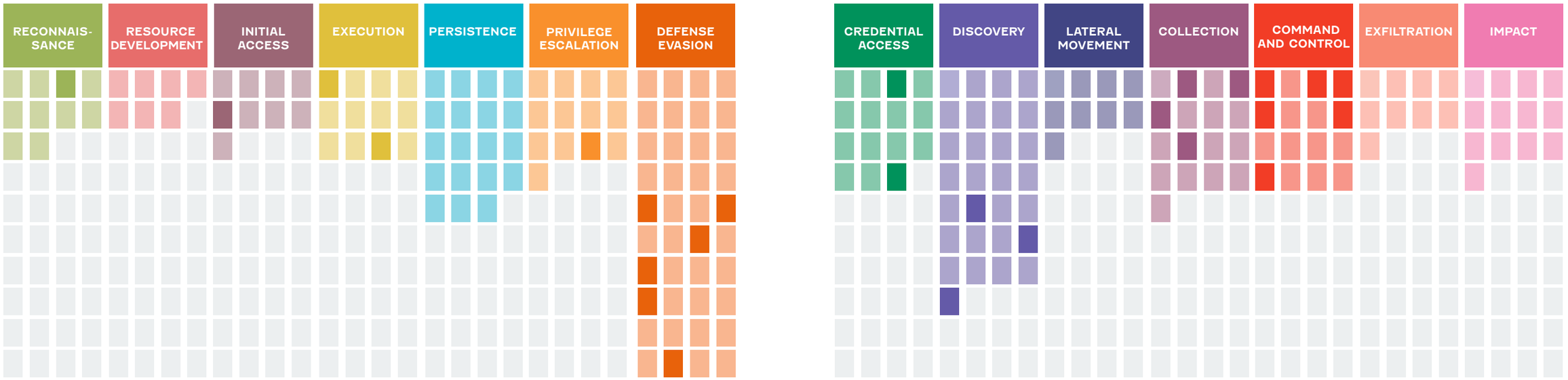
> **July 2020 to December 2020 - TA551 Spam campaign**
Happened on: 2020-07

> **Conversation Hijacking Phishing Campaign Delivering IcedID**
Happened on: 2022-03

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1005 - Data from Local System
T1016 - System Network Configuration Discovery
T1027 - Obfuscated Files or Information
T1027.003 - Steganography
T1036 - Masquerading
T1055 - Process Injection
T1055.012 - Process Hollowing
T1057 - Process Discovery
T1059.003 - Windows Command Shell
T1071.001 - Web Protocols
T1090 - Proxy
T1105 - Ingress Tool Transfer
T1112 - Modify Registry
T1119 - Automated Collection
T1132.001 - Standard Encoding
T1185 - Man in the Browser
T1204 - User Execution
T1204.002 - Malicious File
T1218.005 - Mshta
T1218.010 - Regsvr32
T1218.011 - Rundll32
T1497 - Virtualization/Sandbox Evasion
T1552.004 - Private Keys
T1555.004 - Windows Credential Manager
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1568.002 - Domain Generation Algorithms
T1589.002 - Email Addresses

_CYBER ATTACK PHASES



Threat Actor_

ATK237

A cyber group with a brazilian origin, that was oriented until 2011 against its compatriots before going international.

_Type of attacker: Cyber Criminal

Alias_

_Grandoreiro Operator
_Guildma / Astaroth Operator
_Javali Operator
_Melcoz Operator
_TETRADE

Targeted Sectors_

_Financial Services

Targeted Areas_

WESTERN EUROPE
France

NORTH AMERICA
United States of America

CENTRAL AMERICA
Mexico

SOUTH AMERICA
Brazil

Suspected origin of the attacker_

Latin America

Brazil

2021

2021-01-28
ATK237 (Grandoreiro) campaign against France

2021-02-17
ATK237 (Javali) campaign against Mexico and Brazil

2021-05-06
ATK237 (Javali) campaign against Brazil

2021-05-07
ATK237 (Grandoreiro) campaign against USA

_DESCRIPTION

ATK237 - The analysis of the malware that makes up this threat led to the name TETRADE 4 malware families, believing that they are the result of a Brazilian banking group / operation that is evolving its capabilities by targeting banking users abroad.

New professionally executed, scalable and persistent operations, creating various versions of the malware, with significant infrastructure improvements that allow cybercriminal groups from different countries to collaborate.

The attacks seem to focus on the Latin American victims although casualties from all over the world are possible, the banks being international.

Each campaign runs on its unique identifier, which varies according to the versions and Commands & Controls used.

Brazilian cyber crime is prolific, since then Android malware like Chimob has appeared, directly linked to GUILDMA. The tetrades are just a small part of the threat from Latin America.

It is impossible to know or recognize who are the groups or individuals behind its malware. It is commonly accepted that there is a community which, although competing, shares a lot of information and infrastructures.

_USED MALWARES

- Astaroth
- Chimob
- Grandoreiro
- Guildma
- Javali
- Melcoz

GUILDMA (aka Astaroth)
2015 : Spread primarily through phishing emails disguised as legitimate business communications or notifications. Acquisition of several new evasion techniques, making it difficult to detect.
2019 : malicious payload is hidden in victim's system with the help of special file format.
Storage of its communication with the control server in an encrypted format on Facebook and YouTube pages. Therefore difficulty in detecting communication traffic as malicious and since no antivirus is blocking either of these websites, it ensures that the controlling server can execute commands without interruption.

GRANDEIRO
2016 : First present in Brazil, it extended its attacks in Latin America then in Europe.
Among the tetrades, it is the most widespread.
It focuses its efforts on evasion of detection using modular installers.
The malware allows attackers to conduct fraudulent banking transactions by using victims' computers to bypass security measures used by banking institutions.

JAVALI (aka Ousaban)
2017 : Uses multistage malware and distributes its initial payload via phishing emails, as an attachment or link to a website. These emails include an MSI (Microsoft Installer) file with an embedded Visual Basic Script that downloads the final malicious payload from a remote C2; it also uses DLL sideloading and several layers of obfuscation to hide its malicious activities from analysts and security solutions.

MELCOZ
2018 : Internationalization of the threat of this malware after having evolved for years in Brazil

_ATTACKS HAPPENED ON

> **2021 - ATK237 (Grandoreiro) campaign against France**
Happened on: 2021-01-28

> **2021 - ATK237 (Javali) campaign against Mexico and Brazil**
Happened on: 2021-02-17

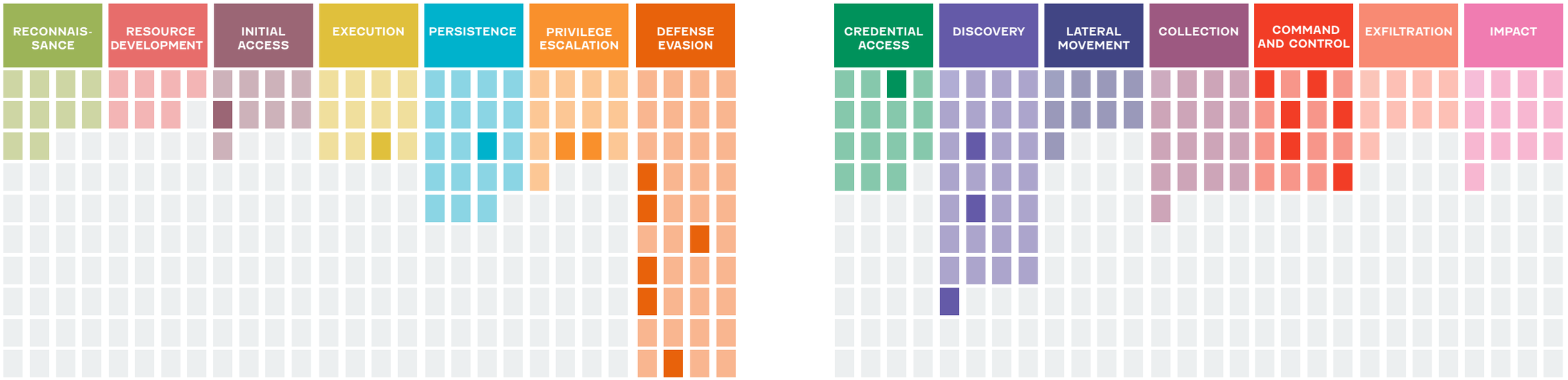
> **2021 - ATK237 (Javali) campaign against Brazil**
Happened on: 2021-05-06

> **2021 - ATK237 (Grandoreiro) campaign against USA**
Happened on: 2021-05-07

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1055 - Process Injection
T1057 - Process Discovery
T1071 - Application Layer Protocol
T1083 - File and Directory Discovery
T1095 - Non-Application Layer Protocol
T1102 - Web Service
T1105 - Ingress Tool Transfer
T1132 - Data Encoding
T1204 - User Execution
T1218 - Signed Binary Proxy Execution
T1497 - Virtualization/Sandbox Evasion
T1555 - Credentials from Password Stores
T1566 - Phishing
T1573 - Encrypted Channel
T1574 - Hijack Execution Flow

_CYBER ATTACK PHASES



Threat Actor_

ATK241

A group using ransomware-like extortion campaigns with data encryption to actually using a wiper to destroy the target's data.

Alias_

_Agrius

Motivations_

_Sabotage
_Coercion

Targeted Areas_

MIDDLE EAST/ WESTERN ASIA

United Arab Emirates

Israel

Suspected origin of the attacker_

Iran

2020

2020-12-31
ATK241 extended its operations to Israeli targets

_DESCRIPTION

ATK241 - It seems that the group's shift in focus from mimicking a criminal modus operandi with ransomware-like extortion campaigns with data encryption to actually using a wiper to destroy the target's data.
This tactic of near luring by pretending to use one modus operandi rather than another is not yet explained and is not common.
In all likelihood, the attacker must be trying to buy time by hiding his original intent behind a classic ransomware attack to have time to erase all the data he wants from his target.

The group is suspected of originating from Iran and of being a sponsored group. The link to Iran is argued by SentinelLabs under four points:

- Firstly, the nature of the motivation and the modus operandi using wipers echoes behaviour observed in other groups suspected of being sponsored by the Iranian state. The nature of the targets is also reminiscent of the geopolitical tension between Iran and Israel. Another target located in the United Arab Emirates had already been targeted by Iranian groups. It is a critical infrastructure facility of the Emirates.
- Secondly, some of the webshells deployed by the group were modified versions of ASPXSpy. Three of these variants were uploaded to VirusTotal from Iran, the rest from other Middle Eastern countries.
- Also, while the group regularly uses public VPN providers (e.g. ProtonVPN), it has used non-VPN nodes from servers linking to Iranian domains in the past.
- Finally, Agrius uses the DEADWOOD wiper in its arsenal. This software has been linked by some sources to ATK35 (APT33), the Shamoon operator. It seems that Agrius and ATK35 share resources in this matter. This is because the variant used by Agrius is an improvement of the original software, which implies that the group had access to the source code of the latter or at least exchanged with the original developers. The use of DEADWOOD came shortly after an attempt by Agrius to use his personal wiper named Apostle. Apostle was probably not fully operational at the time of its deployment, which prompted Agrius to use an equivalent from an outside source.

_USED MALWARES

- Apostle Ransomware variant
- Apostle Wiper variant
- DEADWOOD
- IPsec Helper

_USED VULNERABILITIES

- CVE-2018-13379

_ATTACKS HAPPENED ON

> **2020 Dec - ATK241 extended its operations to Israeli targets**
Happened on: 2020-12-31

Threat Actor_

ATK27
(aka: Dark Caracal) is
an advanced persistence threat group in activity since January 2012, with a suspected origin of Lebanon.

_Type of attacker: State Sponsored

Alias_

_Dark Caracal
_TAG-CT3

Targeted Sectors_

_Military
_Media
_Manufacturing
_Legal Services
_International Organizations
_Healthcare
_Government and administration agencies
_Financial Services
_Education
_Defence

Motivations_

_Ideology
_Financial Gain
_Coercion

Targeted Areas_

NORTH AMERICA
United States Of America

SOUTH AMERICA
Bolivarian Republic Of Venezuela

NORTHEN EUROPE
Netherlands

WESTERN EUROPE
France
Germany
Italy
Switzerland

MIDDLE EAST/ WESTERN ASIA
Lebanon
Saudi Arabia
Syria
Qatar
Jordan

SOUTHERN ASIA
Nepal
India
Pakistan

SOUTH EAST ASIA
Vietnam
Thailand
Philippines

EASTERN ASIA
Korea
China

RUSSIA
Russian Federation

Suspected origin of the attacker_

Lebanon

_DESCRIPTION

ATK27 - It is supposedly linked to the Lebanese government since its activity was traced to the headquarters of the General Directorate of General Security, in Beirut Lebanon. Dark Caracal has been conducting a multi-platform APT-level surveillance operation targeting individuals and institutions globally.

_USED MALWARES

- Bandook
- CrossRAT
- FinFisher
- Pallas

_USED TOOLS

- Adobe Flash Player
- Orbot
- PlusMessenger
- Primo
- Psiphon VPN
- Signal
- Threema
- WhatsApp

_ATTACKS HAPPENED ON

> **January 2012: Dark Caracal First Mobile surveillance Campaign**
Happened on: 2012-01-01

> **Name: November 2012: Dark Caracal Phishing Campaign**
Happened on: 2012-11-01

> **June 2015: Operation Manul**
Happened on: 2015-06-01

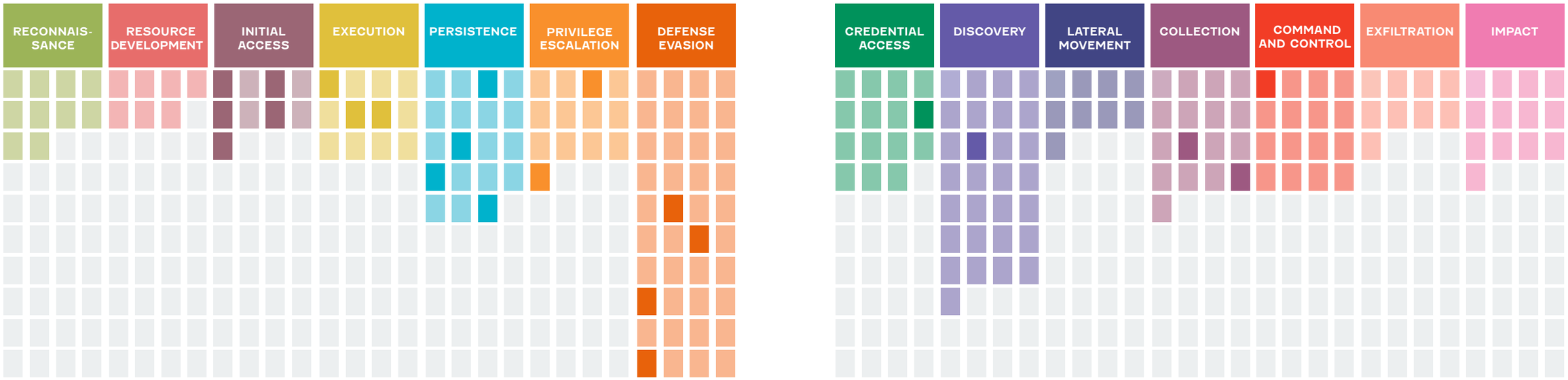
> **December 2016 - January 2018: Dark Caracal Mobile Surveillance Campaign**
Happened on: 2016-12-01

> **July 2020 to November 2020 : New wave of campaigns using a variant of the Backdoor Bandook**
Happened on: 2020-07-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1005 - Data from Local System
T1027 - Obfuscated Files or Information
T1027.002 - Software Packing
T1059 - Command and Scripting Interpreter
T1059.003 - Windows Command Shell
T1071 - Application Layer Protocol
T1071.001 - Web Protocols
T1078 - Valid Accounts
T1083 - File and Directory Discovery
T1106 - Native API
T1113 - Screen Capture
T1133 - External Remote Services
T1189 - Drive-by Compromise
T1195 - Supply Chain Compromise
T1204 - User Execution
T1204.002 - Malicious File
T1218.001 - Compiled HTML File
T1218.002 - Control Panel
T1547.001 - Registry Run Keys / Startup Folder
T1556.003 - Pluggable Authentication Modules
T1566.003 - Spearphishing via Service

_CYBER ATTACK PHASES



Threat Actor_

ATK29
(aka: The TEMP.Periscope or Leviathan group, grouped together with the TEMP.Jumper group); is a state-owned group of Chinese origin.
_Type of attacker: State Sponsored

Alias_

_APT 40
_APT40
_BRONZE MOHAWK
_GADOLINIUM
_Kryptonite Panda
_Leviathan
_TEMP.Jumper
_TEMP.Periscope

Targeted Sectors_

_Transportation
_Research
_Naval
_Maritime transport
_International Organizations
_High-Tech
_Government and administration agencies
_Education
_Engineering
_Defence
_Communication
_Chemicals
_Aerospace

Motivations_

_Information theft
_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

NORTHERN EUROPE
Norway

WESTERN EUROPE
Belgium
Germany
United Kingdom Of Great Britain And Northern Ireland
Switzerland

MIDDLE EAST/ WESTERN ASIA
Saudi Arabia

SOUTH EAST ASIA
Philippines
Malaysia
Cambodia

EASTERN ASIA
Hong Kong

Suspected origin of the attacker_

China

_DESCRIPTION

ATK29 - Known for their attacks on foreign maritime systems to extract data necessary for the development of Chinese navy skills, as well as for its geostrategic use in the context of the New Silk Roads project. This group also campaigned against the Cambodian government in the general elections of 29 June 2018.
The infrastructure used in this attack shares many similarities with that used in campaigns against the maritime domain. These similarities allow us to reinforce the conclusions that link the group to these two different campaigns and that establish the Chinese origin of the latter.
FireEye links the two groups TEMP.Periscope and TEMP.Jumper definitively in a report published in March 2019. Since March 2019, there has been a paradigm shift and a change in the sectors targeted by the group. Thus, while the group had mainly targeted maritime companies in order to catch up with the Chinese Navy, it is increasingly targeting political organizations in Southeast Asia. The purpose of these spying actions is to support the Chinese Silk Roads project on freight transport infrastructure projects.
ATK29 is a group whose campaigns obey the Chinese needs for technological catch-up and Beijing's diplomatic ambitions. The group is always very active, and is composed of competent people. Its arsenal is composed of many tools, which are regularly changed. It is quite reactive and has, in the past, used security vulnerabilities only a few days after their publication. Many of the tools used by this group are also used by other Chinese state attackers, suggesting exchanges of skills and tools between different sections. In addition, the group shared its infrastructure with another group of Chinese attackers, Hellsing.
In January 2020, the group was observed targeting Malaysian Government officials. The attack goal was probably data exfiltration.

_USED MALWARES

- BLACKCOFFEE
- BadFlick
- China Chopper
- Dadbod
- Derusbi
- Eviltech
- Grillmark
- HOMEFRY
- MURKYTOP
- NanHaiShu
- Orz
- PlugX
- Scanbox
- ZXShell
- gh0st RAT

_USED TOOLS

- Cobalt Strike
- Living off the Land
- LunchMoney
- Windows Credential Editor

_USED VULNERABILITIES

- CVE-2014-6352
- CVE-2017-0199
- CVE-2017-11882
- CVE-2017-8759

_ATTACKS HAPPENED ON

> **Leviathan Campaign**
Happened on: 2014-01-08

> **NanHaiShu Campaign**
Happened on: 2015-03-08

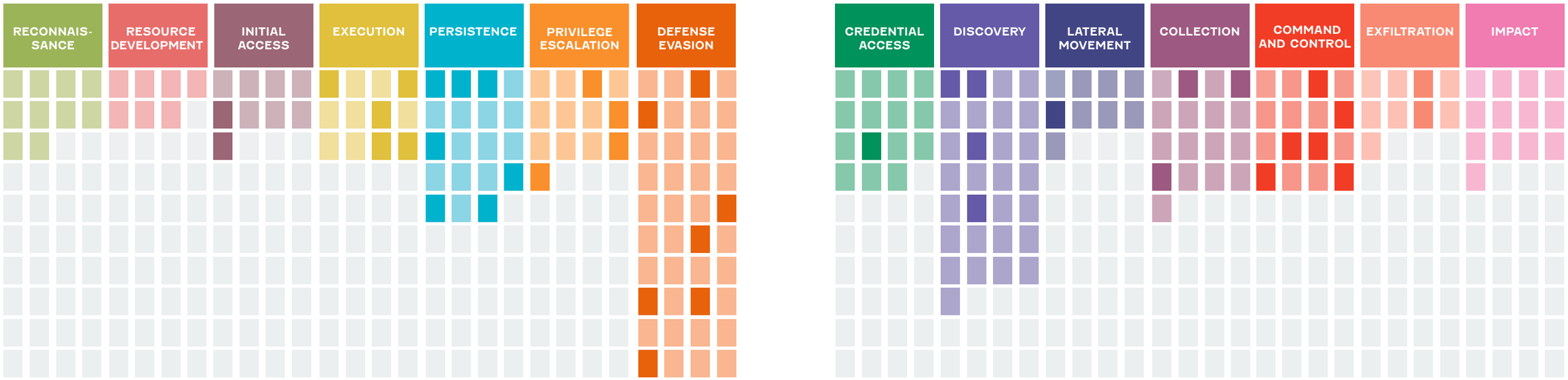
> **Temp.Periscope Targets Cambodia**
Happened on: 2018-07-08

> **February 2020 - takes advantage of the crisis in Malaysia to target government officials**
Happened on: 2020-02-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1003.001 - LSASS Memory
T1010 - Application Window Discovery
T1021 - Remote Services
T1021.001 - Remote Desktop Protocol
T1021.004 - SSH
T1027 - Obfuscated Files or Information
T1027.001 - Binary Padding
T1571 - Non-Standard Port
T1047 - Windows Management Instrumentation
T1048 - Exfiltration Over Alternative Protocol
T1053 - Scheduled Task/Job
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1059.005 - Visual Basic
T1074 - Data Staged
T1074.001 - Local Data Staging
T1078 - Valid Accounts
T1083 - File and Directory Discovery
T1087 - Account Discovery
T1090.003 - Multi-hop Proxy
T1095 - Non-Application Layer Protocol
T1098 - Account Manipulation
T1102 - Web Service
T1102.003 - One-Way Communication
T1105 - Ingress Tool Transfer
T1112 - Modify Registry
T1119 - Automated Collection
T1132 - Data Encoding
T1140 - Deobfuscate/Decode Files or Information
T1197 - BITS Jobs
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1204.001 - Malicious Link
T1204.002 - Malicious File
T1218.010 - Regsvr32
T1505.003 - Web Shell
T1546.003 - Windows Management Instrumentation Event Subscription
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1553.002 - Code Signing
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1567.002 - Exfiltration to Cloud Storage

_CYBER ATTACK PHASES



Threat Actor_

ATK3

This threat group represents the Bureau 121 which is one of the eight Bureaus associated to the Reconnaissance General Bureau. The Bureau 121 is the primary office tasked with cyber operations.

_Type of attacker: State Sponsored

Alias_

_COVELLITE
_Hidden Cobra
_Lazarus
_Lazarus Group

Targeted Sectors_

_Military
_Media
_Manufacturing
_Healthcare
_Government and administration agencies
_Financial Services
_Energy
_Aerospace

Targeted Areas_

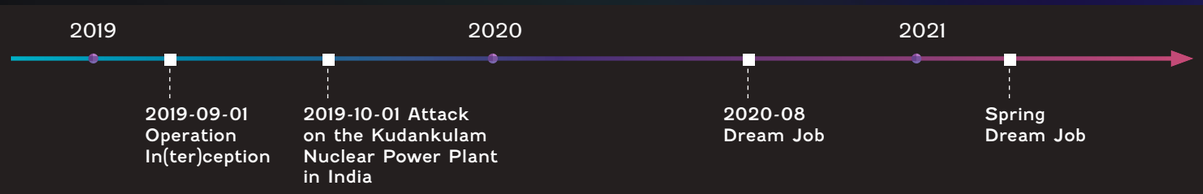
NORTH AMERICA
United States Of America

SOUTH EAST ASIA
Korea

SOUTHERN ASIA
India

Suspected origin of the attacker_

North Korea



_DESCRIPTION

The International Context as a Driver of the North Korean Cyber Strategy.

_Recent history implications

Asia's recent geopolitics is not only structured by China's economic and informational stranglehold, via new international institutions and vassalized digital champions, but also by North Korea, whose recent policies remain difficult to pin down. North Korea's foreign policy orientations are nevertheless indexed to the confrontation with the United States.

It should be recalled that in February 2007 relations between the two countries were due to be normalized following a bilateral agreement signed in Beijing to record the closure of the Yongbyon power station. However, one year after the agreement, North Korea announced the reopening of this power station before firing a Unha-2 rocket which was supposed to carry a communications satellite in April 2009. However, according to military security experts, it was a ballistic missile. Since then, relations have fluctuated between tension and calm as North Korea under embargo is caught by the throat. In order to calm its adversary, the United States is providing food aid in exchange for a restraint effort. However, the aid is not enough, and North Korea has no other choice but to repeat its pressure or to resort to perilous barter. Therefore, for decades, North Korea has been exchanging arms with countries such as Syria, Iran, Congo, Myanmar, Eritrea or Yemen in exchange for food. The year 2018 is interesting from this point of view, since the paradigm of relations between the United States and North Korea has taken an unexpected turn.

_A new relationship with the United States?

After months of great tension between Donald J. Trump and Kin Jung Un, which caused the international community to fear a nuclear incident, the North Korean leader proposed to the American President a meeting to discuss his country's military nuclearization. Prior to the meeting on 12 June 2018, Kim Jung Un redesigned the North Korean army and said he wanted to maintain "the momentum of appeasement with the United States and its willingness to eventually give up its nuclear deterrent. The summit resulted in a joint statement: Joint Statement of President Donald J. Trump of the United States of America and Chairman Kim Jong Un of the Democratic People's Republic of Korea at the Singapore Summit. Four main points emerged from this statement.

First, the United States and North Korea are committed to establishing a new relationship in accordance with the desire of the people of both countries for peace and prosperity. Second, the two countries will join efforts to establish a lasting and stable peace regime on the Korean Peninsula. Thirdly, by reaffirming the Panmunjeom Declaration of 27 April 2018, North Korea is committed to working towards the complete denuclearization of the Korean peninsula. Finally, the two States undertake to recover the bodies of prisoners of war and missing in action, including the immediate repatriation of those already identified. The declaration also mentions that D.J. Trump undertakes to provide security guarantees to North Korea in return.

_Cyber as a new strategic lever for North Korean ambitions

How can we understand this turnaround in the geopolitical situation? A potential answer: a new cyber strategy.

North Korea is not to be outdone in this respect. Already in December 2017, the peninsular state had already distinguished itself with the WannaCry malware affair. In a quasi-joint statement, the United States and Great Britain stated that North Korea was behind this massive attack, which affected almost 300,000 computers in 150 countries and caused billions of dollars in damage. While no hard evidence was provided, Thomas Bossert, who is assisting the US President, said that Australia, Canada and New Zealand shared the same conclusions. The NCSC was more specific in its statement, saying that the North Korean piracy group Lazarus was almost certainly behind the attack. In May 2017 the contaminated computers were instantly locked down and users were asked to pay a ransom in exchange for the restoration of their data. Europol described the scale of the attack as «unprecedented». Already in 2014, North Korea had attacked Sony Pictures. Due to the scale of the damage, the U.S received help from Microsoft and Facebook to counter WannaCry. Microsoft in a publication confirmed the statements of the British NCSC and stated that «by working with Facebook and other members of the security community, we have taken strong measures to protect our customers and the Internet from ongoing attacks by an advanced player in the persistent threats known as ZINC also known as the Lazarus Group». The attack, while reaching known geopolitical enemies such as Britain, whose Health National Service (NHS) was hit hard, also spread to states relatively close to North Korea such as Russia. The country's postal services were also severely disrupted.

_A cyber tool at the service of the regime's domestic and foreign policy

North Korea is using its cyber capabilities for two geopolitical purposes. First, as with the Sony and WannaCry attacks, the country is very simply targeting its classic geopolitical enemies. In June 2018, for example, North Korean hackers targeted a South Korean think tank specializing in national security issues. The hackers took advantage of a zero-day to compromise the organization's website and insert a backdoor for code injection. Earlier in April 2018, Chinese state-sponsored hacking groups targeted Japanese defence companies to obtain information on Tokyo's policy towards North Korea. This information was likely shared. In May it was the Google Play application that

was hacked. Compromised Android applications, hosted on Google Play, were stealing information from the devices and allowing the insertion of codes stealing photos, contact lists and SMS messages.

In addition to these direct attacks or cyber-espionage actions of geopolitical origin, North Korea uses cyber-espionage as a repercussion of geopolitical situations. As we mentioned, the country has to use barter to support itself and to circumvent the Western embargo. Cyber-attacks have become the new tool of this North Korean policy of survival. In August 2018, the Indian bank Cosmos was robbed of 13.5 million dollars by North Korean hackers who, after penetrating the structure's banking system and making thousands of unauthorized ATM withdrawals, made several illegal money transfers via the SWIFT financial network. The same technique was used, and the same consequences were seen in April 2018 at a Central American online casino with the aim of siphoning off funds. Finally, although there are many examples, as early as March 2018 the group of hackers in question targeted several major Turkish banks and government funding agencies.

_What does Lazarus really mean?

The North Korean cyber threat structure is unique. Several high-level groups exist with the characteristic of being dedicated to a specific function. However, all of these groups are linked to the North Korean military apparatus, in particular to Bureau 121 of the Reconnaissance General Bureau, which leads most sources to amalgamate them under a devoted name, Lazarus. Nevertheless, this concentration is detrimental to the analysis insofar as the Lazarus prism leads us to consider that only one group pursues the motivations of APT, cybercriminal, terrorist and hacktivist at the same time. We try as much as possible to specify the Lazarus sub-groups for adequate intelligence.
AKT3 or Lazarus is not a single Threat Group. It represents the Bureau 121 which is one of the eight Bureaus associated to the **Reconnaissance General Bureau**. The Bureau 121 is the primary office tasked with cyber operations. It was reorganized in September 2016 and it is now composed of:

• Lab 110
It is the key cyber unit under the RGB; it applies cyberattack techniques to conduct intelligence operations.

•Office 98
Primarily collects information on North Korean defectors, organizations that support them, overseas research institutes related to North Korea, and university professors in South Korea.

• Office 414
Gathers information on overseas government agencies, public agencies, and private companies.

• Office 35
Office concentrated on developing malware, researching and analyzing vulnerabilities, exploits, and hacking tools.

• Unit 180
Unit specialized in conducting cyber operations to steal foreign money from outside North Korea.

• Unit 91
- focuses on cyberattack missions targeting isolated networks, particularly on South Korea critical national infrastructure such as KHNP and the ROK Ministry of National Defense.
- stealing confidential information and technology to develop weapons of mass destruction.

• 128 and 413 Liaison Office
Responsible of hacking foreign intelligence websites and train cyber experts.

_The Bureau 121 conducted three main types of operations:

- Cyber espionage: The Lazarus Units conducted multiple cyber espionage operations such as the Kimsuki campaign and the Operation KHNP. These espionage operations have different objectives like the tracking of North Korean dissidents, the collection of intellectual properties helping the development of weapons of mass destruction or political espionage.
- Cyber Terrorism: in 2013 North Korea conducted disruptive attacks on South Korean media and financial companies (Operation DarkSeoul) and was responsible for the Sony hack link to the movie «The Interview» in November 2014. These attacks occured before the 2016 reorganization of the Bureau 121, that's why we can't tell which Unit is currently responsible of disruptive operations.
- Money theft: One of the mission of the Bureau 121 is the collection of liquidity to finance these cyber activities and the DPKR itself. It is done by spreading ransomware like the infamous WannaCry which collected $91.000 through bank robbery. The cyber bank robbery is done by infiltrating the banking network to steal the SWIFT credentials and use these credentials to initiate transactions to an account controlled by the attacker. The most known is Bangladesh Central Bank Heist in February 2016 allowing the theft of $81m. This activity was carried on by the Unit 180, which has similar objectives than the North Korean threat group APT38 aka Stardust Chollima or BlueNoroff.

_The Bureau 121 is supported by other Units from the General Staff Department

• The Operation Bureau
tasked to define cyber strategies and plan operations.

• The Command Automation Bureau
composed of three units:
- Responsible for malware development (seems redundant with the Office 35)
- Unit 32: responsible for military software development
- Unit 56: responsible for command and control software development

• The Enemy Collapse Sabotage Bureau
tasked with information and psychological warfare.

A cyber operation involves the interaction of these different teams. For example, the Operation Bureau defines an objective, the Office 35 finds a useable exploit, the Unit 31 develops the backdoor and the lure documents with the help of the Enemy Collapse Sabotage Bureau to create efficient spear-phishing document. The Unit 56 develops C2 software and maintains a C2 infrastructure which will be used by the Lab 110, Unit 180 or Unit 91 to achieve the objective. Due to this configuration, it is expected to find tools and infrastructure overlap between the different operation units.

_USED MALWARES

- CRAT
- DacIs
- MATA
- TFlower
- ThreatNeedle
- Vyveva

_USED VULNERABILITIES

- CVE-2016-0034
- CVE-2017-7269

_ATTACKS HAPPENED ON

> **Operation In(ter)ception**
Happened on: 2019-09-01

> **October 2019: Attack on the Kudankulam Nuclear Power Plant in India**
Happened on: 2019-10-01

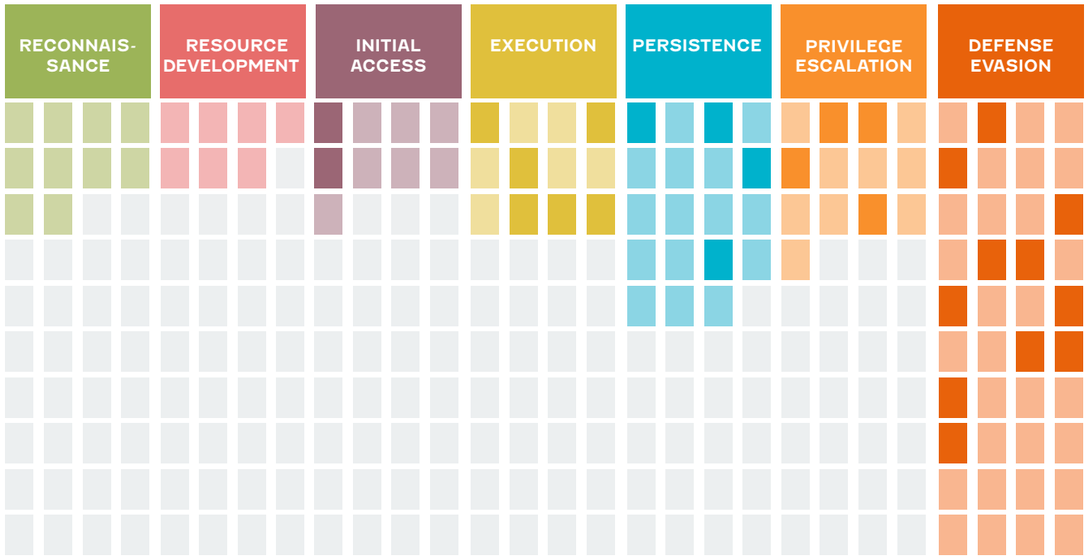
> **Dream Job**
Operation Dream Job involves Lazarus using fake job offers as a means of luring victims into revealing sensitive information about the company, or clicking on malicious links or opening malicious attachments that eventually lead to the installation of malware used for espionage
Happened on: 2020-08

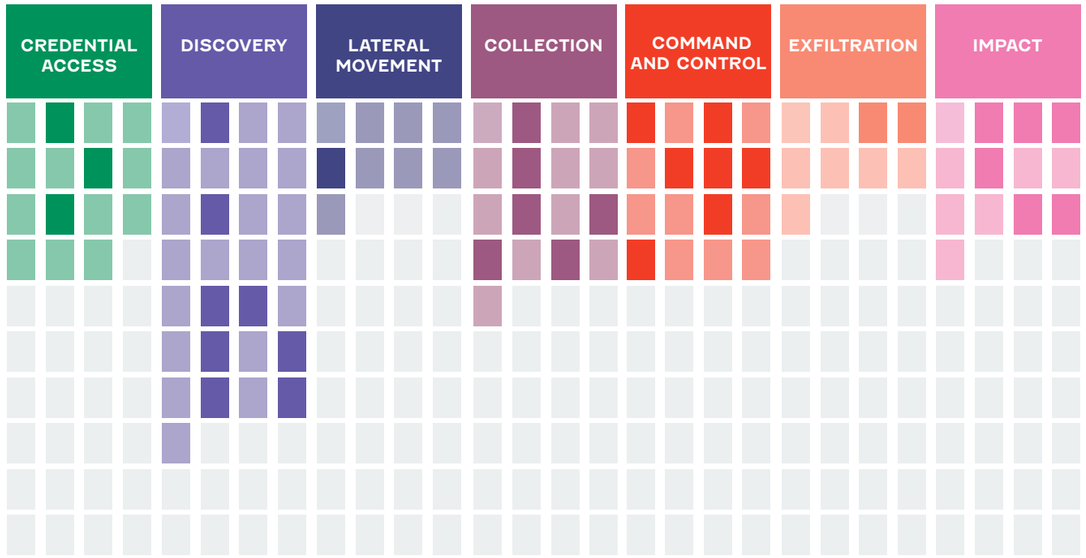
> **Dream Job**
Happened on: Spring 2021

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1005 - Data from Local System
T1008 - Fallback Channels
T1010 - Application Window Discovery
T1012 - Query Registry
T1016 - System Network Configuration Discovery
T1021.001 - Remote Desktop Protocol
T1021.002 - SMB/Windows Admin Shares
T1025 - Data from Removable Media
T1027 - Obfuscated Files or Information
T1027.002 - Software Packing
T1033 - System Owner/User Discovery
T1036.004 - Masquerade Task or Service
T1041 - Exfiltration Over C2 Channel
T1047 - Windows Management Instrumentation
T1048 - Exfiltration Over Alternative Protocol
T1055 - Process Injection
T1056 - Input Capture
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1070 - Indicator Removal on Host
T1070.004 - File Deletion
T1070.006 - Timestomp
T1071 - Application Layer Protocol
T1074 - Data Staged
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1090 - Proxy
T1098 - Account Manipulation
T1105 - Ingress Tool Transfer
T1106 - Native API
T1110 - Brute Force
T1112 - Modify Registry
T1115 - Clipboard Data
T1124 - System Time Discovery
T1132 - Data Encoding
T1134 - Access Token Manipulation
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1218.001 - Compiled HTML File
T1485 - Data Destruction
T1486 - Data Encrypted for Impact
T1489 - Service Stop
T1496 - Resource Hijacking
T1542.003 - Bootkit
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1547.010 - Port Monitors
T1560 - Archive Collected Data
T1560.002 - Archive via Library
T1561.001 - Disk Content Wipe
T1561.002 - Disk Structure Wipe
T1562.001 - Disable or Modify Tools
T1564.001 - Hidden Files and Directories
T1565.001 - Stored Data Manipulation
T1565.002 - Transmitted Data Manipulation
T1565.003 - Runtime Data Manipulation
T1566.001 - Spearphishing Attachment
T1569.002 - Service Execution
T1571 - on-Standard Port
T1573 - Encrypted Channel
T1573.001 - Symmetric Cryptography
T1573.002 - Asymmetric Cryptography

_CYBER ATTACK PHASES





Threat Actor_

ATK32
is a financially motivated group that is active since at least 2013, which primarily targets the retail, hospitality and restaurant sectors, mainly in the U.S..

