Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center
HC3

North Korean and Chinese Cyber Crime Threats to the HPH

September 21, 2023

TLP:CLEAR, ID# *202309211300*

Agenda

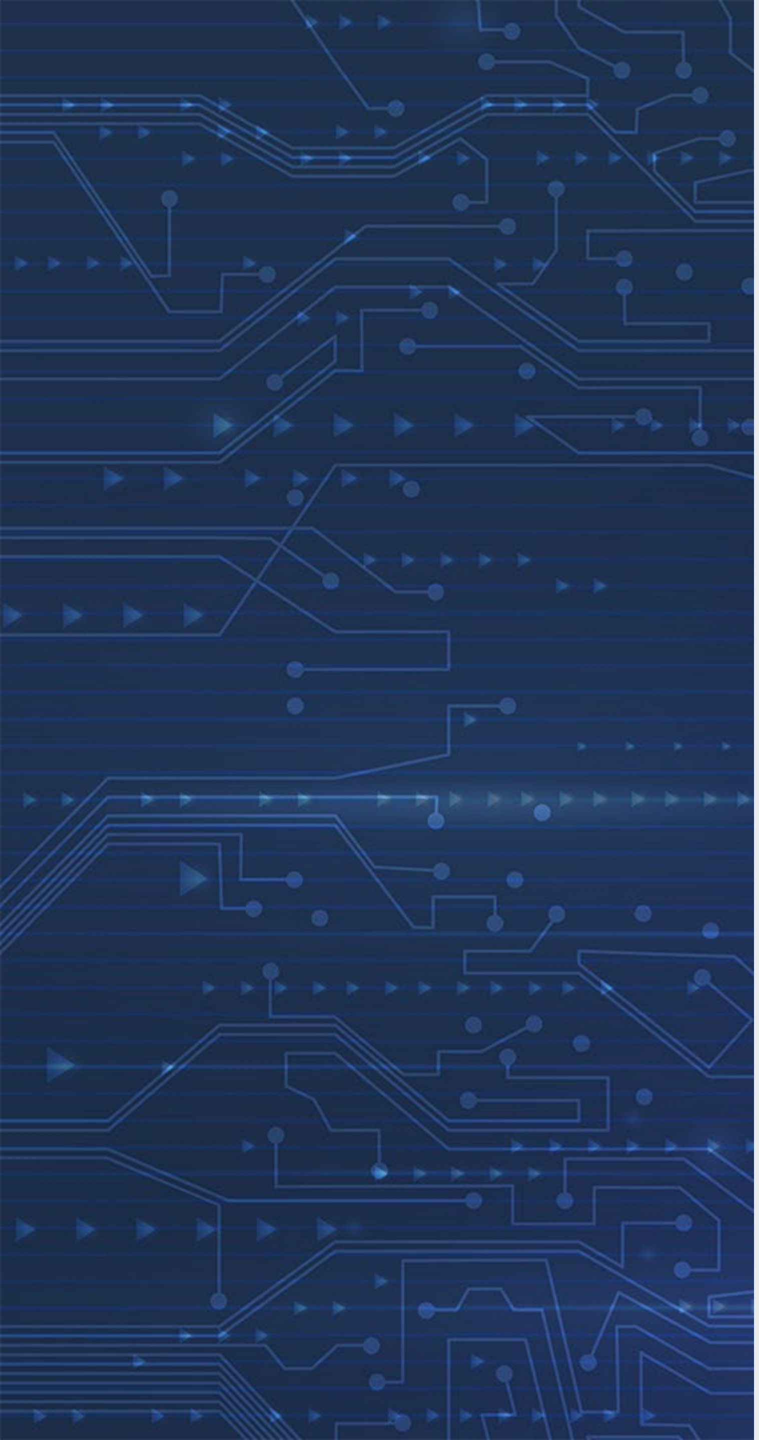
Chinese and North Korean Cybercrime

- Cybercrime Overview and Theory
- China
  - APT41
- North Korea
  - APT43
  - Lazarus Group
- Defense and Mitigations
- Conclusions
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

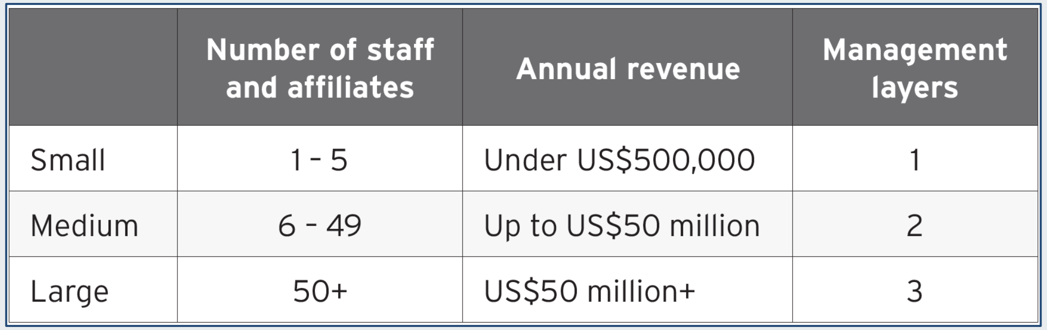


Cybercrime Overview

An overview of common cybercriminal features and characteristics

The Typical, Modern Cybercriminal Gang

- Modern and sophisticated cybercriminal groups are run like companies:
  - Most cybercrime originates from small teams bringing in moderate revenues.
  - They advertise and recruit, track revenues, form partnerships, and track and mimic competition.
  - Larger cybercriminal groups can be organized and operate like a corporation (various departments, staffing challenges, overhead, quality control, etc.).
  - Many groups have political connections and are generally aware of their public relations.
  - They grow capabilities organically/internally and also leverage the black market to bring in new capabilities.

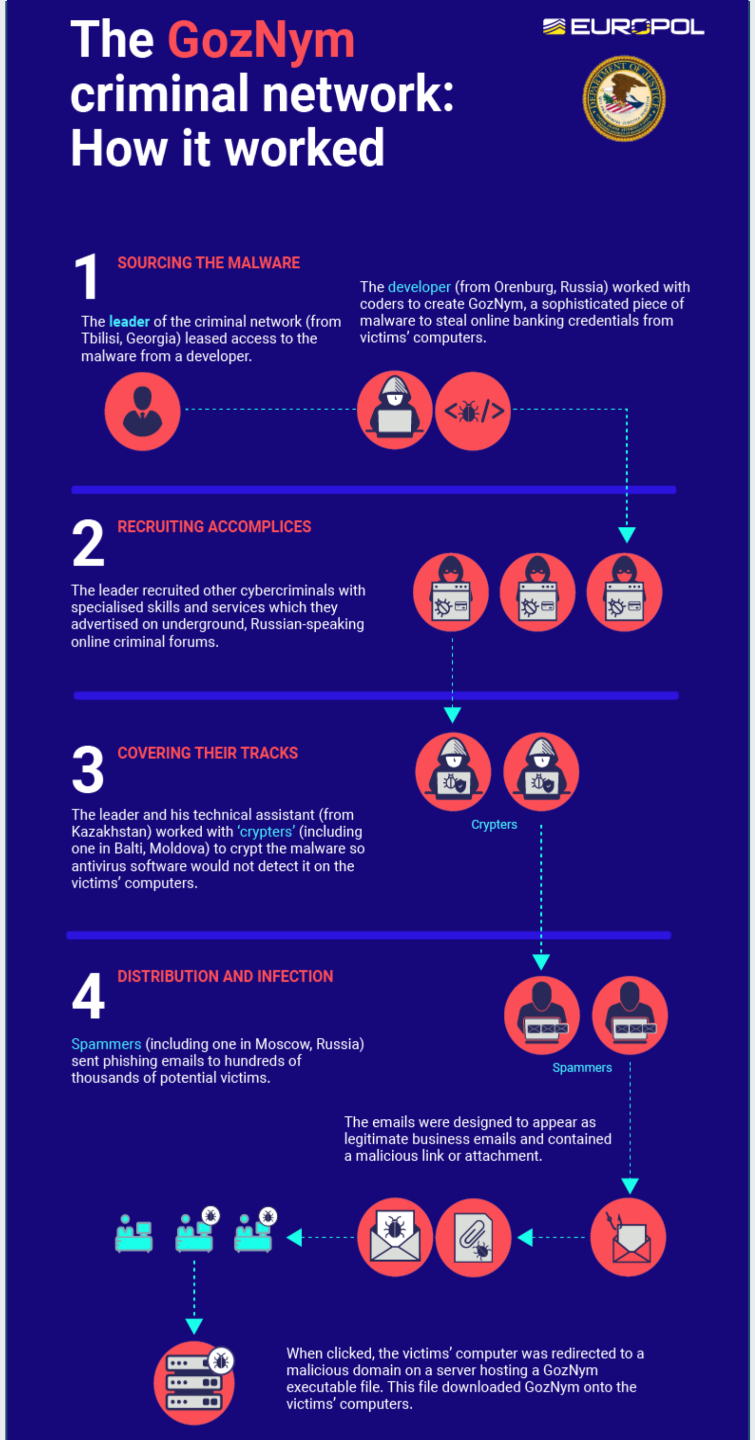


	Number of staff and affiliates	Annual revenue	Management layers
Small	1 - 5	Under US$500,000	1
Medium	6 - 49	Up to US$50 million	2
Large	50+	US$50 million+	3

Guidelines for ascertaining criminal business size.
Image Source: Trend Micro

A Brief Analysis of the GozNym Network

- Midsize cybercriminal gang
  - ~$100M in theft
- Transnational, with members residing in Russia, Georgia, Ukraine, Moldova and Bulgaria
  - Not associated with China or North Korea
- Cybercrime-as-a-service
  - Bulletproof hosting
  - Money mule networks
  - Spammers
  - Crypters



The GozNym criminal network: How it worked

1 SOURCING THE MALWARE

The leader of the criminal network (from Tbilisi, Georgia) leased access to the malware from a developer.

The developer (from Orenburg, Russia) worked with coders to create GozNym, a sophisticated piece of malware to steal online banking credentials from victims' computers.

2 RECRUITING ACCOMPLICES

The leader recruited other cybercriminals with specialised skills and services which they advertised on underground, Russian-speaking online criminal forums.

3 COVERING THEIR TRACKS

The leader and his technical assistant (from Kazakhstan) worked with 'crypters' (including one in Balti, Moldova) to crypt the malware so antivirus software would not detect it on the victims' computers.

4 DISTRIBUTION AND INFECTION

Spammers (including one in Moscow, Russia) sent phishing emails to hundreds of thousands of potential victims.

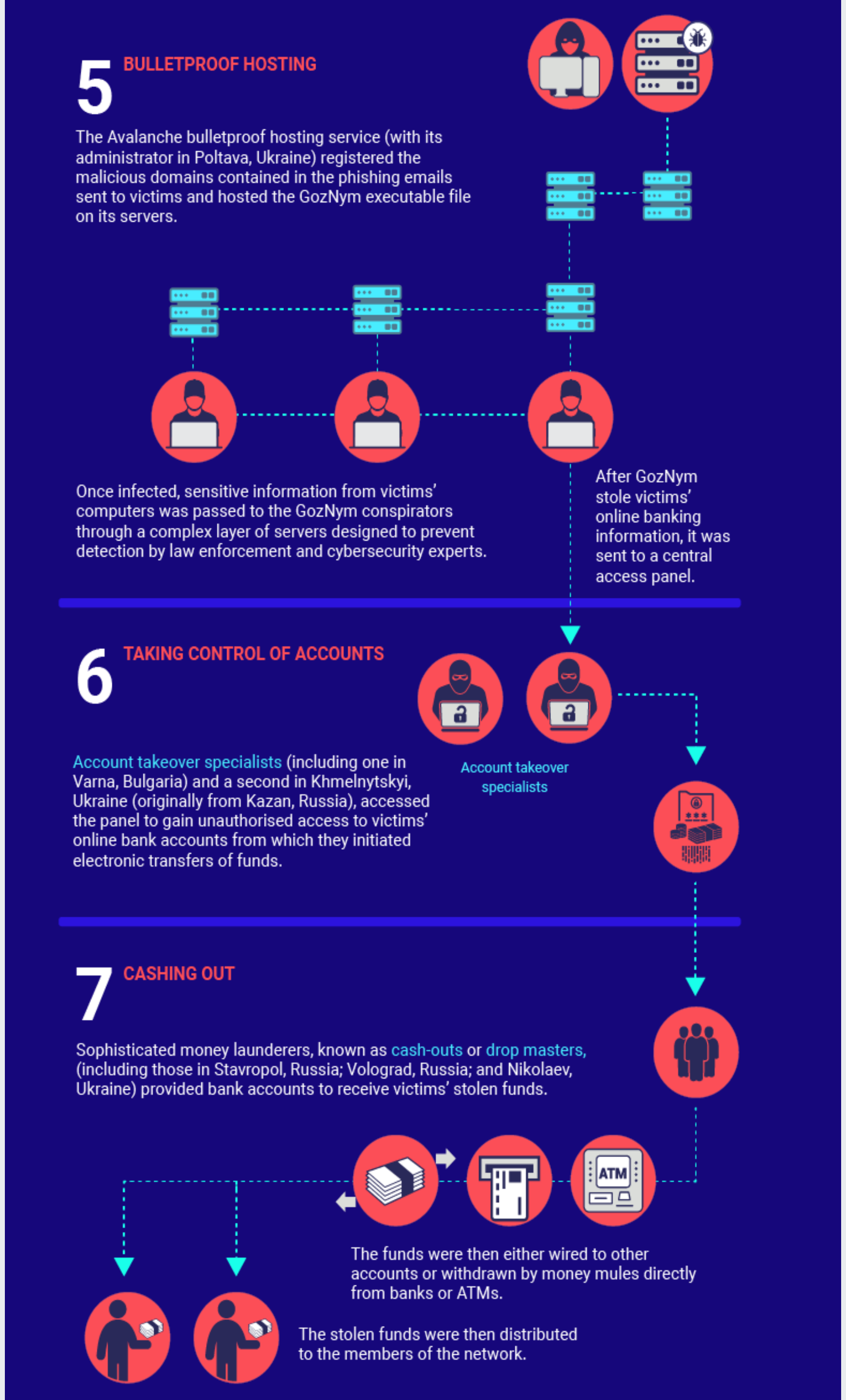
The emails were designed to appear as legitimate business emails and contained a malicious link or attachment.

When clicked, the victims' computer was redirected to a malicious domain on a server hosting a GozNym executable file. This file downloaded GozNym onto the victims' computers.

GozNym diagram.
Image Source: Europol

A Brief Analysis of the GozNym Network (Part 2)

- Bulletproof hosting outsourced to Poland
  - Multiple layers of servers to make detection and disruption more difficult
- Cash-outs facilitated via cryptocurrency and money mules
- Ten members were charged in 2019; five have been detained and prosecuted, five remain on the run



5 BULLETPROOF HOSTING

The Avalanche bulletproof hosting service (with its administrator in Poltava, Ukraine) registered the malicious domains contained in the phishing emails sent to victims and hosted the GozNym executable file on its servers.

Once infected, sensitive information from victims' computers was passed to the GozNym conspirators through a complex layer of servers designed to prevent detection by law enforcement and cybersecurity experts.

After GozNym stole victims' online banking information, it was sent to a central access panel.

6 TAKING CONTROL OF ACCOUNTS

Account takeover specialists (including one in Varna, Bulgaria) and a second in Khmelnytskyi, Ukraine (originally from Kazan, Russia), accessed the panel to gain unauthorised access to victims' online bank accounts from which they initiated electronic transfers of funds.

7 CASHING OUT

Sophisticated money launderers, known as cash-outs or drop masters, (including those in Stavropol, Russia; Vologrod, Russia; and Nikolaev, Ukraine) provided bank accounts to receive victims' stolen funds.

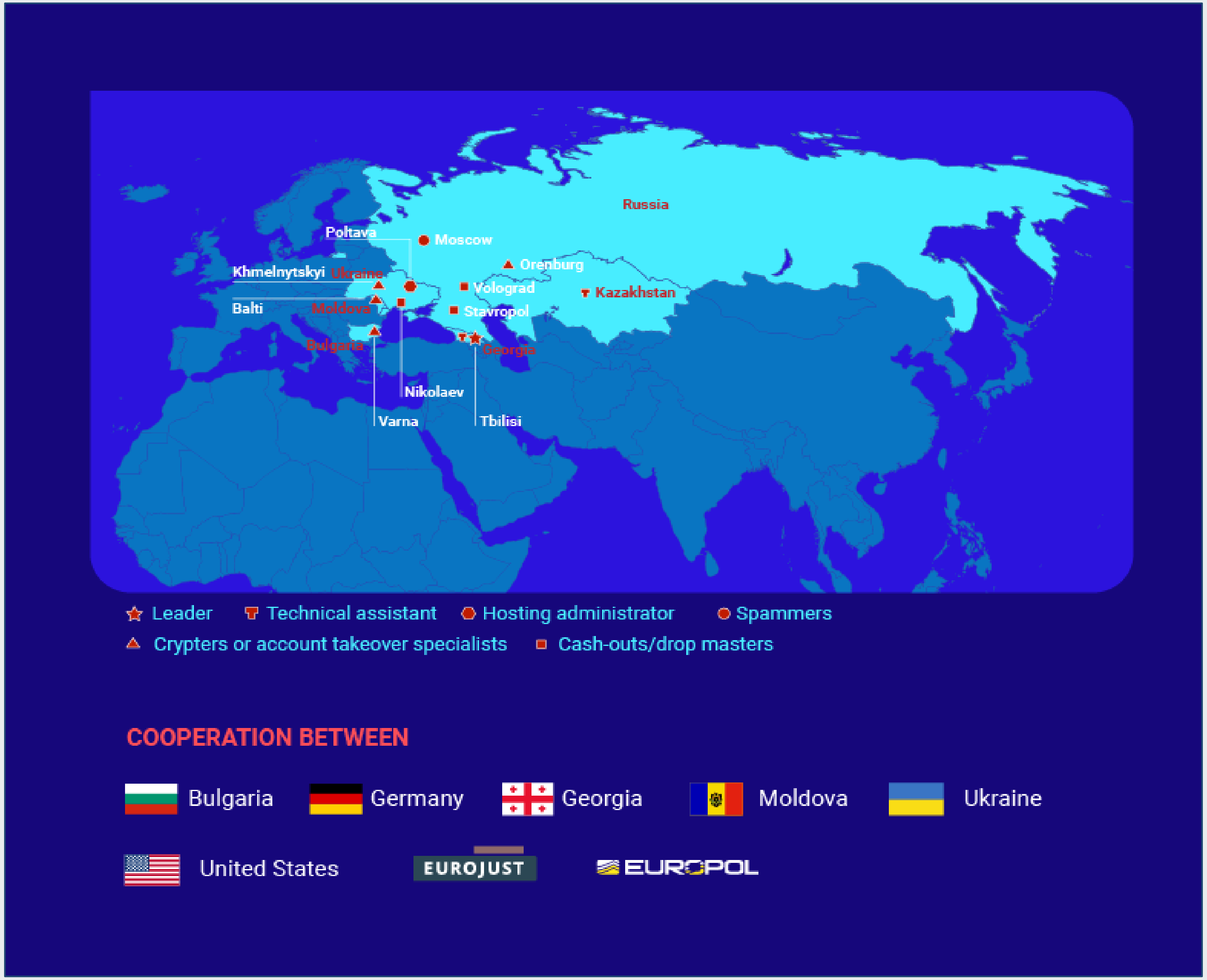
The funds were then either wired to other accounts or withdrawn by money mules directly from banks or ATMs.

The stolen funds were then distributed to the members of the network.

GozNym diagram. *Image Source: Europol*

A Brief Analysis of the GozNym Network (Part 3)

- Map depicts the location of GozNym members
- Flags on the bottom depict the international coalition of law enforcement who brought the gang down



GozNym diagram.
Image Source: Europol

Cyber Threat Actor Characterization/Categorization

What are the different types of threat actors?

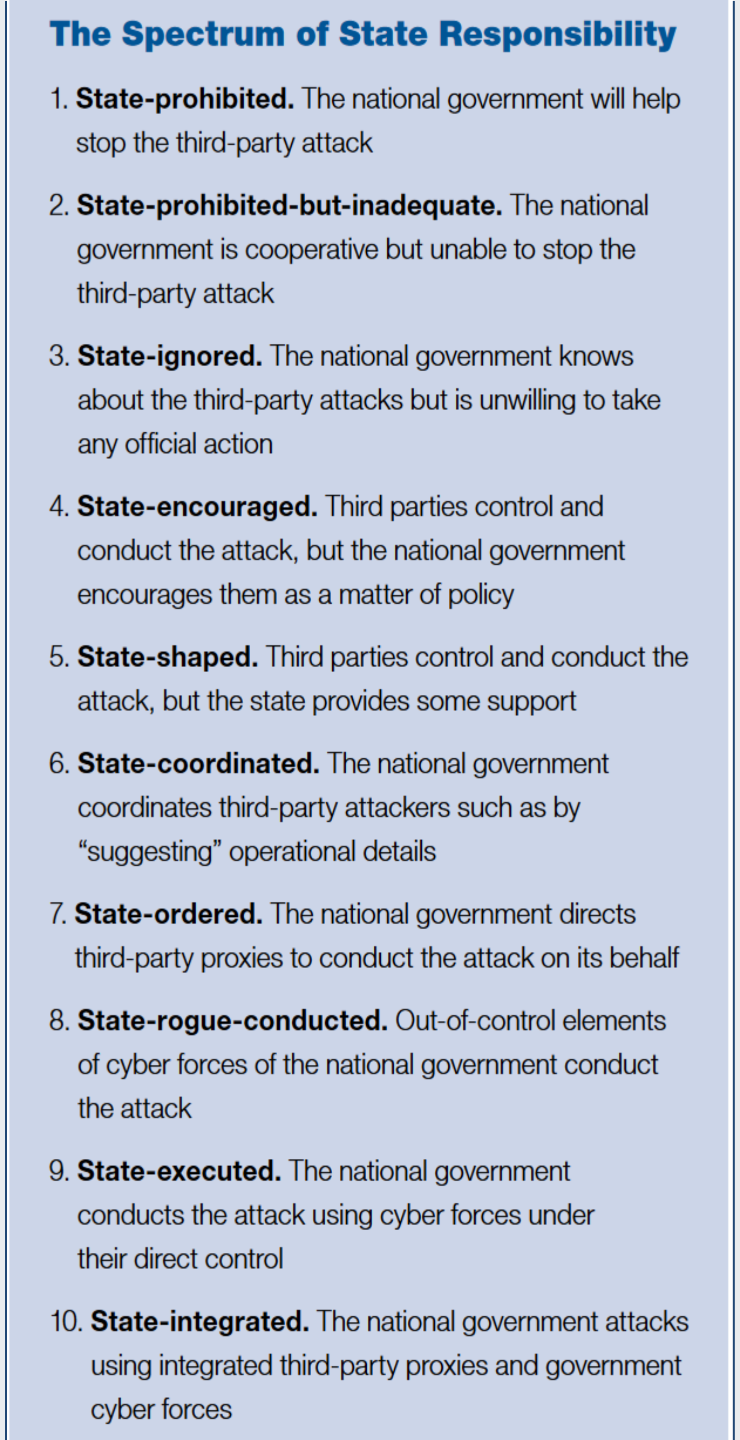
STATE/NON-STATE	TYPE	MOTIVATION
State	Advanced Persistent Threat	Political agenda
Non-state	Cybercriminal groups	Financial fraud/theft
Non-state	Contractors	Political agenda (host)
Non-state	Hacktivists	Political activism
Non-state	Individuals	Any

Examples:

- APTs: Sandworm, APT1, Fancy Bear, Cozy Bear, Ocean Lotus
- Cyber criminal groups: Wizard Spider, FIN7, BlackCat, Emotet
- Contractors: NSO Group, FINFisher
- Hacktivists: Anonymous, Syrian Electronic Army, Shadow Brokers?
- Individuals: Edward Snowden, Chelsea Manning, The Jester

Cyber Threat Actor Characterization/ Categorization (cont.)

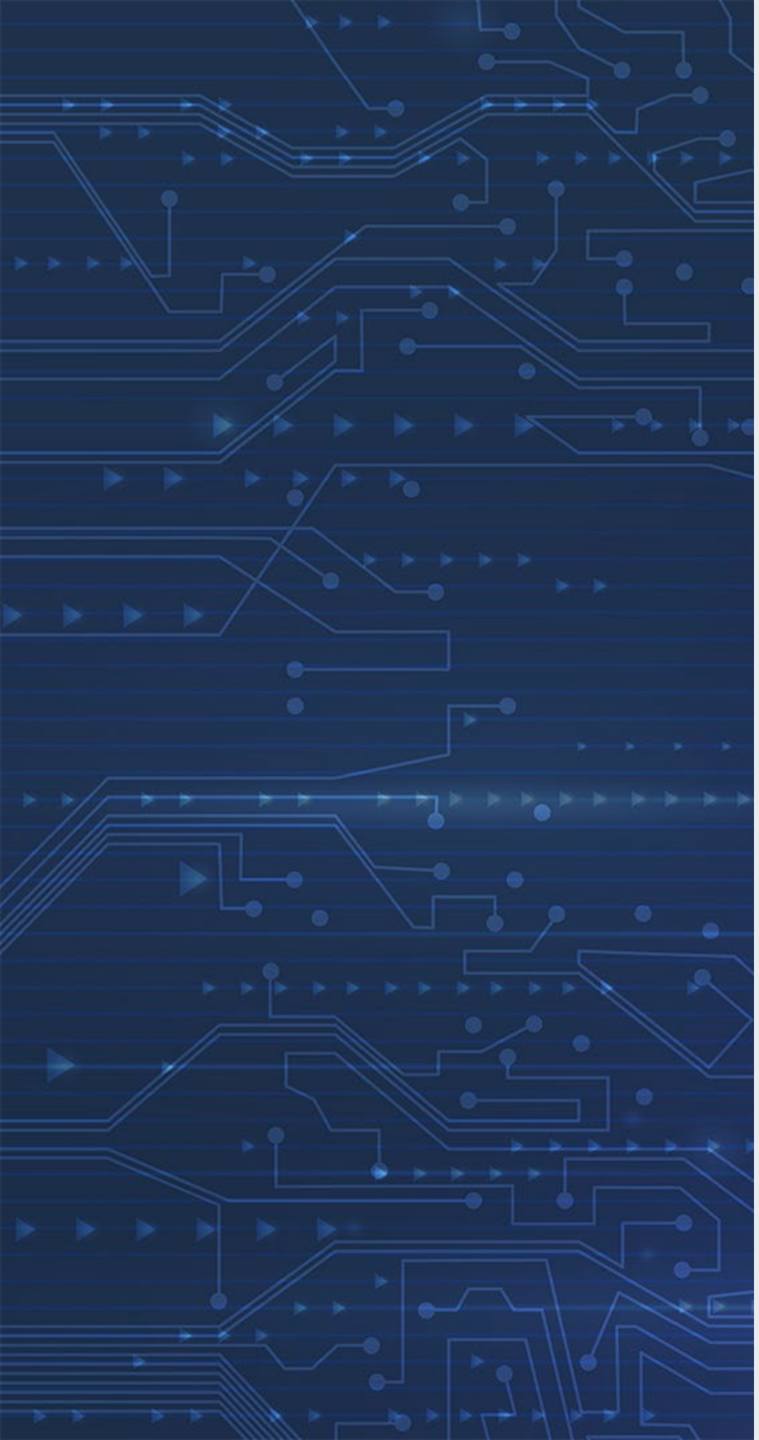
- Jason Healey, Director of the Atlantic Council's Cyber Statecraft Initiative, developed a spectrum to describe the blurred lines between these threats.
- His white paper can be found here: https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF



The Spectrum of State Responsibility

1. **State-prohibited.** The national government will help stop the third-party attack
2. **State-prohibited-but-inadequate.** The national government is cooperative but unable to stop the third-party attack
3. **State-ignored.** The national government knows about the third-party attacks but is unwilling to take any official action
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. **State-shaped.** Third parties control and conduct the attack, but the state provides some support
6. **State-coordinated.** The national government coordinates third-party attackers such as by "suggesting" operational details
7. **State-ordered.** The national government directs third-party proxies to conduct the attack on its behalf
8. **State-rogue-conducted.** Out-of-control elements of cyber forces of the national government conduct the attack
9. **State-executed.** The national government conducts the attack using cyber forces under their direct control
10. **State-integrated.** The national government attacks using integrated third-party proxies and government cyber forces

Image courtesy of the Atlantic Council



China

One of the original cyber superpowers

China as a Cyber Power

- The most powerful cyber power in the region.
- Focuses on data exfiltration (espionage and intellectual property theft) to support economic development across sectors.
- Cyber targeting often aligned with the Five Year Plan:
  - The fourteenth plan (2021 – 2025) includes clinical medicine, genetics, biotechnology, neuroscience and general healthcare research and development.
- Chinese cybercrime is growing but still negligible:
  - China's courts handled less than 300,000 cybercrime cases from 2017 to 2021.
  - Mostly online fraud including bogus loans, fake recruitments and impersonation.