Alias_

_FIN7
_GOLD NIAGARA
_MoneyTaker
_TAG-CR1

Targeted Sectors_

_Transportation
_Retail
_Media
_Hospitality
_High-Tech
_Healthcare
_Government and administration agencies
_Financial Services
_Energy
_Education
_Construction
_Communication
_Casino & Gaming

Motivations_

_Financial Gain

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland
France
Malte

OCEANIA
Australia

Suspected origin of the attacker_

Ukraine Russia

_DESCRIPTION

ATK32 - (aka: FIN7) is a financially motivated group that is active since at least 2013, which primarily targets the retail, hospitality and restaurant sectors, mainly in the U.S.. There are assumptions that this is the same group as Carbanak, but it appears that these are two separate groups using similar tools, and therefore are currently tracked separately. Its main goal is to steal financial assets from companies, such as debit cards, or to get access to financial data or computers of finance department employees in order to conduct wire transfers to offshore accounts. The group's often use phishing as their main attack vector, including tailored spear-phishing campaigns. In addition, the group used a front company dubbed «Combi Security», purportedly headquartered in Russia and Israel, to provide a guise of legitimacy and to recruit hackers to join the criminal enterprise.

_USED MALWARES

- Astra
- AveMaria
- BOOSTWRITE
- Bateleur
- Carbanak
- DNSbot
- GRIFFON
- HALFBAKED
- JSSLoader
- POWERSOURCE
- RDFSNIFFER
- SQLRat
- TEXTMATE
- Powerplant

_USED TOOLS

- Cobalt Strike
- Meterpreter
- TinyMe

_USED VULNERABILITIES

- CVE-2012-0158
- CVE-2013-3906
- CVE-2014-1761
- CVE-2017-11882

_ATTACKS HAPPENED ON

> **2017: Carbanak**
Happened on: 2017-01-01

> **February 2017: US-SEC filings**
Happened on: 2017-02-01

> **March 2017: FIN7 Fileless Malware Campaigns**
Happened on: 2017-03-01

> **April 2017: FIN7 uses Hidden Shortcut Files**
Happened on: 2017-04-01

> **June 2017: Evasive Restaurant Campaign**
Happened on: 2017-06-01

> **October 2017: FIN7 targets Banks and Enterprises**
Happened on: 2017-10-01

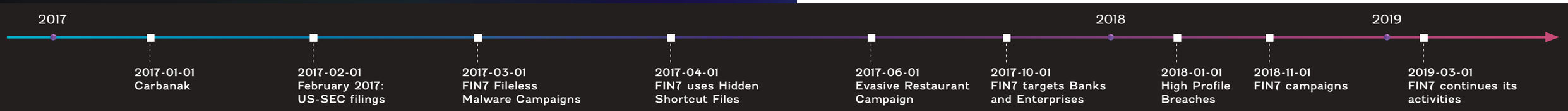
> **2018: High Profile Breaches**
Happened on: 2018-01-01

> **November 2018: FIN7 campaigns**
Happened on: 2018-11-01

> **March 2019: FIN7 continues its activities**
Happened on: 2019-03-01

> **August 2021 - FIN7 hackers target US companies with BadUSB devices to install ransomware**
Happened on: 2021-08

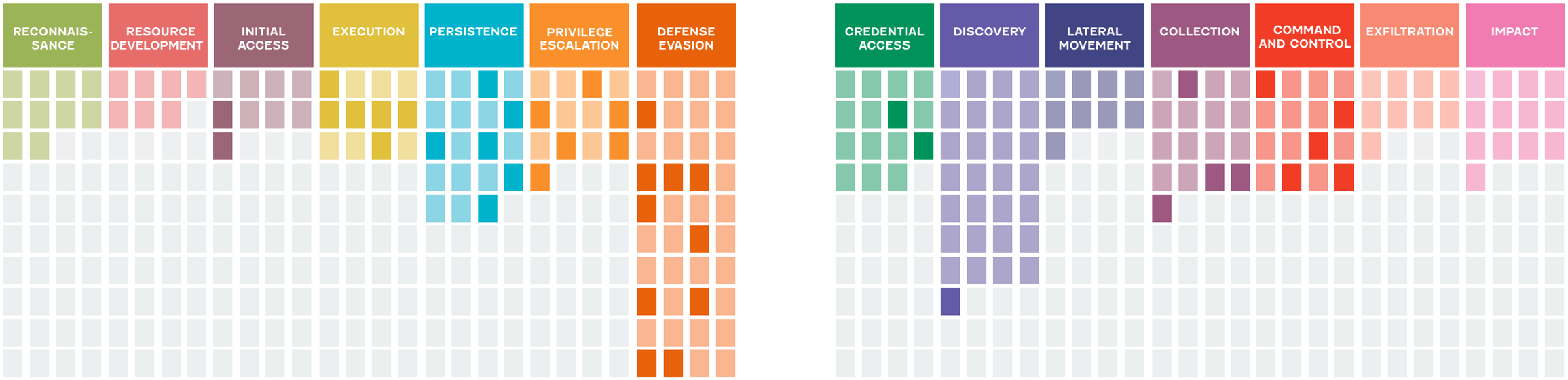
> **August 2021 - FIN7 Recon Campaign:**
Since late August, Infoblox has been tracking a campaign distributing JavaScript malware. The malware's command and control (C&C) domain, distribution method, and code are consistent with those of ATK32 (FIN7).
Happened on: 2021-08



_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1571 - Non-Standard Port
T1053 - Scheduled Task/Job
T1056.004 - Credential API Hooking
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1078 - Valid Accounts
T1102 - Web Service
T1105 - Ingress Tool Transfer
T1106 - Native API
T1113 - Screen Capture
T1125 - Video Capture
T1129 - Shared Modules
T1140 - Deobfuscate/Decode Files or Information
T1204 - User Execution
T1218.005 - Mshta
T1218.011 - Rundll32
T1219 - Remote Access Software
T1497 - Virtualization/Sandbox Evasion
T1543.003 - Windows Service
T1546.011 - Application Shimming
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1553.002 - Code Signing
T1558.003 - Kerberoasting
T1559.002 - Dynamic Data Exchange
T1560 - Archive Collected Data
T1562.001 - Disable or Modify Tools
T1566.001 - Spearphishing Attachment
T1574.001 - DLL Search Order Hijacking

_CYBER ATTACK PHASES



Threat Actor_

ATK33
is a cyber espionage group
active since at least 2009, with the objective to theft information.

Alias_

_PLATINUM
_TwoForOne

Targeted Sectors_

_Military
_International Organizations
_Government and administration agencies
_Financial Services
_Defence
_Communication

Motivations_

_Information theft

Targeted Areas_

SOUTH EAST ASIA
Malaysia
Indonesia

EASTERN ASIA
China

SOUTHERN ASIA
India

Suspected origin of the attacker_

Unknown

2012

2012-01-19
Platinum: EasternRoppls Campaign

_DESCRIPTION

ATK33 - The attacks of this adversory are different from those seen in untargeted or targeted attacks, which makes it peculiar in many ways. When part of the targeted attacks can be qualified as opportunistic: This group will prefer to modify their target profiles and geographic attack zones based on geopolitical events.

Thus, no target is immune in the world. ATK33's objective will be to steal sensitive intellectual property related to government interests, The group has systematically targeted specific governments organizations, defense institutes, intelligence agencies, diplomatic institutions and telecommunications providers in South and Southeast Asia. The recurrent use of spear phishing tactics (phishing attempts targeting specific individuals) and access to previously unknown zero-day exploits have made it a very resilient threat.

For initial access it uses mainly spear-phishing, we have also seen the use of nuisance attacks against vulnerable browser plugins. It uses several zero-day exploits suggesting that this is a well-resourced group. ATK33 is less prolific in the field than ATK9 for example, but focuses on a small number per year trying to hide its infections with self-removing malware and using one-shot delivery servers. It often targets the private email accounts of its victims and uses them to access the organization's networks. It uses custom developed tools which are often updated to avoid detection. Its backdoors are configured to operate during the victim's working hours to hide network traffic from legitimate traffic. Interestingly, there is no code shared between their different backdoors.

The CnC infrastructure is a mixture of registered domains and free subdomains obtained through dynamic DNS providers. The group uses compromised infrastructure based in multiple countries.

Used lure documents often address controversial subjects to incite the reader to open them.

Based on Microsoft's investigations, here is a non-exhaustive list of ATK33 characteristics.

- Implementation of several cyber espionage campaigns since at least 2009.
- Concentration on a small number of campaigns per year, which reduces the risk of detection and helps the group to remain unnoticed and focused longer.
- Targeting of governments and related organizations in South and South East Asia. Using multiple unpatched vulnerabilities in zero-day exploits against its victims.
- Main method: Spear phishing Hiding its traces by automatic removal of malicious components or by using single mode server-side logic where remotely hosted malicious components are only allowed to load once.
- Harassment of its targets via their unofficial or private email accounts, to use them as a springboard to the planned organization's network.
- Use of malicious tools that are tailor-made and have the resources to update these applications often in order to avoid being detected.
- Configuring its backdoor malware to restrict its activities to victims' working hours, in an effort to disguise post-infection network activity from normal user traffic.
- Its espionage activity is not intended to achieve direct financial gain, but rather uses stolen information for indirect economic benefits.

_USED MALWARES

- ATMsol
- Dipsind
- Hot patcher
- JPIN
- adbupd

_USED TOOLS

- Living off the Land

_USED VULNERABILITIES

- CVE-2013-1331
- CVE-2013-7331
- CVE-2015-2545
- CVE-2015-2546

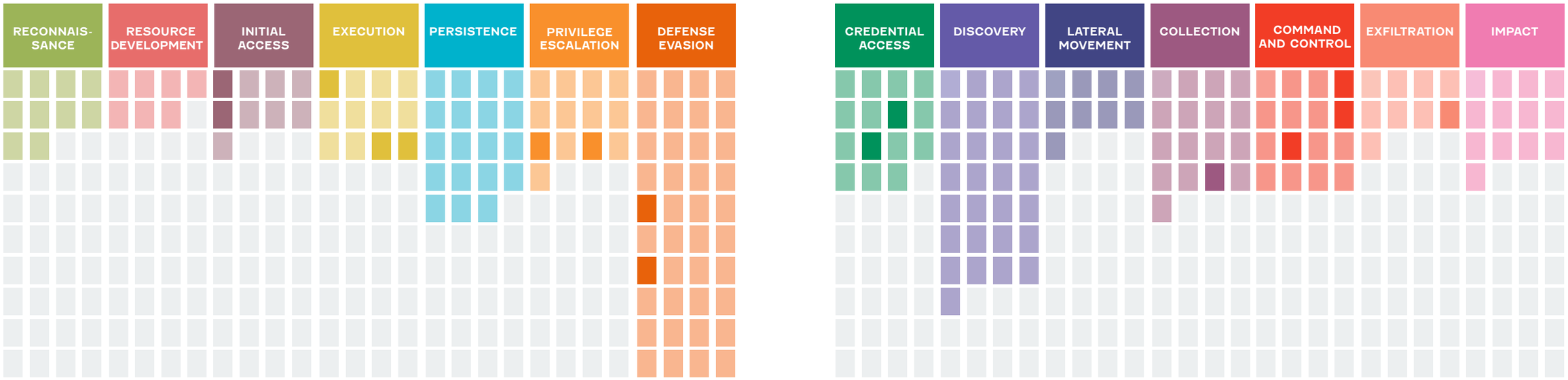
_ATTACKS HAPPENED ON

> **2012 - 2019 «Platinum: EasternRoppls Campaign»**
Happened on: 2012-01-19

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1003 - OS Credential Dumping
T1029 - Scheduled Transfer
T1036 - Masquerading
T1047 - Windows Management Instrumentation
T1055 - Process Injection
T1056 - Input Capture
T1056.004 - Credential API Hooking
T1059.001 - PowerShell
T1068 - Exploitation for Privilege Escalation
T1095 - Non-Application Layer Protocol
T1105 - Ingress Tool Transfer
T1189 - Drive-by Compromise
T1204 - User Execution
T1566.001 - Spearphishing Attachment

_CYBER ATTACK PHASES



Threat Actor_

ATK35
(aka: APT33 by Fireye)
is an Iranian cyberespionage group operating since approximately 2013.

_Type of attacker: State Sponsored

Alias_

_APT 33
_APT33
_COBALT TRINITY
_Elfin
_HOLMIUM
_MAGNALLIUM
_PARISITE
_Refined Kitten

Targeted Sectors_

_Research
_Media
_Manufacturing
_High-Tech
_Healthcare
_Government and administration agencies
_Financial Services
_Energy
_Education
_Dissident
_Defence
_Communication
_Chemicals
_Aviation
_Aerospace

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland

MIDDLE EAST/ WESTERN ASIA
Israel
Iraq
Iran
Saudi Arabia

EASTERN ASIA
Korea

Suspected origin of the attacker_

Iran

_DESCRIPTION

ATK35 - aka APT33 is an Iranian cyberespionage group operating since approximately 2013.
It is known to exploit fraudulent social media profiles to target individuals and organizations of interest through collecting credentials and infecting malware via an IRC-based variant of malware.

The breadth of the elaborate characters and fraudulent organizations created by ATK35 reveals that this adversary engages in a level of preparation and patience rarely seen with targeted intrusion efforts. This actor will also target third party service providers in order to compromise the organizations of interest.

ATK35 usually tries to access private emails and Facebook accounts, and sometimes establishes a foothold on victims' computers as a secondary focus.

The group's TTPs largely overlap with another group, ATK26 (aka Rocket Kitten), resulting in relationships that may not distinguish between the activities of the two groups.

_USED MALWARES

- AutoIt backdoor
- DownPaper
- Mimikatz
- NETWIRE
- Nanocore
- POWERBAND
- POWERTON
- Shamoon
- TURNEDUP

_USED TOOLS

- Living off the Land

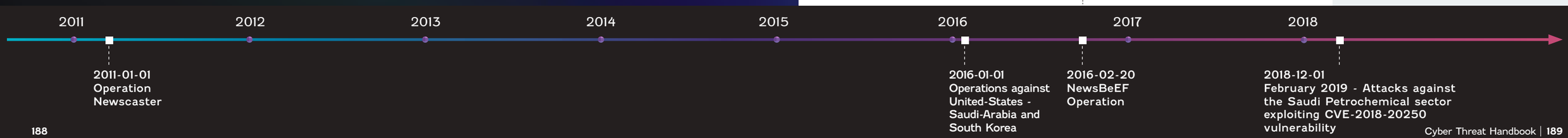
_ATTACKS HAPPENED ON

> **2011-2014 - Operation Newscaster**
Happened on: 2011-01-01

> **2016-2017 - Operations against United-States - Saudi-Arabia and South Korea**
Happened on: 2016-01-01

> **2016 - NewsBeEF Operation**
Happened on: 2016-02-20

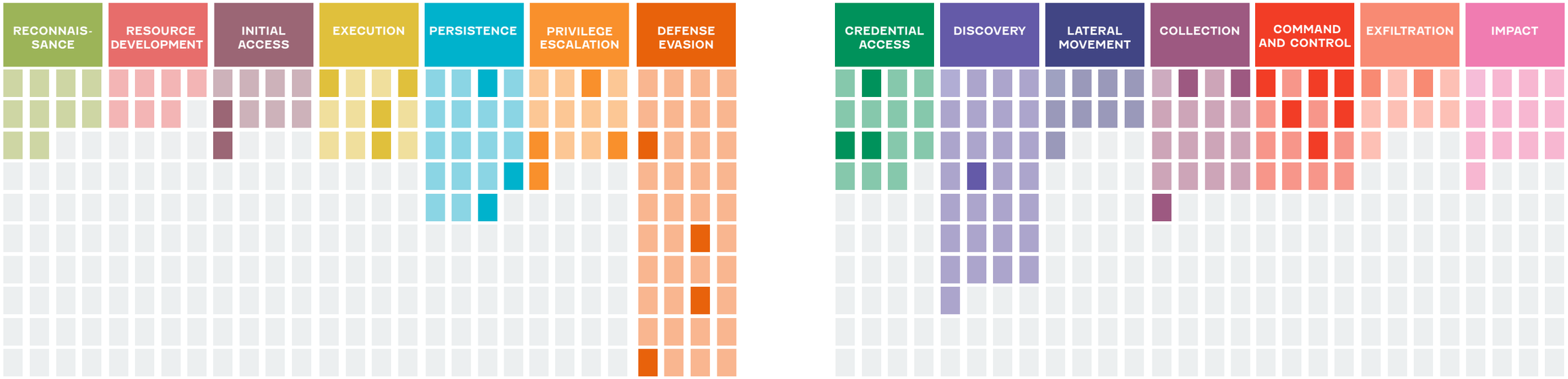
> **December 2018 - February 2019 - Attacks against the Saudi Petrochemical sector exploiting CVE-2018-20250 vulnerability**
Happened on: 2018-12-01



_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1003 - OS Credential Dumping
T1020 - Automated Exfiltration
T1027 - Obfuscated Files or Information
T1040 - Network Sniffing
T1041 - Exfiltration Over C2 Channel
T1048 - Exfiltration Over Alternative Protocol
T1053 - Scheduled Task/Job
T1059.001 - PowerShell
T1068 - Exploitation for Privilege Escalation
T1071 - Application Layer Protocol
T1078 - Valid Accounts
T1105 - Ingress Tool Transfer
T1110 - Brute Force
T1119 - Automated Collection
T1125 - Video Capture
T1132 - Data Encoding
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1480 - Execution Guardrails
T1547.001 - Registry Run Keys / Startup Folder
T1553.004 - Install Root Certificate
T1560 - Archive Collected Data
T1566.002 - Spearphishing Link
T1571 - Non-Standard Port
T1573 - Encrypted Channel

_CYBER ATTACK PHASES



Threat Actor_

ATK4
A North Korean cyber espionage group active since at least 2012, targeting several sectors mainly in South Korea.

_Type of attacker: State Sponsored

Alias_

_APT 37
_APT37
_Dark Seoul
_DarkSeoul
_Group 123
_Group123
_Operation Daybreak
_Operation Erebus
_Operation Erebus.
_Reaper
_Reaper Group
_Red Eyes
_Ricochet Chollima
_ScarCruft
_StarCruft
_TEMP.Reaper
_Venus 121

Targeted Sectors_

_Transportation
_Political Organizations
_Military
_Manufacturing
_High-Tech
_Healthcare
_Government and administration agencies
_Finance
_Energy
_Defence
_Chemicals
_Automotive
_Aerospace

Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland

EASTERN EUROPE
Romania

MIDDLE EAST/ WESTERN ASIA
Kuwait

SOUTH EAST ASIA
Vietnam

SOUTHERN ASIA
India
Nepal

EASTERN ASIA
China
Japan
Korea
Hong-kong

RUSSIA
Russian Federation

Suspected origin of the attacker_

North Korea

Languages_

_Korean

Motivations_

_Espionage

_DESCRIPTION

ATK4 - This group targets the public and private sectors mainly in South Korea. According to FireEye, the group's primary mission is to collect secret intelligence in support of North Korea's strategic military, political and economic interests. This actor is considered competent and resourceful.

Focusing on South Korean targets, this group can be compared to Unit 91 which has similar objectives. While from 2014 to 2017, ATK4 mainly targeted the South Korean government, defense, its industrial fabric and the media sector, ATK4 moved to more international targets with further attacks against the Middle East, Japan and the Vietnam. These new targets are all tied to North Korean interests.

This group uses spear phishing, strategic web compromises, or torrent file sharing as an initial infection vector. From 2014 to 2017, their decoy ducos were written in Korean and related to a theme relating to the Korean Peninsula. It uses various legitimate platforms like C2 and has access to several 0-day vulnerabilities.

The group can integrate newly revealed vulnerabilities into their toolset. This can be explained with the collaboration of different units within the North Korean General Reconnaissance Bureau.

ATK4 uses a C2 infrastructure made up of compromised servers, a messaging platform, cloud services and social networks to communicate or deploy its malware and avoid detection.

_USED MALWARES

- CORALDECK
- DOGCALL
- FinalIstSpy
- GELCAPSULE
- HAPPYWORK
- KARAE
- MILKDROP
- NavRat
- POORAIM
- RICECURRY
- ROKRAT
- RUHAPPY
- SHUTTERSPEED
- SLOWDRIFT
- SOUNDWAVE
- WINERACK
- ZUMKONG
- GoldBackdoor
- Chinotto

_USED VULNERABILITIES

- CVE-2013-0808
- CVE-2013-4979
- CVE-2014-8439
- CVE-2015-2387
- CVE-2015-2419
- CVE-2015-2545
- CVE-2015-3105
- CVE-2015-5119
- CVE-2015-5122
- CVE-2015-7645
- CVE-2016-1019
- CVE-2016-4117
- CVE-2017-0199
- CVE-2018-0802
- CVE-2018-4878

_ATTACKS HAPPENED ON

> **August 2016 - March 2017: Golden Time campaign**
Happened on: 2016-08-01

> **November 2016 - January 2017: Evil New Year campaign**
Happened on: 2016-11-01

> **May 2017: APT37 targets a Middle Eastern company (Freemilk campaign)**
Happened on: 2017-05-01

> **November 2017: North Korean Humain Rights campaign**
Happened on: 2017-11-01

> **January 2018: Evil New Year 2018 campaign**
Happened on: 2018-01-01

> **September 2018 : ScarCruft target a Russian organization related to North Korean affairs**
Happened on: 2018-09-01

> **2021 JAN - ATK4 campaign against the government of South Korea, used a Maldoc with VBA self-decoding technique to inject RokRat**
Happened on: 2021-01-01

> **2021 Jul - Spear phishing campaign pushing Konni Rat to target Russia**
Happened on: 2021-07-01

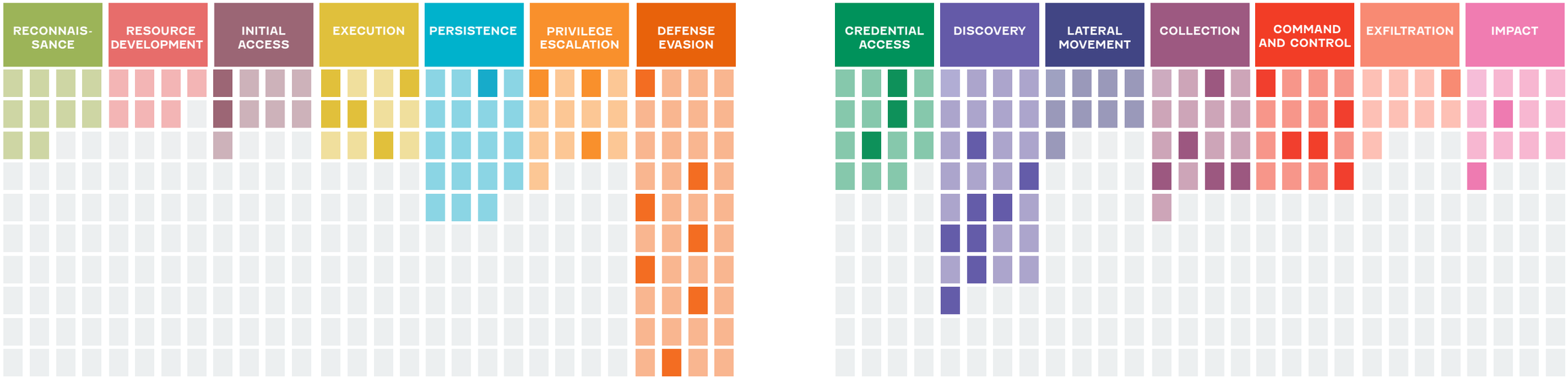
> **August 2021 - APT37 targets journalists with Chinotto multi-platform malware**
Happened on: 2021-08

> **March 2022 - North Korea-linked APT37 targets journalists with GoldBackdoor**
Happened on: 2022-03-18

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1005 - Da ta from Local System
T1012 - Query Registry
T1027 - Obfuscated Files or Information
T1027.002 - Software Packing
T1027.003 - Steganography
T1033 - System Owner/User Discovery
T1036.001 - Invalid Code Signature
T1041 - Exfiltration Over C2 Channel
T1571 - Non-Standart Port
T1055 - Process Injection
T1056 - Input Capture
T1056.001 - Keylogging
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.003 - Windows Command Shell
T1059.005 - Visual Basic
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1071.001 - Web Protocols
T1074 - Data Staged
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1095 - Non-Application Layer Protocol
T1102 - Web Service
T1102.002 - Bidirectional Communication
T1105 - Ingress Tool Transfer
T1106 - Native API
T1113 - Screen Capture
T1120 - Peripheral Device Discovery
T1123 - Audio Capture
T1189 - Drive-by Compromise
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1204.002 - Malicious File
T1497 - Virtualization/Sandbox Evasion
T1497.001 - System Checks
T1518.001 - Security Software Discovery
T1529 - System Shutdown/Reboot
T1547.001 - Registry Run Keys / Startup Folder
T1548.002 - Bypass User Account Control
T1553.002 - Code Signing
T1555.003 - Credentials from Web Browsers
T1555.004 - Windows Credential Manager
T1559.002 - Dynamic Data Exchange
T1561.002 - Disk Structure Wipe
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link

_CYBER ATTACK PHASES



Threat Actor_

ATK40
(aka: OilRig, APT34) is an Iranian cyber espionage threat actor active since at least 2014, primarily operating in the Middle East region.

_Type of attacker: State Sponsored

Alias_

_APT 34
_APT34
_CHRYSENE
_Clayslide
_Crambus
_Greenbug
_Helix Kitten
_Helminth
_IRN2
_OilRig
_Twisted Kitten

Targeted Sectors_

_Transportation
_Hospitality
_High-Tech
_Healthcare
_Government and administration agencies
_Financial Services
_Energy
_Education
_Communication
_Chemicals
_Aviation
_Aerospace

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

MIDDLE EAST/ WESTERN ASIA
United Arab Emirates
Turkey
Saudi Arabia
Qatar
Lebanon
Kuwait
Israel
Azerbaijan

AFRICA
Mauritius

Suspected origin of the attacker_

Iran

_DESCRIPTION

ATK40 - The group targets as a priority the financial institutions of the Sunni Gulf States, but also the United States and Israel, traditional geopolitical opponents of the Republic of the Mullahs. During the OilRig campaign in 2016 against financial institutions in Saudi Arabia, the group demonstrated capabilities to adapt its procedures and to use multiple delivery methods, particularly through well-crafted spear-phishing messages relevant to the interests of targeted personnel and custom PowerShell implants like the Helminth backdoor. He relies heavily on the human factor for the initial access. After the first report by FireEye and PaloAlto, the group has been actively updating his tools and expanding his scope of targets (Qatar, Turkey, Israel and United States). The group continues to use communication through DNS Tunnelling to the command and control server to stay under the radar. In early 2017, the group demonstrated the ability to use digitally signed malware spread through fake websites (University of Oxford conference sign-up page and a job application website). PaloAlto observed an overlap in C&C IP address used by OilRig and used by Chafer for his Remexi backdoor C&C, suggesting that these groups are one entity or that they share resources. Furthermore, the similarity between the malware ISMAgent used by OilRig and ISMDoor used by GreenBug suggests a link between these groups.

This actor shows high capabilities of adaptation, creating new custom delivery documents and backdoor and using multiple TTP to re-infect previous targets who took actions to counter their known TTP. We did not observe this actor using a zero-day exploit, but it quickly used the CVE-2017-0199 and CVE-2017-11882 which are widely used to improve the quality of his lure documents.

DragoS considers that ATK40 (OilRig) and ATK59 (Greenbug) are the same threat group and carried out initial preparations and network intrusion in advance of the Shamoon event. This group test regularly its samples on anti-virus testers like VirusTotal to determine what content of their malwares are detected. This technique helped to build nearly undetected samples but allowed researchers to follow the modifications. In April 2019, multiple OilRig tools were leaked on a Github repository, including BONDUPDATER, the TwoFace WebShell and webmask, a tool linked to DNSpionage. This leak was followed in June 2019 by another about the tool Jason.

OilRig infrastructure is continuously growing but overlaps with previously used infrastructure. The group reuses his tools, uses the same attack protocols and has a consistent victimology which makes it easy to track down.

_USED MALWARES

- ALMA Communicator
- BONDUPDATER
- CANDYKING
- Clayslide
- GOLDIRONY
- Helminth
- ISMAgent
- ISMInjector
- Jason
- KEYPUNCH
- Karkoff
- LaZagne
- Mimikatz
- OopsIE
- POWBAT
- POWRUNER
- QUADAGENT
- RGDoor
- SEASHARPEE
- SideTwist
- TONEDEAF
- ThreeDollars
- TwoFace WebShell
- ZeroCleare

_USED TOOLS

- ConfuserEx
- Invoke-Obfuscation
- Living off the Land
- Net
- Plink
- PsExec
- Reg
- SmartAssembly .NET obfuscator
- SoftPerfect Network Scanner
- Tasklist
- netstat

_USED VULNERABILITIES

- CVE-2017-0199
- CVE-2017-11882
- CVE-2020-0688

_ATTACKS HAPPENED ON

> **2015 - October 2016: Wave of emails containing malicious attachments being sent to multiple organizations in the Middle East**
Happened on: 2015-06-15

> **Late 2016: OilRig set up a fake VPN Web Portal targeting Israeli organizations**
Happened on: 2016-10-24

> **Fox Kitten Campaign**
Happened on: 2017-01-01

2017
- **2017-04-19** Politically motivated targeted campaign carried out against numerous Israeli organizations

2018
- **2018-06-25** Attacks on Middle East entities
- **2018-11-01** Attack on the Telecommunication sector

2020
- **2020-01-01** Oilrig campaign on USA organizations
- **2020-01-27** Karkoff campaign against the Lebanon government
- **2020-03-01** TK40 (APT34) campaign leveraging Microsoft Exchange vulnerability

> **April 2017: Politically motivated targeted campaign carried out against numerous Israeli organizations**
Happened on: 2017-04-19

> **July 2017: Targeted attacks delivering ISMAgent**
Happened on: 2017-07-01

> **August 2017: Use of ISMInjector to deliver ISMAgent to an organization within the United Arab Emirates government**
Happened on: 2017-08-01

> **January 2018: Attack against an insurance agency based in the Middle East using OopsIE and the ThreeDollars delivery document**
Happened on: 2018-01-08

> **May - June 2018: Attack using QUADAGENT**
Happened on: 2018-05-01

> **Summer 2018: Attacks on Middle East entities**
Happened on: 2018-06-25

> **November 2018: Attack on the Telecommunication sector**
Happened on: 2018-11-01

> **January 2020: Oilrig campaign on USA organizations**
Happened on: 2020-01-01

> **Karkoff campaign against the Lebanon government**
Happened on: 2020-01-27

> **TK40 (APT34) campaign leveraging Microsoft Exchange vulnerability**
Happened on: 2020-03-01

Threat Actor_

ATK41
A threat group that appears to originate from China and has been active since approximately 2009.

_Type of attacker: State Sponsored

Alias_

_APT 10
_APT10
_BRONZE RIVERSIDE
_CVNX
_Cicada
_Cloud Hopper
_DustStorm
_HOGFISH
_POTASSIUM
_Red Apollo
_Stone Panda
_happyyongzi
_menuPass
_menuPass Team

Targeted Sectors_

_Media
_Manufacturing
_High-Tech
_Healthcare
_Government and administration agencies
_Financial Services
_Energy
_Defence
_Aerospace

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

CENTRAL AMERICA
Mexico

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland
France
Germany
Belgium

MIDDLE EAST/ WESTERN ASIA
United Arab Emirates

SOUTH EAST ASIA
Vietnam
Thailand
Singapore
Philippines

SOUTHERN ASIA
India

EASTERN ASIA
China
Japan
Korea
Hong-kong
Taiwan

Suspected origin of the attacker_

China

_DESCRIPTION

ATK41 - aka: APT10, Stone Panda, CVNX, MenuPass Group, Potassium, Red Apollo, Hogfish, Cloud Hopper, DustStorm, Happyyongzi) is a threat group that appears to originate from China and has been active since approximately 2009. The group is also used to conduct supply chain attacks in order to infiltrate large groups to conduct industrial espionage campaigns. Among the preferred targets of this group are companies in the energy, high-tech and manufacturing sectors.

However, some of the attackers have been arrested by the US FBI. Indeed, on 17 December 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA , a.k.a. «Afwar», a.k.a. «CVNX», a.k.a. «Alayos», a.k.a. «Godkiller», and ZHANG SHILONG , a.k.a. «Baobilong», a.k.a. «Zhang Jianguo», a.k.a. «Atreexp». The defendants worked for Huaying Haitai
Science and Technology Development Company located in Tianjin, China, and acted in association with the Tianjin State Security Bureau of the Chinese Ministry of State Security.

_USED MALWARES

- ChChes
- EvilGrab
- Mimikatz
- Mis-Type
- Misdat
- PoisonIvy
-Sodamaster
- QuasarRAT
- RedLeaves
- S-Type
- SNUGRIDE
- UPPERCUT
- ZLib

_USED TOOLS

- Impacket
- Living off the Land
- Net
- Ping
- PowerSploit
- PsExec
- QuasarRAT
- certutil
- cmd
- pwdump

_USED VULNERABILITIES

- CVE-2020-1472

_ATTACKS HAPPENED ON

> **Dust Storm**
Happened on: 2010-01-01

> **MenuPass operation: APT10 expands its operations**
Happened on: 2016-01-01

> **Cloud Hopper: a targeted APT10 campaign**
Happened on: 2017-11-01

> **APT10: Campaign against Japan - North-Korea and South American personalities**
Happened on: 2018-01-01

> **APT10 targets government agencies in the Philippines and Southeast Asia**
Happened on: 2019-04-01

> **ATK41 (APT10, Stone Panda) spies on Japanese companies worldwide**
Happened on: 2019-10-15

> **February 2022 - APT10 disguised intrusions behind credential stuffing attack on Taiwanese financial sector**
Happened on: 2022-02

> **February 2022 - APT10 Espionage Attacks against US government**
Happened on: 2022-02

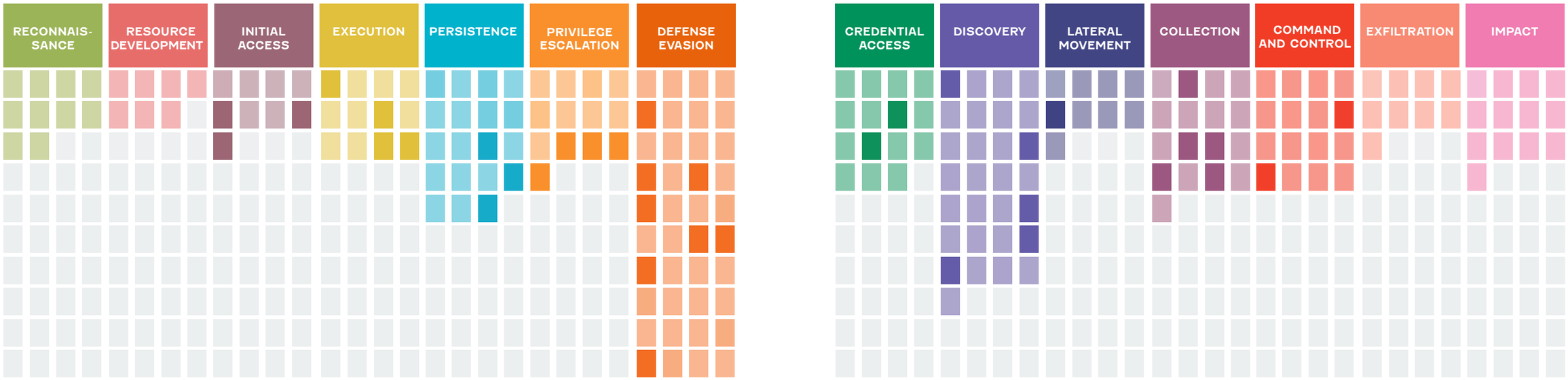
2010 2011 2012 2013 2014 2015 2016 2017 2018 2019

- 2010-01-01 Dust Storm
- 2016-01-01 MenuPass operation: APT10 expands its operations
- 2017-11-01 Cloud Hopper: a targeted APT10 campaign
- 2018-01-01 APT10: Campaign against Japan - North-Korea and South American personalities
- 2019-04-01 APT10 targets government agencies in the Philippines and Southeast Asia
- 2019-10-15 ATK41 (APT10, Stone Panda) spies on Japanese companies worldwide

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1005 - Data from Local System
T1016 - System Network Configuration Discovery
T1018 - Remote System Discovery
T1021 - Remote Services
T1021.001 - Remote Desktop Protocol
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1039 - Data from Network Shared Drive
T1046 - Network Service Scanning
T1047 - Windows Management Instrumentation
T1049 - System Network Connections Discovery
T1053 - Scheduled Task/Job
T1055.012 - Process Hollowing
T1056 - Input Capture
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1070.004 - File Deletion
T1074 - Data Staged
T1078 - Valid Accounts
T1087 - Account Discovery
T1090 - Proxy
T1105 - Ingress Tool Transfer
T1140 - Deobfuscate/Decode Files or Information
T1199 - Trusted Relationship
T1204 - User Execution
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1574.001 - DLL Search Order Hijacking
T1574.002 - DLL Side-Loading

_CYBER ATTACK PHASES



Threat Actor_

ATK5
(aka Sofacy, APT28) is a Russian state-sponsored group of attackers operating since 2004, whose main objective is to steal confidential information from political
and military targets that benefit the Russian government.

_Type of attacker: State Sponsored

Alias_

_APT 28
_APT28
_Fancy Bear
_Group 74
_Group-4127
_IRON TWILIGHT
_Pawn Storm
_PawnStorm
_SIG40
_SNAKEMACKEREL
_STRONTIUM
_Sednit
_Sofacy
_Swallowtail
_TAG_0700
_TG-4127
_Threat Group-4127
_Tsar Team
_TsarTeam
_apt_sofacy

Targeted Sectors_

_Universities
_Transportation
_Think Tank
_Political Organizations
_Media
_International Organizations
_Hospitality
_High-Tech
_Healthcare
_Government and administration agencies
_Energy
_Embassies
_Defence
_Defence contractors
_Cybersecurity
_Aerospace

Targeted Areas_

NORTH AMERICA
United States Of America
Canada

SOUTH AMERICA
Brazil

NORTHERN EUROPE
Sweden
Netherlands

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland
France
Spain
Germany
Belgium

EASTERN EUROPE
Belarus
Bulgaria
Hungary
Latvia
Ukraine
Slovakia
Poland
Romania
Montenegro

MIDDLE EAST/ WESTERN ASIA
Armenia
Azerbaijan
Georgia
Iran
Turkey
Saudi Arabiaz

CENTRAL ASIA
Kazakhstan
Tajikistan

SOUTH EAST ASIA
Malaysia

EASTERN ASIA
China
Japan
Korea
Mongolia

SOUTHERN ASIA
Afghanistan

Languages_

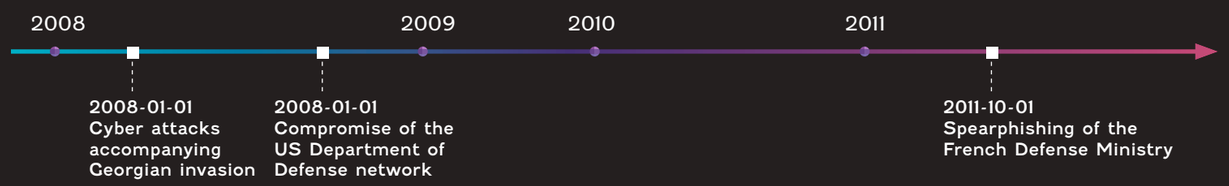
_Russian _Georgian

Suspected origin of the attacker_

Russia

Motivations_

_Political Manipulation
_Espionage



_DESCRIPTION

ATK5 - It is a skilled team which has the capabilities to develop complex modular malwares and exploit multiple zero-days. Their malwares are compiled with Russian language setting and during the Russian office working hours. Despite number of public disclosure from European governments and indictments from the U.S. Department of Justice, this adversary continues to launch operations targeting the political and defense sector in Europe and Eurasia.