> "If each one of the FBI's cyber agents and intel analysts focused exclusively on the China threat, Chinese hackers would still outnumber FBI cyber personnel by at least 50 to 1."
>
> – Christopher Wray, FBI Director

APT41

- Also known as Double Dragon and Wicked Panda; active since 2012.
- Highly sophisticated and innovative:
  - Supply-chain compromises targeting individuals
  - Frequent use of compromised digital certificates
  - Bootkit operations
- Targets the health sector and U.S. organizations.
- Has engaged in financially-motivated activities in “off hours”:
  - It is believed that financially-motivated targeting of the video game industry has ultimately supported the group’s state-sponsored activity.
  - Tradecraft developed and practiced in operations driven by personal gain have become pivotal in executing state-sponsored attacks.
  - Accessing and conducting reconnaissance on video game environments has enabled APT41 to develop TTPs leveraged against software companies to inject malicious code into software updates.

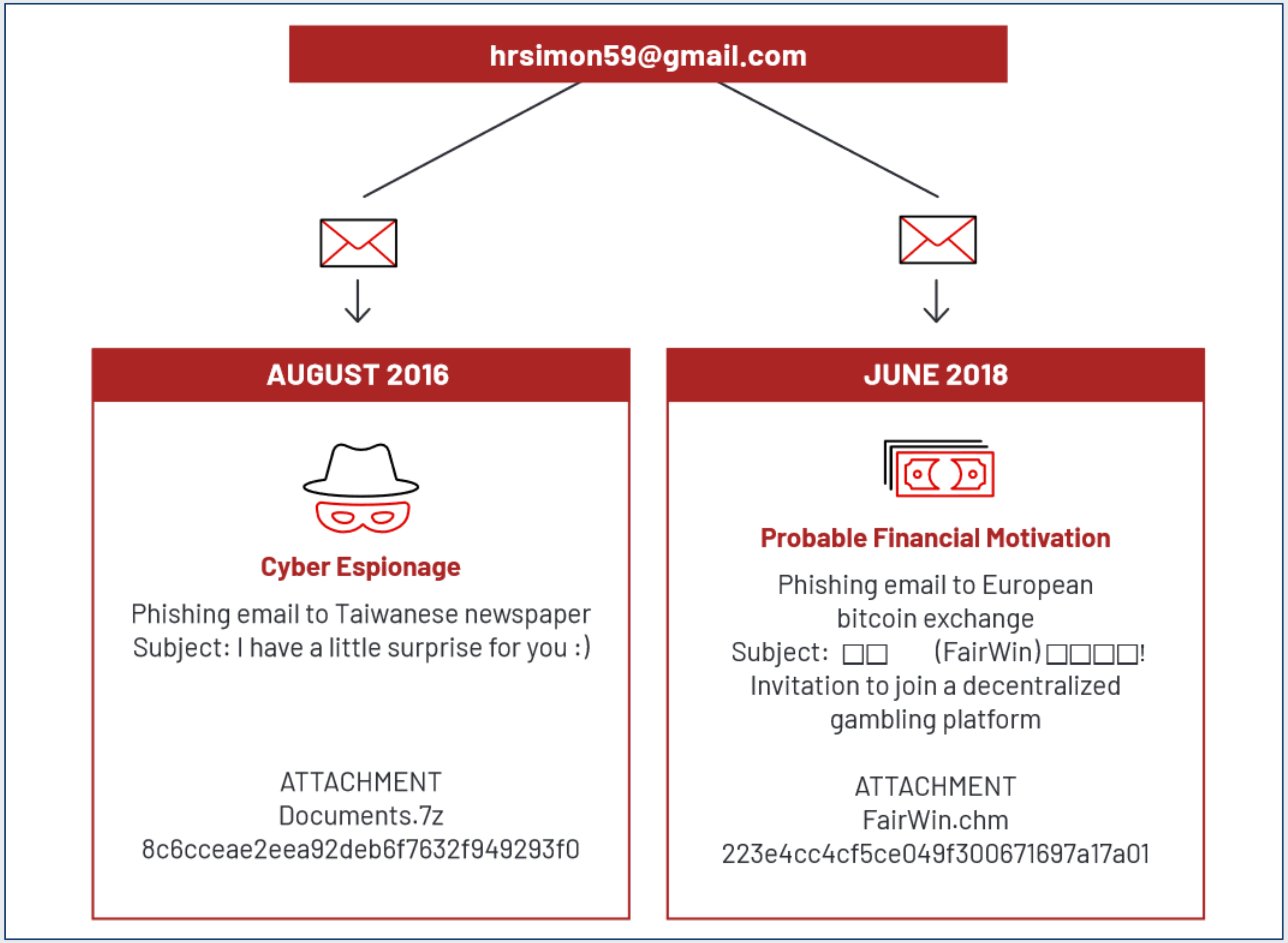
Image courtesy of Mandiant

APT41: Espionage and Financial Operations Overlap

One e-mail is all it takes…

This diagram depicts one of the links between APT41's activities on behalf of the Chinese government and their financially motivated activities.

Note: [hrsimon59 @ gmail.com] is used in both state-directed and criminal attacks.



hrsimon59@gmail.com

AUGUST 2016

Cyber Espionage

Phishing email to Taiwanese newspaper
Subject: I have a little surprise for you :)

ATTACHMENT
Documents.7z
8c6cceae2eea92deb6f7632f949293f0

JUNE 2018

Probable Financial Motivation

Phishing email to European bitcoin exchange
Subject: □□ (FairWin)□□□□!
Invitation to join a decentralized gambling platform

ATTACHMENT
FairWin.chm
223e4cc4cf5ce049f300671697a17a01

Image courtesy of Mandiant

APT41: Espionage and Financial Operations Overlap (Part 2)

[hrsimon59 @ gmail.com] was used to create a Google document that was then used as a command-and-control server for POISONPLUG.

An in-depth technical report on POISONPLUG.SHADOW, also known as SHADOWPAD by the company Sentinel Labs, can be found here: https://assets.sentinelone.com/c/Shadowpad?x=P42eqA

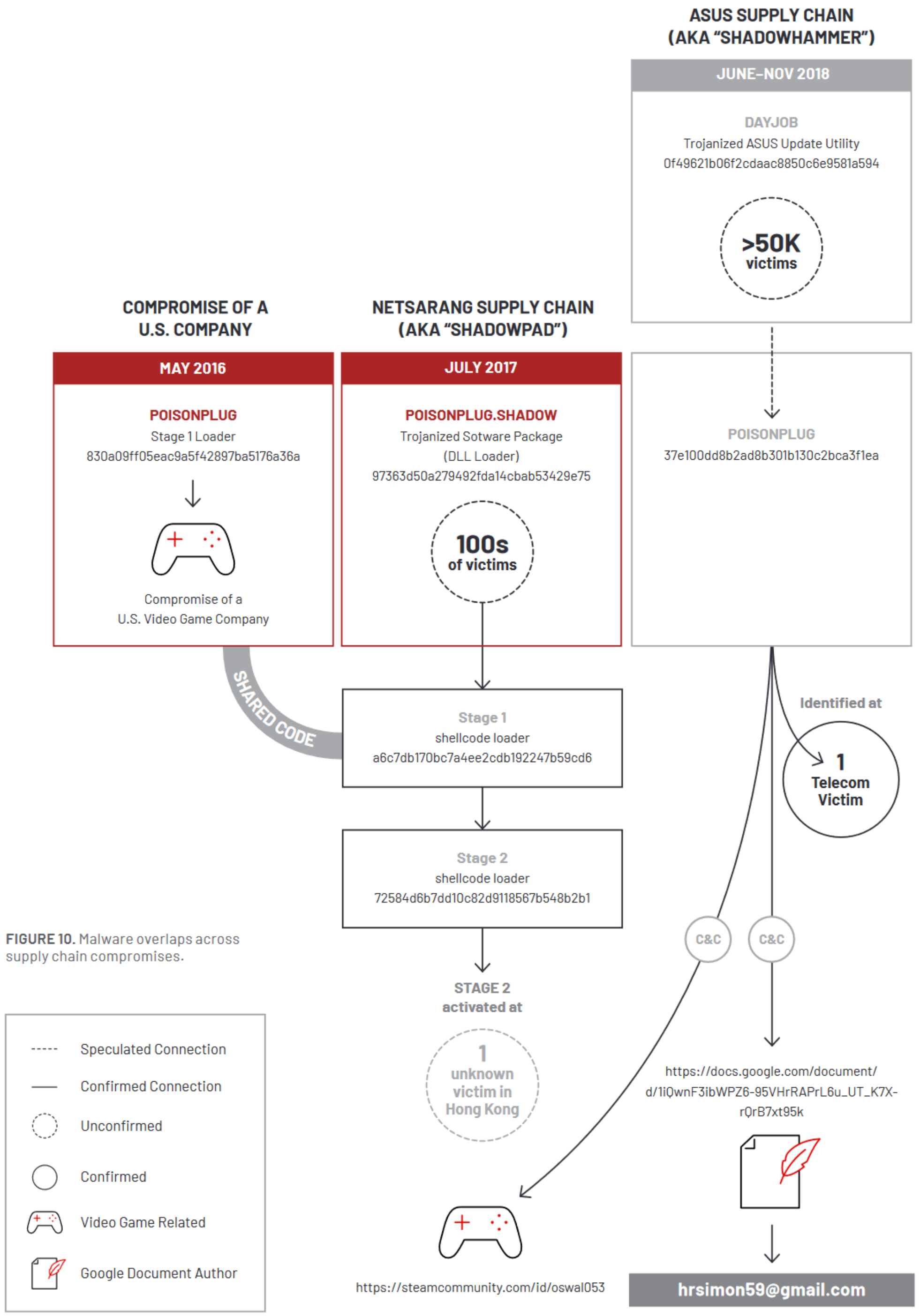
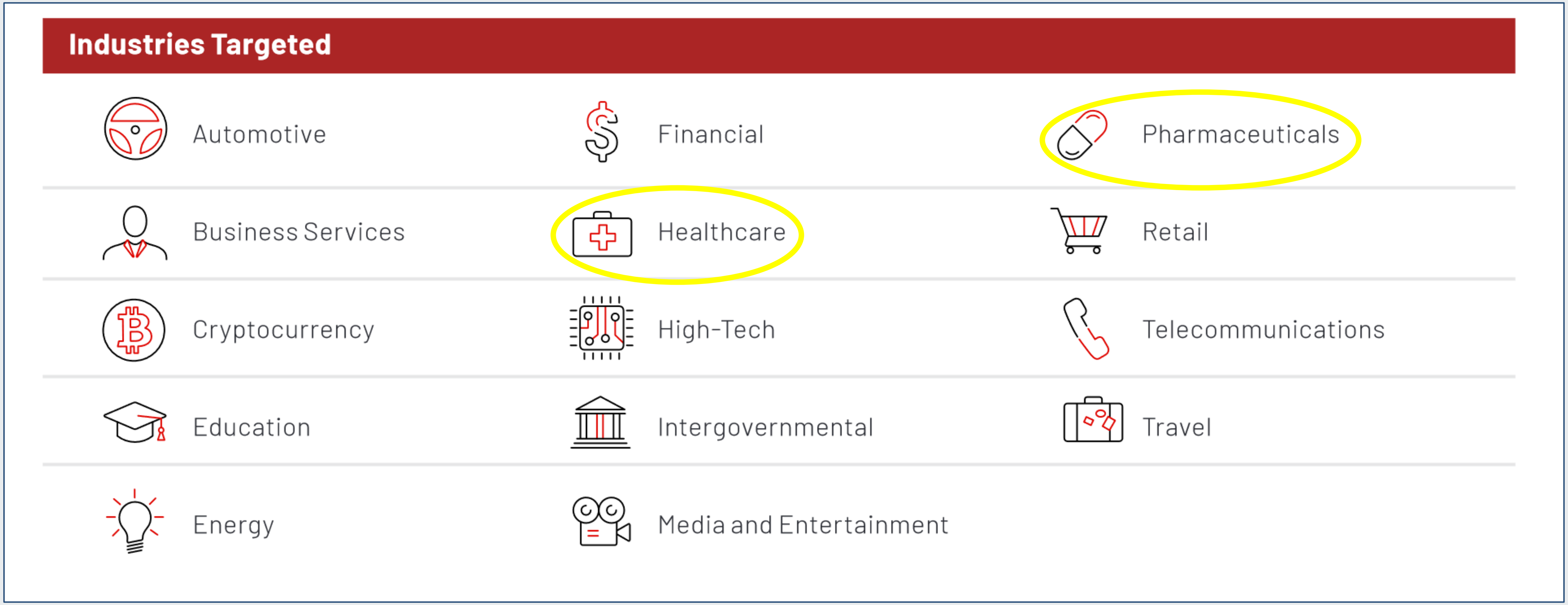

ASUS SUPPLY CHAIN (AKA "SHADOWHAMMER")
JUNE–NOV 2018
DAYJOB
Trojanized ASUS Update Utility
0f49621b06f2cdaac8850c6e9581a594
>50K victims
COMPROMISE OF A U.S. COMPANY
MAY 2016
POISONPLUG
Stage 1 Loader
830a09ff05eac9a5f42897ba5176a36a
Compromise of a U.S. Video Game Company
NETSARANG SUPPLY CHAIN (AKA "SHADOWPAD")
JULY 2017
POISONPLUG.SHADOW
Trojanized Sotware Package
(DLL Loader)
97363d50a279492fda14cbab53429e75
100s of victims
POISONPLUG
37e100dd8b2ad8b301b130c2bca3f1ea
SHARED CODE
Stage 1
shellcode loader
a6c7db170bc7a4ee2cdb192247b59cd6
Stage 2
shellcode loader
72584d6b7dd10c82d9118567b548b2b1
STAGE 2
activated at
1 unknown victim in Hong Kong
Identified at
1 Telecom Victim
C&C
C&C
https://docs.google.com/document/d/1iQwnF3ibWPZ6-95VHrRAPrL6u_UT_K7X-rQrB7xt95k
https://steamcommunity.com/id/oswal053
hrsimon59@gmail.com
----- Speculated Connection
— Confirmed Connection
Unconfirmed
Confirmed
Video Game Related
Google Document Author

FIGURE 10. Malware overlaps across supply chain compromises.