Between 2007 and 2014, ATK5 had three kinds of targets:

- Georgian government agencies (Ministry of Internal Affairs and Ministry of Defense) or citizens
- Eastern European governments
- Security organisations

The attack of the Georgian Ministry of Defense can be a response to the growing U.S.-Georgian military relationship. In 2013, the group targeted a journalist which is a way to monitor public opinion, spread disinformations or identify dissident.

During 2015 and 2016, this group activity increased significantly, with numerous attacks against government departments and embassies all over the world.

Among their most notable presumed targets are the American Democratic National Committee, the German parliament and the French television network TV5Monde. ATK5 seems to have a special interest in Eastern Europe, where it regularly targets individuals and organizations involved in geopolitics. They also have been implicated in the U.S. presidential election attacks in late 2016.

The 2016 attacks were visible and disruptive but in 2017 the group operated a great change to more stealthy attacks to gather intelligence about a range of targets.

One of the striking characteristics of ATK5 is its ability to come up with brand-new zero-day vulnerabilities regularly. In 2015, the group exploited no fewer than six zero-day vulnerabilities. This high number of zero-day exploits suggests significant resources available, either because the group members have the skills and time to find and weaponize these vulnerabilities, or because they have the budget to purchase the exploits. In addition, APT28 tries to profile its target system to deploy only the needed tools. This prevents researchers from having access to their full arsenal.

_USED MALWARES

- ADVSTORESHELL
- Blitz backdoor
- CORESHELL
- Cannon
- DealersChoice
- Delphocy
- Downdelph
- Drovorub
- HIDEDRV
- JHUHUGIT
- Komplex
- LoJax
- OLDBAIT
- USBStealer
- X-Agent
- X-Agent for Android
- XAgentOSX
- XTunnel
- Zebrocy

_USED TOOLS

- Forfiles
- Koadic
- Living off the Land
- Mimikatz
- Responder
- Winexe
- certutil

_USED VULNERABILITIES

- CVE-2010-3333
- CVE-2012-0158
- CVE-2013-1347
- CVE-2013-3897
- CVE-2013-3906
- CVE-2014-0515
- CVE-2014-1761
- CVE-2014-1776
- CVE-2014-4076
- CVE-2015-1641
- CVE-2015-1642
- CVE-2015-1701
- CVE-2015-2387
- CVE-2015-2424
- CVE-2015-2590
- CVE-2015-3043
- CVE-2015-4902
- CVE-2015-5119
- CVE-2015-7645
- CVE-2016-7255
- CVE-2016-7855
- CVE-2017-0144
- CVE-2017-0262
- CVE-2017-0263
- CVE-2020-0688
- CVE-2020-17144

_ATTACKS HAPPENED ON

> **2008: Cyber attacks accompanying Georgian invasion**
Happened on: 2008-01-01

> **2008: Compromise of the US Department of Defense network**
Happened on: 2008-01-01

> **2011: APT28 use lure written in Georgian**
Happened on: 2011-01-01

> **October 2011: Spearphishing of the French Defense Ministry**
Happened on: 2011-10-01

> **January 2012: Spearphishing on the Vatican embassy in Iraq**
Happened at: 2012-01-01

> **Mid-2013: Targeting the Georgian Ministry of Internal Affairs**
Happened on: 2013-01-01

> **Late-2013: Targeting an Eastern European Ministry of Foreign Affairs**
Happened on: 2013-07-01

> **September 2013: Spearphishing on Military officials**
Happened on: 2013-09-01

> **January 2014: Spearphishing on Pakistanes military officials**
Happened on: 2014-01-01

> **2014 - 2016: APT28 uses Android X-Agent to track Ukrainian artillery**
Happened on: 2014-01-01

> **August 2014: Attempt to compromise the Polish government**
Happened on: 2014-08-01

> **September 2014: Typosquatting of European defense exhibition**
Happened on: 2014-09-01

> **October 2014 - September 2015: Operation PawnStorm**
Happened on: 2014-10-01

> **April-Mai 2015: Attack on the German Parliament**
Happened on: 2015-04-01
Summer 2015: Sofacy attack waves
Happened on: 2015-01-01

> **February - April 2015: APT28 compromised TV5Mond**e
Happened on: 2015-02-01

> **April 2015: Operation RussianDoll**
Happened on: 2015-04-01

> **May 2015: APT28 targets the Ukrainian Central Election Commission**
Happened on: 2015-05-01

> **August 2015: APT28 targets Russian rockers and dissidents Pussy Riot**
Happened on: 2015-08-01

> **September 2020: ATK5 (APT28) targets NATO member governments, Middle East governmets adn Azerbaijan**
government with Zebrocy backdoor
Happened on: 2015-11-01

> **Spring 2016: APT28 attacks the U.S. Democratic National Committee**
Happened on: 2016-01-01
> **Summer 2016: APT28 attacks the World Anti-Doping Agency (WADA)**
Happened on: 2016-01-01

> **March 2016: APT28 targets Hillary Clinton Presidential Campaign**
Happened on: 2016-03-01

> **April - May 2016: APT28 targets the Germany's Christian Democratic Union**
Happened on: 2016-04-01

> **May 2016: Spear-phishing attack against a U.S. government entity**
Happened on: 2016-05-01

> **November 2016: APT28 targets the Organization for Security and Co-operation in Europe (OSCE)**
Happened on: 2016-11-01

> **July 2017: APT28 targets the hospitality sector in Europe and MiddleEast**
Happened on: 2017-07-01

> **October 2017: Spearphishing using a new lure document about the Cyber Conflict U.S. conference**
Happened on: 2017-09-01

> **February - October 2018: APT28 attacks various Ministries of Foreign Affairs around the world**
Happened on: 2018-02-01

> **October 4, 2018 - APT28 targets the Organization for the prohibition of chemical weapons**
Happened on: 2018-10-04

> **Late-2013: Targeting a Journalist Covering the Caucasus**
Happened on: 2019-07-01

> **2021 March - ATK5's attack campaign against Kazakhstan**
Happened on: 2021-02-19

> **2021 Jan - ATK5 Leads Global Brute Force Campaign to Compromise Enterprise and Cloud Environments Around the Globe**
Happened on: 2021-08-31

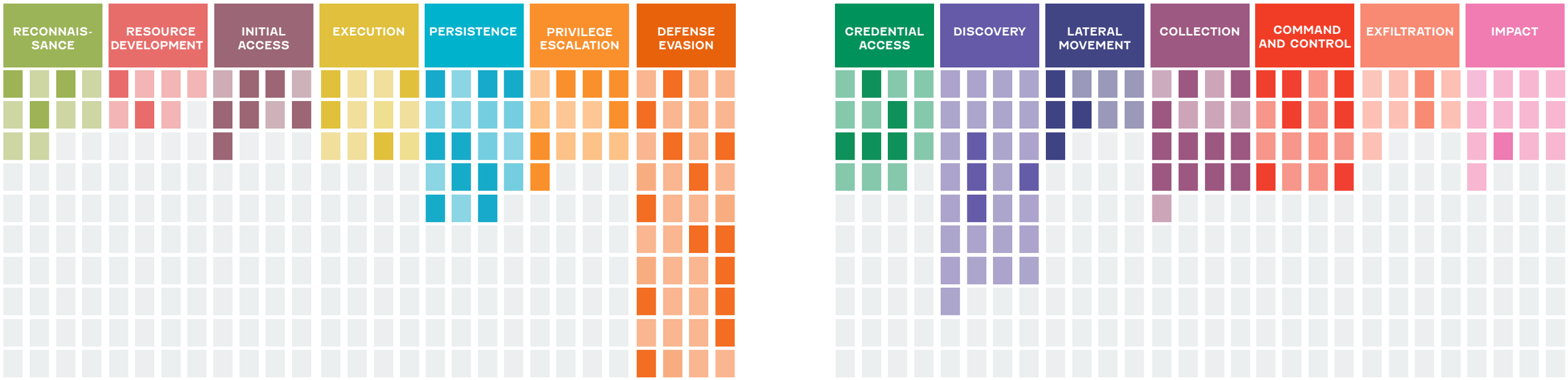
> **September 2021 - 14,000 Gmail users targeted by APT28**
Happened on: 2021-09

> **March 2022 - APT28 phishing campaigns targeting UkrNet**
Happened on: 2022-03

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1001.001 - Junk Data
T1003 - OS Credential Dumping
T1003.001 - LSASS Memory
T1003.003 - NTDS
T1005 - Data from Local System
T1014 - Rootkit
T1021.002 - SMB/Windows Admin Shares
T1025 - Data from Removable Media
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1036.005 - Match Legitimate Name or Location
T1037 - Boot or Logon Initialization Scripts
T1037.001 - Logon Script (Windows)
T1039 - Data from Network Shared Drive
T1040 - Network Sniffing
T1048.002 - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1056 - Input Capture
T1056.001 - Keylogging
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1068 - Exploitation for Privilege Escalation
T1070 - Indicator Removal on Host
T1070.001 - Clear Windows Event Logs
T1070.004 - File Deletion
T1070.006 - Timestomp
T1071 - Application Layer Protocol
T1071.001 - Web Protocols
T1071.003 - Mail Protocols
T1074 - Data Staged
T1074.001 - Local Data Staging
T1074.002 - Remote Data Staging
T1078 - Valid Accounts
T1078.004 - Cloud Accounts
T1083 - File and Directory Discovery
T1090 - Proxy
T1090.002 - External Proxy
T1090.003 - Multi-hop Proxy
T1091 - Replication Through Removable Media
T1092 - Communication Through Removable Media
T1098.002 - Exchange Email Delegate Permissions
T1102.002 - Bidirectional Communication
T1105 - Ingress Tool Transfer
T1110 - Brute Force
T1110.001 - Password Guessing
T1110.003 - Password Spraying
T1113 - Screen Capture
T1114 - Email Collection
T1114.002 - Remote Email Collection
T1119 - Automated Collection
T1120 - Peripheral Device Discovery
T1133 - External Remote Services
T1134 - Access Token Manipulation
T1134.001 - Token Impersonation/Theft
T1137 - Office Application Startup
T1137.002 - Office Test
T1140 - Deobfuscate/Decode Files or Information
T1190 - Exploit Public-Facing Application
T1199 - Trusted Relationship
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1204.001 - Malicious Link
T1204.002 - Malicious File
T1210 - Exploitation of Remote Services
T1211 - Exploitation for Defense Evasion
T1213 - Data from Information Repositories
T1213.002 - Sharepoint
T1218.011 - Rundll32
T1221 - Template Injection
T1498 - Network Denial of Service
T1505.003 - Web Shell
T1528 - Steal Application Access Token
T1542.003 - Bootkit
T1546.015 - Component Object Model Hijacking
T1547.001 - Registry Run Keys / Startup Folder
T1550.001 - Application Access Token
T1550.002 - Pass the Hash
T1559.002 - Dynamic Data Exchange
T1560 - Archive Collected Data
T1560.001 - Archive via Utility
T1564.001 - Hidden Files and Directories
T1564.003 - Hidden Window
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1567 - Exfiltration Over Web Service
T1573 - Encrypted Channel
T1573.001 - Symmetric Cryptography
T1583.001 - Domains
T1588.001 - Malware
T1588.002 - Tool
T1589.001 - Credentials
T1595.002 - Vulnerability Scanning
T1598 - Phishing for Information

_CYBER ATTACK PHASES



Threat Actor_

ATK51
An Iranian threat group targeting primarily Middle Eastern nations. However, attacks against surrounding nations and beyond, including targets in India and the USA, have also been observed.

Alias_

_MERCURY
_MobhaM
_MuddyWater
_NTSTATS
_POWERSTATS
_Seedworm
_Static Kitten
_TEMP.Zagros

Targeted Sectors_

_Media
_International Organizations
_High-Tech
_Healthcare
_Government and administration agencies
_Financial Services
_Energy
_Education
_Defence

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

AFRICA
Mali

EASTERN EUROPE
Austria

MIDDLE EAST/ WESTERN ASIA
Azerbaijan
Bahrain
Iraq
Israel
Georgia
Iran
Jordan
Saudi Arabia
United Arab Emirates
Turkey

SOUTHERN ASIA
India
Pakistan

RUSSIA
Russian Federation

Suspected origin of the attacker_

Iran

_DESCRIPTION

ATK51 - MuddyWater attacks are characterized by the use of a slowly evolving PowerShell-based first stage backdoor we call "POWERSTATS. Despite broad scrutiny and reports on MuddyWater attacks, the activity continues with only incremental changes to the tools and techniques.

_USED MALWARES

- Mori
- MuddyC3
- POWERSTATS
- PowGoop

_USED TOOLS

- CrackMapExec
- LaZagne
- Living off the Land
- Meterpreter
- Mimikatz

_USED VULNERABILITIES

- CVE-2020-1472

_ATTACKS HAPPENED ON

> **MuddyWater targets Middle East - USA and India**
Happened on: 2017-02-20

> **After MuddyWater - ATK51 led a new and broader campaign in early 2018**
Happened on: 2017-05-20

> **ATK51 updates its TTP in Spear Phishing Campaign to target Asia and Middle East**
Happened on: 2018-02-23

> **ATK51: Seedworm's Powermud backdoor campaign**
Happened on: 2018-09-20

> **MuddyWater Operations in Lebanon and Oman**
Happened on: 2018-09-20

> **2019 - ATK51 Attacks Kurdish organizations in Turkey**
Happened on: 2019-04-15

> **2020: MuddyWater continues its attacks against Middle Eastern organizations**
Happened on: 2020-01-01

> **November 2021 - Iranian APT MuddyWater targets Turkish users**
Happened on: 2021-11

> **2022 - Ongoing Attacks by MuddyWater APT**
Happened on: 2022

2017
- 2017-02-20 MuddyWater targets Middle East - USA and India
- 2017-05-20 After MuddyWater - ATK51 led a new and broader campaign in early 2018

2018
- 2018-02-23 ATK51 updates its TTP in Spear Phishing Campaign to target Asia and Middle East
- 2018-09-20 ATK51: Seedworm's Powermud backdoor campaign

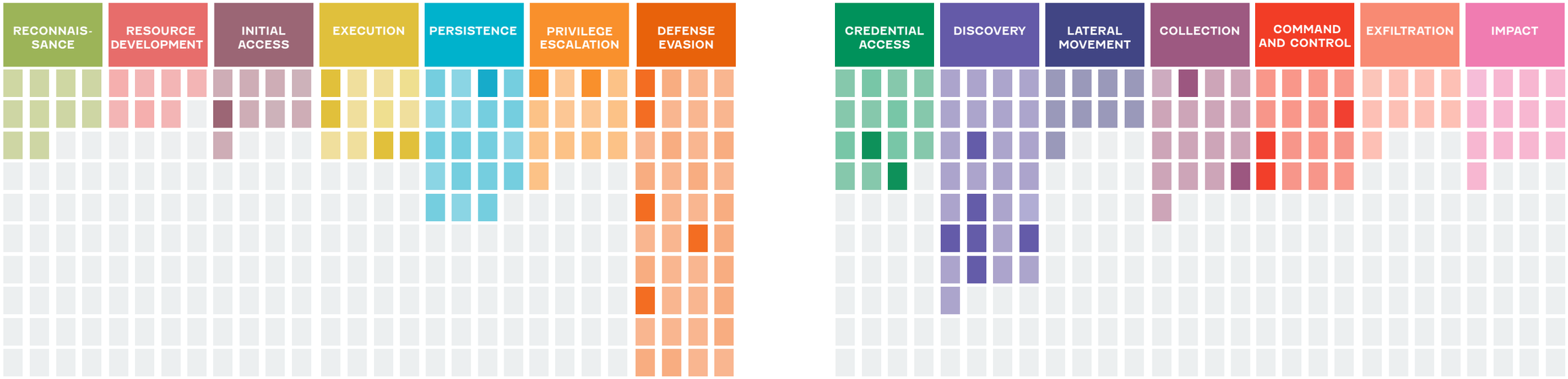
2019
- 2018-09-20 MuddyWater Operations in Lebanon and Oman
- 2019-04-15 ATK51 Attacks Kurdish organizations in Turkey

2020
- 2020-01-01 MuddyWater continues its attacks against Middle Eastern organizations

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1016 - System Network Configuration Discovery
T1027 - Obfuscated Files or Information
T1027.004 - Compile After Delivery
T1033 - System Owner/User Discovery
T1036 - Masquerading
T1047 - Windows Management Instrumentation
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1090 - Proxy
T1104 - Multi-Stage Channels
T1105 - Ingress Tool Transfer
T1113 - Screen Capture
T1140 - Deobfuscate/Decode Files or Information
T1204 - User Execution
T1218.003 - CMSTP
T1218.005 - Mshta
T1218.011 - Rundll32
T1518.001 - Security Software Discovery
T1547.001 - Registry Run Keys / Startup Folder
T1548.002 - Bypass User Account Control
T1552.001 - Credentials In Files
T1559.001 - Component Object Model
T1559.002 - Dynamic Data Exchange
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment

_CYBER ATTACK PHASES



Threat Actor_

ATK52
While some have attributed this attacker to North Korea, notably due to the overlap between the group and ATK4, there is a consensus linking this threat actor to South Korea instead. This actor targets government entities, especially in the diplomatic, defense and law enforcement sectors.

_Type of attacker: State Sponsored

Alias_

_APT-C-06
_DUBNIUM
_DarkHotel
_Fallout Team
_Karba
_Luder
_Nemim
_Nemin
_Pioneer
_SIG25
_Shadow Crane
_Tapaoux

Targeted Sectors_

_Transportation
_Research
_Pharmacy and drug manufacturing
_Military
_Manufacturing
_Hospitality
_Government and administration agencies
_Defence

Languages_

_Korean

Targeted Areas_

EASTERN ASIA
Korea
Japan
China
Taiwan

RUSSIA
Russian Federation

Suspected origin of the attacker_

South Korea

Motivations_

_Espionage

_DESCRIPTION

ATK52 - This Korean speaking attacker is especially active in the Sea of Japan and the East China Sea. Its goal is espionage of specific individuals. The group possesses extended cryptographic knowledge, that allowed it to create fake certificates, a capacity to develop and use 0-days (especially around Flash Player). It also has access to an extended network infrastructure that is reliable, allowing the group to maintain long-term access to the system.

In January 2020, a few days after Microsoft stopped Windows 7 support, DarkHotel used the DoubleStar 0day (CVE-2019-17026?CVE-2020-067) to attack Chinese government-related commerce agencies.

_USED MALWARES

- DarkHotel
- Nemim
- Tapaoux

_USED VULNERABILITIES

- CVE-2010-0188
- CVE-2014-0497
- CVE-2015-5119
- CVE-2016-4117
- CVE-2019-17026
- CVE-2020-0674

_ATTACKS HAPPENED ON

> **Since at least 2007: Precise attacks in hotels and wide spreading through P2P networks**
Happened on: 2007-01-01

> **Attacks in 2015**
Happened on: 2015-01-01

> **Attacks since 2016: New exploits and Overlap with ATK4**
Happened on: 2016-01-01

> **DarkHotel attacking Chinese foreign representatives using a vulnerability in SangFor VPN**
Happened on: 2020-04-07

2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

2007-01-01
Precise attacks in hotels and wide spreading through P2P networks

2015-01-01
Attacks in 2015

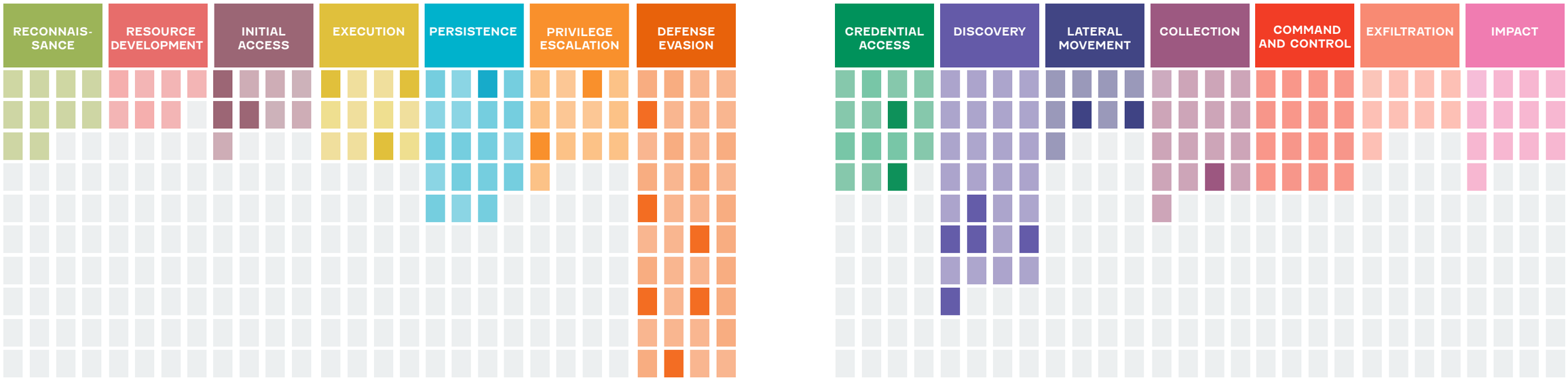
2016-01-01
New exploits and overlap with ATK4

2020-04-07
DarkHotel attacking Chinese foreign representatives using a vulnerability in SangFor VPN

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1016 - System Network Configuration Discovery
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1056 - Input Capture
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1068 - Exploitation for Privilege Escalation
T1080 - Taint Shared Content
T1082 - System Information Discovery
T1091 - Replication Through Removable Media
T1140 - Deobfuscate/Decode Files or Information
T1189 - Drive-by Compromise
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1218.005 - Mshta
T1497.002 - User Activity Based Checks
T1518.001 - Security Software Discovery
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1552.004 - Private Keys
T1553.002 - Code Signing
T1566.001 - Spearphishing Attachment

_CYBER ATTACK PHASES



Threat Actor_

ATK6
A cyber espionage group that has been active since at least 2010. They initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013.

_Type of attacker: State Sponsored

Alias_

_Crouching Yeti
_CrouchingYeti
_DYMALLOY
_Dragonfly
_Energetic Bear
_Group 24
_Havex
_Iron Liberty
_Koala Team
_TG-4192

Targeted Sectors_

_Energy
_Defence
_Aviation

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America
Canada

NORTHERN EUROPE
Norway

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland
France
Germany
Belgium
Italy
Spain
Switzerland

EASTERN EUROPE
Greece
Poland
Serbia

MIDDLE EAST/ WESTERN ASIA
Turkey

Suspected origin of the attacker_

Russia

_DESCRIPTION

ATK6 - Dragonfly's activities can be separated into three periods:
- 2010-2013, the beginning of its activities using large spam campaigns
- 2013-2014, when it started to target the energy sector using spear-phishing
- 2015-2019, a re-launch of its attacks after a break

The intrusions in energy facilities may have two objectives: steal sensitive informations to known how these systems work (intelligence gathering phase) and prepare the nertwork for future sabotage operations.

_USED MALWARES

- CrackMapExec
- Dorshel
- Goodor
- Havex
- Karagany
- Lightsout exploit kit
- MCMD
- Mimikatz
- Oldrea

_USED TOOLS

- Angry IP Scanner
- CrackMapExec
- Inveigh
- Phishery
- PsExec

_ATTACKS HAPPENED ON

> **2013 - ATK6 (Dragonfly) targets the European energy sector and its critical infrastructure**
Happened on: 2013-02-01

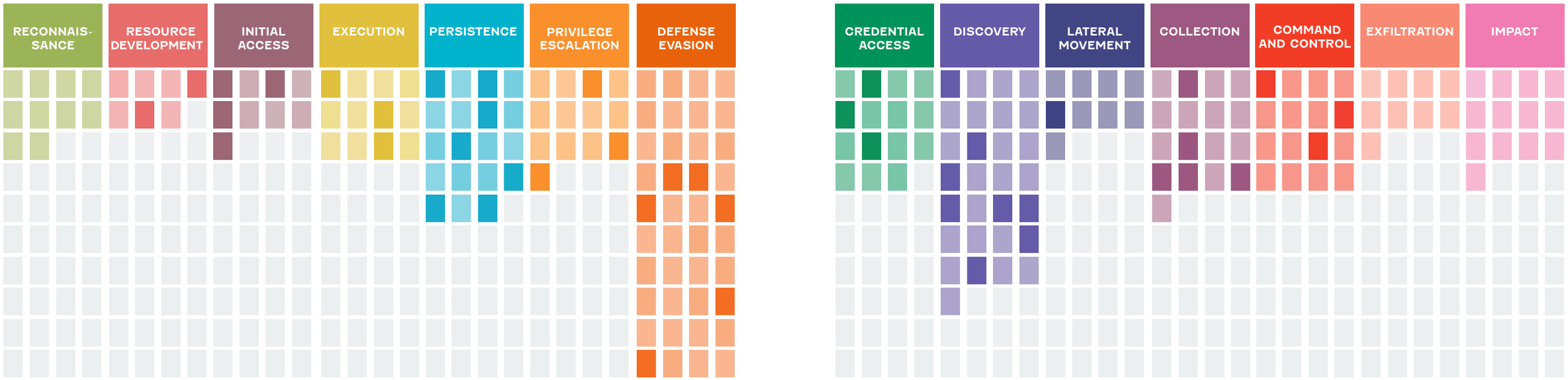
> **2014 - ATK6 (Dragonfly) targets supply chain providers of the European energy sector**
Happened on: 2014-03-01

> **December 2015 - 2018: CASTLE campaign**
Happened on: 2015-12-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1005 - Data from Local System
T1012 - Query Registry
T1016 - System Network Configuration Discovery
T1018 - Remote System Discovery
T1021.001 - Remote Desktop Protocol
T1033 - System Owner/User Discovery
T1036 - Masquerading
T1571 - Non-Standart Port
T1053 - Scheduled Task/Job
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1069 - Permission Groups Discovery
T1070 - Indicator Removal on Host
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1074 - Data Staged
T1078 - Valid Accounts
T1083 - File and Directory Discovery
T1087 - Account Discovery
T1098 - Account Manipulation
T1105 - Ingress Tool Transfer
T1110 - Brute Force
T1112 - Modify Registry
T1113 - Screen Capture
T1114 - Email Collection
T1133 - External Remote Services
T1135 - Network Share Discovery
T1136 - Create Account
T1187 - Forced Authentication
T1189 - Drive-by Compromise
T1204 - User Execution
T1221 - Template Injection
T1505.003 - Web Shell
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1560 - Archive Collected Data
T1562.001 - Disable or Modify Tools
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1587.001 - Malware
T1588.001 - Malware

_CYBER ATTACK PHASES



Threat Actor_

ATK64
A Pakistan-based adversary with operations likely located in Karachi. This adversary uses social engineering and spear phishing to target Indian military and defense entities

Alias_

_APT 36
_APT36
_C-Major
_Mythic Leopard
_Operation C-Major
_Operation Transparent Tribe
_ProjectM
_TMP.Lapis
_Transparent Tribe

Targeted Sectors_

_Military
_Defence

Targeted Areas_

WESTERN EUROPE
Germany

MIDDLE EAST/ WESTERN ASIA
Iran

SOUTHERN ASIA
India
Pakistan
Afghanistan

Suspected origin of the attacker_

Pakistan

_DESCRIPTION

ATK64 - Throughout 2016, these actors used custom .NET downloaders to acquire basic system information and download additional payloads to infect hosts. Based on a generally low level of coding complexity, CrowdStrike assesses this adversary in terms of average technical sophistication.

"The CrowdStrike Falcon Intelligence team tracking of this adversary began in late 2016, when evidence of an attack surfaced against a victim based in India and working in the hospitality sector. The attack used an Excel spreadsheet containing macro code that deployed the previously mentioned simplistic .NET downloader payload. The basic nature of the malicious document and observed coding errors in the downloader payload are the basis for the assessment that this actor demonstrates a low level of technical skills.

MYTHIC LEOPARD was further observed in 2017 developing methods for disguising custom malware implants. Two binder tools used to disguise custom executables as legitimate Microsoft implants — were discovered by Falcon Intelligence and linked to MYTHIC LEOPARD in July 2017.

Since April 2018, Falcon Intelligence has observed ongoing targeted intrusion activity using malicious Microsoft Office Excel documents likely associated with the MYTHIC LEOPARD adversary. As part of this campaign, the adversary leveraged generic themes related to administrative, managerial or supervisory matters alongside a unique Visual Basic Script (VBScript) technique used for installation. Falcon Intelligence has observed MYTHIC LEOPARD using this technique for several years to install multiple first-stage implants and downloaders, including the isqlmanager and Waizsar RAT malware families. However, the use of the UPX packer and timestomping techniques have not previously been associated with this adversary and likely indicates an incremental increase in tradecraft and sophistication.

MYTHIC LEOPARD actors have previously used an indigenously produced .NET obfuscation tool to hide malware implants as legitimate tools. The malicious files visual_HD.exe and skypee.exe both attempt to impersonate a legitimate uTorrent executable once installed and running. Both malicious files use a previously identified MYTHIC LEOPARD command-and-control (C2) domain msupdate.servehttp[.]com. MYTHIC LEOPARD has previously reused old C2 domains across medium to long periods of time, despite operational security concerns.

The related decoy document in this attack simply displays a pay scale without any further identifying information. However, the filename (Pay Matrix Projected After 7th CPC (3).xls) suggests that it is related to India 7th Central Pay Commission recommendations for government salaries. As noted above, India is within the traditional target scope for this adversary."

_USED MALWARES

- Crimson
- ObliqueRAT
- CapraRAT

_ATTACKS HAPPENED ON

> **March 2020 - APT36 delivers CrimsonRAT with covid related phishing emails**
Happened on: 2020-03

> **March 2021 - ObliqueRAT targets South Asia**
Happened on: 2021-03

> **2021 - TransparentTribe targeting India with evolving CrimsonRAT throughout 2021**
Happened on: 2021

> **Early 2022 - APT 36 Targeting Indian Government Officials via Spyware**
Happened on: 2022

Threat Actor_

ATK66
This group is commonly considered as an APT group linked to the Hamas organization ruling the Gaza Strip.

Alias_

_APT-C-23
_Arid Viper
_AridViper
_Desert Falcon
_Gaza cybergang Group2

Targeted Sectors_

_Population
_Political Organizations
_Government and administration agencies

Targeted Areas_

NORTH AMERICA
United States Of America

AFRICA
Egypt
Libya

MIDDLE EAST/ WESTERN ASIA
Turkey
Syria
Qatar
Palestine
Lebanon
Kuwait
Jordan
Israel
Iraq

Suspected origin of the attacker_

Middle East

_DESCRIPTION

ATK66 - Reportedly, the group was established in 2011, but became active starting from 2014, when the first attacks were detected in the wild. By examining the group victims and its TTPs, it is apparent the group mainly attacks targets related to the Palestinian Authority. APT-C-23 members are native Arabic speakers from the Middle East. According to Kaspersky, at its origins, APT-C-23 consisted of 30 members working in three teams and operating mainly out of Palestinian Territories, Egypt and Turkey.

_USED MALWARES

- Micropsia
- SpyC23

_USED TOOLS

- WinRAR

_ATTACKS HAPPENED ON

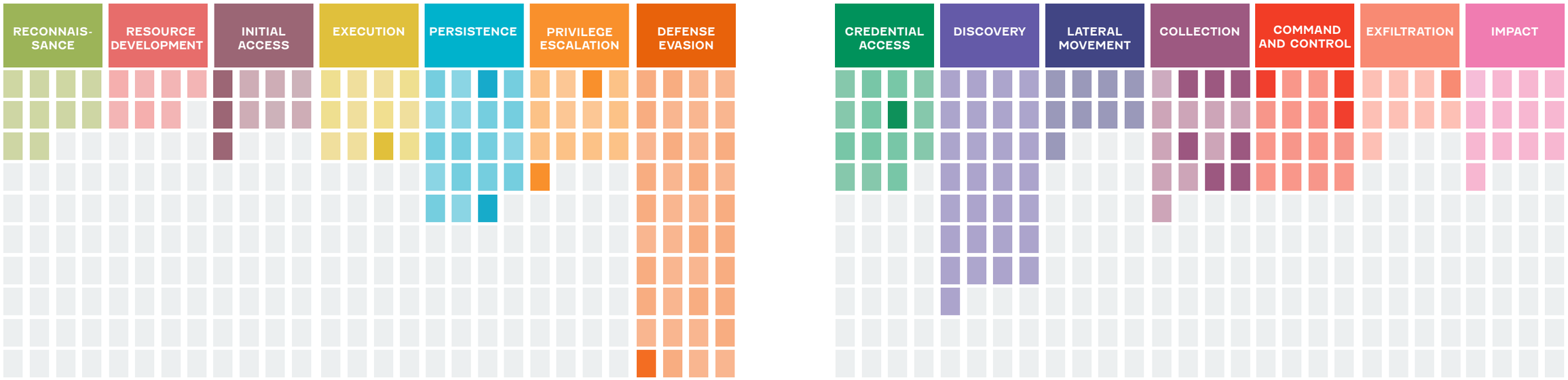
> **2020 / 2019 Jan - ATK66 Campaign Targeting Palestinian Government Officials**
Happened on: 2019-01-31

> **October 2021 - Arid Viper APT targets Palestine with new wave of politically themed phishing attacks, malware**
Happened on: 2021-10

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1005 - Data from Local System
T1025 - Data from Removable Media
T1041 - Exfiltration Over C2 Channel
T1056 - Input Capture
T1071 - Application Layer Protocol
T1078 - Valid Accounts
T1105 - Ingress Tool Transfer
T1113 - Screen Capture
T1119 - Automated Collection
T1123 - Audio Capture
T1189 - Drive-by Compromise
T1204 - User Execution
T1547.001 - Registry Run Keys / Startup Folder
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1566.003 Spearphishing via Service

_CYBER ATTACK PHASES



Threat Actor_

ATK7
An attacker group that exists since at least 2008 and that is believed to act for the Russian government.

Alias_

_APT 29
_APT29
_Cozer
_Cozy Bear
_Cozy Duke
_CozyBear
_CozyCar
_CozyDuke
_Dukes
_EuroAPT
_Grizzly Steppe
_Group 100
_Hammer Toss
_Iron Hemlock
_Minidionis
_NOBELIUM
_Office Monkeys
_OfficeMonkeys
_SeaDuke
_The Dukes
_UNC2452
_YTTRIUM

Targeted Sectors_

_Military
_Media
_International Organizations
_Information Technology
_Healthcare
_Government and administration agencies
_Defence

Motivations_

_Information theft
_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

AFRICA
Uganda

WESTERN EUROPE
Belgium
Portugal
Luxembourg
Spain
Ireland

EASTERN EUROPE
Czechia
Ukraine
Romania
Hungary
Poland

MIDDLE EAST/ WESTERN ASIA
Azerbaijan
Turkey
Georgia

CENTRAL ASIA
Kazakhstan
Kyrgyzstan
Uzbekistan

RUSSIA
Russian Federation

Suspected origin of the attacker_

Russia

Languages_

_Russian

_DESCRIPTION

ATK7 - (aka: APT29, NOBELIUM, UNC2452) is an attacker group that exists since at least 2008 and that is believed to act for the Russian government. The group is composed of highy competent members that are well organized, allowing for complex and long-running campaigns. The group's main goal is espionage and intelligence collection. The group therefore targets Western organizations, with a special focus on governmental bodies, think tanks... It as also occasionally expanded its reach to governments in the Middle East, Asia, Africa, etc. In order to reach its goal, the group has used multiple families of malware.
The group aims to act fast, albeit in a noisy way: Their campaigns are not designed in order to be discrete, but to be distributed to a large number of victims, followed by deployment of a malware that will quickly grab and exfiltrate every potentially interesting information. When a victim of interest has been unmasked, the group will then often switch to a different, stealthier malware, designed for long-term persistence, in order to gather intelligence.
In recent years, the group has been leading these campaigns bi-annually.
The group is suspected to be responsible for the 2015 hack of multiple governmental institutions in the USA, including the White House, the Pentagon and the DoS.
The threat actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, and related components.
They ran an election fraud themed phishing campaign in mid-2021 which delivered a Cobalt Strike beacon.
In the same year, they've also been observed targeting an Israeli and an Irianian embassy, the Indian government with maldoc delivering multiple versions of the same Cobalt Strike beacon.
In 2022, the European government and several diplomatic institutions were targeted in the same way.