Image courtesy of Mandiant

APT41 Targeting by Industry



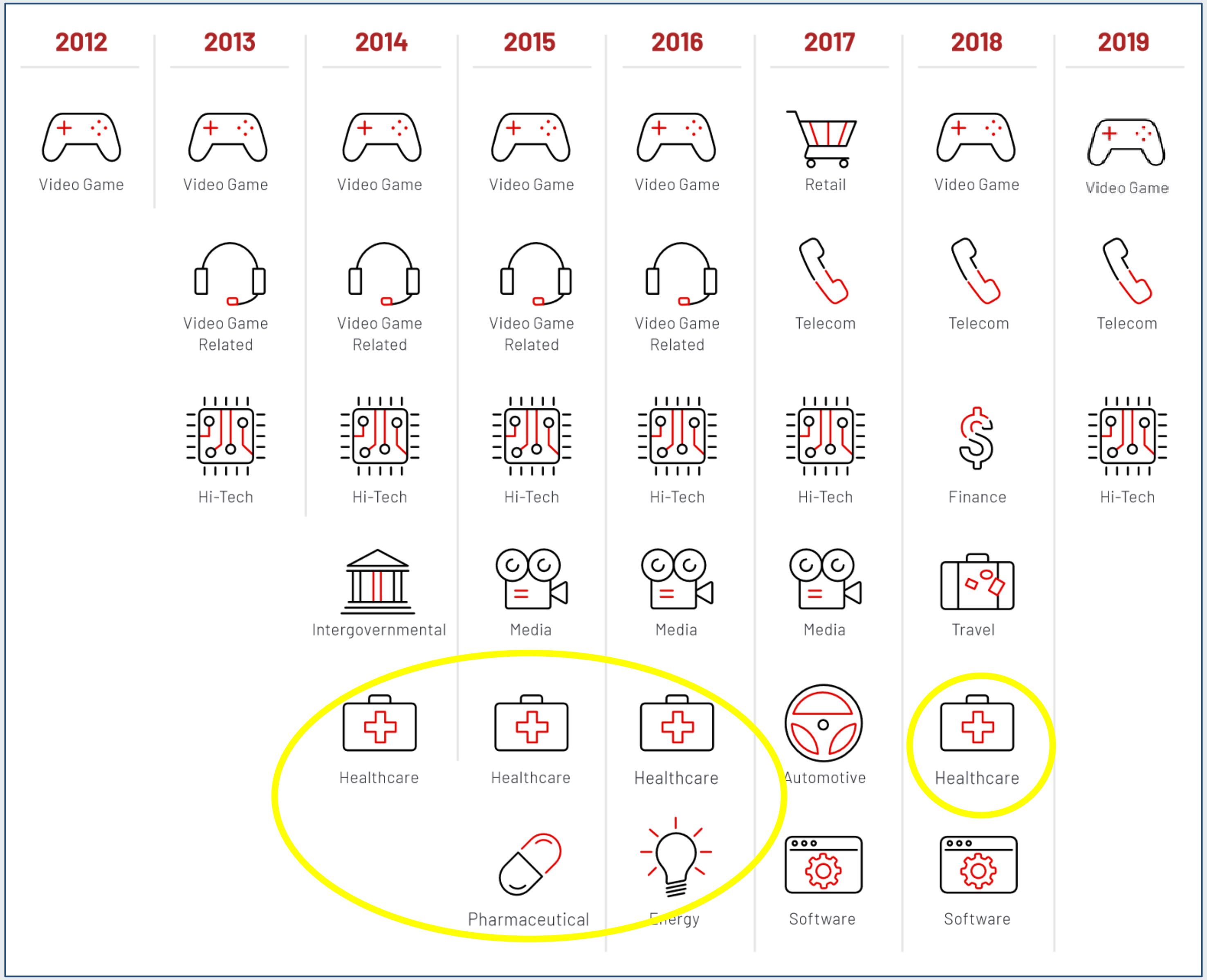
Industries Targeted

- Automotive
- Business Services
- Cryptocurrency
- Education
- Energy
- Financial
- Healthcare
- High-Tech
- Intergovernmental
- Media and Entertainment
- Pharmaceuticals
- Retail
- Telecommunications
- Travel

Image courtesy of Mandiant

APT41 Historic Targeting by Industry

Healthcare targeting by APT41 began in 2014 and continues to the present day. It is expected to continue for the foreseeable future, and this includes the potential for both state-ordered attacks for political purposes, as well as those for financial gain.



2012	2013	2014	2015	2016	2017	2018	2019
Video Game	Video Game	Video Game	Video Game	Video Game	Retail	Video Game	Video Game
	Video Game Related	Video Game Related	Video Game Related	Video Game Related	Telecom	Telecom	Telecom
	Hi-Tech	Hi-Tech	Hi-Tech	Hi-Tech	Hi-Tech	Finance	Hi-Tech
		Intergovernmental	Media	Media	Media	Travel	
		Healthcare	Healthcare	Healthcare	Automotive	Healthcare	
			Pharmaceutical	Energy	Software	Software	

Image courtesy of Mandiant

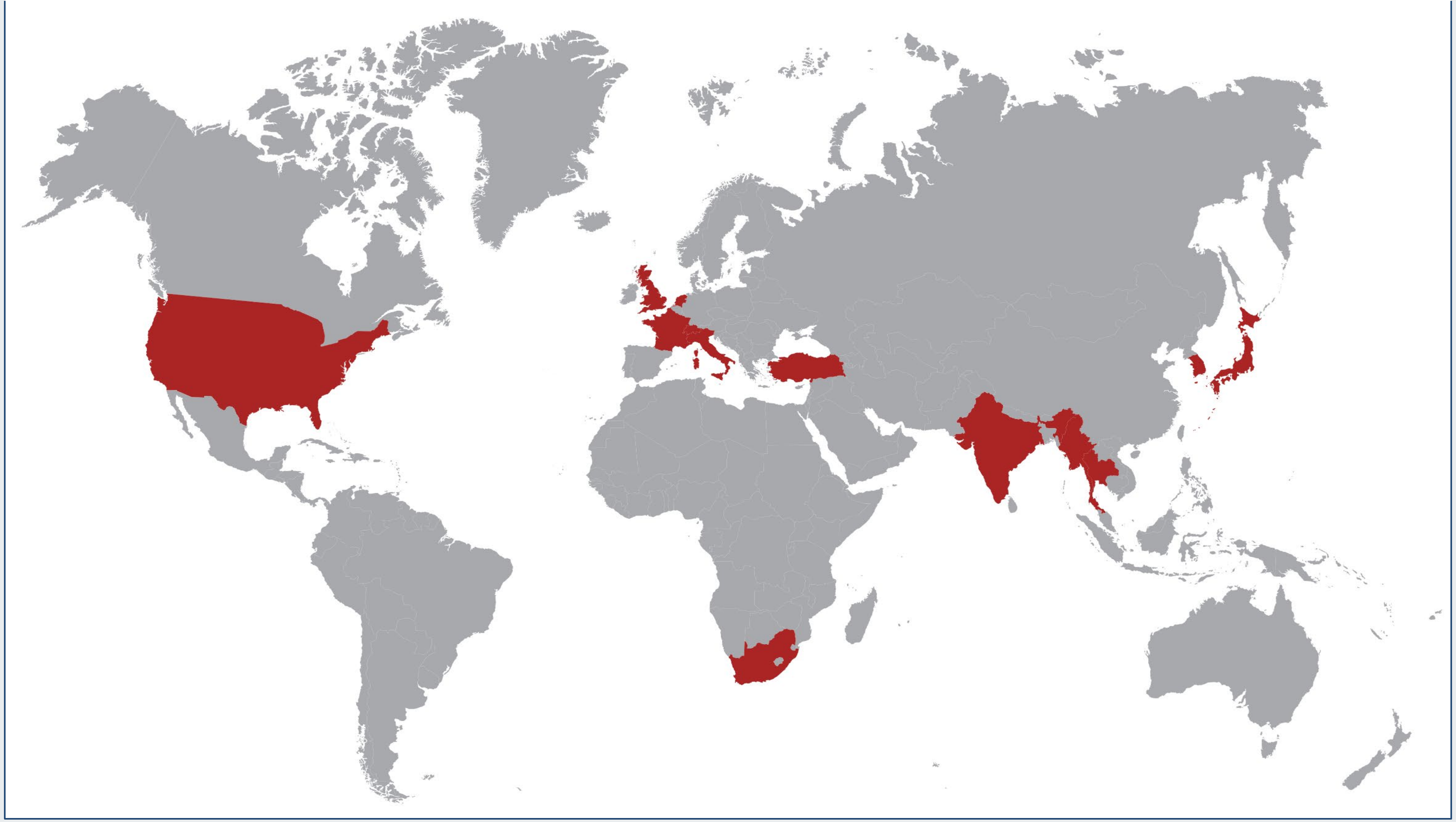


Image courtesy of Mandiant

APT41 geographic targeting

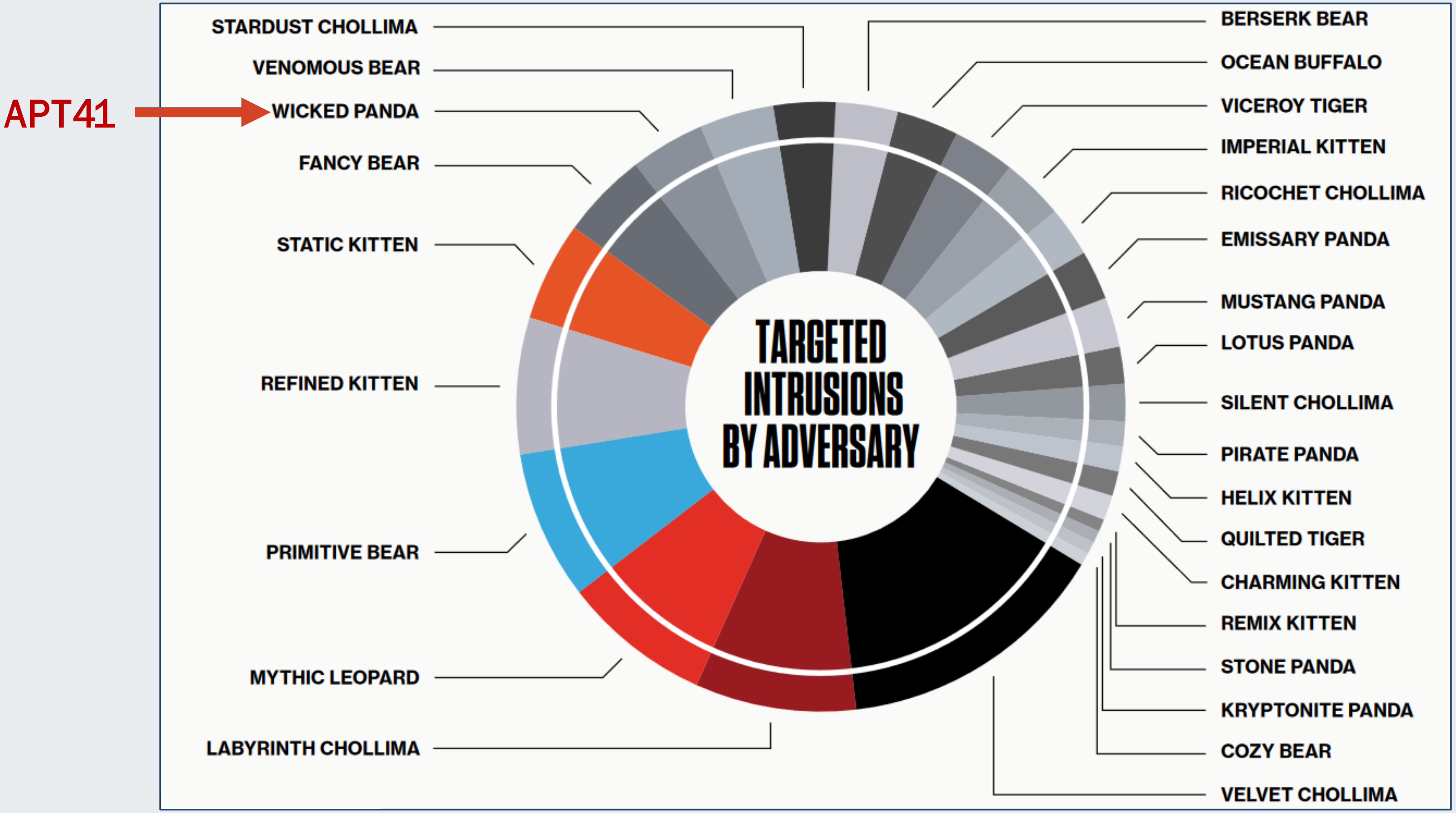


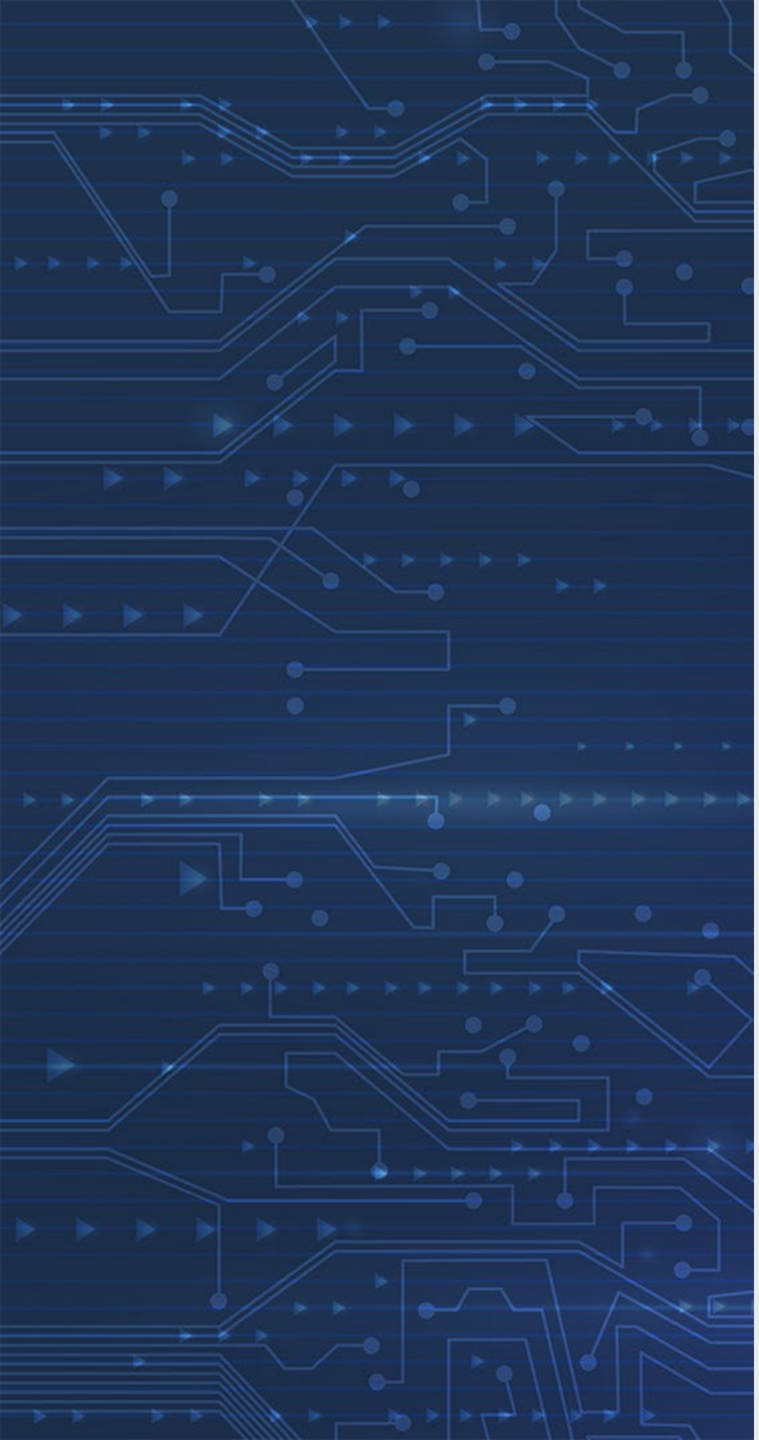
Image courtesy of Crowdstrike

APT41 targeting in 2019

APT41 Healthcare Targeting

APT41 is believed to directly support China's Five Year Plan and specifically augment China's own R&D efforts with targeted attacks on the health sector. An example:

- APT41 conducted sustained and targeted cyberattacks from July 2014 and May 2016 on a medical devices subsidiary of a large corporation.
- Their target was the parent company, however many of the compromised systems were associated with the medical device subsidiary.
- It is believed that APT41 was interested in information technology and software used by the medical device subsidiary.
- A keylogger called GEARSHIFT was deployed to the medical device company; certificates were stolen and later used to target a biotech company.
- Sensitive information about the biotech company's operations was targeted. This included human resources information, tax data, data related to developed drugs clinical trials, academic research, and R&D funding-related information.



North Korea

Punching above their digital weight

North Korea as a Cyber Power

- Communist government since its founding in 1948 has prompted isolation and sanctions from much of the rest of the world.
  - Cyberattacks are used to self-fund cyberwarfare capabilities and provide funding to other aspects of the national government:
    - SWIFT banking network
    - Cryptocurrency exchanges
    - Ransomware attacks
  - Cyberattacks have also been used to retaliate against insults against and regime and the Supreme Leader:
    - Sony pictures cyberattack of 2014 in retaliation for unflattering portrayal of Kim Jong-un in the movie *The Interview*.

North Korean Sanctions

US Sanctions on North Korea (summary)

- Prohibits certain types of U.S. assistance to foreign governments that aid North Korea
- Treasury Department has blocked foreign business or individuals that facilitate trade with North Korea
- Penalizes banks, companies, and individuals (especially in China and Russia) for supporting North Korean weapons programs
- Fines companies for violating U.S. export controls

Australia, Japan, South Korea, and the European Union have also sanctioned North Korea

UN Sanctions on North Korea (summary)

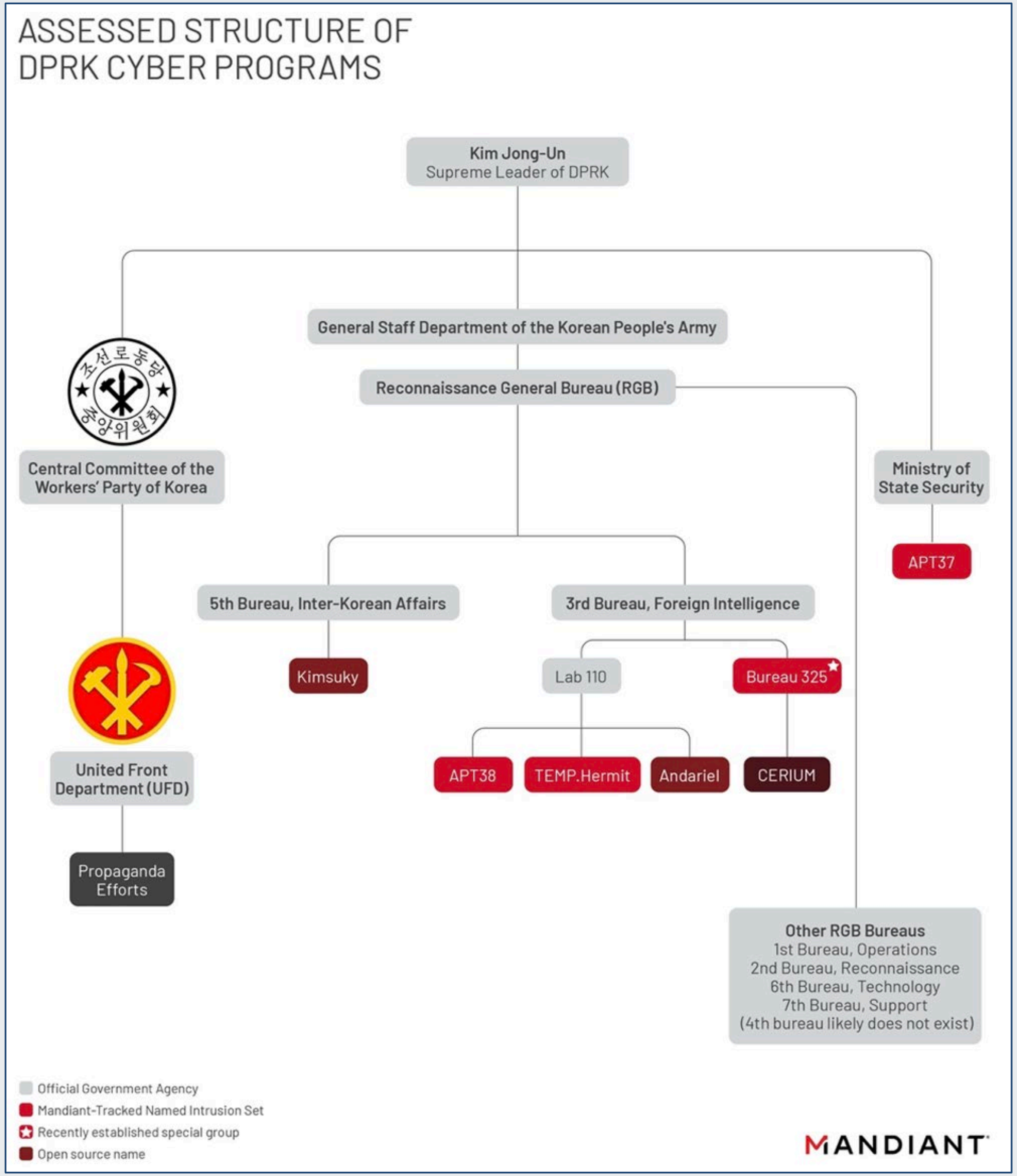
- Bans trade of arms and military equipment, dual-use technologies, vehicles, industrial machinery, and metals
- Freezes assets of individuals involved in the country's nuclear program
- Bans the export of electrical equipment, coal, minerals, seafood, other foods and agricultural products, wood, textiles, and stones
- Caps labor exports, and imports of oil and refined petroleum products
- Bans natural gas imports
- Restricts scientific and technical cooperation

Leadership Structure of North Korea

The Reconnaissance General Bureau is a higher-level organization within the North Korean government that likely includes many of the country's major cyber capabilities.

It is worth noting for this presentation that APT43 aligns with the mission of the Reconnaissance General Bureau. Also, the Lazarus Group likely falls under Lab 110, formerly known as Bureau 121 prior to reorganization.

The People's Liberation Army (not included on this diagram) also includes cyberwarfare capabilities.



ASSESSED STRUCTURE OF DPRK CYBER PROGRAMS

Kim Jong-Un
Supreme Leader of DPRK

General Staff Department of the Korean People's Army

Reconnaissance General Bureau (RGB)

Central Committee of the Workers' Party of Korea

Ministry of State Security

APT37

5th Bureau, Inter-Korean Affairs

3rd Bureau, Foreign Intelligence

Kimsuky

Lab 110

Bureau 325

APT38

TEMP.Hermit

Andariel

CERIUM

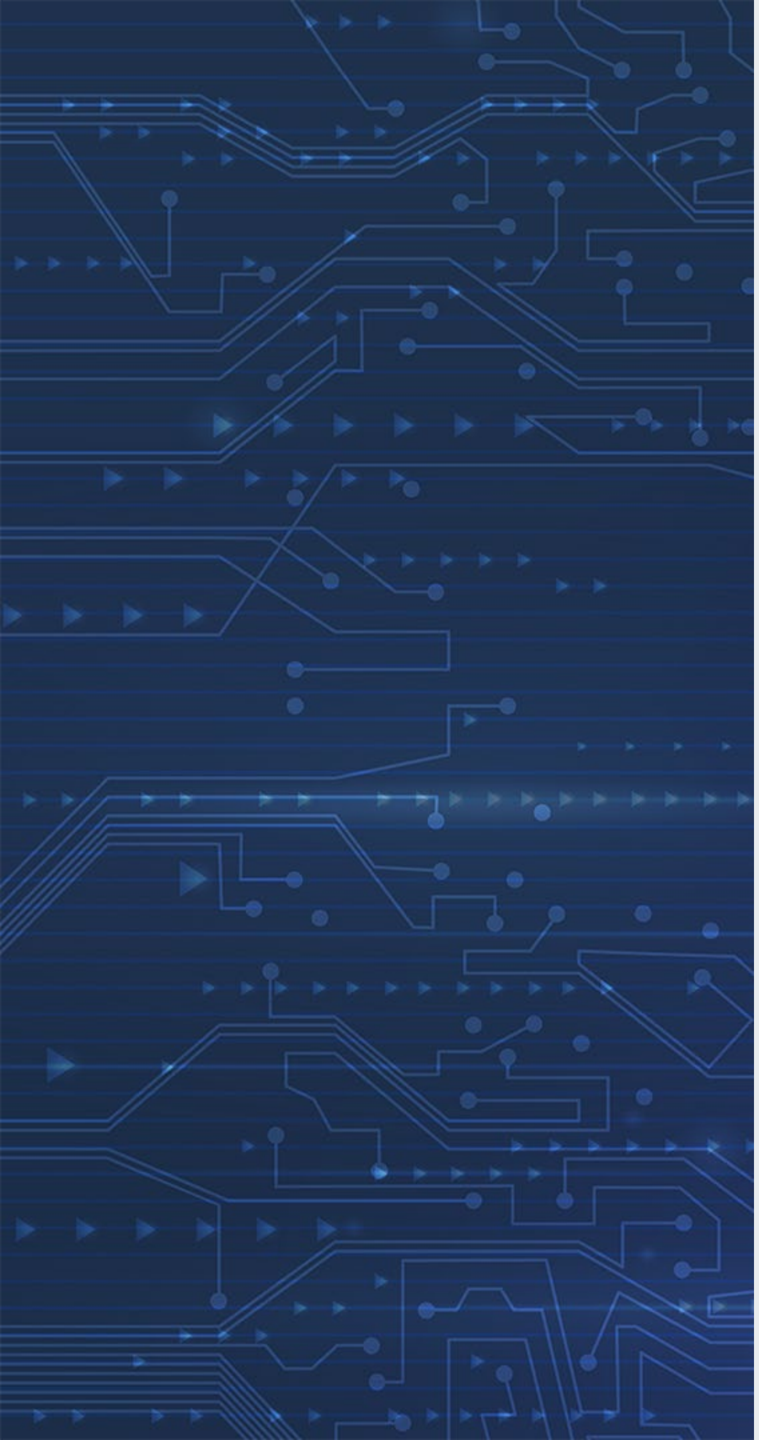
United Front Department (UFD)

Propaganda Efforts

Other RGB Bureaus
1st Bureau, Operations
2nd Bureau, Reconnaissance
6th Bureau, Technology
7th Bureau, Support
(4th bureau likely does not exist)

▨ Official Government Agency
🟥 Mandiant-Tracked Named Intrusion Set
★ Recently established special group
■ Open source name

MANDIANT



APT43

Using cybercrime to fund espionage

Overview of APT43

- Also known as Kimsuky, Velvet Chollima, and Emerald Sleet (THALLIUM)
- Considered moderately sophisticated in its capabilities:
  - Social engineering
    - Spoofed personas
    - Spoofed domains (spear phishing)
  - Credential harvesting
  - Cover identities for purchasing tools and infrastructure
- Not observed using zero days (as of the date of this presentation)
- Highly collaborative with other North Korean state actors; maintain high-tempo operations
- Cybercrime to fund strategic intelligence