_USED MALWARES

- CloudDuke
- CosmicDuke
- CozyDuke
- GeminiDuke
- GoldFinder
- GoldMax
- HammerDuke
- MiniDuke
- OnionDuke
- PinchDuke
- SUNBURST
- SUNSHUTTLE
- SeaDuke
- Sibot
- TEARDROP
- WellMess

_USED TOOLS

- Living off the Land

_USED VULNERABILITIES

- CVE-2010-0232
- CVE-2015-1641
- CVE-2018-13379
- CVE-2019-11510
- CVE-2019-1653
- CVE-2019-19781
- CVE-2019-2725
- CVE-2019-7609
- CVE-2019-9670
- CVE-2020-14882
- CVE-2020-4006
- CVE-2020-5902
- CVE-2021-21972

_ATTACKS HAPPENED ON

> **Campaign against Chechnya in 2008**
Happened on: 2008-11-12

> **Campaign against West countries in 2009**
Happened on: 2009-01-01

> **Campaign in the Caucasus in 2010**
Happened on: 2010-01-01

> **Dukes arsenal expansion campaign in 2011**
Happened on: 2011-01-01

> **Campaign against European countries in 2013**
Happened on: 2013-01-01

> **Campaign against trade of illegal substances in 2013**
Happened on: 2013-01-01

> **Campaign with large-scale spreading of CozyDuke in 2014**
Happened on: 2014-01-01

> **Campaign with OnionDuke botnet in 2014**
Happened on: 2014-01-01

> **Campaign with CozyDuke SeaDuke and HammerDuke in 2015**
Happened on: 2015-01-01

> **Campaign with CloudDuke in 2015**
Happened on: 2015-01-01

> **Campaign against Poland and Georgia in 2015**
Happened on: 2015-01-01

> **Campaign against the USA in 2015**
Happened on: 2015-01-01

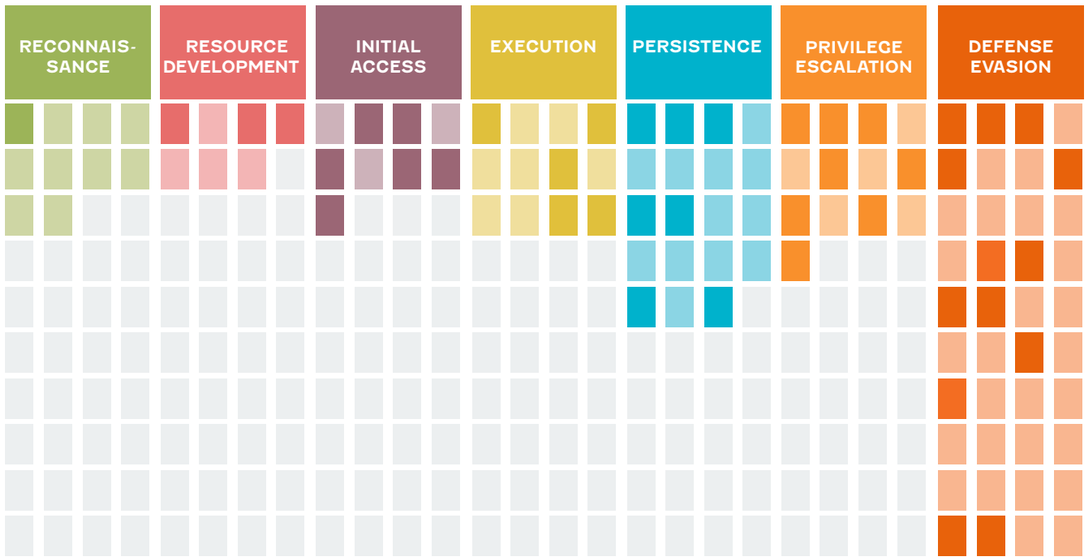
> **Campain in 2018**
Happened on: 2018-01-01

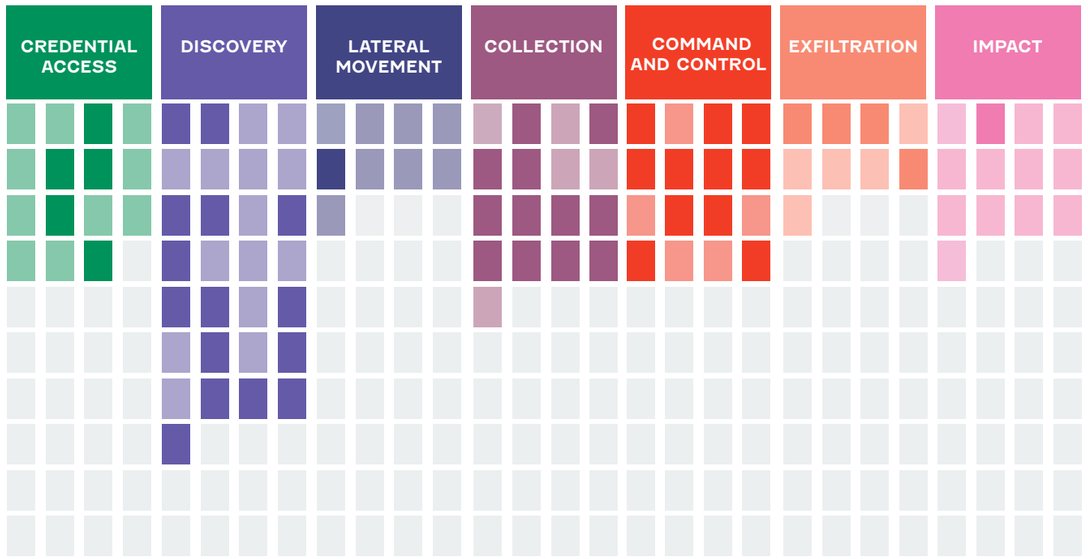
> **SolarWinds supply chain attack**
Happened on: 2020-03-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1001.002 - Steganography
T1003.006 - DCSync
T1005 - Data from Local System
T1007 - System Service Discovery
T1008 - Fallback Channels
T1010 - Application Window Discovery
T1016 - System Network Configuration Discovery
T1018 - Remote System Discovery
T1020 - Automated Exfiltration
T1021 - Remote Services
T1025 - Data from Removable Media
T1027 - Obfuscated Files or Information
T1027.002 - Software Packing
T1029 - Scheduled Transfer
T1030 - Data Transfer Size Limits
T1033 - System Owner/User Discovery
T1036 - Masquerading
T1036.004 - Masquerade Task or Service
T1036.005 - Match Legitimate Name or Location
T1039 - Data from Network Shared Drive
T1571 - Commonly Used Port
T1046 - Network Service Scanning
T1047 - Windows Management Instrumentation
T1048 - Exfiltration Over Alternative Protocol
T1048.002 - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1055 - Process Injection
T1056 - Input Capture
T1057 - Process Discovery
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1059.005 - Visual Basic
T1059.006 - Python
T1068 - Exploitation for Privilege Escalation
T1069 - Permission Groups Discovery
T1070 - Indicator Removal on Host
T1070.004 - File Deletion
T1070.006 - Timestomp
T1071.001 - Web Protocols
T1071.004 - DNS
T1074.002 - Remote Data Staging
T1078 - Valid Accounts
T1082 - System Information Discovery
T1083 - File and Directory Discovery
T1087 - Account Discovery
T1090.001 - Internal Proxy
T1090.003 - Multi-hop Proxy
T1095 - Non-Application Layer Protocol
T1098 - Account Manipulation
T1098.001 - Additional Cloud Credentials
T1098.002 - Exchange Email Delegate Permissions
T1102 - Web Service
T1105 - Ingress Tool Transfer
T1113 - Screen Capture
T1114 - Email Collection
T1114.002 - Remote Email Collection
T1115 - Clipboard Data
T1124 - System Time Discovery
T1132 - Data Encoding
T1133 - External Remote Services
T1134 - Access Token Manipulation
T1135 - Network Share Discovery
T1140 - Deobfuscate/Decode Files or Information
T1185 - Man in the Browser
T1190 - Exploit Public-Facing Application
T1195.002 - Compromise Software Supply Chain
T1197 - BITS Jobs
T1199 - Trusted Relationship
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1482 - Domain Trust Discovery
T1484.002 - Domain Trust Modification
T1485 - Data Destruction
T1497 - Virtualization/Sandbox Evasion
T1505.003 - Web Shell
T1546.003 - Windows Management Instrumentation Event Subscription
T1546.008 - Accessibility Features
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1548.002 - Bypass User Account Control
T1552 - Unsecured Credentials
T1552.004 - Private Keys
T1555 - Credentials from Password Stores
T1560.001 - Archive via Utility
T1562.001 - Disable or Modify Tools
T1562.002 - Disable Windows Event Logging
T1562.004 - Disable or Modify System Firewall
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1568 - Dynamic Resolution
T1573.002 - Asymmetric Cryptography
T1583.001 - Domains
T1583.006 - Web Services
T1584.001 - Domains
T1587.001 - Malware
T1587.003 - Digital Certificates
T1595.002 - Vulnerability Scanning
T1606.001 - Web Cookies
T1606.002 - SAML Tokens

_CYBER ATTACK PHASES





Threat Actor_

ATK73
A highly-skilled cybercrime actor with possibly a well-structured cybercrime syndicate, wich is active since at least mid 2016.

Alias_

_Professional Adversarial
_Threat Group
_TAG-CR4
_TDO
_The Dark Overlord

Targeted Sectors_

_Pharmacy and drug manufacturing
_Naval
_Media
_Manufacturing
_Legal Services
_High-Tech
_Healthcare
_Government and administration agencies
_Financial Services
_Education
_Casino & Gaming

Languages_

_English

Motivations_

_Financial Gain

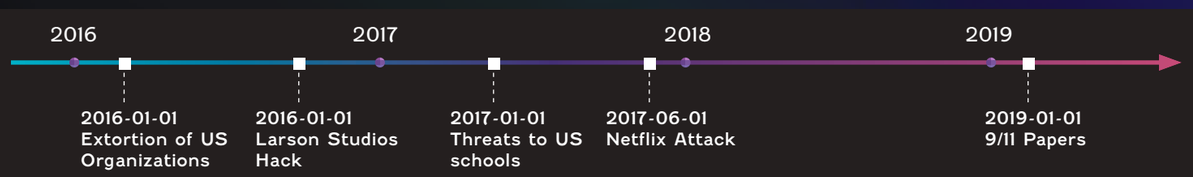
Targeted Areas_

NORTH AMERICA
United States Of America

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland

Suspected origin of the attacker_

United States | United Kingdom | Serbia



_DESCRIPTION

ATK73 - The group entered the public spotlight following the 2017 hack of Larson Studios, and the subsequent release of an entire season of the TV show “Orange is the New Black”. “The Dark Overlord” key business model is to hack into low, medium and high-profile organizations, mostly in the healthcare, education, and media production sectors in the US and the UK, and subsequently put the stolen data up for sale or demand ransom from its victims. The Dark Overlord appears to primarily be a financially-driven threat actor, with a proven history of success, and likely millions of dollars in profits. The threat actor has been prevalently active on Darknet marketplaces and hacking forums, where he tries to sell “private” databases (databases that are not in the public domain yet), but also other goods, such as software source code.

Alleged Members: arrested in September 2016. Grant West AKA “Courvoisier” - alleged member arrested in Kent (UK) in May 2018. S.S. - alleged member arrested in Belgrade (Serbia) on May 16, 2018.

_USED TOOLS

- TrueCrypt
- VeraCrypt

_ATTACKS HAPPENED ON

> **2016 - Extortion of US Organizations**
Happened on: 2016-01-01

> **2016 Larson Studios Hack**
Happened on: 2016-01-01

> **2017 - Threats to US schools**
Happened on: 2017-01-01

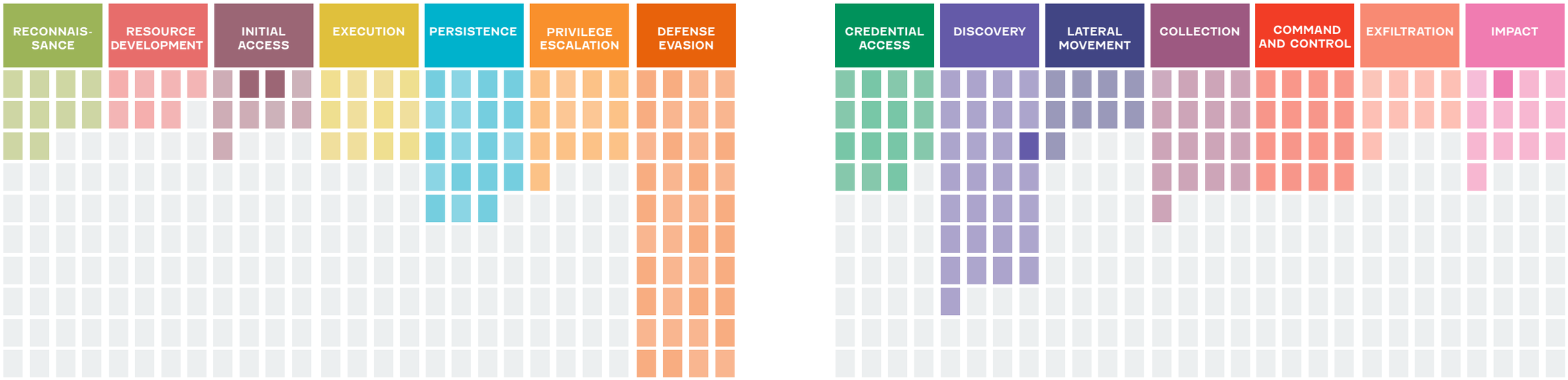
> **June 2017 - Netflix Attack**
Happened on: 2017-06-01

> **January 2019 - 9/11 Papers**
Happened on: 2019-01-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1046 - Network Service Scanning
T1133 - External Remote Services
T1190 - Exploit Public-Facing Application
T1485 - Data Destruction

_CYBER ATTACK PHASES



Threat Actor_

ATK78
A Chinese cyber-espionage group targeting telecommunications, geospatial imaging and defense sectors in the United States and Southeast Asia.

_Type of attacker: State Sponsored

Alias_

_Thrip

Targeted Sectors_

_Satellites and Telecommunications
_Media
_High-Tech
_Education
_Defence
_Communication
_Aerospace

Motivations_

_Information theft
_Espionage

Targeted Areas_

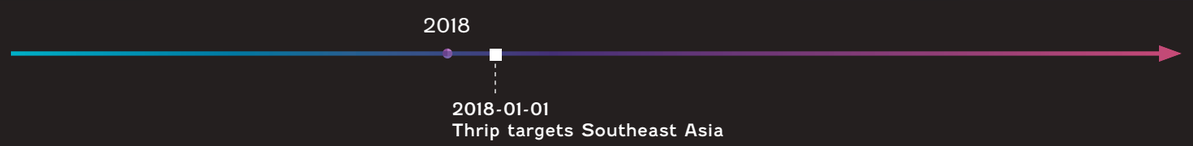
NORTH AMERICA
United States Of America

SOUTH EAST ASIA
Vietnam
Philippines

EASTERN ASIA
Taiwan

Suspected origin of the attacker_

China



_DESCRIPTION

ATK78 - This group was uncovered in January 2018 by Symantec during a campaign targeting an important telecommunication operator in Southern Asia.

The day of its publication, the article from Symantec described five custom malwares: Rikamaru, Catchamas, Mycicil, Spedear and Syndicasec. But this article has been modified, maybe due to a mistake, and nothing remains but the Catchamas info stealer trojan. Because of these circumstances, the information presented here is with moderate confidence.

During the last wave of attack, which began in 2017, Thrip had targeted a satellite communications operator. The attack group seemed to be particularly interested in the operational side of the company, looking for and infecting computers running software that monitors and controls satellites. This suggests to us that Thrip's motives go beyond spying and may also include disruption.

The group uses several *Live off the Land* tools. It uses administrations tools available on the compromised machine to reach its goal. This technique has multiple advantages:
- Reduced costs and development time of an attack.
- The lack of custom malware makes the intrusion difficult to attribute.
- Usage of legitimate tools and legitimates protocol makes the detection of the intrusion difficult to detect.

ATK78 uses PsExec, a legitimate Microsoft Sysinternal for lateral movement in the compromised network. PsExec is used to install the Catchamas trojan which allows the adversary to steal information. This malware is deployed on interesting compromised systems.
Symantec identified three computers based in China used to launch the attack. Thrip targeted a telecommunication satellite operator. It seemed to focus on systems executing the software used to control the satellites. It is possible that the objective was the perturbation besides the espionage. In the same way, when the group targeted a geospatial imaging organization, it focuses on computers executing the software "MapXtreme Geographic Information System", used to develop geospatial applications, Google Earth and Garmin imaging. The group targeted three organizations from Southeast Asia in the telecommunication sector and one in the defense sector. The nature of the attacks indicates that these organizations were targeted, not their clients.

Geographic targets and the kind of targeted entities indicate a correlation with PRC interests in the context of Sino-US tensions in the China Sea especially with issues of sovereignty around Spratly and Paracel islands. This suggests a direct link between Thrip Group and Chinese institutions.

The group therefore appears to act based on a strategic framework defined by the Party, but also on immediate contextual indications. The group's nuisance capabilities and usual targets make it formidable.

We draw attention on the fact that we have chosen to treat only the case of the Thrip group under the ATK78, some sources also link it to the aliases Lotus Blossom, Lotus Panda, Spring Dragon. This state of affairs stems from the high level of sharing that exists between Chinese attackers and the structure of their cyber service leading to confusion in their identification.

_USED MALWARES

- Catchamas
- Hannotog
- Mimikatz
- Mycicil
- Rikamanu
- Sagerunex
- Spedear
- Syndicasec

_USED TOOLS

- LogMeIn
- PowerShell
- PsExec
- WinSCP

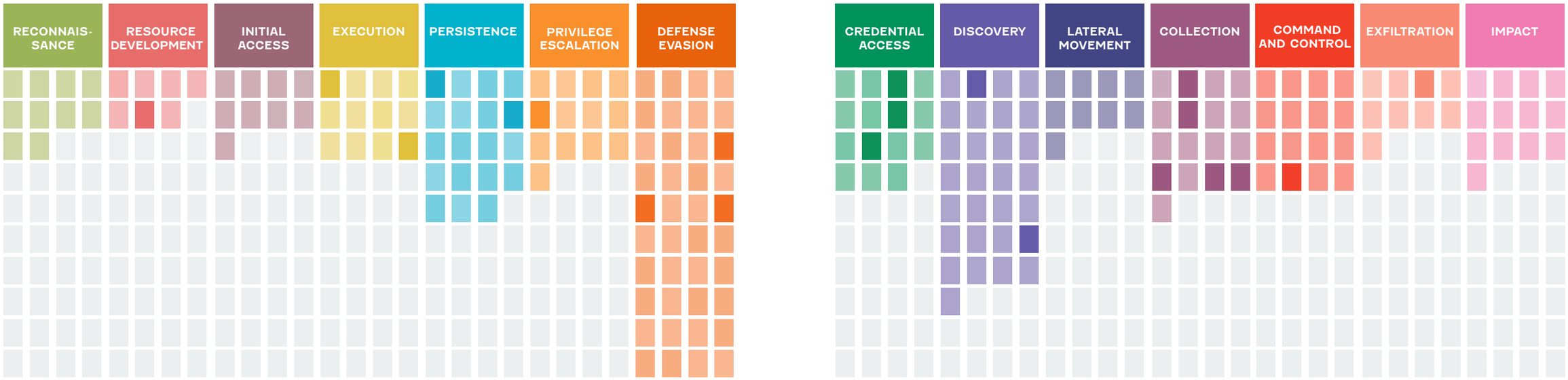
_ATTACKS HAPPENED ON

> **Thrip targets Southeast Asia**
Happened on: 2018-01-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1010 - Application Window Discovery
T1016 - System Network Configuration Discovery
T1036 - Masquerading
T1047 - Windows Management Instrumentation
T1048 - Exfiltration Over Alternative Protocol
T1048.003 - Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
T1056 - Input Capture
T1059.001 - PowerShell
T1074 - Data Staged
T1098 - Account Manipulation
T1112 - Modify Registry
T1113 - Screen Capture
T1115 - Clipboard Data
T1219 - Remote Access Software
T1543.003 - Windows Service
T1555.004 - Windows Credential Manager
T1560 - Archive Collected Data
T1564.001 - Hidden Files and Directories
T1588.002 - Tool

_CYBER ATTACK PHASES



Threat Actor_

ATK8
A group of French origins known for its high quality malware. The group is active since at least 2009, and some of its malwares have been associated with samples from as far as 2007.

Alias_

_Animal Farm
_SNOWGLOBE

Targeted Sectors_

_Military
_Media
_International Organizations

Motivations_

_Espionage

Targeted Areas_

NORTH AMERICA
United States Of America

AFRICA
Algeria
Morocco
Congo

NORTHERN EUROPE
Sweden
Netherlands

WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland
Germany

EASTERN EUROPE
Austria
Ukraine

MIDDLE EAST/ WESTERN ASIA
Israel
Iraq
Iran
Turkey
Syria

SOUTH EAST ASIA
Malaysia

EASTERN ASIA
China

RUSSIA
Russian Federation

OCEANIA
New Zealand

Suspected origin of the attacker_

France

_DESCRIPTION

ATK8 - The group has been discovered in March 2014 after the publication of a series of slides from Edward Snowden. This group is probably supported by a state-nation, considering the fact that it uses advanced techniques but does not seem to be financially motivated. Another more precise indication makes it possible to link the group to France. For good reason, the name "Babar" given to the group's spyware echoes a strictly French fictional character. Also, the backdoor called "Tafacalou" has a name whose meaning in Occitan French regional language is translated as: "it's gonna get hot".

While the group is not associated to any campaign in particular, the tool it uses have been in order to target various organizations, notably in Syria, Iran and Malaysia.
"More broadly, the group deploys its campaigns on a global scale with some twenty countries concerned."

The group mostly develops and uses espionage tools, and the way the malware are deployed to their targets is mostly unknown, though some documents containing zero-day exploits have been used.

_USED MALWARES

- Babar
- Casper
- Dino
- EvilBunny
- Tafacalou

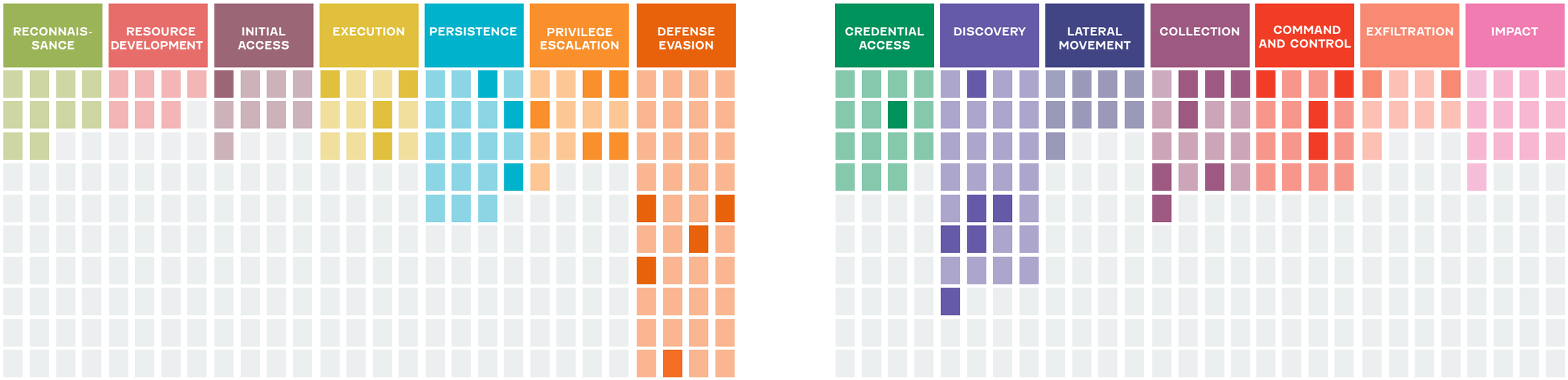
_USED VULNERABILITIES

- CVE-2011-4369
- CVE-2014-0515

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1001 - Data Obfuscation
T1008 - Fallback Channels
T1010 - Application Window Discovery
T1012 - Query Registry
T1020 - Automated Exfiltration
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1041 - Exfiltration Over C2 Channel
T1571 - Non-Standart Port
T1053 - Scheduled Task/Job
T1055 - Process Injection
T1055.012 - Process Hollowing
T1056 - Input Capture
T1056.004 - Credential API Hooking
T1057 - Process Discovery
T1059 - Command and Scripting Interpreter
T1071 - Application Layer Protocol
T1074 - Data Staged
T1082 - System Information Discovery
T1112 - Modify Registry
T1115 - Clipboard Data
T1119 - Automated Collection
T1123 - Audio Capture
T1125 - Video Capture
T1189 - Drive-by Compromise
T1203 - Exploitation for Client Execution
T1497 - Virtualization/Sandbox Evasion
T1518.001 - Security Software Discovery
T1543.003 - Windows Service
T1547.001 - Registry Run Keys / Startup Folder
T1560 - Archive Collected Data

_CYBER ATTACK PHASES



Threat Actor_

ATK80
A threat actor which is active since at least November 2014. This group launched long-term attacks against organizations in the Syrian region using Android and Windows malwares. Its objective is the theft of sensitive information.

Alias_

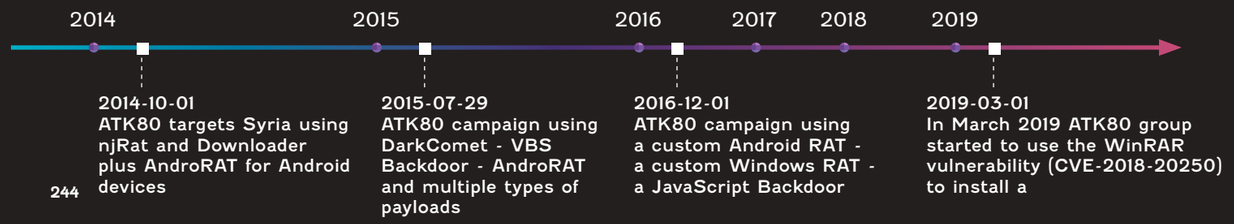
_APT-C-27
_Golden RAT
_Goldmouse

Targeted Areas_

MIDDLE EAST/ WESTERN ASIA
Syria

Suspected origin of the attacker_

Syria



_DESCRIPTION

ATK80 - Its malwares are mainly disguised as common chat software such as ChatSecure or WhatsApp or Telegram. It also uses the njRat, an open-source Remote Access Trojan created in 2012 and often used against targets in the Middle East.
It is supposed that this group is one of the branch of the Syrian Electronic Army, with:

- The initial access techniques include the conception of fake websites helped by typosquatting used to lead the user to download the malicious messaging app. The group also used social media like Facebook to induce users to download the malicious softwares from a specified link. 360 NetLab reserchers assess that lure documents could be used to deliver the payload through spear-phishing.

- Its Android spyware has the ability of recording, photographing, GPS positioning, uploading contacts/call records/sms/files, executing cloud commands, etc. These capabilities allow the attacker to efficiently track a person. In a four years period, the group improved from using open-source malwares such as njRat or Downloader to its own custom Android RAT, Windows RAT and JS backdoor. This developpement indicated that the group has ressources but it used a small C2 infrastructure with 9 known C2 domains in the same period. Furthermore this group on advanced phishing techniques than exploiting sophisticated vulnerabilities.

This group attacks in waves :
- October 2014 - July 2015 : Attacks against Syria using njRat and Downloader plus AndroRAT for Android devices
- July 2015 - November 2016 : Attacks using DarkComet, VBS Backdoor, AndroRAT and multiple types of payloads
- December 2016 - July 2018 : Attacks using a custom Android RAT, a custom Windows RAT, a JavaScript Backdoor

In March 2019, the group started to use the WinRAR vulnerability (CVE-2018-20250) to install an embedded njRat on a vulnerable computer. The language used in the malwares and in the lure documents is Arabic. The lure documents are about terrorist attacks, a sensible subject in the Middle East region and other theme that can easily lead to user curiosity.

Android RAT
The Android RAT is an application pretending to be «ChatSecure», «WordActivation», «whatsappupdate_2017», and other common chat office software. It incites the user to activate Android Device Manager to protect itself from being easily uninstalled and hide its icon to run in background. After establishing a connection with the C2 he wait for command and steal data from WhatsApp, Viper and other softwares. It has the ability of recording, photographing, GPS positioning, uploading contacts/call records/sms/files, executing cloud commands in xml format, etc.

Windows RAT
This Windows RAT pretends to be the Telegram chat application, using strong phishing techniques (well chosen icons, names, well made interfaces) with a fake installation interface to lead the user to install the malware and, if needed, malicious updates. It is created using .net and has common backdoor abilities like upload/download/create/move/delete/rename/run/zip/unzip files, get process list and kill a process, take and upload a screenshot or execute a command.

VBS Backdoor
This group used a large number of VBS scripts which are obfuscated. These scripts have backdoor fonctionalities.

JS Backdoor
A JavaScript script able to create a file or a script in the tmp directory and run it, get a specified environment variable, executing a command and update itself.

Other Mobile TTP
- Access Installed Applications
- Create File and Directory
- Uncommonly Used Port

Notable behaviors:
- Using of .scr (screen saver in Windows) file format for its decoy documents
- Theme of decoy documents titles adapted to Syrian targets
- Use copy of normal software's update page to lead the user to download malicious updates
- Use of fake installation interface

_USED MALWARES

- DarkComet
- Raddex
- njRAT

_USED VULNERABILITIES

- CVE-2018-20250

_ATTACKS HAPPENED ON

> **October 2014 - July 2015: ATK80 targets Syria using njRat and Downloader plus AndroRAT for Android devices**
Happened on: 2014-10-01

> **July 2015 - November 2016: ATK80 campaign using DarkComet - VBS Backdoor - AndroRAT and multiple types of payloads**
Happened on: 2015-07-29

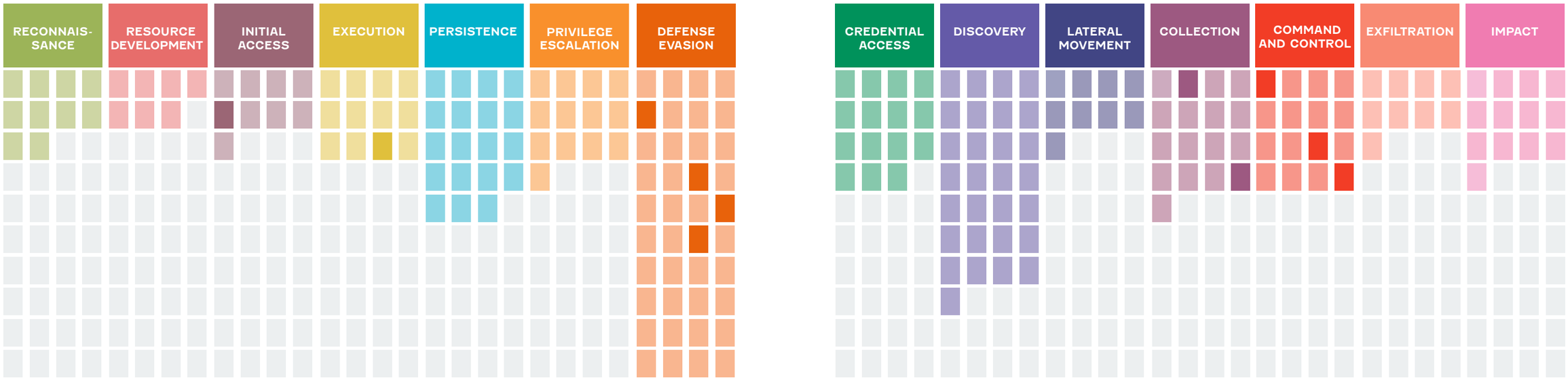
> **December 2016 - July 2018: ATK80 campaign using a custom Android RAT - a custom Windows RAT - a JavaScript Backdoor**
Happened on: 2016-12-01

> **In March 2019 ATK80 group started to use the WinRAR vulnerability (CVE-2018-20250) to install an embedded njRat on a vulnerable**
Happened on: 2019-03-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1027 - Obfuscated Files or Information
T1027.002 - Software Packing
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1102 - Web Service
T1112 - Modify Registry
T1113 - Screen Capture
T1140 - Deobfuscate/Decode Files or Information
T1204 - User Execution
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1566.003 - Spearphishing via Service
T1571 - Non-Standard Port

_CYBER ATTACK PHASES



Threat Actor_

ATK86
A Cybercrime group that has been active since the end of 2016, and that has attacked mostly banks all over the world. The group is believed to be from Russia, because most of their attacks (at least at the beginning), were directed against banks from Russia and former Soviet Union countries.

_Type of attacker: Cyber Criminal

Alias_

_Silence
_Silence APT group
_Silence group
_WHISPER SPIDER

Targeted Sectors_

_Government and administration agencies
_Financial Services

Languages_

_Russian
_English

Motivations_

_Financial Gain

Targeted Areas_

WESTERN EUROPE
- Germany
- United Kingdom Of Great Britain And Northern Ireland

EASTERN EUROPE
- Czechia
- Ukraine
- Romania
- Poland
- Belarus
- Greece
- Latvia
- Austria
- Serbia

AFRICA
- Kenya

MIDDLE EAST/ WESTERN ASIA
- Azerbaijan
- Armenia
- Saudi Arabia
- Turkey
- Israel
- Georgia
- Cyprus

CENTRAL ASIA
- Kazakhstan
- Uzbekistan
- Kyrgyzstan

SOUTHERN ASIA
- Bangladesh

SOUTH EAST ASIA
- Vietnam
- Malaysia

EASTERN ASIA
- Taiwan
- Hong-Kong

RUSSIA
- Russian Federation

Suspected origin of the attacker_

Eastern Europe

_DESCRIPTION

ATK86 - The group was using very high level of Russian in their phishing emails, and it was found that some of the commands of their tools were in Russian. However, along the years, the group has shifted to attack banks all over the world such as in East Asia, Europe and more.

The group is known for their sophisticated and profound attacks, in which usually they take a long period of time to study the potential victim, to maximize the attack against them. In most cases, Spear-phishing emails were sent to bank employees, while having a malicious file attached to them. This usually downloaded the Silence Trojan that has many capabilities of stealing data, downloading additional tolls, track victims and more. A few versions of the toll were found, and it has shown that the group is continuing to enhance them. Furthermore, the group uses malwares to attack ATMs specifically, such as Atmosphere. At the begenning, the tools used to target ATM were developped by other cyber criminals but the group is currently using homemade tools. Through this, the group was able to steal millions of dollars in cash along the years, mostly from banks in Russia, and Eastern Europe.

Some IP addresses used during theses attacks seems to be located in France, mostly from the OVH hoster.

In 2020 the group started to target Banks in Sub-Saharian Africa and to threaten Australian banks of DDoS attacks if they will not pay large sums in Monero cryptocurrency.

According to Group-IB the Silence group started to buy access from TA505 to banks which correlate with the diminution of spear-phishing attempt from Silence. TA505 seems to have sold at least the access to one European bank to Silence in end 2019.

_USED MALWARES

- Atmosphere
- EDA
- Farse
- Ivoke
- Kikothac
- Perl IrcBot
- Silence Downloader (TrueBot)
- Silence.proxybot(.net)
- Smoke Bot
- SurveillanceModule (Slowroll)
- xfs-disp.exe

_USED TOOLS

- CARDCAM
- Living off the Land
- Meterpreter
- RAdmin
- SDelete
- Winexe

_USED VULNERABILITIES

- CVE-2017-0199
- CVE-2017-0262
- CVE-2017-11882
- CVE-2018-0802
- CVE-2018-8174

_ATTACKS HAPPENED ON

> **July - August 2016: Silence targets the Automated Work Station Client of the Russian Central Bank**
Happened on: 2016-07-01

> **September 2017: Silence targets banks**
Happened on: 2017-09-01

> **October 2017: Silence Group attacked ATMs**
Happened on: 2017-10-01

> **January 2018 - February 2018: Attacks against financial institutions**
Happened on: 2018-01-01

> **February - April 2018: Attacks against Russian and Eastern European banks**
Happened on: 2018-02-01

> **May 2018 - October 2018: spear-phishing campaigns against banks in Russia**
Happened on: 2018-05-01

> **October 2018 - January 2019: reconnaissance campaigns against banks**
Happened on: 2018-10-01

> **March 2019 - May 2019: ATM attacks**
Happened on: 2019-03-01

> **June 2019 - July 2019: Silence targets banks using the EDA trojan**
Happened on: 2019-06-01

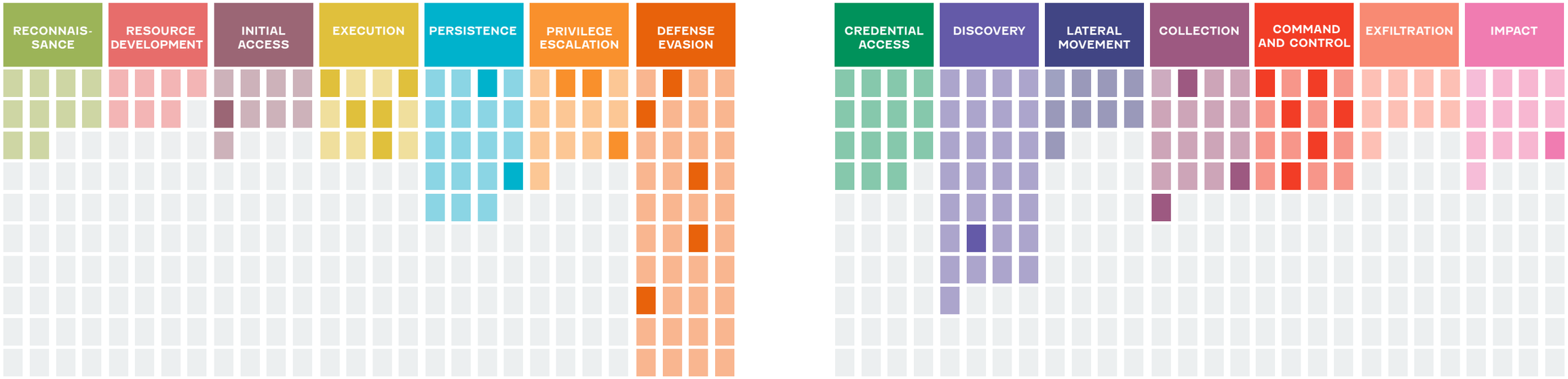
> **June 2019 - July 2019: Attack of the Russian IT bank**
Happened on: 2019-06-01

> **Attacks on major banks located in the sub-Saharan Africa (SSA) region**
Happened on: 2020-01-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1027 - Obfuscated Files or Information
T1571 - Non-Standart Port
T1053 - Scheduled Task/Job
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1082 - System Information Discovery
T1105 - Ingress Tool Transfer
T1106 - Native API
T1113 - Screen Capture
T1125 - Video Capture
T1132 - Data Encoding
T1134 - Access Token Manipulation
T1140 - Deobfuscate/Decode Files or Information
T1203 - Exploitation for Client Execution
T1204 - User Execution
T1218.001 - Compiled HTML File
T1218.005 - Mshta
T1219 - Remote Access Software
T1489 - Service Stop
T1547.001 - Registry Run Keys / Startup Folder
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1569.002 - Service Execution
T1573 - Encrypted Channel

_CYBER ATTACK PHASES



Threat Actor_

ATK88
A cybercrime group active since at least 2015, focusing mostly on the financial sector. Their claim to fame is in attacking Point-of-Sales and stealing credit card data from them.

_Type of attacker: Cyber Criminal

Alias_

_FIN6
_ITG08
_Skeleton Spider
_TAG-CR2

Targeted Sectors_

_Retail
_Manufacturing
_Hospitality
_Healthcare
_Financial Services
_Energy

Languages_

_Russian
_English

Motivations_

_Financial Gain

Targeted Areas_

NORTH AMERICA
United States Of America

Suspected origin of the attacker_

Unknown

_DESCRIPTION

ATK88 - (aka: FIN6) is a cybercrime group active since at least 2015, and focuses mostly on the financial sector. Their claim to fame is in attacking Point-of-Sales and stealing credit card data from them. Millions of cards were stolen using this method in recent years, and subsequently found to be sold on the dark web. Furthermore, in some cases, if they are unable to steal this data, they move to target card-not-present (CNP) data. They usually use specifically POS malware, and their victims are from companies that have many transactions. Therefore, most of their activity is against victims in the US and Europe. Of note, since mid-2018, it was spotted that the group has started to deploy ransomware on non Ecommerce networks.
The group may also be part of attacks that deploy ransomware such as Ryuk, LockerGoga and MegaCortex, again in likely partnership with banking Trojan botnets, which could be a further attempt to move into new "markets" that do not rely on the need to monetize credit card data.

_USED MALWARES

- FlawedAmmyy
- FrameworkPOS
- GRABNEW
- GratefulPOS
- HARDTACK
- LockerGoga
- More_eggs
- Ryuk
- SHIPBREAD
- TRINITY

_USED TOOLS

- Adfind
- Cobalt Strike
- Living off the Land
- Metasploit
- Meterpreter
- PowerShell
- PsExec
- Query Express
- Windows Credential Editor

_USED VULNERABILITIES

- CVE-2010-4398
- CVE-2011-2005
- CVE-2013-3660

_ATTACKS HAPPENED ON

> **2015: FIN6 steal millions of credit cards**
Happened on: 2015-01-01

> **June 2016: FIN6 deploys FrameworkPOS**
Happened on: 2016-06-01

> **Since July 2018: FIN6 deploys Ryuk and LockerGoga ransomwares**
Happened on: 2018-07-01

> **September 2018: FIN6 targets PoS in the USA and Europe**
Happened on: 2018-09-01

> **Late 2018: FIN6 phishing campaign**
Happened on: 2018-09-01

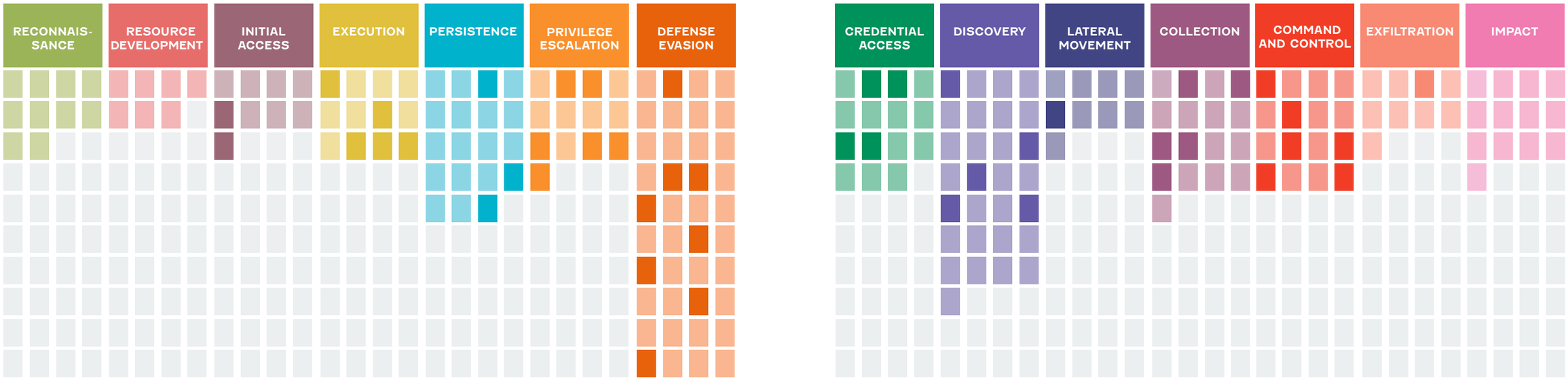
> **March 2020: Attack against EVRAZ**
Happened on: 2020-03-05

> **April 2020: FIN6 Partners With TrickBot Gang, Uses Anchor Framework**
Happened on: 2020-04

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1003.001 - LSASS Memory
T1003.003 - NTDS
T1005 - Data from Local System
T1018 - Remote System Discovery
T1021.001 - Remote Desktop Protocol
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1036.004 - Masquerade Task or Service
T1040 - Network Sniffing
T1046 - Network Service Scanning
T1047 - Windows Management Instrumentation
T1048 - Exfiltration Over Alternative Protocol
T1048.003 - Exfiltration Over Unencrypted/ Obfuscated Non-C2 Protocol
T1053 - Scheduled Task/Job
T1053.005 - Scheduled Task
T1055 - Process Injection
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1059.003 - Windows Command Shell
T1059.007 - JavaScript
T1068 - Exploitation for Privilege Escalation
T1069 - Permission Groups Discovery
T1070.004 - File Deletion
T1071 - Application Layer Protocol
T1074 - Data Staged
T1074.002 - Remote Data Staging
T1078 - Valid Accounts
T1087 - Account Discovery
T1087.002 - Domain Account
T1095 - Non-Application Layer Protocol
T1102 - Web Service
T1110.002 - Password Cracking
T1119 - Automated Collection
T1134 - Access Token Manipulation
T1204.002 - Malicious File
T1213 - Data from Information Repositories
T1547.001 - Registry Run Keys / Startup Folder
T1553.002 - Code Signing
T1555 - Credentials from Password Stores
T1555.003 - Credentials from Web Browsers
T1560 - Archive Collected Data
T1560.003 - Archive via Custom Method
T1562.001 - Disable or Modify Tools
T1566.001 - Spearphishing Attachment
T1566.003 - Spearphishing via Service
T1569.002 - Service Execution
T1572 - Protocol Tunneling
T1573 - Encrypted Channel
T1573.002 - Asymmetric Cryptography

_CYBER ATTACK PHASES



Threat Actor_

ATK89
An Arabic politically motivated APT group, active all over the world, including in Europe and the US. They are mainly active in the Middle East and North Africa (MENA) and in Palestine in particular.

_Type of attacker:
- State Sponsored
- Cyber Terrorist

Alias_

_Extreme Jackal
_Gaza Hackers Team
_Gaza cybergang
_Gaza cybergang Group1
_Molerats
_Moonlight
_Operation Molerats
_TA402

Targeted Sectors_

_Media
_High-Tech
_Government and administration agencies
_Financial Services
_Energy
_Defence
_Aerospace

Motivations_

_Ideology

Targeted Areas_

NORTH AMERICA
- United States Of America
- Canada

SOUTH AMERICA
- Chile

NORTHERN EUROPE
- Denmark

WESTERN EUROPE
- Germany
- United Kingdom Of Great Britain And Northern Ireland

EASTERN EUROPE
- Latvia
- North Macedonia
- Serbia
- Slovenia

AFRICA
- Algeria
- Egypt
- Djibouti
- Libya
- Morocco
- Somalia

MIDDLE EAST/ WESTERN ASIA
- Iran
- Iraq
- Jordan
- Israel
- Lebanon
- Kuwait
- Oman
- Palestine
- Qatar
- Saudi Arabia
- Syria
- Turkey
- United Arab Emirates
- Yemen

SOUTHERN ASIA
- India
- Afghanistan

EASTERN ASIA
- China
- Korea

RUSSIA
- Russian Federation

OCEANIA
- New Zealand

Suspected origin of the attacker_

State of Palestine

_DESCRIPTION

ATK89 - ATK89 (aka: Molerats, Gaza Cybergang) is an Arabic politically motivated APT group, active all over the world, including in Europe and the US, but they are mainly active in the Middle East and North Africa (MENA) and in Palestine in particular. The group is comprised of three sub-groups:

Gaza Cybergang Group 1: aka MoleRATs: The group's aim is to the infection of the victim in a RAT and it often makes use of text-sharing platforms, such as: PasteBin, github.com, upload.cat and more.
Gaza Cybergang Group 2: aka Desert Falcons: the group makes use of homemade malware, tools and techniques. Victims are often infected by social engineering methods such as fake websites that promise political information or spear phishing emails and social messaging.
Gaza Cybergang Group 3: aka Operation Parliament: The group is focused on espionage, covering on executive and judicial bodies all over the world, and focusing on MENA, particularly Palestine. the group used malware with CMD/PowerShell commands for its attacks. Each group is different in TTPs, but they make use of the same tools after gaining the initial grip on their victims.
ATK89 is a persistent threat to organizations and governments in the Middle East, routinely updating not only their malware implants, but also their delivery methods.

_USED MALWARES

- DHS Spyware
- DHS2015 / iRat
- DropBook
- DustySky
- Falcons' Backdoor
- Falcons' Downloader
- LastConn
- MoleNet
- Molerat Loader
- Pierogi
- PoisonIvy
- Scote
- SharpStage
- Spark
- TajMahal APT Framework
- XtremeRAT

_USED TOOLS

- Cobalt Strike
- Enigma Protector
- QuasarRAT
- njRAT

_USED VULNERABILITIES

- CVE-2017-0199

_ATTACKS HAPPENED ON

> **January 2012 - Defacement of Israeli Websites**
Happened on: 2012-01-10

> **October 2012 - Operation "MoleRATs"**
Happened on: 2012-10-10

> **March 2013 - 2014: 1st Campaign of the Falcon Desert Subgroup**
Happened on: 2013-03-10

> **March 2013 - 2014: 2nd Campaign of the Falcon Desert Subgroup**
Happened on: 2013-03-10

> **March 2013 - 2014: 3nd Campaign of the Falcon Desert Subgroup**
Happened on: 2013-03-10

> **June-July 2013 - Poison Ivy Attacks**
Happened on: 2013-06-10

> **2014 - 2016 - Operation Moonlight**
Happened on: 2014-01-10

> **April 2014 - MoleRATs Attacks on US and European targets**
Happened on: 2014-04-10

> **Summer 2014 - Attacks against Israeli and Palestinian Interests**
Happened on: 2014-06-10

> **September 2015 - Operation DustySKy**
Happened on: 2015-09-10

> **September 2016 - Operation DustySKy part 2**
Happened on: 2016-09-01

> **2017 - Mobile Espionage, Macros and CVE-2017-0199**
Happened on: 2017-01-01

> **2017 - Operation Parliament**
Happened on: 2017-01-01

> **The Spark campaign**
Happened on: 2019-01-01

> **February 2019 - Middle East Attack**
Happened on: 2019-02-01

> **April 2019 - "SneakyPastes" Campaign**
Happened on: 2019-04-01

> **April 2019 - TajMahal APT Framework**
Happened on: 2019-04-01

> **Name: The Pierogi Campaign**
Happened on: 2019-12-01

> **2020 - Renewed arsenal and Cloud platform usage**
Happened on: 2020-01-01

> **2021 to 2022 - NimbleMamba targeting Middle Eastern governments**
Happened on: 2021

2012 2013 2014 2015 2016 2017 2018 2019 2020

2012-01-10
Defacement of Israeli Websites

2014-04-10
MoleRATs Attacks on US and European targets

2014-06-10
Attacks against Israeli and Palestinian Interests

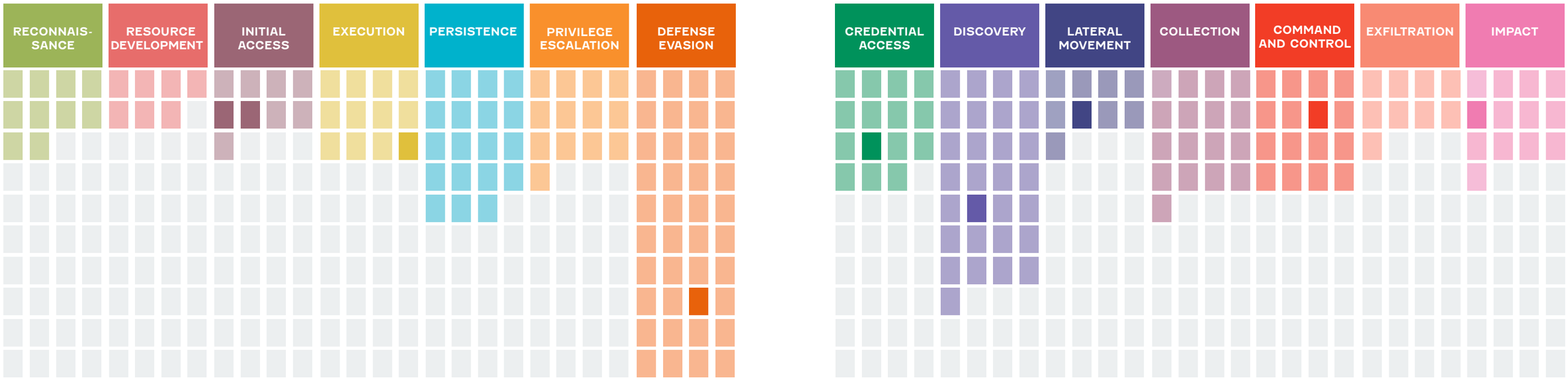
2019-02-01
Middle East Attack

2020-01-01
Renewed arsenal and Cloud platform usage

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1008 - Fallback Channels
T1047 - Windows Management Instrumentation
T1057 - Process Discovery
T1091 - Replication Through Removable Media
T1491 - Defacement
T1553.002 - Code Signing
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link

_CYBER ATTACK PHASES



Threat Actor_

ATK91
This group is known for the Triton malware. Triton is an attack framework allowing the manipulation of Security Systems, Industrial Control Systems (ICS) of critical infrastructures, discovered at the end of 2017 when it has caused an accidental shutdown of the machines.

Alias_

_TEMP.Veles
_TRITON group
_XENOTIME

Targeted Sectors_

_Energy

Motivations_

_Sabotage
_Espionage

Targeted Areas_

MIDDLE EAST/ WESTERN ASIA
Saudi Arabia

Suspected origin of the attacker_

Russia

2017

2017-01-09
Campaign leveraging the Triton malware

_DESCRIPTION

ATK91 - FireEye has awarded the development of TRITON to a Muscovite research institute linked to the Russian government. The attacker's tools and TTPs indicate that he has prepared to conduct operations that can last several years and require a long preparation. In the 2017 attack, the group compromised the target's network almost a year before reaching the SIS (Safety Instrument System). During this period, priority seems to have been given to safety operational. His lack of curiosity during the operation may indicate that the attacker is waiting for something before acting visibly.

Group description

Triton is a highly sophisticated malware for manipulating the Industrial Control Systems (ICS) of critical infrastructures discovered at the end of 2017. It is difficult to determine definitively the motivation behind this campaign. According to several observers, the main objective of the campaign was to test the tools and refine the techniques.

It should be noted that according to Dragos, the ATK91 (Xenotime) group is probably one of the most dangerous groups known to date, since it attacks industrial security systems almost exclusively with destructive intent resulting in loss of life. The Thales Cyber Threat Intelligence team shares this observation. Certainly, in its report of the 66 most dangerous attackers in the world, the Centre for Technical Threat Analysis ranks the group only 30th with a score of 59 out of 100. This score means above all that the group does not represent a global threat to date, as it is extremely specialized and is not yet operational to our knowledge. However, the motivation and the technical level reached by ATK91 (Xenotime), to compromise industrial control systems, makes it a formidable attacker whose attacks can have serious consequences on the security of people and infrastructures.

A particular international context

This initial attack on Saudi interests by a group whose origin appears to be Russian is taking place in an unusual international context. It should be recalled that since the end of 2017, Russia and Saudi Arabia have been moving closer together on the diplomatic front. However, if we look at the sector targeted, namely oil, we must remember that since 2014 and the annexation of Crimea, pressure from the West on Russia has been added to the fall in world oil prices, which has plunged Russia into a recession. To stimulate investment, the Kremlin had to find capital and foreign exchange. For this reason, Russia has moved closer to Saudi Arabia, whose alliance with the United States had weakened under the Obama era in the alder of the Iranian nuclear agreement, supported by the former US President. On 1 January 2017, the two countries decided to reduce oil production volumes to 1.8 million barrels/day in order to increase the price of black gold. The attack on Triton at the end of 2017 took place 9 months later, when King Salman travelled to Moscow (November 2017) to prepare for the next OPEC+ meeting, which was supposed to lead to a further reduction in production after March 2018. Nevertheless, the last 9 months have been marked by two important events that have redefined everyone's interests. The change in US position in favor of Saudi Arabia during the Trump era by denouncing the Iranian nuclear agreement and the Gulf crisis of June 2017, which increased tension between the Kingdom and its Shiite alter ego, weakened relations between Russia and the Saudis. After the meeting of the two leaders and the attack on Saudi Arabia that paralyzed its oil company, Triton launched new attacks in 2018 in the Middle East region and against the United States. Good relations between Saudi Arabia and Russia were reconfirmed in the second week of June 2018, when Saudi Arabia and Russia agreed to stabilize oil prices at an average level of 75 dollars per barrel, while King Ben Salman and President Putin were meeting in Moscow for opening the Football World Cup, which took place on the 14th.

It should be noted that according to Dragos, the Triton group (Xenotime) is undoubtedly one of the most dangerous groups known to date since it attacks industrial security systems almost exclusively with destructive intent involving loss of human life.

Kill Chain

At the end of 2017, an oil and gas facility in Saudi Arabia experienced downtime due to an infection with a strain of malware capable of interfacing with the facility's industrial control systems. The malware was targeted at Schneider's Triconex instrumented security system. Access to the system was achieved in the classic way with phishing and hacking of the ID by changing the telephone number to receive the SMS message giving the administrator password. The group then compromised a system administrator workstation, after having laterally crossed the demilitarized zone constituting the airlock between the IT and OT network. The identifiers were then used to access and compromise the SIS controllers. The controllers were placed in Program Mode during their operation, allowing the attackers to reprogram them. The attackers stayed for almost a year in the Triconex system engineering station. It was from this starting point that they were able to send a Trojan horse to infect the memory of the SIS controllers via a zero-day operation allowing a privilege upgrade. From that point on, the attacker had complete control of the plant. One year after the intrusion, on June 3, 2017, ATK91 (Xenotime) went into attack mode. Quickly, the procedure for securing the petrochemical plant was triggered and the temperature and pressure began to drop. The machines stopped in emergency. Two months later, almost to the day, the same phenomenon occurred, suggesting a major cyber-attack.

It is believed that on the first attempt the group inadvertently shut down the plant, as some controllers shut themselves down when their

logic code failed a validation check. The protocol attacked by the group is proprietary, suggesting prior reverse engineering. In addition, the development of the tool would require access to both hardware and software that are difficult to acquire. Such an attack requires a high level of technical knowledge and, although it is unlikely to be reproducible on a large scale, it shows that the attacker is sufficiently capable of attacking and potentially causing physical damage to plants and industrial systems. The group would be linked to the Central Scientific Research Institute of Chemistry and Mechanics in Moscow for the following reasons:
- Personal links with that Institute,
- An IP address used by the attacker,
- Correspondence between business hours and working hours in Moscow.

This institution studies ways to protect critical infrastructure and develops weapons and military equipment. The group has been using test environments to check the internal workings of its malware since at least 2013. Other intrusions by this attacker into the Middle East were carried out at undisclosed dates, focusing on oil and gas companies until the end of 2018. It should be noted that the group has also begun probing energy systems in the United States and other countries.
Xenotime uses a dozen custom and public tools to carry out its attacks. The custom tools reimplement features of the public tools by adding anti-detection methods. These tools appear to be used during critical phases of the intrusion.

Attacks on industrial systems are long (several months or years) since they require learning how to exploit the target's industrial process and developing the appropriate tools. The attack is therefore preceded by a discovery, learning and preparation phase during which the attacker will set up his attack infrastructure. The infrastructure uses VPS servers from international hosting providers (OVH or UK-2 Limited), VPNs and Dynamic DNS allowing regular changes of IP addresses. After penetrating the target's network, the attacker needs to ensure persistent and very discreet access throughout the mission.

Xenotime therefore uses several methods to hide its activities:
- Renaming files to make them appear legitimate (using Microsoft Update file naming)
- Use of standard tools simulating the activity of an administrator (RDP, PsExec, WinRM)
- Editing legitimate Outlook Exchange files to open web access,
- Use of encrypted communication for sending commands and programs
- Use of multiple subfolders rarely used by users or programs,
- Regular cleaning of attack tools, activity logs, temporary files after use
- Changes to the dates contained in the files (creation and modification dates)
- Use of VPN networks, allowing to hide the IP address of the attacker

Malware persistence on compromised machines is achieved by creating an Image File Execution Options registry key or scheduled tasks. After reaching the targeted SIS controllers, the attacker focuses on deploying TRITON by limiting his activities to off-peak hours to avoid being discovered. TRITON then allows full control of these systems.

This modus operandi, largely based on a concern for non-detection, allows us to draw two conclusions. Firstly, this line of development is typical of state-sponsored attackers. The latter do not wish to be linked to offensive computer systems with a geo-strategic dimension and demand that the groups finance the greatest possible discretion. In the present case, the fact that the group is linked to a national research institution and that its modus operandi is devoted to destruction reinforces this hypothesis. The second conclusion that can be drawn from this emphasis on concealment is that it confirms the non-operational nature of the attacker's arsenal at the time of the attack. The ambition is to remain as long as possible in the target's systems in order to increasingly test his tool.

The case of this group shows that the theory of security by darkness, which consists in thinking that an ICS/SCADA system is complex and therefore secure, no longer holds. The rise in the quality of attacker groups, the generalization of protocols and the standardization of systems have changed the situation.

_USED MALWARES

- Cryptcat
- Mimikatz
- SecHack
- Triton/Trisis

_USED TOOLS

- Plink

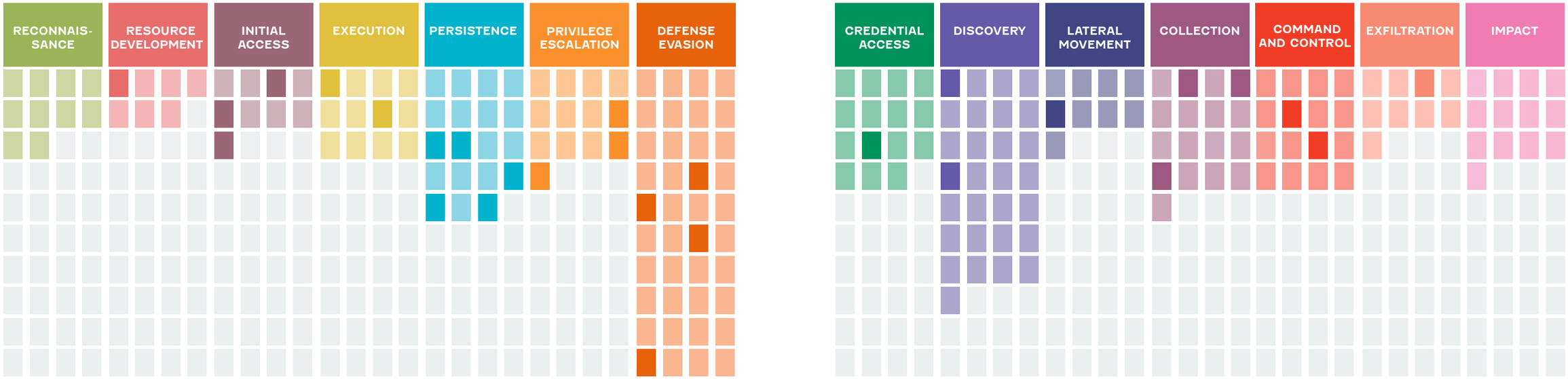
_ATTACKS HAPPENED ON

> **Campaign leveraging the Triton malware**
Happened on: 2017-01-09

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1003 - OS Credential Dumping
T1021 - Remote Services
T1021.001 - Remote Desktop Protocol
T1027.005 - Indicator Removal from Tools
T1036 - Masquerading
T1048 - Exfiltration Over Alternative Protocol
T1053 - Scheduled Task/Job
T1059.001 - PowerShell
T1070.004 - File Deletion
T1070.006 - Timestomp
T1074 - Data Staged
T1078 - Valid Accounts
T1087 - Account Discovery
T1119 - Automated Collection
T1133 - External Remote Services
T1135 - Network Share Discovery
T1505.003 - Web Shell
T1546.012 - Image File Execution Options Injection
T1560 - Archive Collected Data
T1566.001 - Spearphishing Attachment
T1566.002 - Spearphishing Link
T1571 - Non-Standard Port
T1573 - Encrypted Channel
T1583 - Acquire Infrastructure

_CYBER ATTACK PHASES



Threat Actor_

ATK92
The group is engaged both in cyber criminal attacks as well as in targeted attacks against worldwide governmental organizations.

Alias_

_Gorgon group
_Subaat
_TAG-CR5

Targeted Sectors_

_Government and administration agencies

Languages_

_Urdu

Motivations_

_Financial Gain

Targeted Areas_

NORTH AMERICA
United States Of America

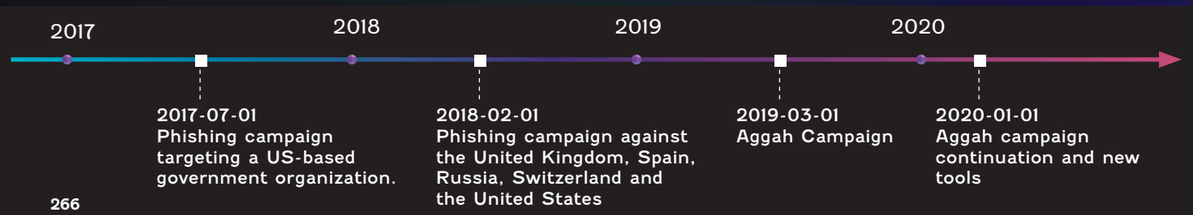
WESTERN EUROPE
United Kingdom Of Great Britain And Northern Ireland
Spain

MIDDLE EAST/ WESTERN ASIA
Saudi Arabia

RUSSIA
Russian Federation

Suspected origin of the attacker_

Pakistan



_DESCRIPTION

ATK92 - (aka: Gorgon Group, or Aggah) is engaged both in cyber-criminal attacks as well as targeted attacks against worldwide governmental organizations. The group is active since 2017 and is believed to be operating from Pakistan. The group's campaigns targeted government organizations in the United Kingdom, Spain, Russia, and the United States. The infection chain of their attacks usually starts by phishing emails containing trojanized documents, which will launch powershell commands and configure the C2.

_USED MALWARES

- Crimson
- LokiBot
- Nanocore
- QuasarRAT
- RemcosRAT
- RevengeRAT
- njRAT

_USED TOOLS

- Bitly
- Living off the Land
- PowerShell
- QuasarRAT

_USED VULNERABILITIES

- CVE-2012-0158
- CVE-2017-0199

_ATTACKS HAPPENED ON

> **July 2017: Phishing campaign targeting a US-based government organization.**
Happened on: 2017-07-01

> **February 2018: Phishing campaign against the United Kingdom, Spain, Russia, Switzerland and the United States**
Happened on: 2018-02-01

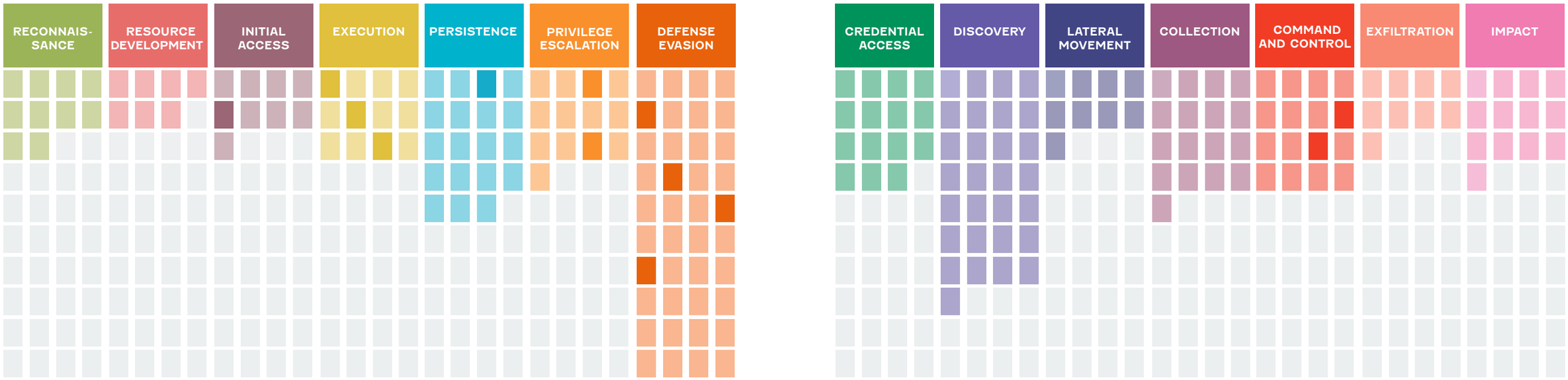
> **March 2019: Aggah Campaign**
Happened on: 2019-03-01

> **2020 — Aggah campaign continuation and new tools**
Happened on : 2020-01-01

_MITRE ATT&CK® TECHNIQUES USED BY THIS ATTACKERS GROUP

T1055 - Process Injection
T1055.012 - Process Hollowing
T1059 - Command and Scripting Interpreter
T1059.001 - PowerShell
T1105 - Ingress Tool Transfer
T1106 - Native API
T1112 - Modify Registry
T1140 - Deobfuscate/Decode Files or Information
T1204 - User Execution
T1547.001 - Registry Run Keys / Startup Folder
T1547.009 - Shortcut Modification
T1562.001 - Disable or Modify Tools
T1566.001 - Spearphishing Attachment
T1571 - Non-Standard Port

_CYBER ATTACK PHASES



Targeted sectors

Targeted sectors

_Automotive

_UNDERSTANDING THE CYBER THREAT

Billions are being lost due to the rise of cyber attacks in the automotive industry. Industry experts argue that there are several factors that can cause cyber attacks to target this innovating sector. Over the years, cyber attacks have evolved and the emergence of highly autonomous vehicles in the automotive fleet has aroused the interest of attackers in the cyber domain. Today, if the research of vulnerabilities is focusing on this industry, it indicates the importance and destructive potential of the forthcoming threat to the sector. In order to protect vehicles from these malicious behaviors, it is imperative to dive into the type of threats that can affect a vehicle.

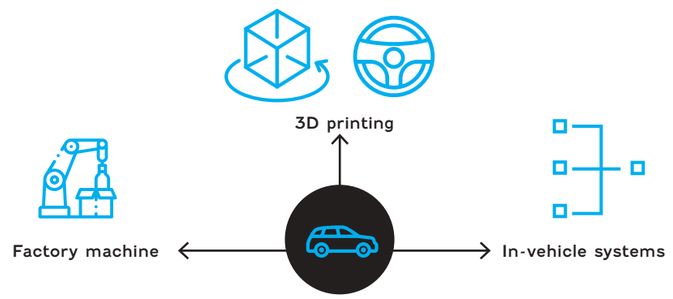
_THE MAIN ENTRY POINTS FOR ATTACKERS

- The three most common attack vectors over the past decade were servers, keyless entry systems and mobile applications, with a 73% growth in server attacks in 2020.
- IIn 2020, 77.8% of all incidents were remote attacks and 89.9% of the attacks were related to vehicle's communication channels
- Threats against vehicle data and code account for 86.7% of all incidents
- There were 110 CVEs related to the automotive industry, 33 in 2020 and 24 in 2019
- 40% of cyber activities against vehicles resulted in car theft, which makes it the category with the greatest impact on mobility

_THE JEEP HACK (MILLER AND VALASEK)

The Jeep hack is widely regarded as a landmark event in the automotive industry's understanding of the cybersecurity challenges it faces. In 2015, two researchers, Miller and Valasek exploited a vulnerability in the CAN (controller area network) bus of the Chrysler-manufactured vehicle. The bus corresponds to the car's internal network. It oversees the various components within the vehicle such as the engine, sensors and transmission. Taking control of the CAN bus allowed them to send commands to the car, cutting the brakes or running it off the road. This event is not isolated since in 2016, a team of Chinese hackers managed to take control of a Tesla Model S by creating a Wi-Fi hotspot to which the car automatically connects if it is performing Web browsing. This allowed them to access the CAN bus from which they could send commands and engage the brakes. By connecting physical device to internet, for convenience, car manufacturers have created multiple entry points for agile and malicious attackers.

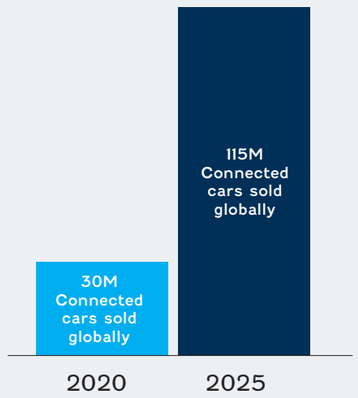
Potential macro entry point



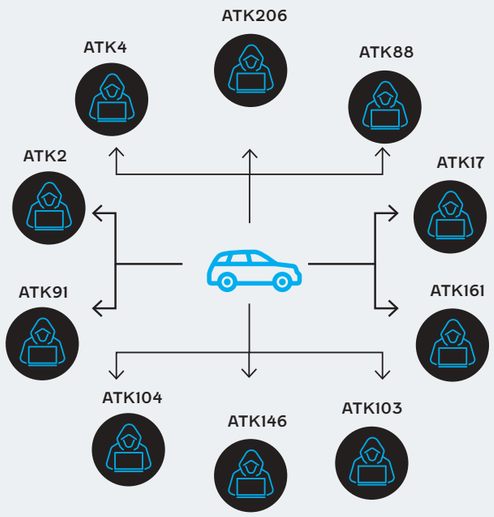
_ATTACKER'S MOTIVATIONS

- In 2020, 55% of hacks were carried out by hackers to disrupt business, steal property and demand ransom
- In 2020, 38.6% of hacks were committed by hackers and researchers with 36% of incidents in 2020 involving data and privacy breaches, and 28% of incidents involving theft or break-ins, including in the context of an automotive bug bounty scheme
- In 2019, for the first time, the number of black hat hacks surpassed the number of white hat intrusions

Number of connected cars sold worldwide



Attackers known to have targeted the automotive sector



Components exposed to the cyber threat

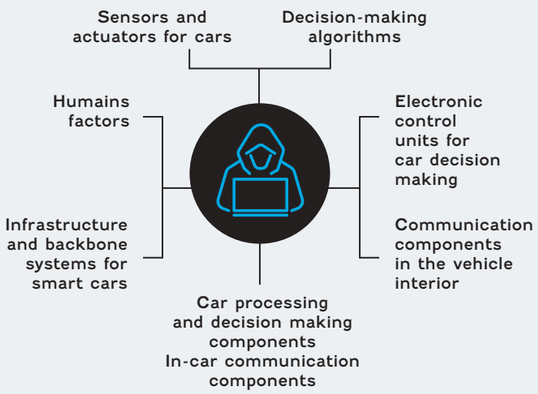
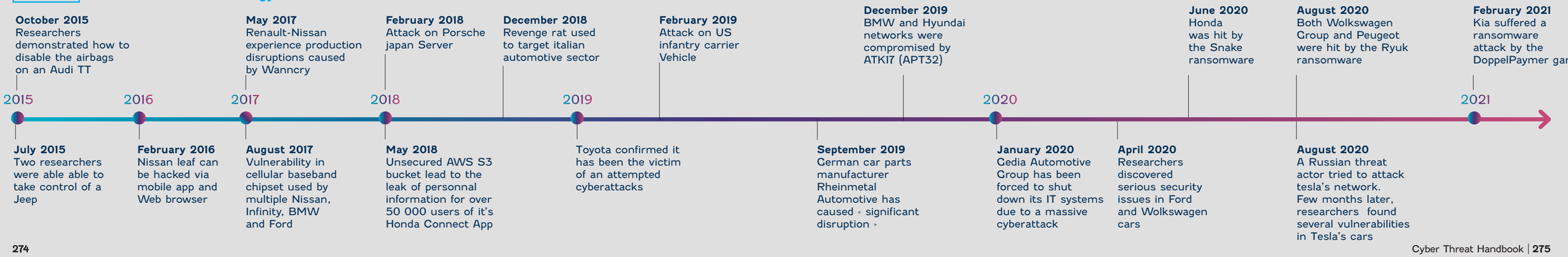


FIGURE 4 Timeline of the Victimology



_Aviation

_UNDERSTANDING THE CYBER THREAT

The protection of airport IT systems is a major issue today and in the very near future. Even a relatively minor bug can cause chaos, resulting in flight delays and legal action by disgruntled passengers. The Delta Airlines computer system failure in 2016 is a good example of this phenomenon, as it caused problems for hundreds of thousands of people worldwide who had their flights delayed or cancelled. The threat to the airport sector concerns simultaneously the ground infrastructure, the aircraft and the passengers. Now, taking into account its destructive potential, this particular threat has emerged as a real concern for the Aviation industry.

_CYBER THREAT LANDSCAPE

Attacks are up in all threat categories, and better reporting alone does not fully account for the 530% year-on-year rise in reported incidents. Airlines are the first in the line of fire, targeted by 61% of all 2020 aviation-related cyber-attacks in 2020. In 2020, international passenger traffic fell by 75.6% and domestic traffic by 48.8%. However, as passenger traffic declined, cyber attacks on the aviation sector are reported to have increased.

_MAJOR THREATS

At 36% of all reported incidents, data theft topped the cyber charts in 2020, followed by website fraud (35%) and phishing (16%). A notable and growing threat, which currently accounts for only 5%. but whose negative effects can be immense if successful, is ransomware.
A worrying 39% of organizations experiencing cyber-attacks in 2020 assessed that these attacks had a medium to high impact on their operations. Indeed, according to the severity of the attacks, 12% of the attacks were classified as high, 27% as medium and 61% as low severity.

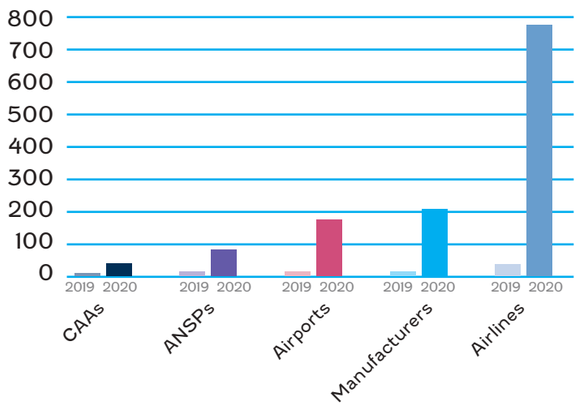
_RANSOMWARE AND THE AVIATION SECTOR

- Every week, an aviation actor suffers a ransomware attack somewhere in the world, with big impacts on productivity and business continuity, let alone data loss and/or costly extortion demands paid in order to restart operations.
- Ransomware may only comprise 5% of detected cyber-attacks on aviation in 2020, but it can have far-reaching impact for the individual players who fall victim to it.

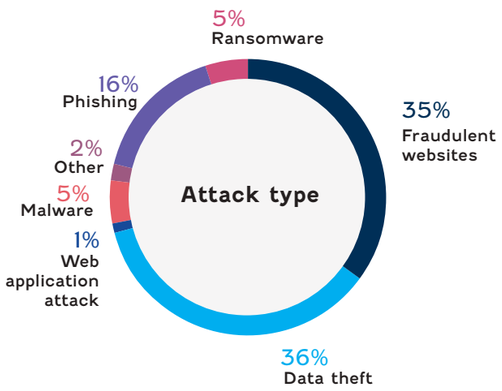
_CYBER-HIJACKING

If serious incidents involving the cyber-hijacking of an aircraft have not been observed in the wild, tampering with airplane systems is a source of concern for researchers. In 2015, expert Chris Roberts claimed to the FBI that he had successfully penetrated multiple in-flight entertainment systems and was able to briefly change an aircraft's direction. This case caught the attention of the DHS (Department of Homeland Security), which issued an alert recognizing the potential for an attack on an airplane. In 2019, DHS released another document highlighting that a malicious threat actor with physical access to a small aircraft would be able to alter flight information via the autopilot system. In addition, exploiting vulnerabilities in satellite communication technology (SATCOM) could be a vector for compromising in-flight communication devices according to Sanatamarta's research work.

Number of cyber attacks by segment



Breakdown of reported cyber attacks



Attackers targeting the aviation sector

ATK206	ATK57
ATK223	ATK123
ATK231	ATK129
ATK35	ATK130
ATK11	ATK133
ATK6	ATK134
ATK19	ATK140
ATK40	ATK157
ATK44	ATK163

The growing ransomware tab, all sectors between 2017-2020

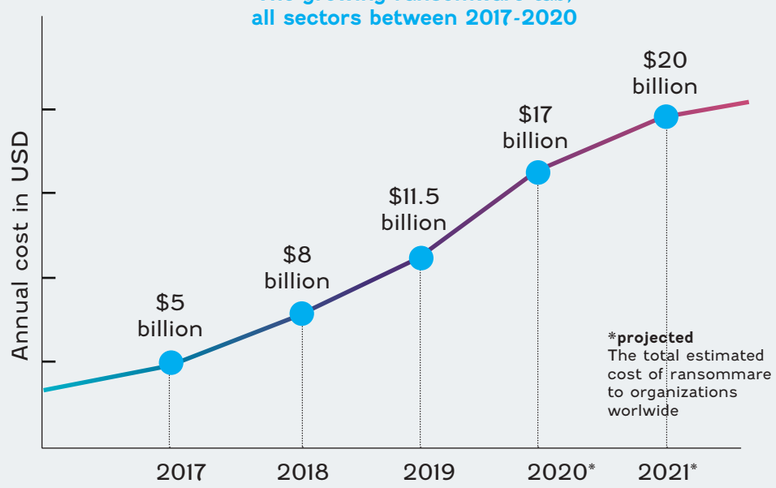
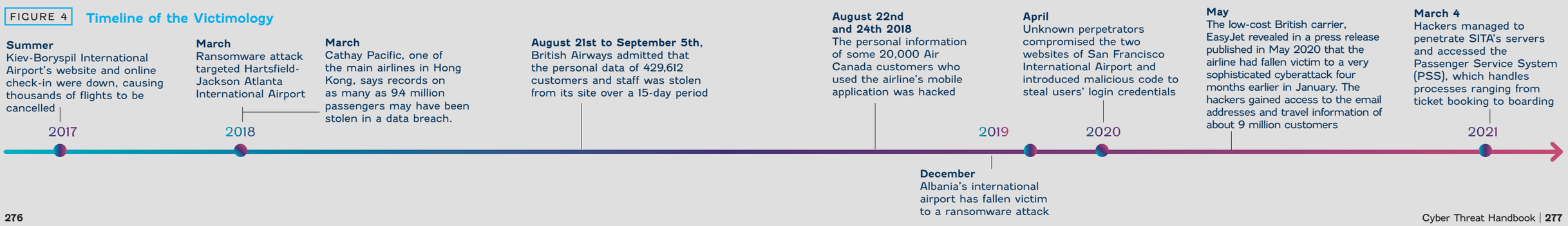


FIGURE 4 **Timeline of the Victimology**



_Communication

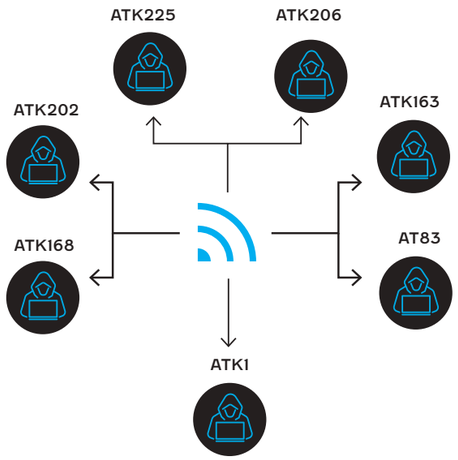
_UNDERSTANDING THE CYBER THREAT

The telecommunications industry is a significant target for both cybercriminal and state-sponsored attacks. Cyberattacks on this industry can affect a wider range of victims beyond the industry itself because the use of telecommunications services by businesses and consumers alike is so pervasive. In particular, many businesses in other industries depend on telecommunications service providers to manage relationships with customers, or for their own phone and internet services. Breaches at telecommunications service providers can impact other companies' external internet traffic and customer relationships.