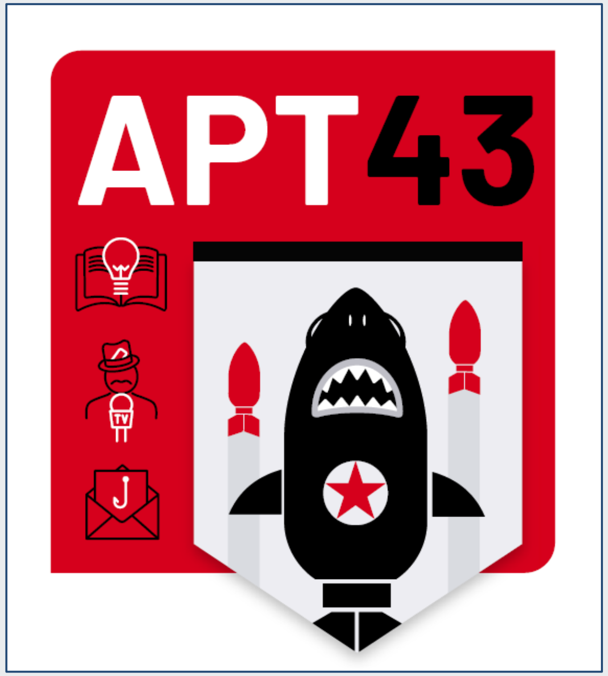


Image courtesy of Mandiant

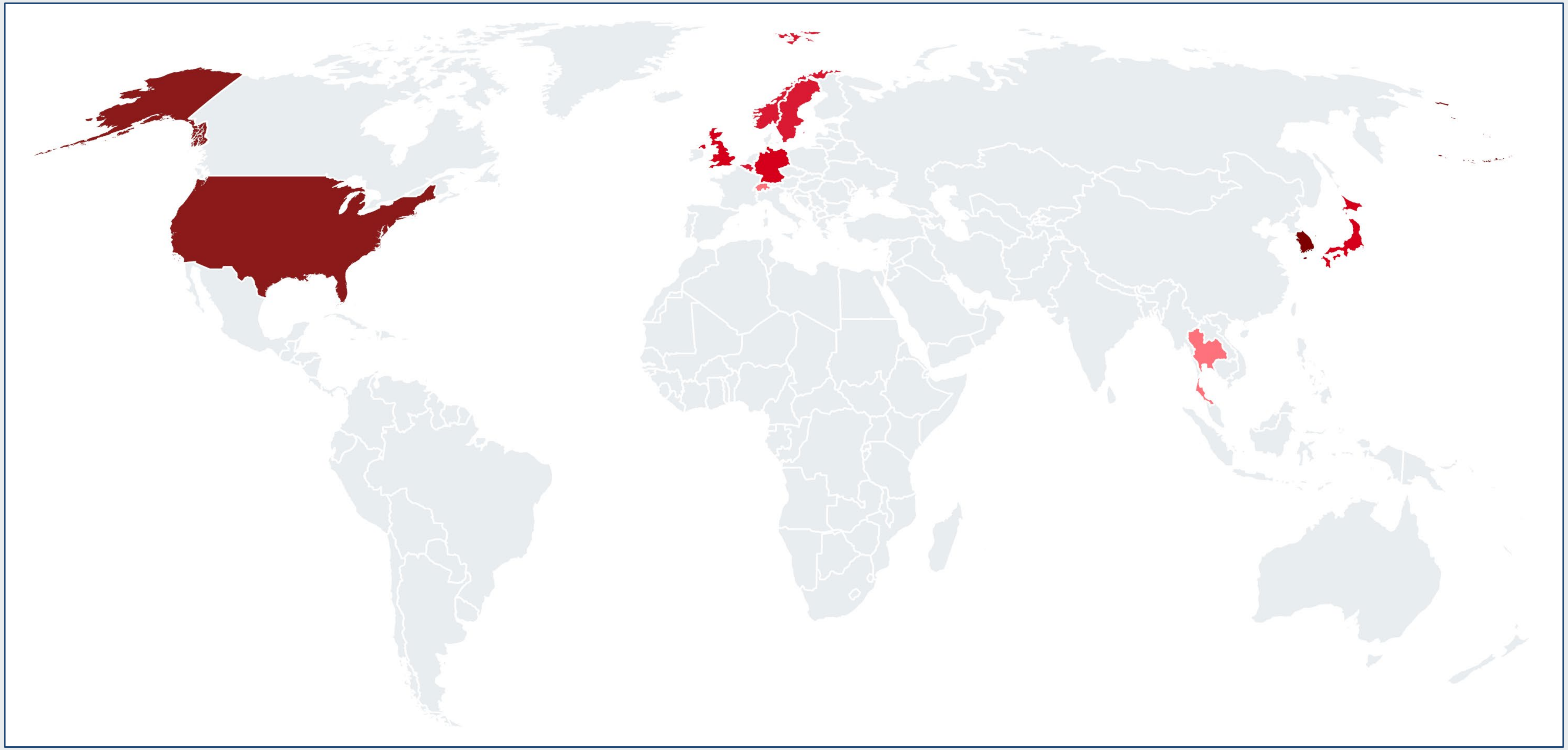
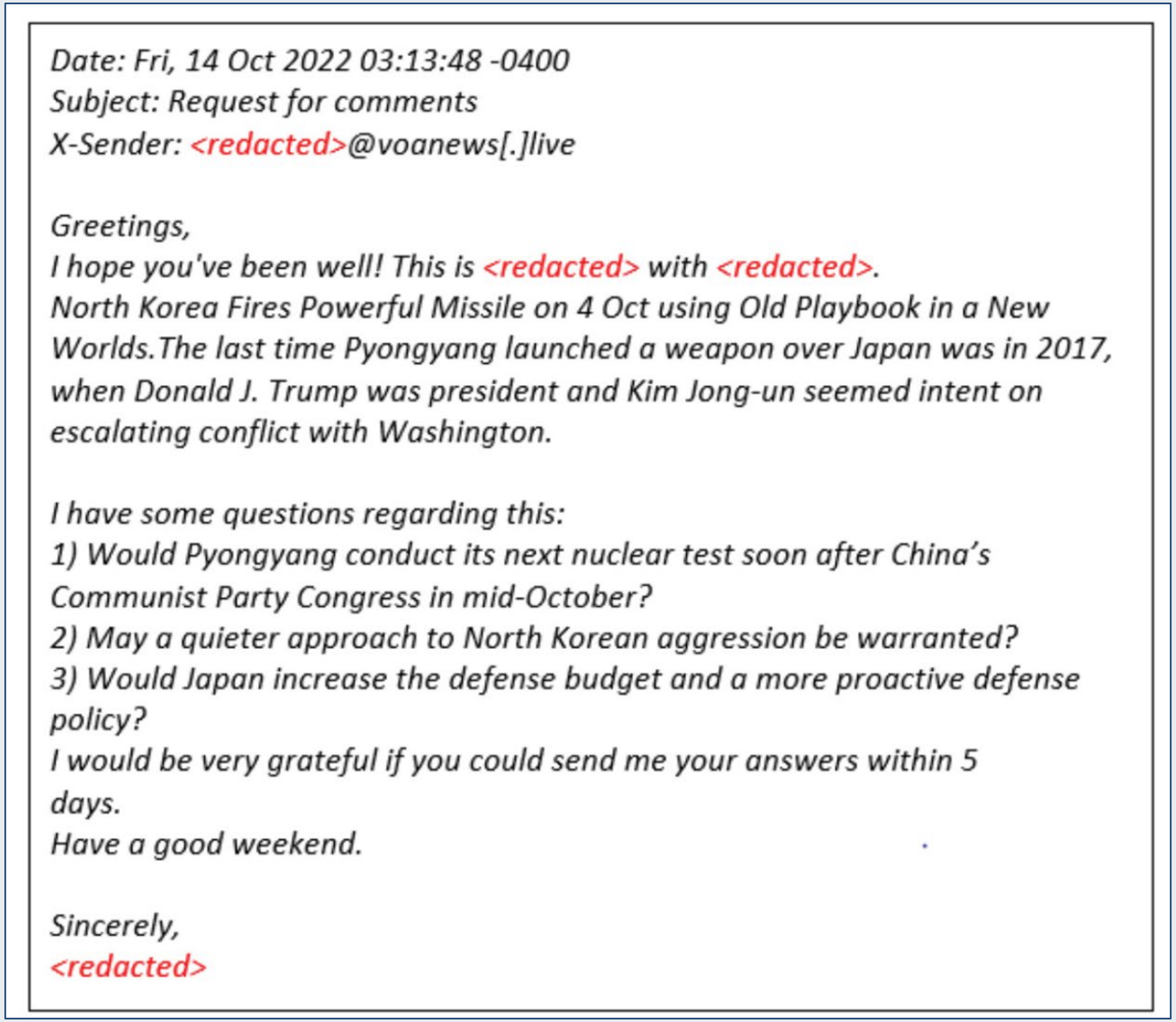


Image courtesy of Mandiant

APT43 targeting

APT43 and Social Engineering

APT43 develops and releases highly customized spear phishing e-mails as an infection vector.



Date: Fri, 14 Oct 2022 03:13:48 -0400
Subject: Request for comments
X-Sender: <redacted>@voanews[.]live

Greetings,
I hope you've been well! This is <redacted> with <redacted>.
North Korea Fires Powerful Missile on 4 Oct using Old Playbook in a New Worlds.The last time Pyongyang launched a weapon over Japan was in 2017, when Donald J. Trump was president and Kim Jong-un seemed intent on escalating conflict with Washington.

I have some questions regarding this:
1) Would Pyongyang conduct its next nuclear test soon after China's Communist Party Congress in mid-October?
2) May a quieter approach to North Korean aggression be warranted?
3) Would Japan increase the defense budget and a more proactive defense policy?
I would be very grateful if you could send me your answers within 5 days.
Have a good weekend.

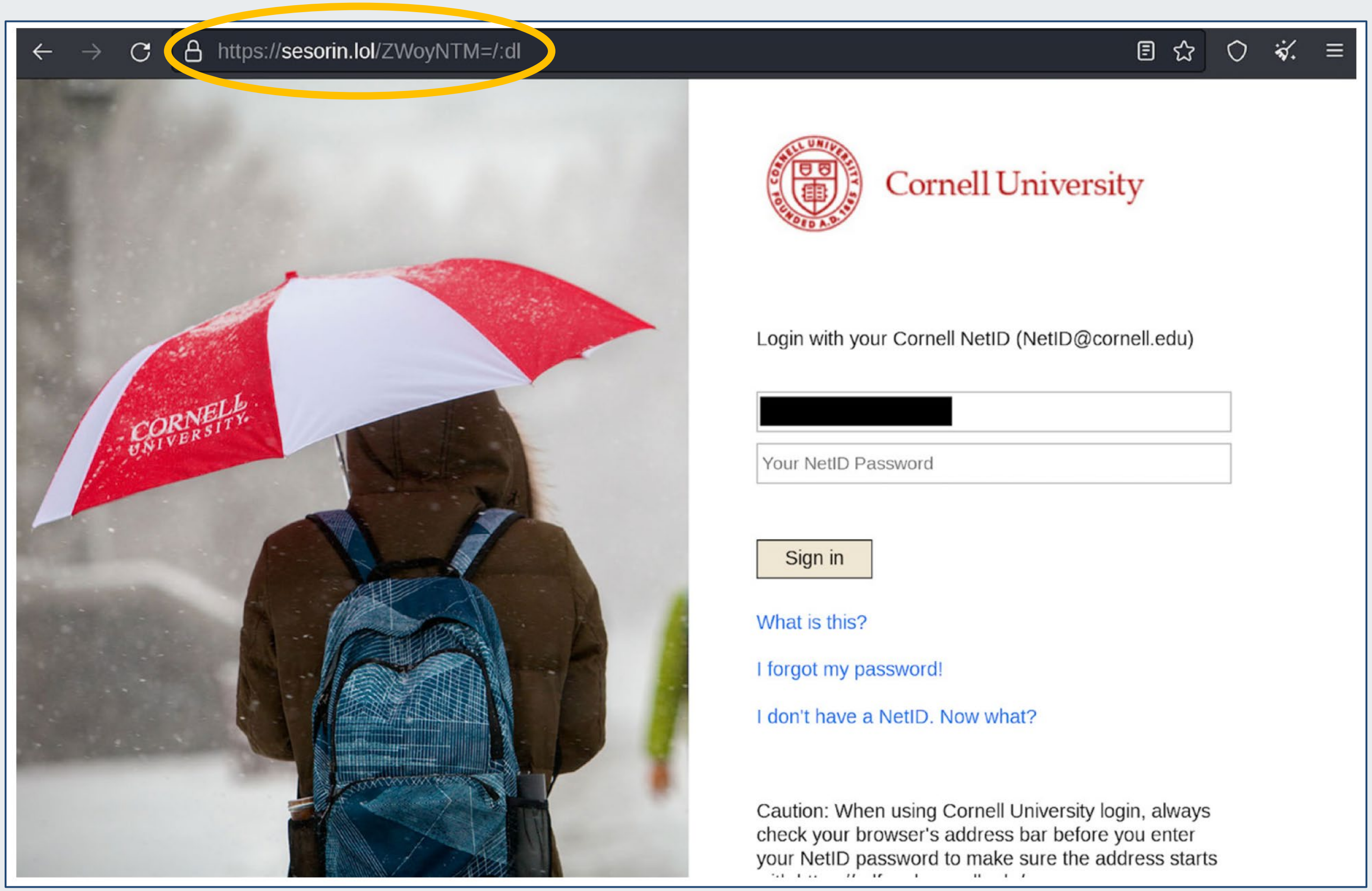
Sincerely,
<redacted>

Image courtesy of Mandiant

APT43 and Social Engineering (Part 2)

APT43 develops highly detailed and realistic spoofed webpages.

Notice the obviously inaccurate web address in the browser.



https://sesorin.lol/ZWoyNTM=/:dl

Cornell University

Login with your Cornell NetID (NetID@cornell.edu)

[redacted]

Your NetID Password

Sign in

What is this?

I forgot my password!