_IMPACTS OF CYBERSECURITY ON TELECOMMUNICATIONS

Hackers understand the importance of the sector that keeps the world connected and broadly supports economies and business infrastructures. A successful attack on a telecommunication service provider has far-reaching consequences, not just on the organization and its clients but also on a nation.
On the other hand, the telecommunication sector acts as a gateway to millions of other businesses. Hackers will attempt to infiltrate on the telecom core infrastructure to intercept user calls or penetrate subscribers' networks. Such scenarios cause significant damage to business reputation and data privacy.

Attackers known to have targeted the telecommunication sector

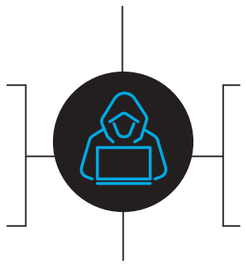


Common Cyber threats Affecting the Telecommunication Sector

Vendor and Supply Chain Risks
In 2017, an estimated 19% of data breaches were directly attributed to vendors. Telecommunication firms outsource less essential processes to service providers.

Malware
Cyber attackers engage in malware activities to target subscribers and devices connected to telecommunication services. They infect smartphones with malware downloaded through untrusted and insecure apps.

Social Engineering
Cybercriminals use social engineering and phishing attacks to infiltrate businesses and subscribers in the telecommunication sector.



DDoS Attacks
Distributed denial of service (DDoS) is a common direct attack in the telecommunication sector. While DDoS is not unique only for this industry, telecommunication firms receive these attacks more than any other sector.

Man-in-the-Middle Attacks (MITM)
Cybercriminals target telecommunication service providers by intercepting routes and misconfiguring services. This attack allows hackers to spy on victims, steal sensitive information, and disrupt services.

Government Surveillance
Government agencies launch infiltration attempts on telecommunication infrastructure and service providers to establish surveillance on citizens. With a vast pool of resources, government actors deploy advanced persistent threats.

Map showing the victims of the scam

_TELECOMMUNICATIONS AND MESSAGING APPLICATIONS: MAJOR VECTOR OF CYBERCRIME

Applications such as WhatsApp, Telegram or Signal still contain numerous security holes that make it difficult for malicious actors to carry out attacks and target a wide range of users. For example, a new automated as-a-service scam has been discovered exploiting Telegram bots to steal money and payment data from their European victims.

_TELECOMMUNICATIONS AND MESSAGING APPLICATIONS: CYBERESPIONNAGE CAMPAIGN

Today, instant messaging applications are often confronted with nation-state sponsored attacker groups carrying out cyber espionage campaigns via messaging applications like Telegram or Signal.
The main risk is that APT attackers will take advantage of the influx of WhatsApp users to Telegram or Signal to expand their victim base without users being aware of the threat.
Several APT threat actors such as ATK51 or ATK66 (APT-C-23) have played a major role in attacks using WhatsApp or even Telegram.
Furthermore, applications such as Telegram can become a placeholder for the DarkWeb as shown by the leak of several malware source codes belonging to the ATK51 group (MuddyWater). Indeed, a group calling itself «Green Leakers» used Telegram channels to sell ATK51 data.

_TELECOMMUNICATIONS AND MESSAGING APPLICATIONS : MAJOR CONSEQUENCES

The same users who decided to change their email application such as WhatsApp, due to non-compliance with the data policy, are not yet sufficiently aware of the increasing number of cybercriminal attacks on applications such as Telegram or even Signal, which are becoming a new theatre of operations for organized cybercrime.
With the rise of WhatsApp users migrating to Telegram for example, the risk of a benevolent user ending up on a GreenLeakers type channel is very high.

_Civil Society

_UNDERSTANDING THE CYBER THREAT

Civil society refers to non-profit, citizen-based groups that are organized at the local, national or international level. These groups can take a variety of forms, ranging from unions and communities to think tanks and NGOs. The very nature of their activities (often related to the political sphere) coupled with limited budgets (non-profit) to implement protective security measures make them an enticing target for malicious actors. This intuition is borne out in the wild as civil society organizations and faces a dense cyber threat landscape, both in terms of numbers and variety of threat actors. From a hacker's perspective, the Civil Society represents a rich environment as organizations process credit card data for donations and may store personal information or even IP data.

_CYBERTHREAT LANDSCAPE: NGOS AND CHARITIES

NGOs appear in many aspects as the embodiment of the challenges faced by the Civil Society as a whole. According to a survey conducted by the Institute for Critical Infrastructures over NGOs and NPOs, 50% of the respondents revealed they had been targeted by a ransomware and nearly half (49%) admitted they did not rely on a specific unit to deal with cybersecurity issues. This gap can be explained in part by the participatory funding of these organizations and the prioritization of expenditures towards operational needs.

Looking at charities, which are critical in the civil society ecosystem, a few trends are worth noting. First, while many services have gone digital, the rate of reporting cyberattacks has remained steady. Just over one in four charities (26%) reported being the target of a cyberattack in 2020, and this trend seems to correlate with the size of the organization, as 68% of very high revenue charities recorded at least one cyber incident. 80% of breaches involve a phishing scheme.

_AN APPEALING TARGET FOR STATE ACTORS

At 32%, NGOs represent the largest sector targeted by nation-state nefarious activities, ahead of professional services and government organizations at only 13%. While both government agencies and politically oriented NGOs collect public policy information, the lack of safeguards encourages threat actors to prioritize targeting the latter civil society organizations. In 2019, Microsoft observed 740 intrusion attempts from nation-state actors targeting democracy-focused civil society organizations in the U.S.-including political parties and think tanks involved in the election process. The structure of American civil society is interesting because organizations in this ecosystem are hailed as major players in the national political debate. This has prompted adversaries of the United States - namely China, Iran and Russia - to launch cyber operations to retrieve any sensitive political content that these organizations may have. This includes projections on the leading policy issues as well as staff and contact information.

Chinese-affiliated actors have launched particularly aggressive campaigns targeting U.S.-based NGOs working on issues related to human rights and democracy in China. In these campaigns, the exfiltration of sensitive data has not been limited to the NGO's programming but has included a wide range of internal information, including legal and research resources. This gave them a very clear picture of how these civil society groups operate.

_MAIN THREAT VECTORS

- Spear-phishing: use of spoofed email address to send malicious URLS and ultimately gain credential access of employees
- CEO fraud: combines spear-phishing and identity theft to lure naïve employees into making money transfer. The associations Save the Children and Roots for Peace both lost more than $1 million following a CEO fraud

_INTERFERENCES IN POLITICAL CAMPAIGNS

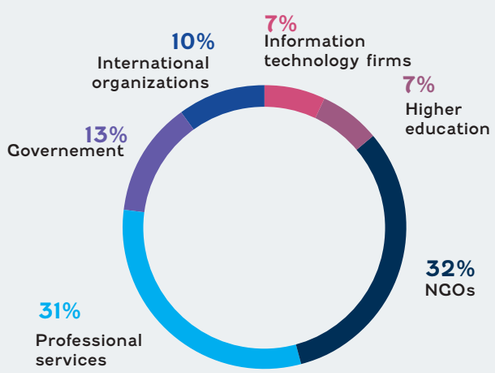
It is undeniable that political campaigns represent an opportunity for attackers seeking to undermine trust in the electoral process. As such, democracy-based organizations face intensive malicious activity as election periods approach. The 2016 U.S. and 2017 French presidential elections were marked by numerous cyberattacks, which attempted to undermine Western democracies. In 2016, two groups of Russian hackers successfully penetrated the U.S. Democratic National Committee network and exfiltrated sensitive emails in an effort to support Donald Trump's candidacy.

_A BROADER DEFINITION OF CIVIL SOCIETY: DISSIDENTS, JOURNALISTS, MINORITIES

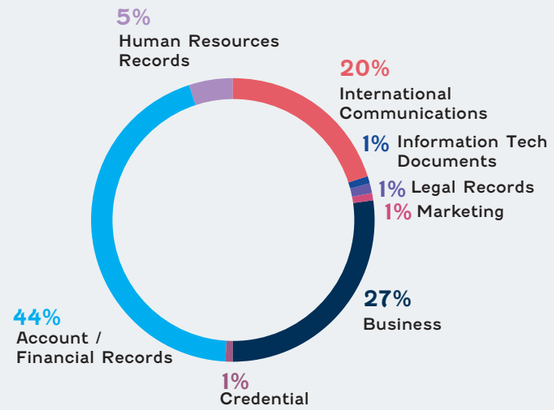
- 2014: a report by FireEye revealed APT28's activities and its specific targeting of civil society particularly journalists - to monitor public opinion and political dissent. This pattern was echoed by TrendMicro, which identified civil society as the primary target of APT28's domestic operations
- October 2018: Citizen Lab released a report revealing that the Saudi Arabian government had infected with a spyware the phone of the political dissident Omar Abdulaziz. The spyware was identified as "Pegasus", a product developed by Israeli company NSO group
- May 2021: High-profile targets within the Uyghur community in China and Pakistan were targeted by a phishing campaign in which Chinese hackers posed as the United Nations to trick users into opening a link that would install a backdoor. The objective of this campaign was cyber-espionage

Interestingly, cyber attacks against civil society receive little attention from leading CTI firms. This may be due to the lack of financial resources for civil society to purchase threat intelligence. Therefore, one should keep in mind that commercial threat reporting will tend to focus on sectors that can afford CTI services rather than segments that cannot.

Top 6 industry targeted by nation-state actors



Resources targeted by threat actors in civil society organizations



Ohio church : April 2019
Near Cleveland, a church fell victim to a business email compromise (BEC) scam, leading to a loss of $1.75 millions.

Vietnamese Overseas Initiative for Conscience Empowerment (VOICE) : May 2021
VOICE fell off to a cyberattack allegedly perpetrated by ATK17 (aka Ocean Lotus), a hacker group affiliated with the Vietnamese government.

EU DisinfoLab: July 2021
EU DisinfoLab was targeted by a phishing scheme in an attack attributed to Nobelium, the gang responsible for the SolarWinds cyberattack

Royal Dublin Society (RDS) : February 2022
The RDS systems were crippled by a ransomware attack that affected the confidentiality of personal information belonging to employees and exfiltrated by the attackers

2019 — 2020 — 2021 — 2022

Philadephia Food Bank: December 2020
Philadelphia Food Bank, the region's largest hunger relief organization, lost $1 million to a business email compromise (BEC) scam. This occurred while 5.6 million U.S. citizens were dependent on food distributions due to COVID-19.

Volunteer Service Abroad : May 2021
Volunteer Service Abroad, the largest international development volunteer agency based in New Zealand, was hit hard by a ransomware attack that locked down its networks.

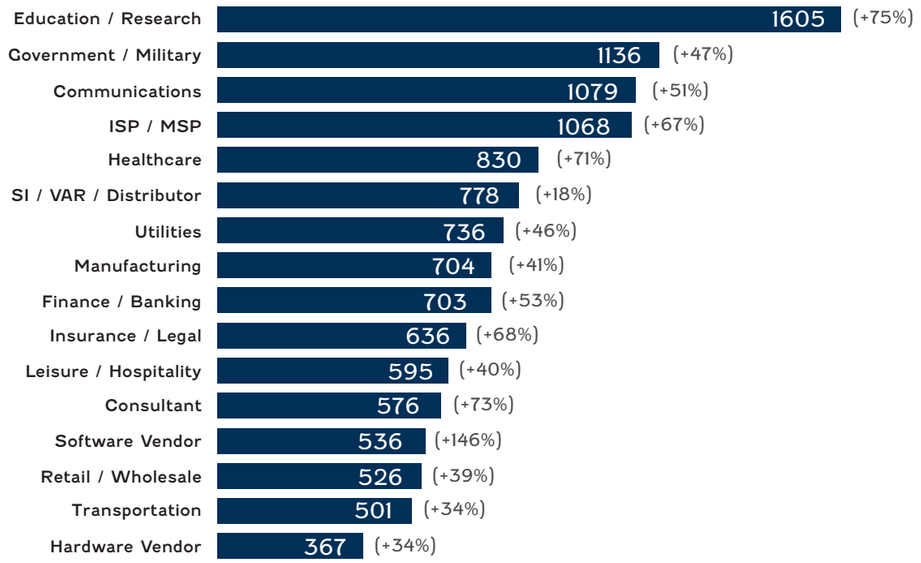
Red Cross : January 2022
The International Committee of the Red Cross fell victim to a cyberattack that compromised the data of 515,000 persons

_Education

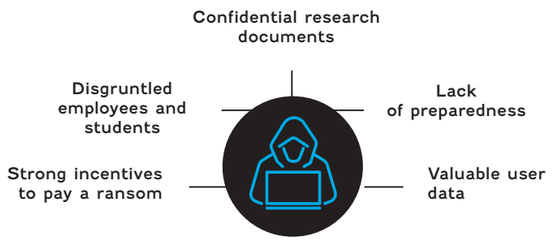
_UNDERSTANDING THE CYBER THREAT

Schools and higher education institutions were among the most popular targets in 2021. According to Checkpoint, Education and Research was the industry most targeted by cyberattacks in 2021, with organizations facing 1605 security attacks per week. This figure represents a 75% year-on-year surge. For comparison, cyberattacks across all industries have increased by 50% over the period. The reasons behind this growth appear as both structural (valuable user data, chronic under-appreciation of cybersecurity), as well as cyclical with the complex adaptation of pedagogical methods to the COVID 19 pandemic. This combination of factors seems to explain why, despite the sector facing major challenges such as a lack of staff and a lack of funding and resources, the prevalence of cyberattacks seems to be increasing year after year, as breaches in schools and higher education are widely reported.

Average weekly attacks per organization, by industry 2021, compared to 2020



Five key reasons why Education is a target for cybercriminals.



_EVIDENCE THAT EDUCATION IS A TARGET FOR CYBER-CRIME

The NCSC (National Counterintelligence and Security Center) continues to respond to an increased number of ransomware attacks affecting education establishments in the UK, including schools, colleges, and universities. Three reasons can be put forward to explain the attractiveness of the sector for the cybercriminal ecosystem.

First, universities and educational institutions hold valuable data that can be mined. They have valuable information about students and employees, namely medical records, PII (personable identifiable information) and financial information.

Second, their attack surface has grown rapidly over the past two years. Most companies are increasingly adopting new cloud and digital platforms, allowing them to be much more effective than in the past. Educational institutions are no exception to this trend. Indeed, many had to react quickly to challenging remote working conditions to add new capabilities for engaging learners and storing files. COVID 19 in that regard created avenues for hackers to exploit remote systems. The limited budgets of certain institutions and notably pubic schools further contribute to their vulnerability.

Third, paying ransom in the event of computer systems being encrypted by ransomware often appears to be the most viable option for organizations that cannot justify halting educational services.

These arguments are reflected in the fact that 13% of educational institutions have experienced a ransomware attack. This compares to 5.9% for government institutions and 3.5% for healthcare organizations.

_OTHER MOTIVATION : USE CASE SHED LIGHTS ON ESPIONAGE-DRIVEN PLAYERS

As part of a campaign that begun in April 2017, cyberattacks from Chinese attacker groups have targeted U.S. universities in an effort to collect military type intelligence. The information sought was related to underwater technology and although no public notice has been issued, some institutions may have been compromised. This demonstrates the value of academic research for states seeking information of strategic interest. Between 2013 and 2017, Iranian hackers had already implemented a phishing scam to recover the passwords of hundreds of professors of American universities.

_CYBERATTACKS WITH SIGNIFICANT CONSEQUENCES

Far reaching consequences often arise from cyberattacks on the education and research industry. The NSW Department of Education was hit by a cyberattack in July 2021, provoking an utter paralysis of the education system. In January 2022, Albuquerque Public Schools district fell off to a cyberattack. The attack forced the superintendent Scott Elder to announce the cancellation of classes for two days in a row. This affected 75,000 students, or one in five school children in New Mexico. Likewise, a ransomware attack forced Howard University to cancel classes and shut down campus network in September 2021. Some organizations turn to another solution, paying the ransom, thus having to bear a financial drop-off. The University of California, San Francisco decided to pay part of the ransom ($1,14 millions) demanded by the Netwalker extortion group in order to decrypt their system and recover their data. In 2020, 77 individual cyber-extortion attacks affected nearly 1800 schools and resulted in $6.6 billions of recovery costs alone.

ATK206	ATK17	ATK73	ATK129
ATK217	ATK18	ATK77	ATK130
ATK219	ATK19	ATK78	ATK131
ATK1	ATK27	ATK98	ATK133
ATK2	ATK29	ATK101	ATK134
ATK32	ATK40	ATK103	ATK135
ATK35	ATK49	ATK109	ATK136
ATK22	ATK51	ATK115	ATK137
ATK9	ATK37	ATK121	ATK140
ATK13	ATK55	ATK123	ATK142
ATK15	ATK67	ATK127	ATK143
ATK153	ATK157	ATK167	

_OTHER MOTIVATION : DISGRUNTLED EMPLOYEES/STUDENTS

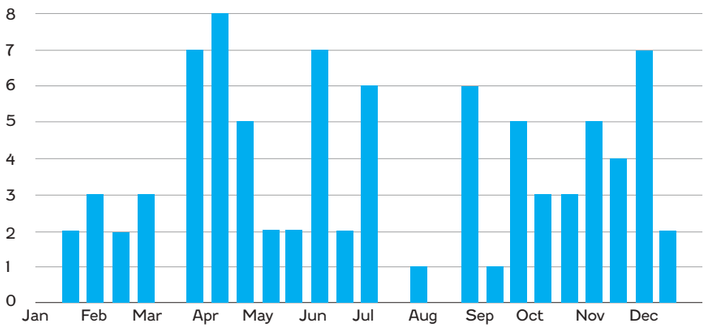
With 20% of attacks being the work of an internal actor, educational services are one of the sectors most affected by this threat. It can result in DDoS attacks from disgruntled students or staff. In September 2015, the University of London was affected by a DDoS attack from an employee who was targeting the senior executive responsible for his dismissal.

_FAMOUS RANSOMWARE GANGS

Plenty of different behaviors are observed from ransomware operators with regards to the education and research industry. Some operators have an ethic chart preventing them from infecting essential services such as government, healthcare organizations and education institutions. Other operators do not abide by those strict principles and contemplate the sector as an easy target. In March 2021, the FBI issued a FLASH, a document alerting education institutions of the surge of attacks directed at the sector by the actor dubbed PYSA. The Grief ransomware is another cyber-extortion actor targeting education institutions. In May 2021, the group stated it had exfiltrated 10 Gb of personal and internal data belonging to a school district in Mississippi. Schools in Virginia and Washington state were also allegedly hit by the Grief operators.

Ransomware victims in the education sector in 2021

01 Jan 2021 - 01 Jan 2022



_Energy

_UNDERSTANDING THE CYBER THREAT

There are three characteristics that make the sector particularly vulnerable to contemporary cyber threats:

- First, an increased number of threats and actors targeting public services: state actors seeking to cause security and economic disruption, cyber criminals who understand the economic value represented by the sector, and hacktivists seeking to publicly express their opposition to general utility projects or programs
- Second, the extensive and growing attack surface of utilities, resulting from their geographic and organizational complexity, including the decentralized nature of many organizations' cyber security leadership
- Finally, the electricity and gas sector's unique interdependencies between physical and cyber infrastructure make companies vulnerable to exploitation

_POWER LANDSCAPE

- The Power Sector is in transition. Global trends are creating an environment of disruption and driving the need for digital industrial software and services for the energy industry to become more efficient, reliable, secure, and sustainable
- At the end of 2018, more than 456 commercial nuclear power reactors (>400 GW) are in operation and provide about 12 percent of the world's electricity. More than 140 GW of new capacity are foreseen by 2025
- Organizations in the sector are thus expanding their networks and making them more efficient and dedicated through increased digitalization. This implies an extension and a strengthening of SCADA and ICS systems

Potential threat impacts

GENERATION

Disruption of service and ransomware attacks against power plants and clean-energy generators

TRANSMISSION

Large-scale disruption of power to customers through remotely disconnecting services

DISTRIBUTION

Disruption of substations that leads to regional loss of service and disruption of service to customers

NETWORK

Theft of customer information, fraud, and disruption of services

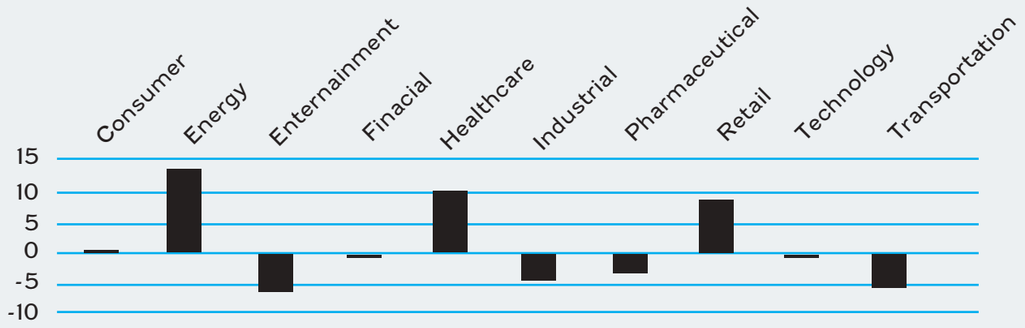
Attackers targeting the energy sector

ATK178	ATK26	ATK23	ATK49	ATK97
ATK119	ATK35	ATK25	ATK51	ATK99
ATK217	ATK22	ATK28	ATK37	ATK101
ATK228	ATK11	ATK34	ATK50	ATK103
ATK3	ATK6	ATK40	ATK65	ATK106
ATK243	ATK9	ATK41	ATK120	ATK115
ATK4	ATK10	ATK42	ATK88	ATK116
ATK5	ATK14	ATK36	ATK89	ATK117
ATK32	ATK19	ATK46	ATK91	ATK118
ATK157	ATK146	ATK142	ATK140	ATK134
ATK131	ATK122			

_POWER LANDSCAPE

Energy was the most targeted industry for cyber attacks worldwide in 2019.
Attacks in the energy sector are becoming increasingly expensive.
The energy sector saw the largest increase in data breach costs in 2020.

% change in average data breach cost by industry, 2019/2020



_USE CASE 1: THE DARKSIDE RANSOMWARE AND THE COLONIAL PIPELINE COMPANY

In early May 2021, the Colonial Pipeline suffered a ransomware attack that forced it to shut down its entire network to prevent the malware from spreading.
Indeed, Colonial Pipeline, the largest oil pipeline in the United States, halted its operations after suffering what is believed to be a ransomware attack. Colonial Pipeline transports refined petroleum products between refineries on the Gulf Coast and markets in the southern and eastern United States. The company transports 2.5 million barrels per day through its 5,500-mile pipeline and supplies 45% of all fuel consumed on the East Coast.

_THE DARKSIDE RANSOMWARE:

- Interestingly, the malware used by Darkside does not seem to target CIS (Community of Independent States) countries and has a very good debugger and detection of virtual environments. The sample was found in multiple versions, using multiple packers, which may indicate that the attacker is running tests. One uncommon thing is that the URL of the data is in the hardcoded ransom note, which indicates that the malware was compiled after the data was stolen
- High profile attacks previously conducted by the DarkSide gang include CompuCom, Discount Car and Truck Rentals, Brookfield Residential, and Brazil's Companhia Paranaense de Energia (Copel)

_WHAT THE ATTACKS DEMONSTRATE:

- This attack demonstrates how a cybercriminal attack can affect the national security of a state. Indeed, the attack forced the company to shut down 5,500 miles of fuel lines, and led the Federal Motor Carrier Safety Administration (FMCSA) to issue a regional emergency declaration affecting 17 east coast states and the District of Columbia.

Colonial Pipeline system map

_REMEMBER

In 2015, Ukraine also suffered a cyberattack that had dramatic consequences for national security, causing a major electrical blackout in the west of the country. This incident is a landmark as it was the first successful cyberattack on a power grid. Hackers managed to access the systems of three energy distribution companies, forcing them to temporarily shut down their operations.

_TARGETED AND NON-TARGETED ATTACKS IN THE ENERGY SECTOR

In order to describe the threat landscape, we need to distinguish between two major types of attacks:

- **Non-Targeted attacks**: Not Power Sector specific. Could be targeting and overall vulnerability in an IT and / or OT system. Main intention is to maximize, spread the attack surface to multiple targets. Often IT focused, via Internet / Email, but also seen on OT / ICS equipment
- **Targeted attacks**: Specialized on the target or the industry. Often is tailored to infiltrate a specific type of equipment and using tailored attack methods. Actors are often extensively planning the attack in detail, have access to above average resources and using unknown methods

FBI statement concerning the attack's attribution

_SPECIFIC OT VULNERABILITIES / CHALLENGES

- The relatively small userbase of the OT local area control network and lack of a direct connection to the internet or email greatly diminishes the attack surface available to ambitious cybercriminals compared to the much more exposed IT environment.
- This difference tends to influence-hackers to utilize the IT network as an easier attack vector into OT (indirect attack). Forensic analysis of some focused attacks on critical infrastructures show that access to the control network was gained by first compromising the more exposed IT network
- The preferred attack vector is often a successful email phishing campaign that either sophisticated malware to be installed which later allows successful harvesting of usernames and passwords and network architecture

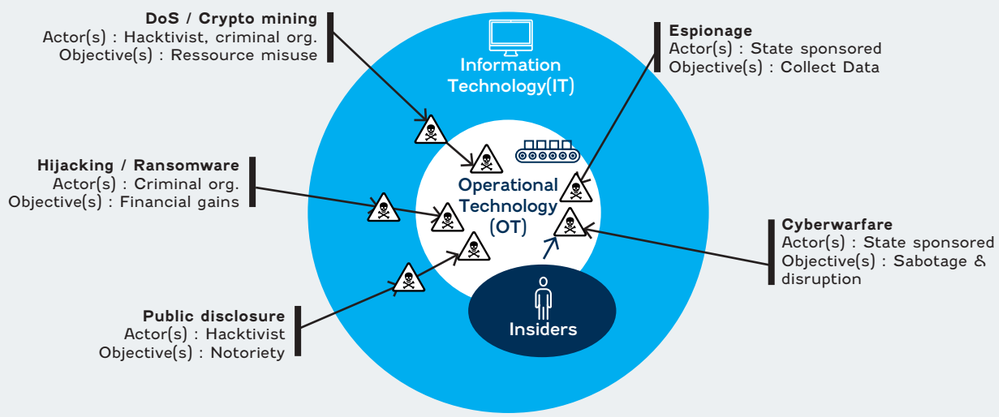
_ICS/SCADA THREATS AND THREAT ACTORS

- Industrial control systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems play a critical role in critical infrastructure and industrial sector
- The number of vulnerabilities discovered in industrial control system (ICS) products in 2020 (893 flaws) was 24,72% higher compared to 2019 (716 flaws)
- 449 vulnerabilities were disclosed affecting ICS products from 59 vendors in the second half of 2020. The situation is worrisome considering that more than 70

Archetypes of the sector threat and use cases developed

	TARGETED	UNTARGETED
Direct	ATK91 (Xeontime) attack on saudi petrochimical plant	DragonFly 2.0 changes target and focuses on the energy sector
Indirect	ATK6 targets suppliers in the energy sector who offer devices and services for ICS Systems	ATK88 crashes Norsk Hydro's OT system with LockerGoga ransomware

Examples of Direct vs In-direct OT attacks and objectives



percent of the issues received a high or critical CVSS (Common Vulnerability Scoring System) score
- The most affected critical infrastructure sectors in the second half of 2020 are manufacturing (194 vulnerabilities), energy (186), water and wastewater (111), and commercial facilities (108)

_USE CASE 2: ENEL GROUP : RANSOMWARE EKANS ET SYSTÈMES ICS

- June 6, 2020: Disruption of the company's internal computer network
- June 7, 2020: Confirmation of the attack. The incident is the work of ransomware operators EKANS (SNAKE). Enel has not commented on the name of the ransomware used in the attack, but security researcher Milkream found a SNAKE / EKANS sample submitted to VirusTotal on 7 June that shows it is looking for the domain «enelint.global»
- June 8, 2020: All connectivity has been safely restored

_THE EKANS RANSOMWARE:

- EKANS is an obfuscated ransomware written in the Go programming language, first observed in late December 2019. Its activity is similar to MEGACORTEX version 2 which appeared in mid-2019
- It checks for the existence of a Mutex value, «EKANS», on the victim
- If present, the ransomware will stop with an «already encrypted!» message and if present the encryption proceeds using standard encryption library functions
- The main functionality on victim systems is achieved via WMI (Windows Management Instrumentations) calls
- Before data encryption: EKANS stops the processes listed by process name in a hard-coded list in the malware's coded strings for the majority of listed processes, databases, data backup solutions or ICS-related processes
- After that EKANS displays a ransom note

_ICS SYSTEMS:

- IIT-focused ransomware could impact control system environments if it could migrate to Windows parts of control system networks, thus disrupting operations
- EKANS modifies this narrative seen above as ICS-specific functionality is directly referenced in the malware
- Some of these processes may reside in typical corporate computer networks, such as :
- Proficy servers or Microsoft SQL servers
- the inclusion of GUI software
- All of this indicates minimal knowledge of the processes and functionality of the control system environment

Programming language

_Financial

_UNDERSTANDING THE CYBER THREAT

Financial institutions are leading targets of cyber attacks. Banks are where the money is, and for cybercriminals, attacking banks offers multiple avenues for profit through extortion, theft, and fraud. Nation-states and hacktivists also target the financial sector for political and ideological motivations. Regulators are taking notice, and implementing new controls for cyber risk to address the growing threat to the banks they supervise.

_WHO IS BEHIND THE THREAT?

The malicious actors behind these attacks include not only increasingly daring criminals, such as the Carbanak group, which targeted financial institutions to steal more than $1 billion during 2013-18, but also states and state-sponsored attackers (see table). North Korea, for example, has stolen some $2 billion from at least 38 countries in the past five years.
Financial services companies are well aware of the problem and are working hard to combat cybercrime, but huge amounts of money are still being siphoned off every year by cybercriminals ($4.2B in 2020 according to the FBI).
State-sponsored adversaries may attack the financial services sector to the extent that it disrupts an activity essential to the functioning of a state. In 2020, New Zealand stock exchange was halted by a DDoS cyber attack, disrupting during two days the cash and debt market.
In summary, the motivations of the attackers can be divided into several categories: purely financial (96%), espionage (3%) grudge (2%), Fun (1%), ideology (1%).

_THE CYBERTHREAT SITUATION

In the financial sector, in 51% of those cases, the attackers succeeded in encrypting company data. But 62% of victims said they were able to restore fully from backups, and only 25% paid a ransom, the second lowest payment rate of all industries surveyed, 7% below the average.
In 2021, 44% of the breaches in this vertical were caused by Internal actors (having seen a slow but steady increase since 2017) (Figure 2). The majority of actions performed by these individuals are accidental actions, including sending emails to the wrong people, which account for 55% of all error-based breaches (and 13% of all breaches for the year).

_COST OF RANSOMWARE ATTACK IN FINANCIAL SECTOR

As shown in figure 3, healthcare, energy and financials services and pharmaceuticals experienced an average total cost of a data breach significantly higher than less regulated industries such as hospitality, media and research. This can also be explained by the value of the assets detained by financial services. Indeed, bank account and credit card number are high value commodities for cybercriminals looking to monetize information on Dark Web forums.
Cyber-extortion actors have understood that well and often target financial institutions specifically. Banco BCR, the largest state-owned commercial bank of Costa Rica was hit twice by Maze operators in a one-year span. The Maze team boasted about having exfiltrated over 11 millions credit card credentials.

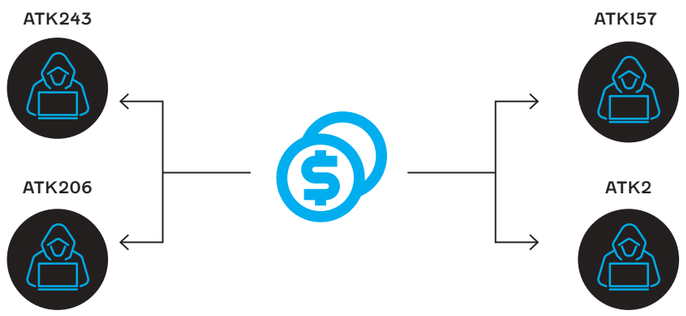
_CNA FINANCIAL HIT BY A CYBERATTACK

In March 2021, the Chicago-based insurance company CAN Financial fell victim to an attack by ransomware. The attackers masqueraded the malware as a fake browser update to gain initial access to the system. More than 15,000 servers were encrypted by the Phoenix Locker, a malware officially developed by the Phoenix threat actor but believed to have a connection with Evil Corp. Sensitive personal information (SSN, medical records, etc.) was stolen by the attackers and the 7th largest insurance company in the US decided to pay off the amount of the ransom, which, at $40 millions, is the highest amount ever recorded.

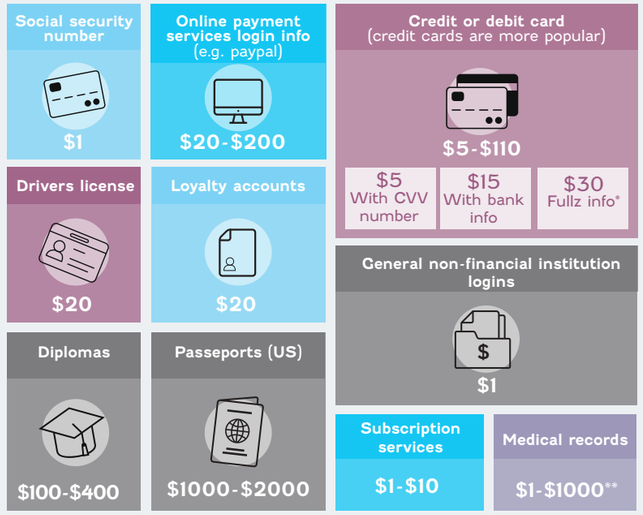
_LARGE-SCALE FRAUDS

Threat actors are increasingly turning to large-scale frauds, targeting directly banks networks rather than relying on stolen payment information in order to achieve fraudulent transaction. One player that illustrates this trend is the Lazarus Group. Affiliated to North Korea, the group has pioneered the targeting of SWIFT terminals. SWIF is a messaging network providing financial institutions with a secure place to perform monetary transactions.

Attackers known to have targeted the financial sector

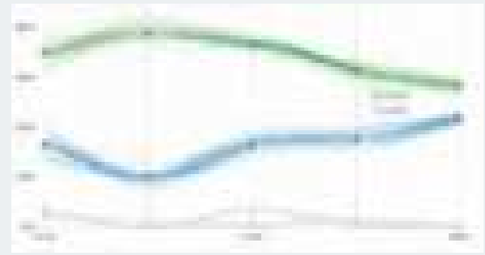


Your identity is a steal on the Dark Web



* Fullz info is a bundle of information that includes a «full» package for fraudsters: name, SNN, birth date, account numbers and other data that make them desirable since they can often do a lot af immediate damage.
** Depends on how complete they are as well as if ot a single record or an entire database.
Note: Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and hands on experience of Experian cyber analyst the last two years.

Actors in Finance breaches over time



Cost of data leaks in the finance sector

_Government

_UNDERSTANDING THE CYBER THREAT

For several years now, the strategic risks for the security of France, Europe and, more generally, the West, have changed in nature and intensity. Today, the monopoly of violence escapes the States and war has become hybrid: civil and interstate, internal and external, material and immaterial. This observation applies particularly to cyber attacks. These transformations are profoundly disrupting democracies, their values and their institutions. Many governments, particularly in Europe, have had to face a much more dangerous cyber threat targeting the very institutions of those states and jeopardizing the proper functioning of the targeted governments.

_PUBLIC ADMINISTRATION

When it comes to governments, it is necessarily appropriate to talk about public administrations. By far the biggest threat in this industry is the social engineer. Actors who can craft a credible phishing email are absconding with Credentials at an alarming rate in this sector.
Frequency of incidents in 2021: 3,236 incidents, 885 with confirmed data disclosure.
Top threats used by the attackers: Social Engineering, Miscellaneous Errors and System Intrusion represent.
Threat Actors External: (83%), Internal (17%) (breaches)

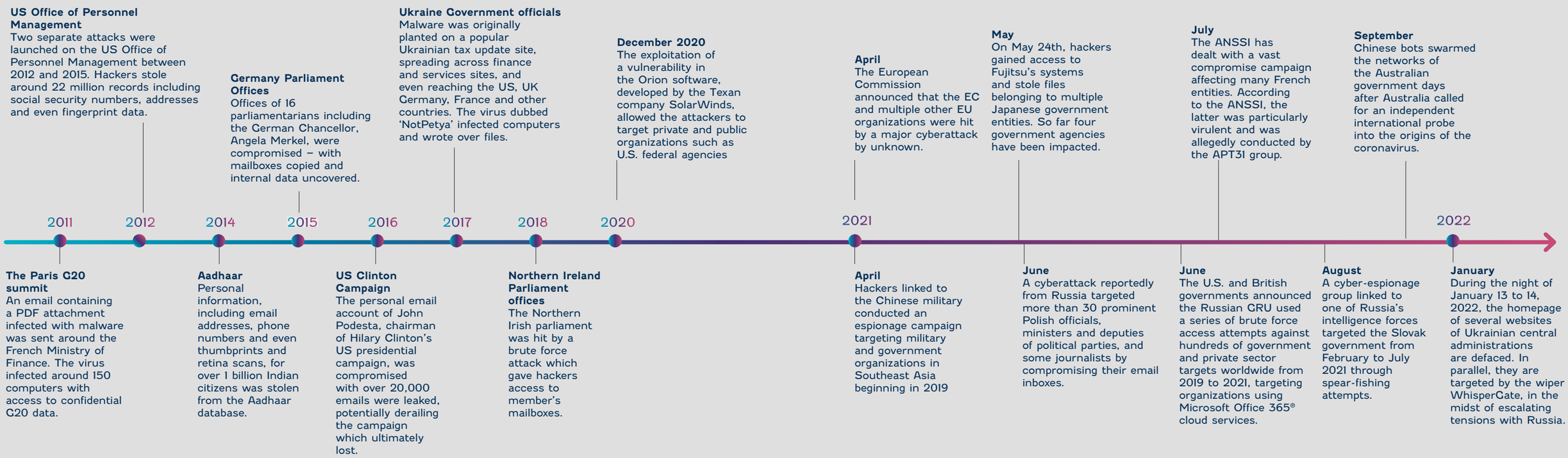
_DESTABILISING GOVERNMENTS BY TARGETING THE MILITARY SECTOR

The military is high on the list for most nation-states, compromising another nation's military through cyber actions that often cannot be traced back to the attacker.
Military vulnerability to cyber attacks is a concern for obvious reasons: weapons are dangerous, and those working in the military at this level are the highest-ranking Defence staff who are most qualified to protect the public. Yet, through underinvestment, lack of awareness, rapid technological advancements in hacking software and any number of factors, cyber attacks on military weapons are an increasingly prevalent threat.
Indeed, many weapons or the systems that control them are vulnerable to some form of cyber attack. These attacks can occur without the military teams controlling the weapons being aware of them. These weaknesses have been referred to as 'critical cyber vulnerabilities'. For five years, US Department of Defense testers have routinely discovered these vulnerabilities in almost every weapon system under development or in circulation.
This is made possible by a large number of advanced weapons systems developed by private companies, which have factory-defined passwords on arrival. These passwords have remained unchanged, allowing them to be easily found online. Vulnerabilities found in military systems included the ability to turn a weapon on or off, affect missile targeting, adjust oxygen levels or manipulate what controllers see on their computer screens. All would be devastating in a real combat operation and could result in loss of life.

_LOCAL MUNICIPALITIES

As local governments and municipalities have gone increasingly digital and process more and more data, they have become attractive to cybercriminals. Indeed, these local entities combine two central elements that make them particularly appealing to malicious adversaries: the possession of high-value data that can be used in identity theft, including tax records that compile PII, and the magnitude of vulnerabilities that are the result of these organizations' underinvestment in their IT security due to financial constraints. A 2020 study showed that 97% of city employees transfer sensitive documents via their email boxes. Finally, the criticality of certain operations performed by local makes them prone to paying ransomware to ensure business continuity. In 2018, Iranian hackers launched a massive ransomware attack against city computer networks. The scale of the incident created a disruption in the operation of law enforcement, court processing boxes, payment of parking tickets and a halt in operations at Hartsfield-Jackson airport. The city of Baltimore also fell victim to ransomware attacks in 2018 and 2019, causing server paralysis and disruption to its 911 emergency call center. A coordinated ransomware attack also targeted 22 small towns in Texas, resulting in ransom payments of hundreds of thousands of dollars.

The Biggest Government Cyberattacks in the last 10 years



_Health

_UNDERSTANDING THE CYBER THREAT

Healthcare organizations are increasingly exposed to online attacks, threatening daily work and compromising confidential patient data. It has become apparent from the many attacks that have occurred in recent years that healthcare staff does not have the time or resources to minimally counter the attacks. The potential disruption caused by a complete overhaul of online security is simply too great for many organizations to even consider. Despite the willingness of governments to successfully limit the number of attacks on critical infrastructure, new threats continue to be discovered every day. The high demand for patient information and often outdated systems are among the many reasons why the healthcare sector is now the main target for online attacks.

_CYBERTHREAT SITUATION

Since 2019, the healthcare sector has seen a shift from breaches caused by internal actors to primarily external actors. It brings this vertical in line with the long-term trend seen by other industries. While one of the primary concerns in the healthcare industry remains miscellaneous errors, with delivery mistakes being the most common incident (36% of human error), these are not intentional in nature. As a matter of fact, malicious insider breaches have not been among the top three trends in the healthcare industry for several years.
While basic human error continues to plague the healthcare industry, organized cybercriminal groups with a financial motivation continue to target it, with ransomware deployment a preferred tactic.

_HEALTHCARE CYBERSECURITY STATISTICS

- Ransomware attacks have hit 34% of healthcare organizations in 2021[1]
- The Secretary of U.S. Department of Health and Human Services (HHS) Breach of Unsecured Protected Health Information lists 592 breaches of unsecured protected health information affecting 500 or more individuals that are currently under investigation by the Office for Civil Rights. 306 of the breaches were submitted in 2020 alone.
- From 2017 to 2020, more than 93 percent of healthcare organizations have experienced a data breach and 57 percent have had more than five data breaches during the same time frame.
- The average bill to recover from a ransomware attack was $1.27 million in 2021, the lowest of any industry over the year.
- Data compromised: Personal (66%), Medical (55%), Credentials (32%), Other (20%), (breaches)
- Actors motivations: Financial (91%), Fun (5%), Espionage (4%), Grudge (1%) (breaches)

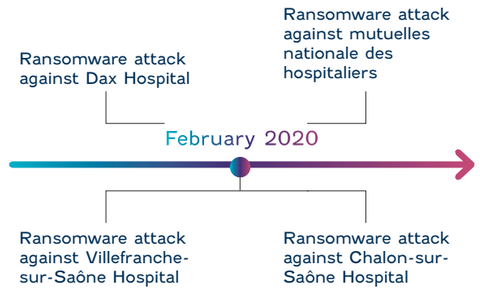
_THE RANSOMWARE ATTACKS ON HOSPITALS AND HEALTHCARE

Between 2020 and 2021, France recorded 27 major cyberattacks on healthcare institutions. February 2021 was the most impactful month for attacks on hospitals.
Likewise, UHS (Universal Health Services), which has 3.5 million patients in 400 US and UK facilities, has faced major cyber attacks: cybercriminals have used Ryuk. This ransomware has recently been used in numerous attacks on healthcare systems around the world. The sector's attractiveness to cyber criminals stems from the information held by hospitals, namely PII (personally identifiable information, medical records and payment information.

_IMPACT OF RANSOMWARE ATTACKS ON HOSPITALS AND HEALTHCARE SERVICES

- Increased mortality rate
- More complications from medical procedures
- Delays in procedures and tests that resulted in poor outcomes
- Retake of patients transferred or diverted to other facilities
- Longer stays
- Significant financial impact due to cyber attacks: by the end of 2020, security breaches cost $6 trillion dollars for healthcare companies.

Cyber attacks on French health facilities in February 2021



_COVID-19 AND THE HEALTH SECTOR

- The global containment situation is thus indirectly introducing, by virtue of its exceptional nature in all areas of everyday life, a great deal of excitement in the world of cyber security. This feverishness has been identified by the cyber threat ecosystem. This has been particularly noticeable with many institutions in the health sector falling victim to numerous groups of attackers:
- Hackers managed to penetrate the system of one of the largest test centres of Covid-19 in Antwerp, Belgium. While its network was still offline on Tuesday, the laboratory refused to pay the ransom and filed a complaint.
- The European Medicines Agency (EMA), which is responsible for reviewing the dossiers of candidate vaccines, was hit by a cyber attack. Scientific data on the Pfizer-BioNTech vaccine, the first treatment on the market, was accessed by the criminals.
- On 15 September, the Paris Hospitals (AP-HP) reported that the personal data of 1.4 million people who had undergone Covid screening tests in the Ile-de-France region in mid-2020 had been stolen during the summer. E-mail, telephone number, address, social security number and test results were found in the wild and on dark web sites.

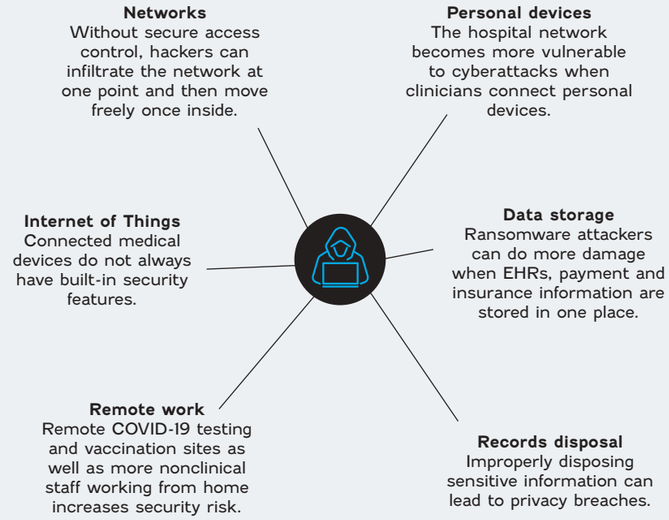
_THE INTERNET OF MEDICAL THINGS (IOMT)

In order to improve efficiency and performance, many hospitals are equipped with connected devices (15 to 20 in one hospital room on average). Some of them, such as ultrasound scanners and physiological monitors, are connected to both the Internet and the hospital's computer network, thus providing an entry point for an attacker. Internet of Things devices have many intrinsic vulnerabilities, are rarely protected by antivirus software and are not regularly updated, which explain why they are exploited by malicious actors.

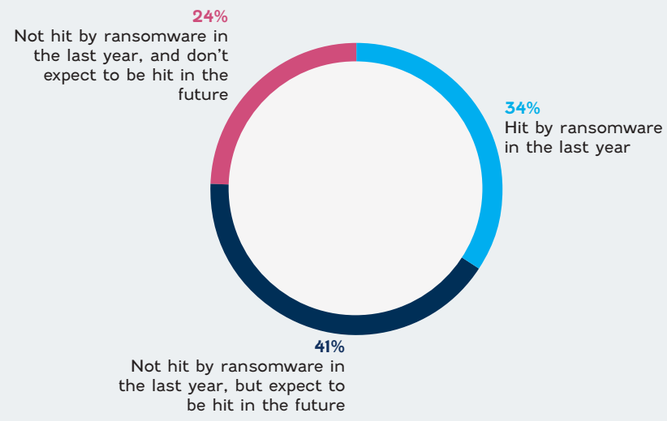
Malicious actors known to have targeted the health sector

ATK177	ATK22	ATK37	ATK118
ATK206	ATK7	ATK117	ATK119
ATK219	ATK9	ATK67	ATK123
ATK233	ATK18	ATK73	ATK127
ATK2	ATK19	ATK83	ATK129
ATK3	ATK27	ATK88	ATK130
ATK4	ATK38	ATK100	ATK131
ATK5	ATK40	ATK103	ATK140
ATK32	ATK41	ATK113	ATK143
ATK35	ATK49	ATK115	ATK157
ATK51			

Six vulnerability points hackers target in hospital cyberattacks



Survey of Healthcare organizations



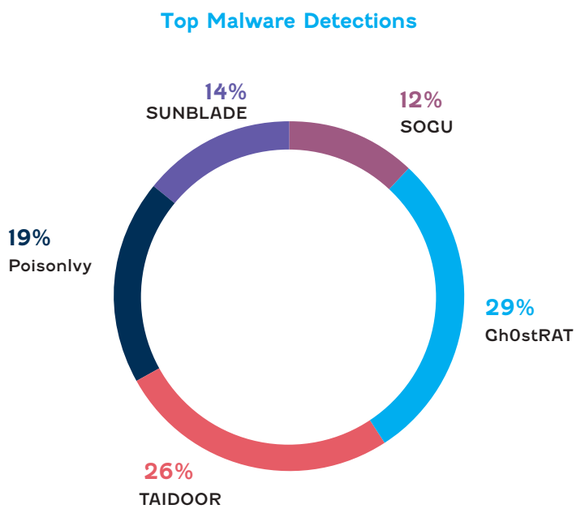
_Information Technology

_UNDERSTANDING THE CYBER THREAT

The high tech and IT sector's relevance to economic, intelligence, and security concerns likely make it a target for a variety of threat actors. The high-tech sector is often ground zero for cyberattacks. One obvious reason is that these organizations have very valuable information to steal. However, another more subtle reason is the very nature of high-tech organizations. High-tech companies generally have a higher risk appetite than their counterparts in other industries. In addition, they tend to be early adopters of new technologies that are still maturing and are therefore particularly vulnerable to attacks and exploits. Parts of the high-tech sector provide a path of attack to other sectors, as high-tech products are a key part of the infrastructure for all kinds of organizations. Technology is a key enabler, but it can also be a key source of vulnerability. For example, because of the tremendous need to build trust on the Internet, attacks on certificate authorities have caused serious privacy breaches in a number of industries. In addition, vulnerabilities in point-of-sale systems have led to major security breaches for retailers, and backdoors in communications equipment have exposed organizations in all sectors to a wide range of attacks.

_HIGH-TECH INDUSTRIES HAVE BECOME A POPULAR TARGET FOR CYBERCRIMINALS

The global technology market has grown considerably in recent years. According to the Forbes Global 2000 , the 184 technology companies on the list represent more than $9 trillion in market value, $4 trillion in assets, and nearly $3 trillion in sales.
These high-tech organizations, as well as those not on the top 2,000 list, come from a wide range of sub-industries, from electronics manufacturing and software development to digital media and space. Although they apply their skills and knowledge to different sectors, high-tech organizations all have something in common: they operate at the cutting edge of technology. Innovation, secrecy, intellectual property and, most importantly, security are imperative.
FireEye researchers most frequently detected threat actors using the following targeted malware families to compromise organizations in the high tech and IT industry.



_20 ADVANCED THREAT GROUPS COMPROMISE COMPANIES IN THESE SUBSECTORS

- Computer Software
- Information Technology Services
- Control, Electromedical, Measuring & Navigational Instruments Manufacturing
- Consumer Electronics & Personal Computer Manufacturing
- Electronics Component Manufacturing & Wholesalers
- Logic Device Manufacturing
- Network Access & Communications Device Manufacturing
- Networking & Connectivity Software
- Routing & Switching Equipment Manufacturing
- Search, Detection, Navigation & Guidance System Manufacturing
- Security Software
- Semiconductor Equipment Manufacturing
- Storage & Systems Management Software

_DATA STOLEN FROM HIGH TECH AND IT SECTOR CLIENTS

- Blueprints
- Proprietary Product & Service Information
- Testing Results & Reports
- Production Processes
- Hardware & Software Descriptions & Configurations
- Security & Risk Management Documents
- Diagrams and Instruction Manuals
- Marketing Strategies & Plans

_THREAT ACTORS TARGET CLOUD ENVIRONMENTS

The cloud security threat landscape highlighted threat actors' continued efforts to shift targeting into cloud environments. Data gathered showed that threat actors used a variety of methods to gain initial access into organizations' cloud assets, with nearly a quarter of incidents stemming from threat actors pivoting into the cloud from on-premise networks. In addition, API misconfiguration issues were involved in nearly two-thirds of studied incidents. This targeting coincided with a robust underground marketplace for cloud-related credentials, with tens of thousands of accounts for sale online. As organizations move into the cloud, threat actors are following right alongside. Maintaining properly hardened systems, enacting effective password policies, and ensuring policy compliance is critical to maintaining a robust cloud security posture.

_Legal

_UNDERSTANDING THE CYBER THREAT

Organizations in the Legal industry, such as law firms, are increasingly relying on IT for many of their critical operations. Besides, the very nature of this industry makes them prime candidates for ransomware attacks, as they handle large volumes of sensitive data (confidential information related to mergers and acquisitions, documents under professional secrecy) that threat actors perceive as valuable. This combination of factors opens the door to cyberattacks by groups with primarily financial objectives.

_CYBER-EXTORTION AND LEGAL SECTOR

The nature of cyber-extortion has changed in recent years, from an ecosystem dominated by the use of ransomware as both a data encryption and ransom negotiation tool to an environment where operators use various blackmail techniques, sometimes not even encrypting the data. This new tactic, often referred as double-extortion reflects a reality : for some companies, the possibility of having their sensitive data published is a greater risk than having their servers paralyzed. This observation applies to companies in the legal sector for two main reasons.

First, a law company whose name and sensitive documents were leaked by a cyber-extortion gang will suffer from reputational damage as clients will move away from the firm. A law company loses on average 5% of their clients after a data breach.

Second, for European firms, the provisions of the GDPR (General Data Protection Regulation) provides for fines up to 4% of the company's turnover in case of dissemination of confidential content.

Despite the uncertainty of negotiating with cybercriminals, those elements may explain why some law firms decide to pay the ransom.

_EVOLUTION OF THE RANSOMWARE THREAT

Cybersecurity researchers at Digital Shadows reported the compromise of 18 legal services organizations at the end of 2020 and 32 in the first quarter of 2021, an increase of 78%.

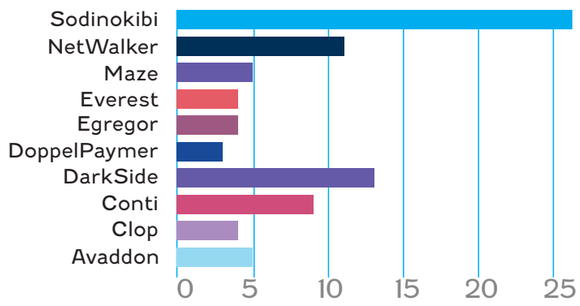
From Q1 2020 to Q1 2021, ransomware attacks targeting the legal services sector increased by 967%, from 3 reported organizations to 32.

In a survey conducted in April 2021, with the participation of 1,263 professionals from different countries, 50% of legal businesses were forced to lay off employees after falling to a ransomware attack. It accounts for the highest rate across all industries, followed by Retail (48%) and Automotive (42%).

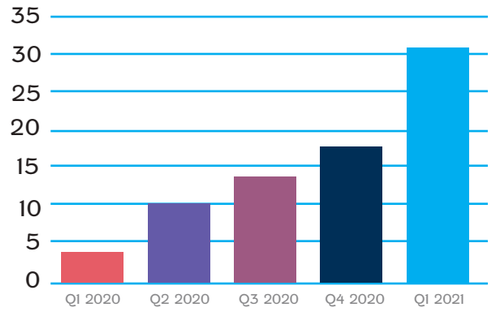
Other Figures:

- The sending of malicious attachment was multiplied by 7 due to COVID 19.
- The average ransom payed by legal companies increased from $5,000 in 2018 to $200,000 in 2021

Number of targets per ransomware between Feb 202 and May 2021



Number of legal services victim organization (Feb 2020 – May 2021)



_RANSOMWARE AND LEGAL SECTOR

While the majority of the major ransomware operators have already successfully exploited a legal-related organization, the REvil/Sodinokibi group of operators topped the list (Figure 2).

Ransomware operators DarkSide and NetWalker follow with double-digit victim numbers in the legal sector.

_RANSOMWARE AND LEGAL SECTOR: USE CASE

In May 2020, the entertainement law firm Grubman Shire Meiselas & Sacks was hit by a ransomware attack.

Revil/Sodinokibi operators initially demanded a ransom of $21 million, which they doubled to $42 million after the law firm refused to pay the initial amount. Sodinokibi went on to leak the purported data of 12 clients of Grubman, Shire, Meiselas, & Sacks by posting it to their auction page in a failed attempt to push the firm to pay the ransom.

The notorious REvil hacker group, believed to be from Eastern Europe, stole private emails, contracts and personal information from the New York-based law firm.

Leak post on REvil darkweb blog

Why law firms are increasingly being targeted

Easy targets
In October 2020, the American Bar Association reported that 29 percent of law firms said they had experienced a data breach, and 1 in 5 law firms did not know if they had experienced a data breach.

Higher chance of a payout
Organizations facing a ransomware attack typically pay the ransom when other options are not viable, such as using backups to restore data, not being able to afford the downtime, and preventing confidential data from being released.

Valuable data
Law firms keep many different data types, including personally identifiable information on clients and their families, case information, and confidential business information of their clients. When this type of information is exfiltrated, it creates a unique situation of the firm weighing the options of paying the ransom or facing the consequences.

High-Profile Ransomware Attacks on legal sector

Grubman Shire Meiselas & Sacks : May 2020
One of the most high-profile ransomware incidents across all sectors in 2020 was the ransomware attack on the entertainment law firm, Grubman Shire Meiselas & Sacks (CSMS). The REvil group was behind this incident, and they set the ransom demand at $42 million.

Campbell Conroy & O'Neil: February 2021
Campbell Conroy & O'Neil, P.C. is a large law firm that works with A-list clients such as Ford, Boeing, and Walgreens. A July 2021 press release revealed that the organization became the victim of a ransomware attack in February 2021.

4 New Square: June 2021
4 New Square is a London-based commercial barristers' (lawyers) Chambers. In June 2021, reports emerged that the organization was targeted by a ransomware attack that involved blackmailing the company to avoid having its sensitive data exposed online.

2020

2021

Jones Day: February 2021
The notorious Clop ransomware group could count law firm Jones Day among its victims after they successful infected the company's networks. Reports suggest the exploitation of a zero-day vulnerability in the Accellion file transfer service.

_Manufacturing

_UNDERSTANDING THE CYBER THREAT

The manufacturing sector, due to the nature of its activities, has long been kept away from the prerogatives of protecting computer systems. The reason for this is twofold: first, manufacturing companies have long been able to operate disconnected from the Internet and second, the general perception was that hackers were not interested in the information and assets owned by manufacturing organizations. The emergence of Industry 4.0 and the need for manufacturing companies to connect their industrial control systems (ICS) to the Internet has challenged this paradigm. Thus, the novelty of the emergence of network protection issues for these companies is accompanied by a gap compared to other sectors. This multiplies the opportunities for intrusion by malicious actors, which can leverage Intellectual property (IP) assets in order to generate income.

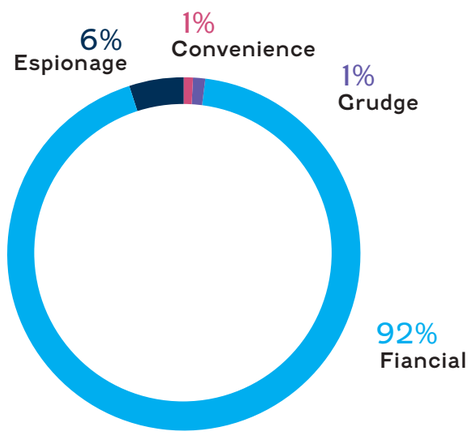
_THE STATE OF THE THREAT IN THE MIDST OF COVID 19

The manufacturing sector was particularly affected by the global COVID19 pandemic and continues its rise among the sectors most affected by cyberattacks. According to the 2021 Global Threat Intelligence Report (GTIR), the sector has become the second most impacted by cyberattacks, behind finance and insurance, with a rise of 300% in a year (2020 to 2021). A study conducted by Deloitte also shows that nearly 40% of manufacturing companies have suffered a cyber attack this year and that among these companies, 38% have experienced a loss of over 1 million dollars. Critical manufacturing firms involved in the vaccine cold chain were targeted by a phishing campaign in a larger effort to gain access to sensible information pertaining to the COVID 19 vaccine.

_THE MOST COMMON THREATS FOR MANUFACTURING COMPANIES

Phishing and Ransomware seem to be the most common types of threats targeting companies operating in the manufacturing sector.
Phishing techniques (represent 75.4% of social engineering attacks conducted for this sector) are the most common vector used to gain initial access along with the use of stolen credentials. The lack of preparation of the sector explains the vulnerability of the industry to phishing attacks.
Ransomware operators and more broadly cyber-extortion actors target heavily the manufacturing companies. Figures show that 92% of the attackers targeting the sector are financially motivated. Manufacturing companies have a particular incentive to pay large ransoms insofar as a downtime would be detrimental to their activity. As a result the cost-effective option is often the payment of the ransom. In 2021, the manufacturing industry is the sector most represented among cyber-extortion victims, with more than 350 enterprises in the ransomware leaks for the year.

Attacker's motivations



_OTHER COMMON THREATS

- Manufacturing ranks 5th among sectors with the highest risk of internal threat. Employees working in the sector are often untrained and thus considered as weak links that can be leveraged by hackers. Malicious insiders are also common in manufacturing organizations, whether they are after a fincancial or personnal objective.

- Manufacturing companies represent 22% of cyber espionage victims according to Verizon. This figure demonstrate the importance of Intellectual property as a valuable asset that can be levergaed by cyber attackers.

_REVIL'S ATTACK ON JBS FOODS

June, 1, 2021, The meat supplier JBS fell victim to a cyberattack by the group REvil that affected the company's production activities in several countries. This attack led to a paralysis of servers, leading to the suspension of production lines, particularly in Australia and the United States, where several slaughterhouses suspended their activities. This attack is a landmark for the manufacturing industry as JBS supplies almost a quarter of the world's meat. This incident resulted in a $11 million ransom being payed to REvil's operators.

_MANUFACTURING SECTOR AND CRITICAL INFRASTRUCTURES

The critical manufacturing sector is particularly at risk of being targeted by malicious actors. In December 2021, the CISA released a report tackling the issue and providing insights on the evolution of the cyberthreat for this sector. In particular, the CISA has identified vulnerabilities in ICS (Industrial Control Systems) that are even more crucial with the COVID pandemic forcing companies to adapt to remote working. Managing cybersecurity risks has become more complex, as companies are incited to resort to process automation. ICS play a key role in the securization of critical infrastructure, notably with regards to energy-related infrastructure.

Attackers targeting the Manufacturing sector

ATK180	ATK27	ATK79
ATK187	ATK28	ATK88
ATK223	ATK38	ATK100
ATK3	ATK41	ATK103
ATK4	ATK36	ATK117
ATK35	ATK46	ATK118
ATK22	ATK52	ATK119
ATK10	ATK37	ATK123
ATK15	ATK50	ATK129
ATK17	TA505	ATK134
ATK19	ATK73	ATK140
ATK143		

_Maritime

_UNDERSTANDING THE CYBER THREAT

With 80% of world trade by volume and 70% by value, the shipping industry is at the heart of the various supply chains, making its operation critical at the economic and strategic level. The sector's need for efficiency has driven the maritime industry to increasingly integrate IT systems into existing OT systems, whose limited connectivity had reduced the risk of intrusion for many years. Today, the increasing digitalization of the maritime sector induces a significant cyber risk on ports, communication channels and vessels by creating opportunities for malicious actors to destroy them.

_INTERWOVEN OT/IT SYSTEMS

The explosion in the trade of goods by sea, the increase in carrier capacity, and industrial digitization have increased the complexity of the maritime industry environment. Operational needs for competitiveness have pushed ships and ports towards automation of systems and integration of IT with OT. Yet, by connecting these two models, the maritime industry has expanded the surface, while neglecting cybersecurity investments.
The COVID 19 pandemic by inducing travel restrictions forced original equipment manufacturers (OEMs) to connect standalone systems to the internet, making them vulnerable. These OEMs have also asked port personnel to establish brief connections between the terrestrial network and their OT system in order to perform security updates. These connections, by creating entry points, expose already permeable OT systems.

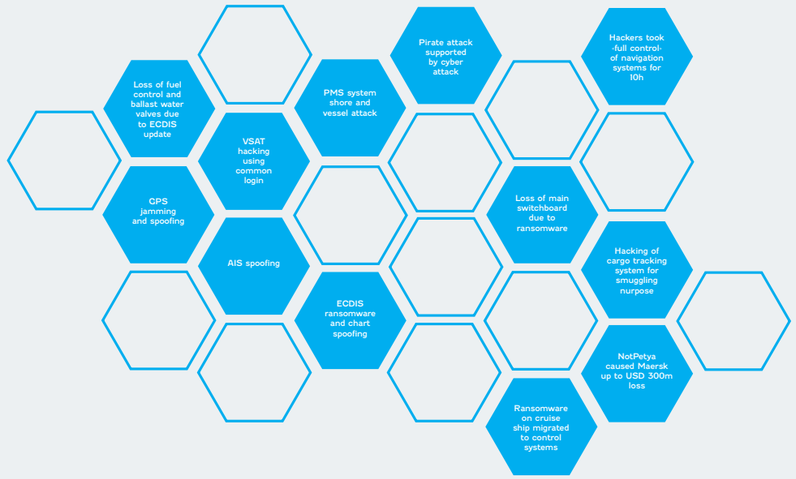
_THE CYBERTHREAT SITUATION

The first half of the year 2020, marked by the COVID-19 pandemic, has exponentially increased the cyber risk on maritime transport. In fact, over this period, attempted attacks increased by 400%. Over the three years prior to the pandemic, cyberattacks targeting ships and port systems had surged by nearly 900 percent. In 2021, the Port of Houston was the victim of a cyberattack, carried out by advanced threat actors, creating a sense of security urgency among shipping stakeholders.

_DISASTROUS FINANCIAL AND POTENTIALLY HUMAN CONSEQUENCES

The blocking of the Suez Canal by the Ever Given cargo ship symbolizes the potential damage of a cyber attack on a ship's navigation system, resulting in the daily loss of $10 billion in trade. While an intrusion on the IT system can result in financial losses as well as reputational damage, the compromise of the OT system can have consequences on the physical safety of a ship and its crew. By taking control of a ship containing sensitive products (vaccines, liquid energy supply), an attacker has a major destructive potential that may appeal to certain malicious actors.

Scenarios of cyberattacks for the Maritime industry



Actors having an interest in launching cyberattacks on the Maritime industry

Terrorists
Terrorist organizations could be interested in the maritime sector for the destructive potential of a cyber attack on the sector. A terrorist actor, by compromising industrial control systems, could cause ships to collide or even explode.

Cybercriminals
The value of the data exchanged, the importance of operations continuity as well as the lack of preparedness of the sector are important factors of motivation in the logic of cybercriminals

State-sponsored
State or state-sponsored actors might be interested in retrieving sensitive information via cyber espionage methods. In 2019, Chinese-origin actors had targeted universities as well as the US Navy to retrieve data on maritime technologies.

Hacktivists
The potential impact of a destructive attack on the maritime sector is fertile ground for the emergence of hacktivism

FIGURE 5 **High-Profile Ransomware Attacks on Maritime sector**

June 2011, Antwerp
From 2011 to 2013, a drug cartel was able to spy on the port of Antwerp's operations after having successfully breached the container management system

2018
A wave of cyberattacks hit several international port : Long beach (July), Barcelona (September) and San Diego (September)

May 2020, Shahid Rajaee
A cyberattack disrupted the Iranian port's operation in the midst of a conflict between the country and Israel.

November 2020, Kennewick
The small US port of Kennewick (Washington State) lost access to its servers after being hit by a ransomware attack.

August 2021, Houston
Port Houston admitted being the target of cyberattacks by a state-sponsored actor seeking to spy on the port's operation.

2011 — 2017 — 2018 — 2020 — 2021

June 2017, Rotterdam
The port of Rotterdam was hit by a modified version of the NotPetya malware, causing the paralysis of two container terminals.

March 2020, Marseilles
The port of Marseilles was affected by the ransomware PYSA/ Mespinoza, initially targeting the information systems of Aix-Marseilles-Provence.

June 2020, Langsten, Norway
Cybercriminals were able to encrypt and exfiltrate the data of a shipyard belonging to the company Vard

July 2021, South Africa
A cyberattack on the Transnet National Port Authority disrupted the operations of four major south African ports (Cape town, Ngqura, Port Elizabeth and Durban). The incident was labelled as a case of "force majeure".

_Media and Entertainment

_UNDERSTANDING THE CYBER THREAT

In December 2015, the online video gaming distribution platform Steam revealed that 77,000 of its gamer accounts were hacked every month. Steam has leveraged the increased digitalization of the industry to establish itself as a key player. This very digitalization appears as a reason for the growing interest of cyber attackers towards the media and entertainment sector, which has been characterized by a constant underappreciation of cyber risks. The multiple companies affecetd by attacks and the growing concern with regards to the security of Iot devices did not help move the needle and companies in the sector continue to suffer from IP theft andreputation damage.

_2014: THE SONY'S HACK

On November 24, 2014, Sony's employees realized their corporate network had been hacked by a group calling itself The Guardians of Peace. The threatening message displayed on their computers (figure 1) reports the possession of sensitive internal information. A few days later, torrent links of unreleased Sony's movies and confidential information about employees are leaked. This attack, supposedly operated by a North Korean group stands out as a landmark for the media and entertainment industry, alerting the sector about the risks of neglecting cybersecurity.

_INTELLECTUAL PROPERTY IS A VALUABLE ASSET

Copyrighted material is an important resource in the media and entertainment industry. Many cybercriminals have realized the value of these assets and have started to target this industry in a double threat strategy. Not only does data encryption put pressure on companies, but the exfiltration of such information and the threat of its release serves as an additional blackmail technique. Indeed, the pre-release of copyrighted content is a major financial and reputational risk that a media company cannot afford to take. This logic is leveraged by cyber attackers specifically targeting the sector. The average cost related to data breach for the entertainment industry stands at $4.8 millions.

_THIRD-PARTY THREATS

Third-party compromise is a classic tactic that is particularly applicable to the industry as media production models are built on a decentralized supply chain. Film directors, for example, delegate specific tasks such as editing, stunts, or art design to subcontractors, thus multiplying the entry points for an agile attacker. The leak of several episodes of Netflix's series Orange is The New Black in April 2017 exemplifies this tendency as the hack originated from the compromise of a third-party entrepreneur working for the show.

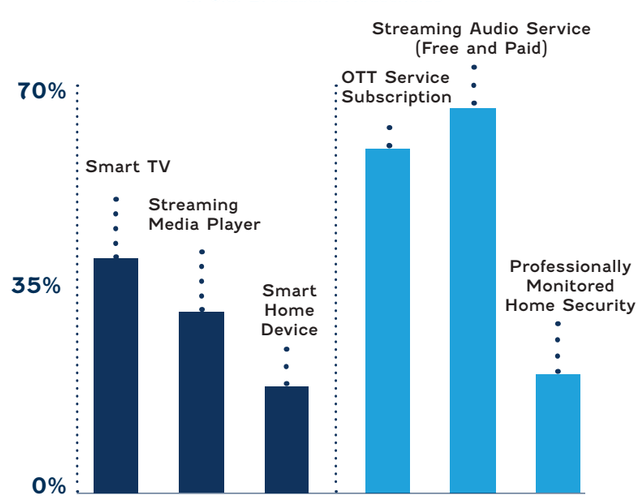
_ACTORS WITH DIFFERENT MOTIVATIONS

High visibility as well as valuable assets that can be leveraged are enough to prompt different players to express an interest in the sector. First, the airing of audiovisual content may spark political controversies. 2014's Sony Hack is widely believed to be the work of a North Korean APT group responding to Sony's release of "The Interview", a comedy movie staging the assassination of the north Korean leader Kim Jong-un. State-sponsored gangs may also target the industry in a larger effort to destabilize a political adversary and excert influence. This motive is exemplified by the hack of TV5 Monde in April 2015. Hacktimism is another reason for the targeting of this sector. Indeed, individuals or groups of individuals may try to retrieve email correspondence or personal information belonging to celebrities in order to generate buzz. The most crucial threat to the sector remains financially motivated actors. The ecosystem is dominated by double-extortion schemes (encryption and leaks of Intellectual property (IP)), and facilitated by the decentralization of the model and the intrinsic vulnerabilities of companies working in the media and entertainment sector.

Message displayed on Sony employee's computers

Connected Entertainment and Smart Home Adoption

In U.S. Broadband Households



November 2014
Sony Pictures is hacked by an APT group believed to be affiliated with North Korea. Sensitive information is leaked.

April 2015
a cyberattack caused the International French-language television channel TV5 Monde to stop broadcasting between 8 and 9 April 2015,

April 2015
The Jerusalem post's homepage is defaced by hackers and replaced by references to the killing of Iranian general Qassem Soleimani by the US, two years ago

April 2017
The compromise of thirdparty contractor lead to the leak of several episodes of Netflix's series Orange is The New Black

July, 27, 2017
HBO suffers from a massive data breach, affecting 1.5 terabytes of IP and business documents

December 2018
All Tribune Publishing newspapers experienced printing outage after Ryuk crippled their servers

December, 22, 2020
German newspaper Funke Media group fell victim to a ransomware attack

February, 18, 2021
National Burmese TV and radio broadcasting units are disrupted by a hacker group, protesting against the military coup

April, 2021
Norwegian media company Amedia suffers from a cyberattack crippling its systems, disrupting print production

January 2022
A ransomware attack, conducted by Lapsus$ hit Portugal media giant Impresa. The company owns the largest Newspaper and TV station in the country

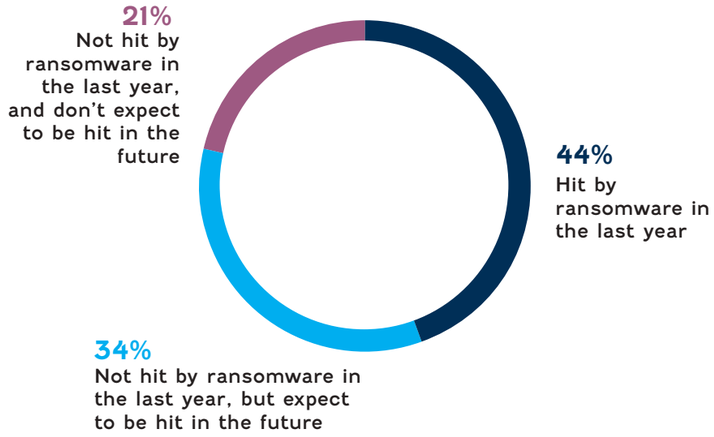
2014 2015 2017 2018 2020 2021 2022

_Retail

_UNDERSTANDING THE CYBER THREAT

The Retail industry continues to be a target for financially motivated criminals looking to cash in on the combination of payment cards and personal information. Social tactics include pretexting and phishing, with the former commonly resulting in fraudulent money transfers.
Retail is one of the most targeted sectors for cyber-attacks in 2021. The coronavirus pandemic has forced retailers to adapt to survive, regardless of their size. While smaller retailers have moved to card payments and online operations, larger retailers have focused on harnessing big data to achieve efficiencies and maximize profit margins.
This has introduced new threat vectors as retailers' attack surfaces have expanded, and these vectors are being exploited by cybercriminals keen to steal money and confidential financial information. Data is the new currency for cybercriminals, who focus not just on money and goods but also customers' personal data that can be stolen and sold online. And with high staff turnover and seasonal workers, retailers face threats from not just cybercriminals, but also insiders.

Retail's experience with ransomware last year



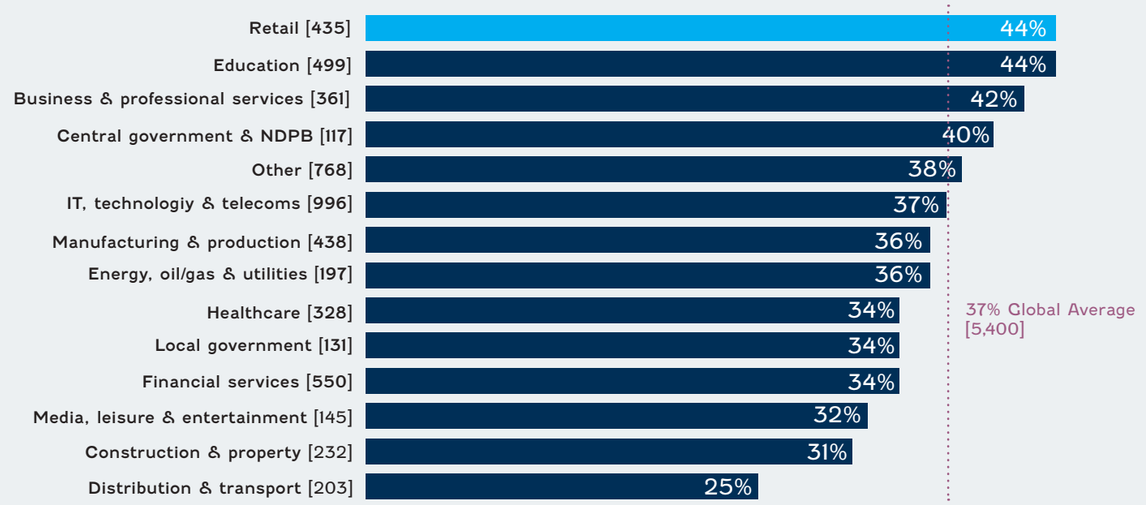
_RANSOMWARE AND RETAIL SECTOR

In 2021:
- 44% of retail organizations were hit by ransomware
- 54% of organizations hit by ransomware said the cybercriminals succeeded in encrypting their data
- 32% of those whose data was encrypted paid the ransom to get their data back
- The average ransom payment was $147,811
- However, those who paid the ransom got back just 67% of their data on average, leaving almost a third of the data inaccessible
- The average bill for recovering from a ransomware attack in the retail sector was $1.97 million
- 56% of those whose data was encrypted used backups to restore data
- 91% of retail organizations have a malware incident recovery plan

_RETAIL SAW THE HIGHEST LEVEL OF RANSOMWARE ATTACK

Looking at the prevalence of ransomware across all the sectors surveyed, retail, along with education, experienced the highest level of ransomware attacks: 44% of respondents in these sectors reported being hit compared to the global average of 37%.
Globally across all sectors, the percentage of organizations hit by ransomware in the last year has dropped considerably from last year, when 51% admitted being hit. This drop can be partly explained by the evolution of attackers behaviors.

% respondents hit by ransomware in the last year



_RETAIL SECTOR AND THE COST OF RANSOMWARE

Of the 357 respondents across all sectors who reported that their organization paid the ransom, 282 also shared the exact amount paid, including 36 in the retail sector.
Globally across all sectors, the average ransom payment was $170,404. However, in retail, the average ransom payment was almost $23,000 lower, coming in at $147,811.