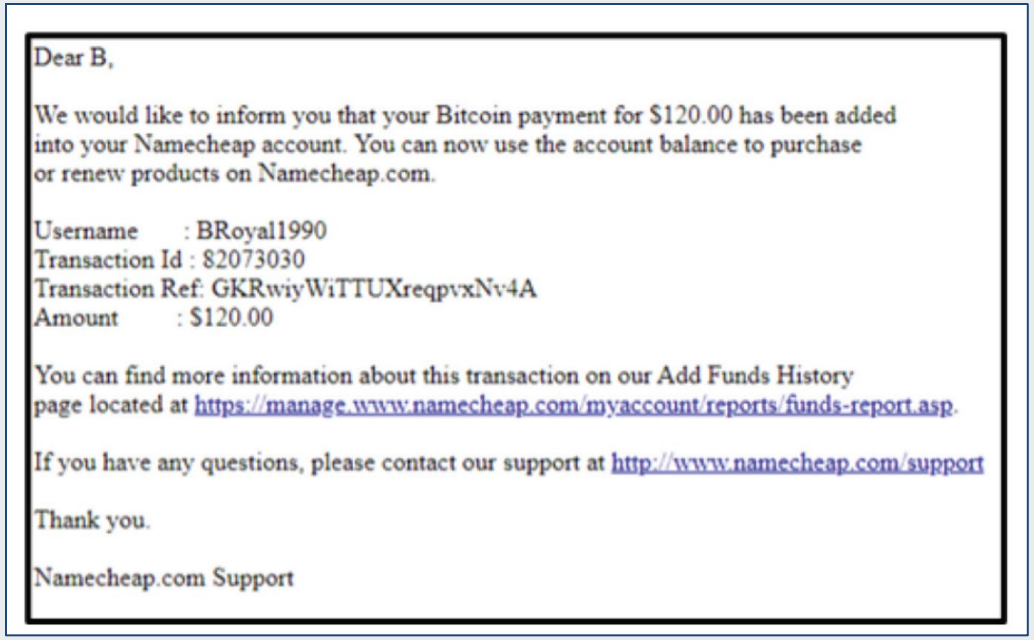
I don't have a NetID. Now what?

Caution: When using Cornell University login, always check your browser's address bar before you enter your NetID password to make sure the address starts

Image courtesy of Mandiant

Cryptocurrency Laundering

APT43's cryptocurrency laundering techniques – purchasing mining power – makes on-chain transaction tracing impossible.



Dear B,

We would like to inform you that your Bitcoin payment for $120.00 has been added into your Namecheap account. You can now use the account balance to purchase or renew products on Namecheap.com.

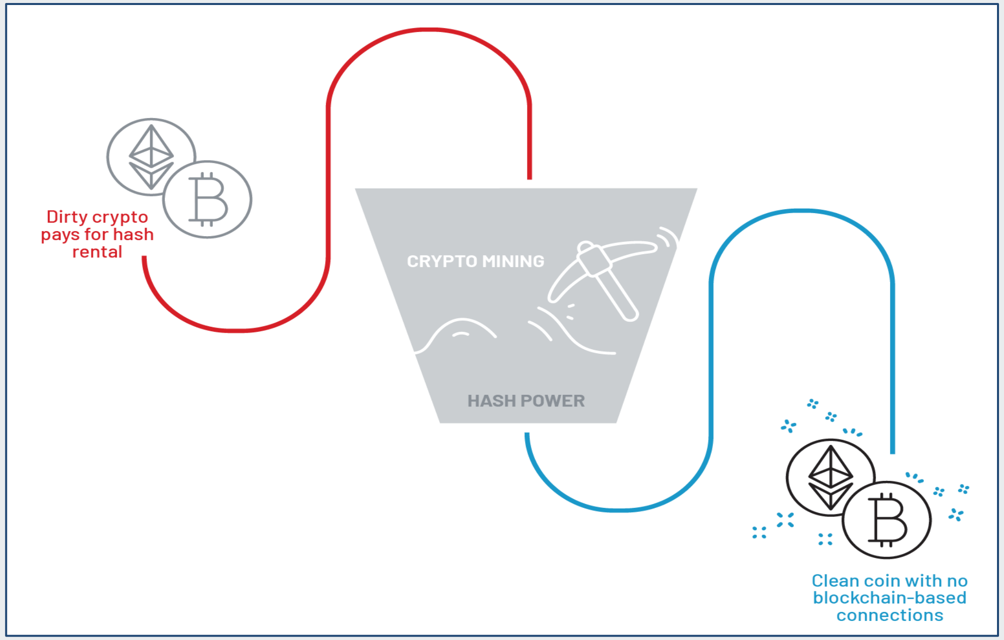
Username : BRoyal1990
Transaction Id : 82073030
Transaction Ref: GKRwiyWiTTUXreqpvxNv4A
Amount : $120.00

You can find more information about this transaction on our Add Funds History page located at https://manage.www.namecheap.com/myaccount/reports/funds-report.asp.

If you have any questions, please contact our support at http://www.namecheap.com/support

Thank you.

Namecheap.com Support


Dirty crypto pays for hash rental
CRYPTO MINING
HASH POWER
Clean coin with no blockchain-based connections

Images courtesy of Mandiant

APT43 and Malware Deployment as Compared to Other North Korean Groups

There is not significant code sharing between APT43 and other North Korean groups.

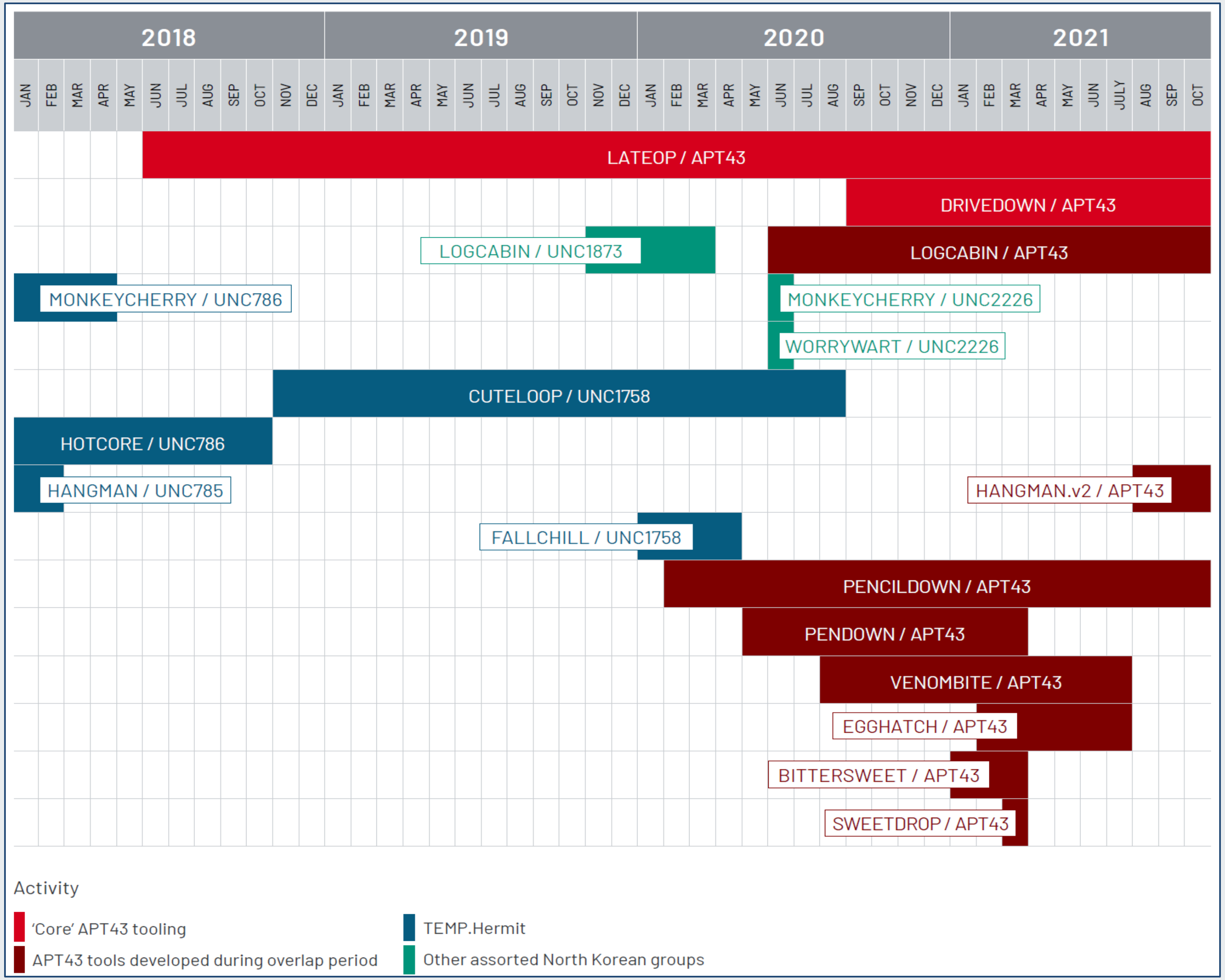
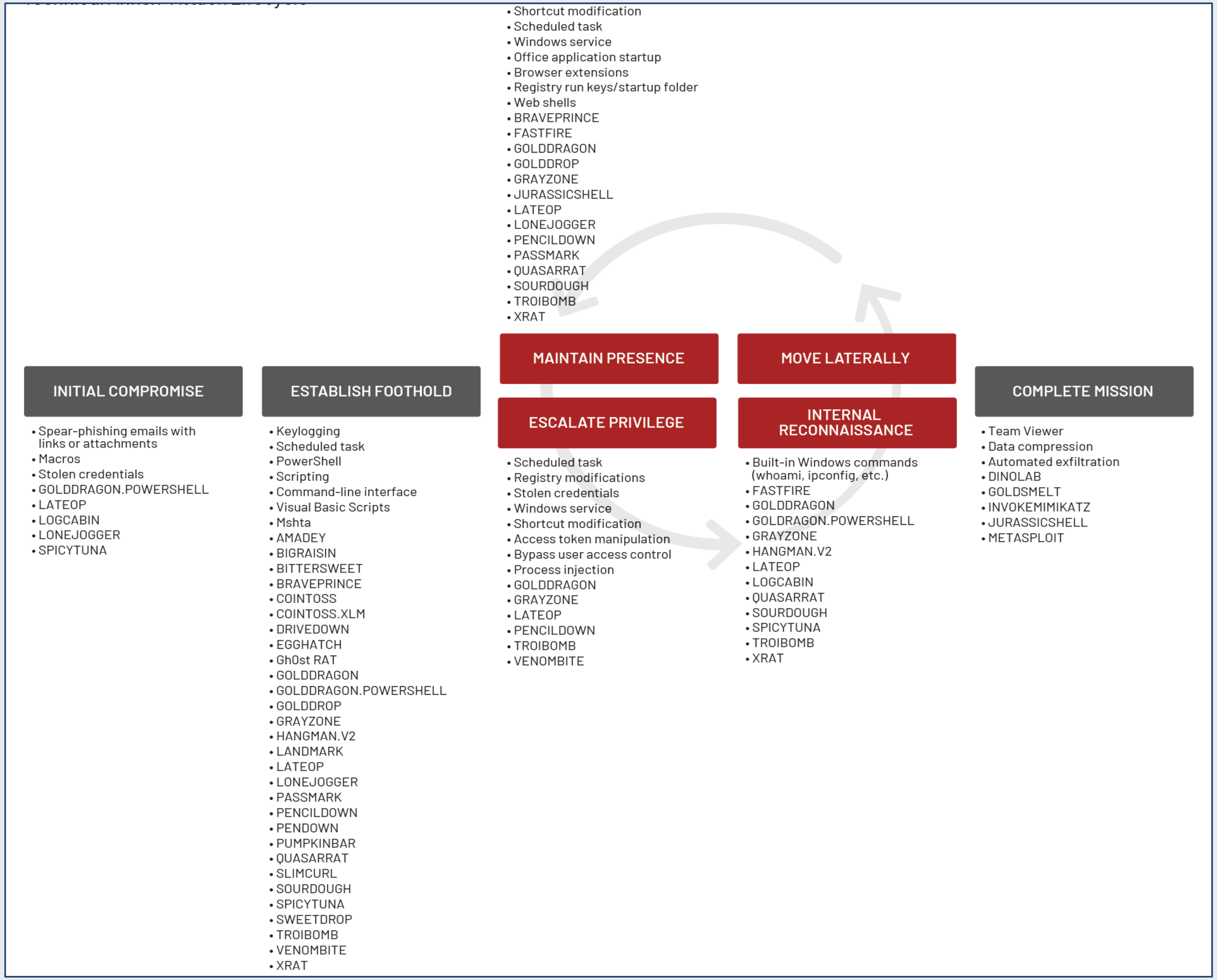


Image courtesy of Mandiant

APT43: Mapping of Malware and TTPs to Attack Lifecycle

These are the malware variants and TTPs available to APT43 for each step of the attack lifecycle.