_RETAIL SECTOR AND CRITICAL INFRASTRUCTURE

Many companies in the retail sector are considered critical infrastructure. That is the case of the New Cooperative, a US based merchant wholesaler, hit by BlackMatter in September 2021.
The attack was first discovered after a sample of the ransomware was downloaded from a public malware analysis site.
This sample provided access to the BlackMatter ransom note, the ransomware negotiation page and a non-public data leak page containing screenshots of allegedly stolen data.
Indeed, it is important to show through this attack that when the BlackMatter ransomware first appeared, the attackers stated that they would not target critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
From screenshots of the trading page shared on Twitter, the New Cooperative asked BlackMatter why they were attacked as they are considered critical infrastructure and the attack would lead to a disruption in the food supply for grain, pork and chicken.
BlackMatter responded that they did not «fall under the rules» and threatened to double the ransom if the New Cooperative did not change its approach to the negotiation.

Attackers targeting the retail sector

ATK187	ATK123
ATK206	ATK124
ATK32	ATK129
ATK13	ATK132
ATK67	ATK134
ATK88	ATK140
ATK100	ATK164
ATK113	ATK165
ATK115	ATK166

The ransom payments

$ 170,404
Average GLOBAL ransom payment

$ 147,811
Average RETAIL ransom payment

Tweet showing the negotiations between BlackMatter and the New Cooperative

_Space

_UNDERSTANDING THE CYBER THREAT

Satellites are increasingly providing essential services. They have become an essential element for the successful accomplishment of military missions.
Nevertheless, for a number of years, and especially with the onset of the New Space, the issue of cybersecurity in space systems has been sidelined, if not completely ignored. The reasoning was that since cyber attack techniques were not as developed as they are today, the functional and budgetary priority was not necessarily allocated to the issue of cyber security.

_VULNERABILITIES IN SPACE SYSTEMS

The Space industry is organized around several segments:
- Ground Segment
- Link Segment
- User Segment
- Space Segment

_GROUND SYSTEM

Compromising the ground station is ultimately the easiest way to control a satellite because it provides the equipment and software to legitimately control and track it. Besides, it uses existing and established ground systems and attack vectors. The types of threats are generally the same throughout the life cycle of a satellite.

_SPACE SEGMENT

Once in orbit, a satellite has limited physical contact with humans, although this does not mean that security threats are not present. Vulnerabilities in the software and hardware used the satellite can arise and impact the operation of the satellite and the robustness of security controls

_USER SEGMENT

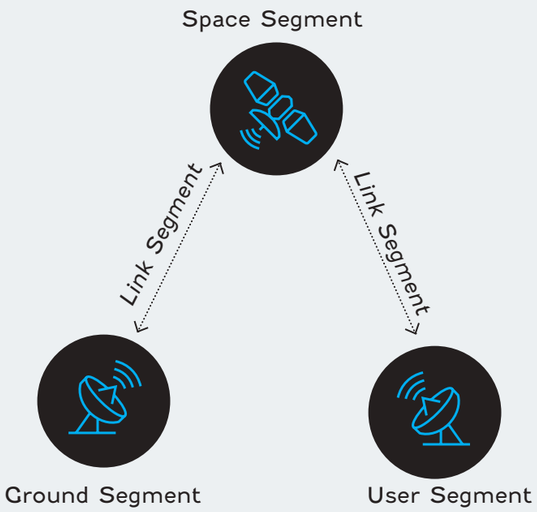
Compared to the Link Segment which corresponds to the interactions between the three segments, the User Segment deals with the applications of satellite systems. Applications such as navigation, television and communications often require dedicated hardware. Other systems use the data collected by these dedicated receivers to serve a specific product or application. For satellite television transmissions, a satellite dish and decoder must be installed to receive the channels provided and to perform the subsequent tuning and decoding of the broadcasts for viewing.

_EACH SEGMENT IS A POTENTIAL THREAT SURFACE

When we talk about threats to the space sector it is first important to recall the different dimensions of the threat surface created by the sector's morphology. In reality 4 segments are to be identified: space, ground, link, and user.
In the following section, we will provide examples to explain the ways in which attackers have found to target these specific segments. These examples focus mainly on use cases of state-sponsored attacker groups, but they should not suggest that organized cybercriminal gangs are not capable of acting on these threat surfaces.

Center for space policy and strategy: Defending spacecraft in the cyber domain

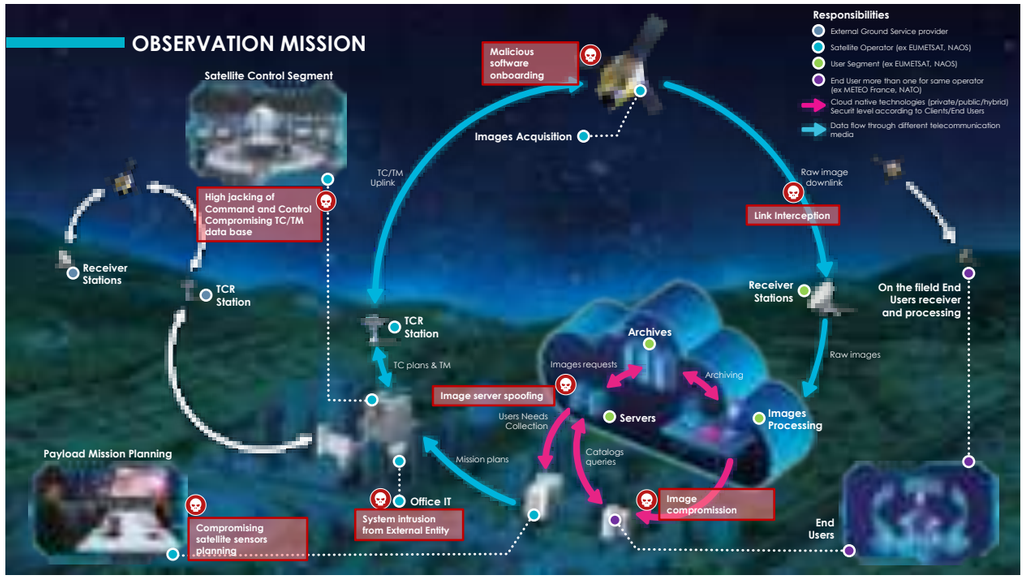
The space segments



_LINK SEGMENT AND ATK13'S ATTACK EXAMPLE

The main advantage for an espionage group to leverage the Link segment is that it is difficult to identify. Indeed, the geographical location of the C&C server is very difficult to trace with this tactic since Internet-based satellite receivers can be located anywhere in the area covered by the satellite. The only drawback is the instability of the connection and its slowness. In this case ATK13 used a very simple method: Hijacking of DVB-S satellite links.
The question is, how is this possible? As Kaspersky reminds us, four basic elements are necessary:

- A satellite dish – the size depends on geographical position and satellite,
- A low-noise block downconverter (LNB),
- A dedicated DVB-S tuner (PCIe card)
- A PC, preferably running Linux



_GROUND SEGMENT AND ATK78'S ATTACK EXAMPLE

In January 2018, Symantec's Targeted Attack Analytics TAA issued an alert for a major telecom operator in South-East Asia. The alert was linked to an attack by a group called Thrip, which collects information on satellite-operating infrastructure.
To date, known targets are satellite operators in the USA and South-East Asia but also defence contractors, telecom operators and organizations processing satellite imagery. In particular, the group looks for information linked to satellite operations and geospatial imagery.
Thrip's tactics are referred to here as 'living off the land' and employ legitimate tools often already installed on its victims' computers with some scripting and shell code that is hardly visible. It is therefore a dualisation of legitimate tools used by satellite operators on the ground for strategic and economic espionage.

Living Off the Land tactic

1 INCURSION	2 PERSISTENCE	3 PAYLOAD
Exploit in memory e.g. SMB EternalBlue	Non-persistent	Dual-use tools e.g. netsh or PsExec.exe
Email with Non-PE file e.g. document macro	Memory only malware e.g. SQL Slammer	Memory only payload e.g. Mirai DDoS
Remote script dropper e.g. LNK with PowerShell from cloud	Persistent Fileless persistence loadpoint e.g. JScript in registry	Non-PE file payload e.g. PowerShell script
Weak or stolen credentials e.g. RDP password guess	Regular non-fileless method	Regular non-fileless payload

Spoofing against over 20 ships in the Black Sea.

_USER SEGMENT: DATA SPOOFING TO LURE THE USER

There are many ways to spoof a GPS satellite. One way is to compromise the satellite's receiver and alter its output signal. In 2017, the U.S. Maritime Administration reported the first GPS spoofing attack against over 20 ships in the Black Sea. Correspondence between one of the impacted vessels and their command center indicates that over the course of the attack, the GPS position displayed on their navigation tool sometimes showed 'lost GPS fixing position'. At one point during the attack, the spoofed location showed the ship was located near the Gelendzhik airport but was in fact 25 nautical miles from the reported location. According to a non-profit organization called Resilient Navigation and Timing, which monitors GPS incidents, anecdotal spoofing reports are not uncommon in Russian waters.

_SPACE SEGMENT: THE RISK OF TAKEOVER

Attacks on the satellites themselves are less common in recent times. Nevertheless, most of the typologies of attacks described above (living off the land tactic, links hijacking, GPS Spoofing/Jamming, etc.) can be means to reach the space segment as a final target. Here, the most important risk is a takeover or an OT attack on a satellite. In 2008 in a scientific article by Jessica A. Steinberger reported on a Trojan horse attack that allowed hackers to break into the computer system of the Johnson Space Center in Houston, Texas.
With this access they managed to reach the International Space Station (ISS) and disrupt on-board operations. This use case, which seemed unthinkable, was facilitated using old software on board with an almost non-existent patching policy for vulnerabilities.

_Transportation

_UNDERSTANDING THE CYBER THREAT

In the age of automation and networking, recent years have seen an overwhelming increase in cyber attacks against the transport industry. As a result of the proliferation of attackers and their modus operandi, IT systems are often too vulnerable. As a result, attackers are finding more and more entry points into increasingly vulnerable systems. In addition, in 2020, a number of global events have favoured attacks against this sector of activity, such as the COVID-19 pandemic. Indeed, in this period of coronavirus, attacking those in the second line unfortunately makes sense for malicious individuals. The transport and logistics sector fulfils vital missions and therefore needs more than ever to have fully operational information systems.

It is important to know that the transport sector is made up of six sub-sectors: public transport and passenger rail, pipeline systems, road and highway transport, the maritime transport system, rail freight, and postal and maritime transport. The vitality of the sector's interconnectedness and global presence makes it a tempting target for hackers.

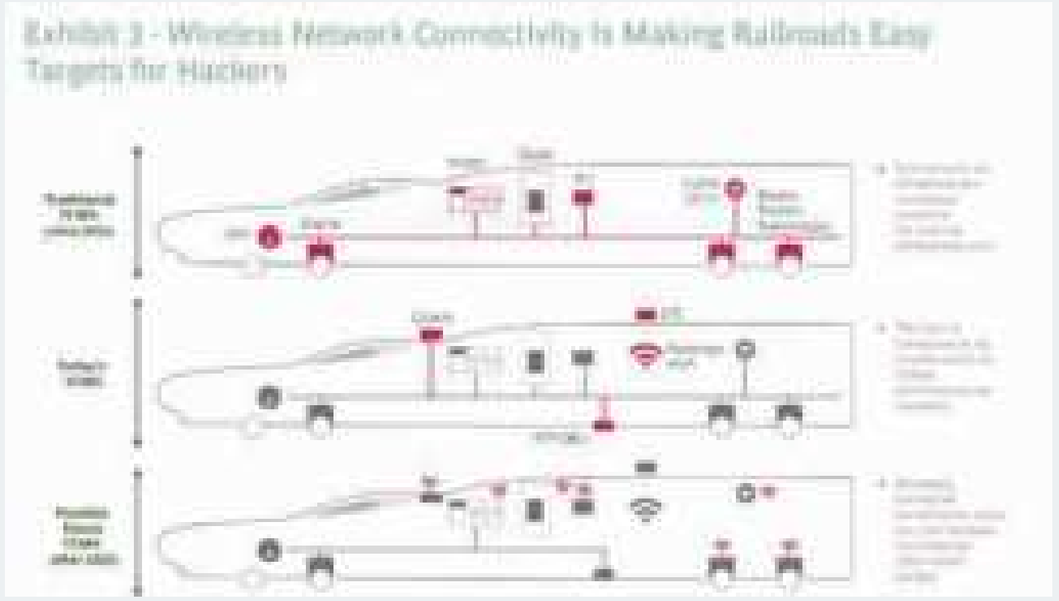
_WHERE THE WEAKNESSES ARE: THE RAIL INDUSTRY

In the rail industry, traditional wire-based train control and management systems (TCMS), which had only limited communication with external systems, are giving way to wireless standards like GSM-Railway, a relatively broad network linking trains to railway regulation control centers. As is the case for all mobility providers these days, T&L companies use vehicle infotainment services and other equipment that add another layer of internet-connected communications.

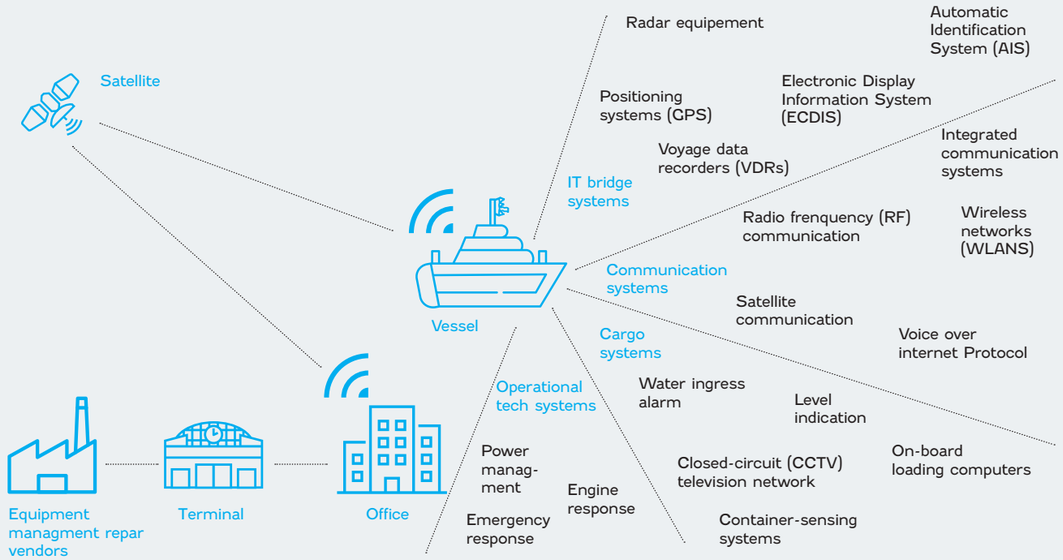
_WHERE THE WEAKNESSES ARE: THE MARITIME SECTOR

In every segment of the transportation industry, the widened cyber-attack surface is evident. For instance, among maritime companies, relatively simple distress-and-safety systems have been replaced by full-fledged, cloud-based, local area networks, like the International Maritime Organization's (IMO) e-navigation program. These networks are a tempting target for hackers because they collect, integrate, and analyze on-board information continuously to track ships' locations, cargo details, maintenance issues, and a host of oceanic environmental considerations.

Wireless network connectivity is making railroads easy target for hackers



Cargo ships are increasingly connected to communications systems that leave them vulnerable



_THE IMPACT OF CYBERCRIME IN THE TRANSPORTATION SECTOR

The fallout from cyber attacks can sometimes be felt by organizations for many months.
In addition to service interruptions, cybercrime can also impact daily operations and result in the exposure of sensitive data.

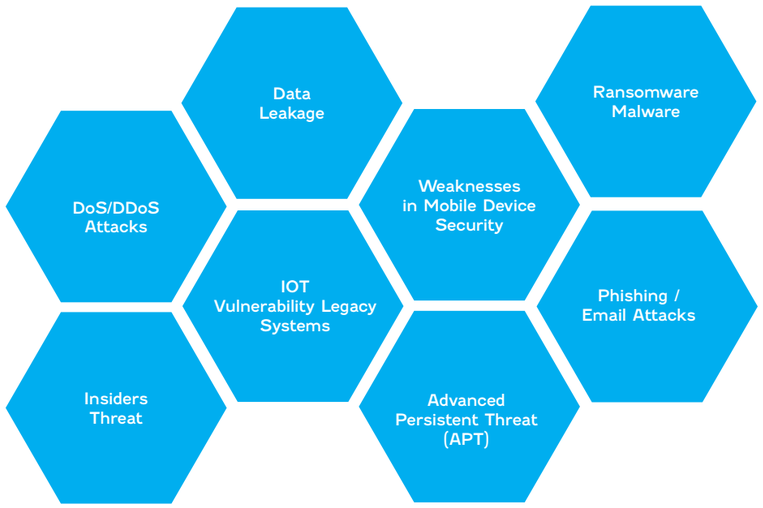
- Below are sample impacts of cyber attacks in the transportation sector:
- Disruption to traffic lights, toll booths and electronic traffic signs
- Interruption of ticket machines and fare gates
- Blocked access to important files and data
- Theft of sensitive information from emails
- Interruption of payroll services
- Theft of personally identifiable information (“PII”)
- Blocked access to computer systems, resulting in employees using personal devices for work.

_TRANSPORTATION CYBERATTACKS CAN BE DEVASTATING

Transportation is the tenth most costly industry for experiencing a data breach. On average, breaches cost transit companies $3.58 million per incident and take 275 days to contain. As cyberattacks on the sector grow increasingly common, these figures could grow, leading to incredible losses.
Example of devastating attack: in early May 2021, the Colonial Pipeline suffered a ransomware attack that forced it to shut down its entire network to prevent the malware from spreading.

Indeed, Colonial Pipeline, the largest oil pipeline in the United States, shut down operations after suffering what is believed to be a ransomware attack. Colonial Pipeline transports refined petroleum products between refineries on the Gulf Coast and markets in the southern and eastern United States. The company transports 2.5 million barrels per day through its 5,500-mile pipeline and supplies 45% of all fuel consumed on the East Coast

Top threats in the transportation industry



Our experts

Cyber Competencies Center

Cybels Train & Experiment

Thales SOC (Security Operation Centre)

References

ZONE EUROPE

Page 12-17

1 The foundation treaty of the European Union. Came into force in 1993.

2 Vitali Kremez, 'Let's Learn: In-Depth on APT28/Sofacy Zebrocy Golang Loader', accessed 20 September 2021, https://www.vkremez.com/2018/12/lets-learn-dissecting-apt28sofacy.html.
Malpedia, 'Zebrocy (Malware Family)', Malpedia, accessed 20 September 2021, https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy.
Accenture, 'Snakemackerel Delivers Zekapab Malware', WordPressBlog, 29 November 2018, https://www.accenture.com/us-en/blogs/cyber-defense/snakemackerel-delivers-zekapab-malware.
MITRE ATT&CK®, 'Zebrocy, Software S0251', MITRE ATT&CK®, 23 April 2021, https://attack.mitre.org/software/S0251/.

3 Dark Reading Staff, 'France's TV5Monde Was Victim Of Vicious Cyberattack In 2015', Dark Reading, 11 October 2016, https://www.darkreading.com/attacks-breaches/frances-tv5monde-was-victim-of-vicious-cyberattack-in-2015.

4 Dominique Filippone, 'Ransomware Maze : Bouygues Construction remédie, l'ANSSI documente - Le Monde Informatique', LeMondeInformatique, 6 February 2020, https://www.lemondeinformatique.fr/actualites/lire-ransomware-maze-bouygues-construction-remedie-l-anssi-documente-78010.html.

5 Lawrence Abrams, 'Sopra Steria Confirms Being Hit by Ryuk Ransomware Attack', BleepingComputer, 26 October 2020, https://www.bleepingcomputer.com/news/security/sopra-steria-confirms-being-hit-by-ryuk-ransomware-attack/.

6 Ionut Ilascu, 'Enel Group Hit by Ransomware Again, Netwalker Demands $14 Million', BleepingComputer, 27 October 2020, https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/.

7 Jason Sattler, 'The Kaseya Ransomware Case Continues Ransomware Groups' Abuse of Trust', F-Secure Blog, 7 July 2021, https://blog.f-secure.com/the-kaseya-ransomware-case-continues-ransomware-groups-abuse-of-trust/.

8 Johan Ahlander and Joseph Menn, 'Major Ransomware Attack against U.S. Tech Provider Forces Swedish Store Closures', Reuters, 4 July 2021, sec. Technology, https://www.reuters.com/technology/cyber-attack-against-us-it-provider-forces-swedish-chain-close-800-stores-2021-07-03/.

9 Naveen Goud, 'Cyber Attack on Airbus', Cybersecurity Insiders, 27 September 2019, https://www.cybersecurity-insiders.com/cyber-attack-on-airbus/.

10 Daphne Leprince-Ringuet, 'This New Hacking Group Is Using "island Hopping" to Target Victims', ZDNet, 3 October 2019, https://www.zdnet.com/article/this-new-hacking-group-is-using-island-hopping-to-target-victims/.

11 Orlee Berlove, 'Airbus Attacked by Avivore – China's Bird Eater', Security Boulevard (blog), 8 October 2019, https://securityboulevard.com/2019/10/airbus-attacked-by-avivore-chinas-bird-eater/.

12 https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

13 https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

14 European Commission, 'A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans', Text, EEAS - European External Action Service - European Commission, 12 February 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/39720/credible-enlargement-perspective-and-enhanced-eu-engagement-western-balkans_en.

15 Živilė Kalibataitė, 'Le spectre des menaces russes dans les Pays baltes', Les Champs de Mars N° 30 + Supplément, no. 1 (25 May 2018): 139–46.

16 https://www.thenationalnews.com/world/europe/dutch-intelligence-warns-of-iran-s-continued-quest-for-weapons-of-mass-destruction-1.1216375

ZONE CIS

Page 18 to 23

1 The Republic of Abkhazia is recognised by Russia, Nicaragua, Venezuela, Nauru and Syria.

2 Ethnic group with a predominantly Sunni culture and religion.

3 Mathieu Duchâtel et Al., Eurasian integration and the EU, ECFR, May 2016.

4 https://www.washingtonpost.com/world/asia_pacific/in-central-asias-for-bidding-highlands-a-quiet-newcomer-chinese-troops/2019/02/18/78d4a8d0-1e62-11e9-a759-2b8541bbbe20_story.html?utm_term=.74eb2b2e2901

5 As a reminder, Georgia, Ukraine and the Baltic States are not or no longer part of the CIS.

A https://commons.wikimedia.org/wiki/File:Commonwealth_of_Independent_States_in_2020.png

B https://s1.qwant.com/thumbr/0x380/3/9/c4149572278 4d4424d010c134a-79905944fa532d46999194a11efb82e1f7b3/b05831936e8cd1d543a3b04fab184a3c.jpg?u=https%3A%2F%2Fi.pinimg.com%2Foriginals%2Fb0%2F58%2F31%2Fb05831936e8cd1d543a3b04fab184a3c.jpg&q=0&b=1&p=0&a=0

ZONE AFRICA

Page 24 to 29

1 Patrick Manning, 'African Population Totals, 1850-1960' (Harvard Dataverse, 14 December 2014), https://doi.org/10.7910/DVN/28045.

2 McKinsey, 'Lions Go Digital: The Internet's Transformative Potential in Africa', McKinsey Global Institute, 1 November 2013, https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/lions%20go%20digital%20the%20internets%20transformative%20potential%20in%20africa/mgi_lions_go_digital_full_report_nov2013.pdf.

3 Symantec (Broadcom), 'Cybercrime and Cybersecurity Trends in Africa – Global Forum on Cyber Expertise', Global Forum on Cyber Expertise – GFCE, 20 June 2016, https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf.

4 Internet World Stats, 'Africa Internet Users, 2021 Population and Facebook Statistics', Internet World Stats, 2021, https://www.internetworldstats.com/stats1.htm.

5 Dominique Tabutin and Bruno Schoumaker, 'La démographie de l'Afrique subsaharienne au XXIe siècle', Population Vol. 75, no. 2 (1 December 2020): 169–295.

6 United Nations, Department of Economic and Social Affairs, Population Division, 'Population of Africa (2021)', Worldometer, 2021, https://www.worldometers.info/world-population/africa-population/.

7 Symantec (Broadcom), 'Cybercrime and Cybersecurity Trends in Africa – Global Forum on Cyber Expertise'.

8 Servicesmobiles.fr, 'Le Nigéria peut compter sur 184,6 millions d'abonnés actifs sur mobile !', Servicesmobiles.fr, 4 March 2020, https://www.servicesmobiles.fr/le-nigeria-peut-compter-sur-1846-millions-dabonnes-actifs-sur-mobile-55840.

9 GSMA, 'The Mobile Economy: Sub-Saharan Africa', The Mobile Economy (blog), 2021, https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf.

10 Nathaniel Allen, 'Africa's Evolving Cyber Threats'.

11 Kit Chellel, 'The Hacker Who Took Down a Country', Bloomberg.Com, 20 December 2019, https://www.bloomberg.com/news/features/2019-12-20/spider-man-hacker-daniel-kaye-took-down-liberia-s-internet.

12 Sergiu Gatlan, 'Ransomware Attack Cripples Power Company's Entire Network', BleepingComputer, 25 July 2019, https://www.bleepingcomputer.com/news/security/ransomware-attack-cripples-power-company-s-entire-network/.

13 Sergiu Gatlan, 'Ransomware Attack Shuts Down City of Johannesburg's Systems', BleepingComputer, 25 October 2019, https://www.bleepingcomputer.com/news/security/ransomware-attack-shuts-down-city-of-johannesburgs-systems/

14 Joey Shea, 'Egypt's Digital Foreign Policy', The Tahrir Institue for Middle East Policy (TIMEP), 2 February 2021, https://timep.org/commentary/analysis/egypts-digital-foreign-policy/.

15 Catherine Chapman, 'How Africa Is Tackling Its Cybersecurity Skills Gap', The Daily Swig | Cybersecurity news and views, 22 August 2018, https://portswigger.net/daily-swig/how-africa-is-tackling-its-cybersecurity-skills-gap.

16 Nathaniel Allen, 'Africa's Evolving Cyber Threats', Africa Center for Strategic Studies (blog), 19 January 2021, https://africacenter.org/spotlight/africa-evolving-cyber-threats/.

17 Symantec (Broadcom), 'Cybercrime and Cybersecurity Trends in Africa – Global Forum on Cyber Expertise'.

18 Nathaniel Allen, 'Africa's Evolving Cyber Threats'.

WESTERN ASIA AREA

Page 44 to 51

1 https://www.bestvpnanalysis.com/man-middle-attack/

ZONE EAST ASIA

Page 52 to 57

1 Franck Manuelle, 'Une géographie de l'Asie du Sud-Est', Document, Géoconfluences (ENS Lyon), 3 June 2020, http://geoconfluences.ens-lyon.fr/informations-scientifiques/dossiers-regionaux/asie-du-sud-est/cadrage.

2 Hyonhee Shin, 'N.Korea's Trade with China Plunges 80% as COVID-19 Lockdown Bites', Reuters, 19 January 2021, sec. China, https://www.reuters.com/world/china/nkoreas-trade-with-china-plunges-80-covid-19-lockdown-bites-2021-01-19/.

3 Lee Seong-hyon, 'China-N. Korea Defense Treaty', koreatimes, 26 July 2016, https://www.koreatimes.co.kr/www/opinion/2021/10/197_210355.html.

4 Kristian McGuire, 'Dealing With Chinese Sanctions: South Korea and Taiwan', 12 May 2017, https://thediplomat.com/2017/05/dealing-with-chinese-sanctions-south-korea-and-taiwan/.

5 The association between these two groups is evident in particular by their shared link with a third actor: ATK159 (SideWinder).

6 Dominique André, 'Vietnam-Chine : la guerre des nerfs en mer de Chine méridionale', Franceinfo, 8 March 2017, https://www.francetvinfo.fr/monde/chine/vietnam-chine-la-guerre-des-nerfs-en-mer-de-chine-meridionale_2086893.html.

7 Trend Micro Security, 'ESILE Targeted Attack Campaign Hits APAC Governments', Trend Micro, 28 July 2014, https://www.trendmicro.com.my/vinfo/my/security/news/cyber-attacks/esile-targeted-attack-campaign-hits-apac-governments.

8 Robert Falcone et al., 'Operation Lotus Blossom (Reports)', Palo Alto Networks, 16 June 2015, https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.

9 Kevin Stear, 'Lotus Blossom Continues ASEAN Targeting', RSA Link, 13 February 2018, https://community.rsa.com/t5/netwitness-blog/lotus-blossom-continues-asean-targeting/ba-p/518891.

10 lia Wallace, 'Cambodia Charges Opposition Leader Kem Sokha With Treason', The New York Times, 5 September 2017, sec. World, https://www.nytimes.com/2017/09/05/world/asia/cambodia-kem-sokha-treason.html.

11 Matt Spetalnick and Rosemarie Francisco, 'Obama Puts South China Sea Dispute on Agenda as Summitry Begins', Reuters, 17 November 2015, sec. Emerging Markets, https://www.reuters.com/article/us-apec-summit-idUSKCN0T60RM20151117.

12 Adam Pilkey, 'NanHaiShu: Threat Intelligence Brief on Intelligence Gathering Attacks', F-Secure Blog, 4 August 2016, https://blog.f-secure.com/nanhaishu-threat-intelligence-brief-on-intelligence-gathering-attacks/.

13 Ji Young Kong, Jong In Lim, and Kyoung Gon Kim, 'The All-Purpose Sword: North Korea's Cyber Operations and Strategies' (Tallinn: 2019 11th International Conference on Cyber Conflict, 2019), https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf.

ZONE SOUTH ASIA

Page 58 to 63

1 Cybleinc, 'Transparent Tribe Operating with a New Variant of Crimson RAT', Cyble, 30 April 2021, https://blog.cyble.com/2021/04/30/transparent-tribe-operating-with-a-new-variant-of-crimson-rat/.

2 CisoMag, 'Pakistani APT Group 'SideCopy' targets officials in India and Afghanistan', 6 December 2021 https://cisomag.eccouncil.org/pakistani-apt-group-sidecopy-targets-officials-in-india-and-afghanistan//

ATTACKERS' PAGES :

Page 70-269

ATK103
- https://blog.morphisec.com/explosive-new-mirrorblast-campaign-targets-financial-companies

ATK132
- 16/11/2021, Meta, https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/
- 24/07/2013, Malwarebytes Lab, Syrian Electronic Army Hacks Tango and Viber Servers
- 06/02/2014, The Hacker News, Facebook domain hacked by Syrian Electronic Army
- 22/06/2014, medium, How Reuters got compromised by the Syrian Electronic Army
- 29/08/2014, FireEye, Connecting the Dots: Syrian Malware Team Uses BlackWorm for Attacks
- 27/11/2014, Reuters, Western media websites hacked by Syrian Electronic Army
- 21/01/2015, The Telegraph, Le Monde hacked: 'Je ne suis pas Charlie' writes Syrian Electronic Army
- 03/04/2015, Vice, The Syrian Electronic Army's Most Dangerous Hack
- 13/08/2015, Krebs on security, Washington Post Site Hacked After Successful Phishing Campaign
- 05/12/2018, Forbes, Syrian Electronic Army Hackers Are Targeting Android Phones With Fake WhatsApp Attacks
- 13/10/2019, 360 Core Security, Uncover the Secrets of the Syrian Electronic Army: The role and influence of cyber-attacks in the Syrian Civil War

ATK2
- https://web.archive.org/web/20180505155305/https://401trg.pw/burning-umbrella/
- https://web.archive.org/web/20180505155305/https://401trg.pw/burning-umbrella/
- https://www.mandiant.com/resources/apt41-us-state-governments
- https://wws.cert-ist.com/private/fr/IocAttack_details?format=html&objectType=ATK&ref=CERT-IST/ATK-2017-014
- https://www.mandiant.com/resources/apt41-us-state-governments

ATK236
- https://www.intezer.com/blog/research/conversation-hijacking-campaign-delivering-icedid/.
- https://unit42.paloaltonetworks.com/ta551-shathak-icedid/
- https://unit42.paloaltonetworks.com/atoms/ta551-shathak/
- https://unit42.paloaltonetworks.com/atoms/ta551-shathak/

ATK3
- 13/08/2020, ClearSky, https://www.clearskysec.com/operation-dream-job/
- 06/07/2021, AT&T, https://cybersecurity.att.com/blogs/labs-research/lazarus-campaign-ttps-and-evolution
- 27/01/2022, MalwareBytes, https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/
- 08/02/2022, Qualys, https://blog.qualys.com/vulnerabilities-threat-research/2022/02/08/lolzarus-lazarus-group-incorporating-lolbins-into-campaigns
- 14/04/2022, Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical
- Stairwell, https://stairwell.com/news/threat-research-the-ink-stained-trail-of-goldbackdoor/
- 26/04/2022, SecurityAffairs, https://securityaffairs.co/wordpress/130606/apt/apt37-targets-journalists-goldbackdoor.html
- https://www.bleepingcomputer.com/news/security/apt37-targets-journalists-with-chinotto-multi-platform-malware/

ATK41
- https://therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector/
- https://duo.com/decipher/apt10-espionage-attacks-on-u-s-orgs-uncovered
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks

ATK5
- https://www.bleepingcomputer.com/news/security/google-warns-14-000-gmail-users-targeted-by-russian-hackers/
- https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

ATK51
- https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html
- https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html
- https://blog.polyswarm.io/muddy-water-uses-sloughrat-in-recent-campaigns
- https://duo.com/decipher/cisa-warns-of-ongoing-attacks-by-muddywater-apt

ATK66
- https://blog.talosintelligence.com/2022/02/arid-viper-targets-palestine.html

ATK64
- https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html
- https://anchorednarratives.substack.com/p/trouble-in-asia-and-the-middle-east?s=r
- https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
- https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/
- https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/
- https://blog.cyble.com/2022/02/11/deep-dive-analysis-caprarat/

ATK91
- https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who

AUTOMOTIVE SECTOR

Page 274 to 275

1 https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/
2 https://www.inc.com/minda-zetlin/chinese-hackers-take-control-of-a-tesla-from-12-miles-away-most-cars-are-probabl.html
3 https://smartcar.com/blog/connected-cars-worldwide/
4 https://www.trustonic.com/opinion/the-changing-face-of-automotive-cyber-attacks/

AVIATION SECTOR

Page 276 to 277

1 https://www.pandasecurity.com/en/mediacenter/mobile-news/can-airplanes-get-hacked/
2 https://www.newsweek.com/flight-airplanes-can-now-be-hacked-ground-cyber-expert-warns-962420

CIVIL SOCIETY SECTOR

Page 280 to 281

1 https://www.devex.com/news/opinion-why-civil-society-remains-so-vulnerable-to-cyberattacks-102016
2 https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658;
3 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf
4 https://eu.usatoday.com/story/tech/2019/07/17/microsoft-finds-more-election-related-cyber-crimes-russia-and-iran/1761507001/
5 https://cyberpeaceinstitute.org/news/the-dark-side-of-cyberspace-the-threat-to-ngos-and-nonprofits
6 https://heimdalsecurity.com/blog/cybersecurity-in-non-profit-and-non-governmental-organizations/
7 https://www.fireeye.com/blog/threat-research/2014/04/ngos-fighting-human-rights-violations-and-now-cyber-threat-groups.html
8 https://www.forbes.com/sites/leemathews/2019/04/30/cybercriminals-steal-1-75-million-from-an-ohio-church/?sh=11d7d4fe420c
9 https://www.rte.ie/news/2022/0215/1280931-rds-cyberattack/
10 https://www.civilsociety.co.uk/news/26-of-charities-had-a-cyber-attack-last-year.html
11 https://srdefenders.org/voice-subjected-to-cyber-attack-in-viet-nam-joint-communication/
12 https://cyberpeaceinstitute.org/news/non-profit-organization-targeted-by-cyberattack-valuable-lessons-for-you/
13 https://www.zdnet.com/article/red-cross-hit-with-cyberattack-that-compromised-data-of-515000-highly-vulnerable-people/
14 https://startupdigital.in/cyber-security/philly-food-bank-loses-1m-in-bec-scam/
15 https://www.technologyreview.com/2021/05/27/1025443/chinese-hackers-uyghur-united-nations/

GOVERNMENT SECTOR

Page 294 to 295

1 https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/
2 https://www.lebigdata.fr/solarwinds-cyberattaque-historique-usa
3 https://www.csoonline.com/article/3391589/why-local-governments-are-a-hot-target-for-cyberattacks.html

HEALTHCARE SECTOR

Page 296 to 297

1 https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf
2 https://www.morganfranklin.com/insights/company-insight/healthcare-cyber-threat-landscape/

INFORMATION TECHNOLOGY SECTOR

Page 298 to 299

1 https://media-exp1.licdn.com/dms/document/C4E1FAQHEze5bFLekjA/feedshare-document-pdf-analyzed/0/1645722319173?e=1645876800&v=beta&t=5y0iesX3cHLhEwK0kjPc6eqYTqN8MC_0iyyaXPAfSgQ
2 https://twitter.com/threathunting_
3 https://www.itic.org/policy/cybersecurity
4 https://kryptokloud.com/cyber-threats-facing-high-tech-businesses/
5 https://library.cyentia.com/report/report_001520.html
6 https://www.fireeye.com/current-threats/reports-by-industry/high-tech-threat-intelligence.html#dismiss-lightbox
7 https://www.senetas.com/the-importance-of-cybersecurity-in-high-tech-industries/

LEGAL SECTOR

Page 300 to 301

1 https://ironscales.com/blog/ransomware-legal/
2 https://www.darktrace.com/en/resources/ds-legal.pdf
3 https://atlasvpn.com/blog/31-of-us-companies-close-down-after-falling-victim-to-ransomware
4 https://www.lawsoc-ni.org/DatabaseDocs/med_7625870__thecyberthreattouklegalsectorncsc.pdf
5 https://www.centripetal.ai/legal-sector-cyber-threat-intelligence/
6 https://www.legalfutures.co.uk/blog/the-rising-risk-of-cybercrime-for-law-firms
7 https://www.legalfutures.co.uk/latest-news/service-provider-hack-sees-100gb-of-data-stolen-from-top-law-firm
8 https://iasme.co.uk/cyber-blog/why-is-it-important-for-the-legal-sector-to-fully-address-their-cyber-security/
9 https://www.sra.org.uk/sra/research-report/cyber-security/

10 https://carecomputers.co.uk/key-cybersecurity-considerations-for-the-legal-sector/
11 https://www.digitalshadows.com/blog-and-research/ransomware-and-the-legal-services-sector/
12 https://ironscales.com/blog/ransomware-legal/

MARITIME SECTOR

Page 304 to 305

1 https://www.secureworld.io/industry-news/port-houston-thwarts-cyberattack
2 https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/
3 https://www.csoonline.com/article/3410236/modernized-maritime-industry-transports-cyberthreats-to-sea.html
4 https://www.securitymagazine.com/gdpr-policy?
5 url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F92541-maritime-industry-sees-400-increase-in-attempted-cyberattacks-since-february-2020
6 https://www.cpomagazine.com/cyber-security/maritime-cyber-attacks-are-among-the-greatest-unknown-threats-to-the-global-economy/
7 https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/
8 https://securityintelligence.com/articles/maritime-cybersecurity-rising-tide/
9 https://www.dnv.com/maritime/insights/t

RETAIL SECTOR

Page 308 to 311

1 https://www.6dg.co.uk/blog/cyber-threat-retailers/
2 https://www.helpnetsecurity.com/2021/11/09/retail-industry-security-incidents/
3 https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/ib-retail-consumer.pdf
4 file:///C:/Users/POMMATEAU%20Antoine/Downloads/sophos-state-of-ransomware-retail-2021-wp%20(1).pdf
5 https://www.triskelelabs.com/blog/identifying-and-handling-common-cybersecurity-threats-in-the-retail-industry
6 https://www.cybersecuritydive.com/news/retailers-cyber-monday-attacks/610701opics/maritime-cyber-security/index.html

cyberdefencesolutions@thalesgroup.com

> cyberthreat.thalesgroup.com <