INITIAL COMPROMISE

- Spear-phishing emails with links or attachments
- Macros
- Stolen credentials
- GOLDDRAGON.POWERSHELL
- LATEOP
- LOGCABIN
- LONEJOGGER
- SPICYTUNA

ESTABLISH FOOTHOLD

- Keylogging
- Scheduled task
- PowerShell
- Scripting
- Command-line interface
- Visual Basic Scripts
- Mshta
- AMADEY
- BIGRAISIN
- BITTERSWEET
- BRAVEPRINCE
- COINTOSS
- COINTOSS.XLM
- DRIVEDOWN
- EGGHATCH
- Gh0st RAT
- GOLDDRAGON
- GOLDDRAGON.POWERSHELL
- GOLDDROP
- GRAYZONE
- HANGMAN.V2
- LANDMARK
- LATEOP
- LONEJOGGER
- PASSMARK
- PENCILDOWN
- PENDOWN
- PUMPKINBAR
- QUASARRAT
- SLIMCURL
- SOURDOUGH
- SPICYTUNA
- SWEETDROP
- TROIBOMB
- VENOMBITE
- XRAT

MAINTAIN PRESENCE

- Shortcut modification
- Scheduled task
- Windows service
- Office application startup
- Browser extensions
- Registry run keys/startup folder
- Web shells
- BRAVEPRINCE
- FASTFIRE
- GOLDDRAGON
- GOLDDROP
- GRAYZONE
- JURASSICSHELL
- LATEOP
- LONEJOGGER
- PENCILDOWN
- PASSMARK
- QUASARRAT
- SOURDOUGH
- TROIBOMB
- XRAT

ESCALATE PRIVILEGE

- Scheduled task
- Registry modifications
- Stolen credentials
- Windows service
- Shortcut modification
- Access token manipulation
- Bypass user access control
- Process injection
- GOLDDRAGON
- GRAYZONE
- LATEOP
- PENCILDOWN
- TROIBOMB
- VENOMBITE

MOVE LATERALLY

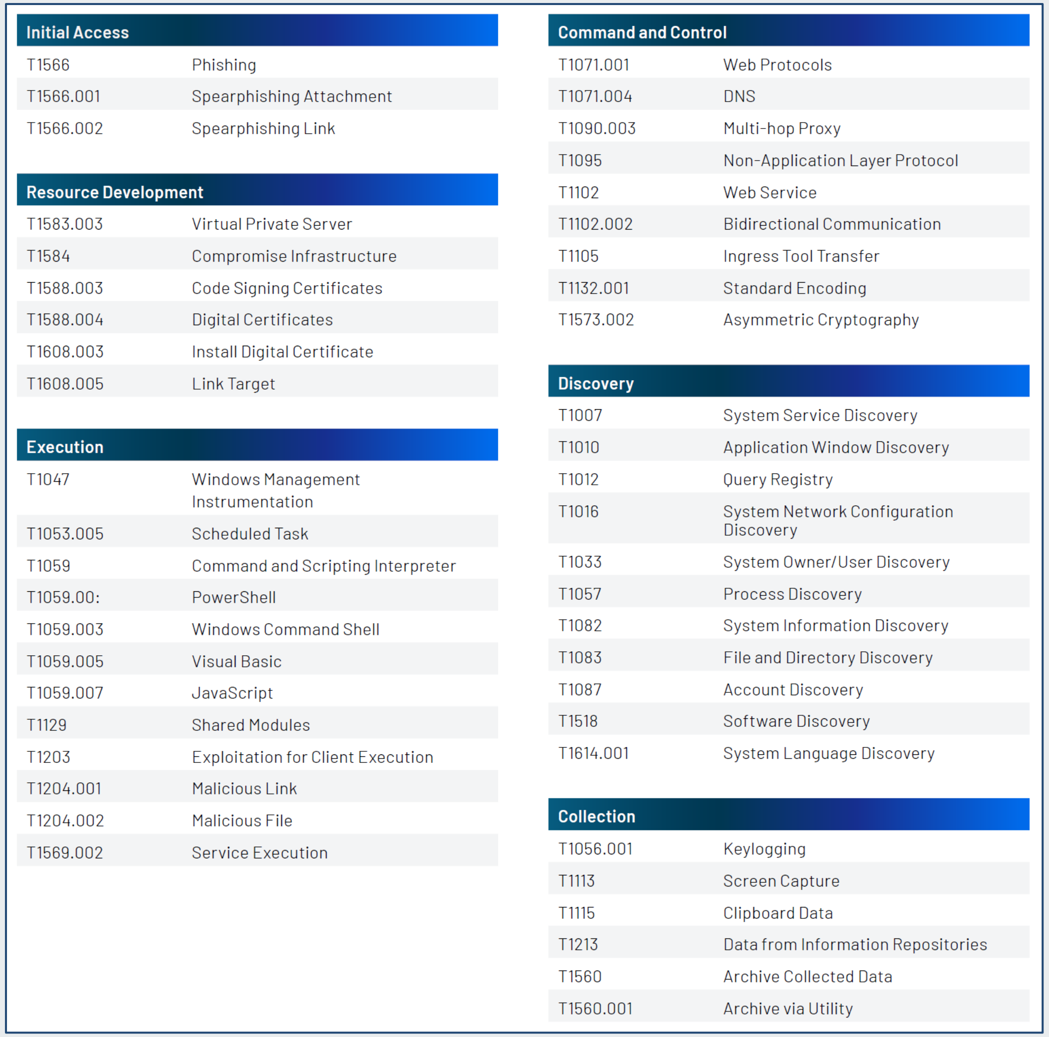
INTERNAL RECONNAISSANCE

- Built-in Windows commands (whoami, ipconfig, etc.)
- FASTFIRE
- GOLDDRAGON
- GOLDRAGON.POWERSHELL
- GRAYZONE
- HANGMAN.V2
- LATEOP
- LOGCABIN
- QUASARRAT
- SOURDOUGH
- SPICYTUNA
- TROIBOMB
- XRAT

COMPLETE MISSION

- Team Viewer
- Data compression
- Automated exfiltration
- DINOLAB
- GOLDSMELT
- INVOKEMIMIKATZ
- JURASSICSHELL
- METASPLOIT

Image courtesy of Mandiant



Initial Access	
T1566	Phishing
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link

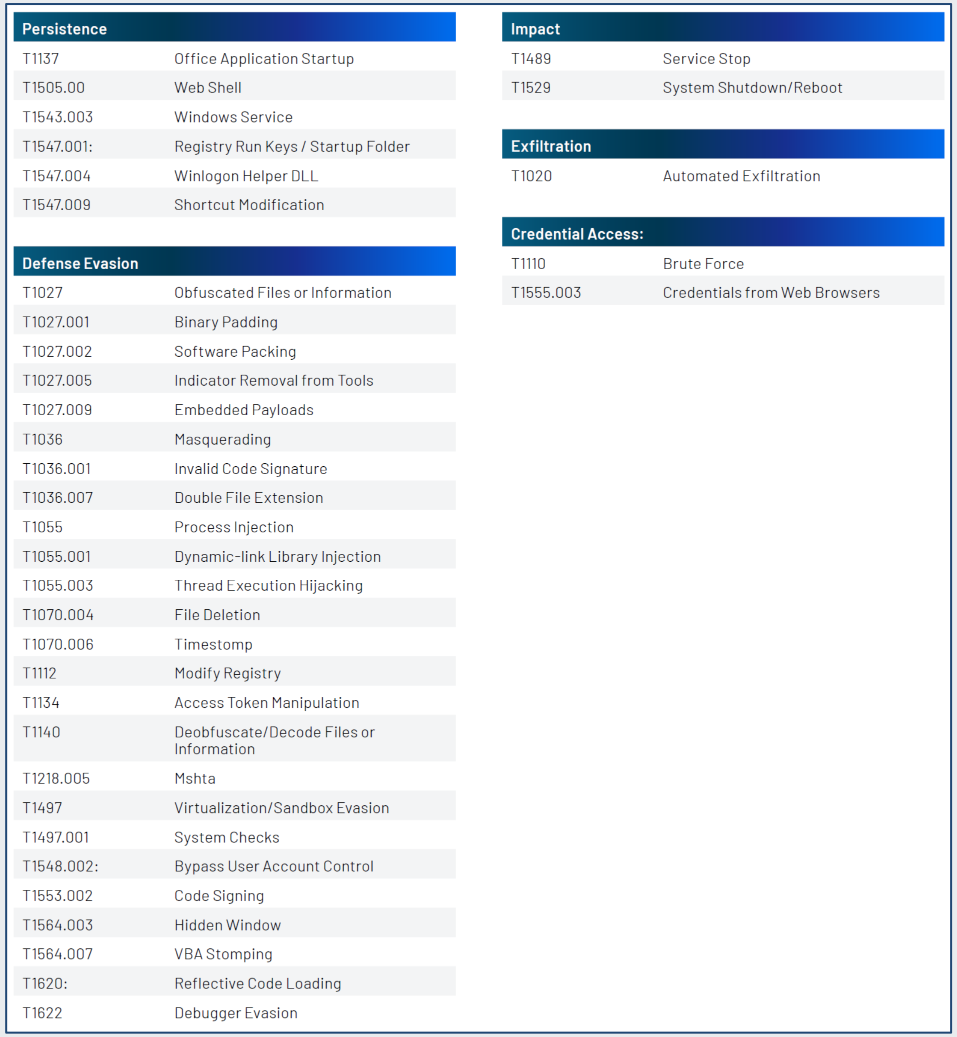
Resource Development	
T1583.003	Virtual Private Server
T1584	Compromise Infrastructure
T1588.003	Code Signing Certificates
T1588.004	Digital Certificates
T1608.003	Install Digital Certificate
T1608.005	Link Target

Execution	
T1047	Windows Management Instrumentation
T1053.005	Scheduled Task
T1059	Command and Scripting Interpreter
T1059.00:	PowerShell
T1059.003	Windows Command Shell
T1059.005	Visual Basic
T1059.007	JavaScript
T1129	Shared Modules
T1203	Exploitation for Client Execution
T1204.001	Malicious Link
T1204.002	Malicious File
T1569.002	Service Execution

Command and Control	
T1071.001	Web Protocols
T1071.004	DNS
T1090.003	Multi-hop Proxy
T1095	Non-Application Layer Protocol
T1102	Web Service
T1102.002	Bidirectional Communication
T1105	Ingress Tool Transfer
T1132.001	Standard Encoding
T1573.002	Asymmetric Cryptography

Discovery	
T1007	System Service Discovery
T1010	Application Window Discovery
T1012	Query Registry
T1016	System Network Configuration Discovery
T1033	System Owner/User Discovery
T1057	Process Discovery
T1082	System Information Discovery
T1083	File and Directory Discovery
T1087	Account Discovery
T1518	Software Discovery
T1614.001	System Language Discovery

Collection	
T1056.001	Keylogging
T1113	Screen Capture
T1115	Clipboard Data
T1213	Data from Information Repositories
T1560	Archive Collected Data
T1560.001	Archive via Utility



Persistence	
T1137	Office Application Startup
T1505.00	Web Shell
T1543.003	Windows Service
T1547.001:	Registry Run Keys / Startup Folder
T1547.004	Winlogon Helper DLL
T1547.009	Shortcut Modification

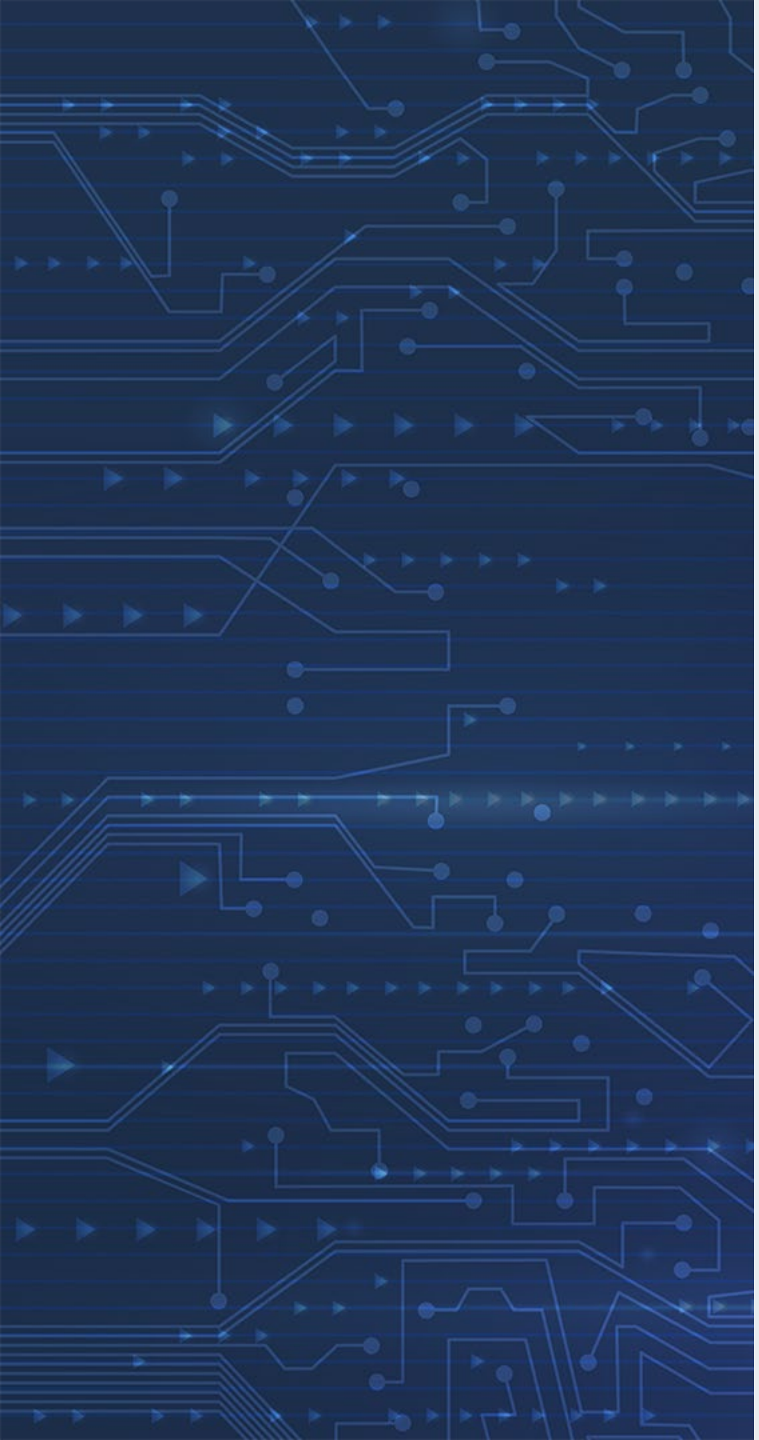
Defense Evasion	
T1027	Obfuscated Files or Information
T1027.001	Binary Padding
T1027.002	Software Packing
T1027.005	Indicator Removal from Tools
T1027.009	Embedded Payloads
T1036	Masquerading
T1036.001	Invalid Code Signature
T1036.007	Double File Extension
T1055	Process Injection
T1055.001	Dynamic-link Library Injection
T1055.003	Thread Execution Hijacking
T1070.004	File Deletion
T1070.006	Timestomp
T1112	Modify Registry
T1134	Access Token Manipulation
T1140	Deobfuscate/Decode Files or Information
T1218.005	Mshta
T1497	Virtualization/Sandbox Evasion
T1497.001	System Checks
T1548.002:	Bypass User Account Control
T1553.002	Code Signing
T1564.003	Hidden Window
T1564.007	VBA Stomping
T1620:	Reflective Code Loading
T1622	Debugger Evasion

Impact	
T1489	Service Stop
T1529	System Shutdown/Reboot

Exfiltration	
T1020	Automated Exfiltration

Credential Access:	
T1110	Brute Force
T1555.003	Credentials from Web Browsers

APT43 tradecraft mapped to MITRE ATT&CK framework



Lazarus Group

One of the most active North Korean cyber threat groups for over a decade

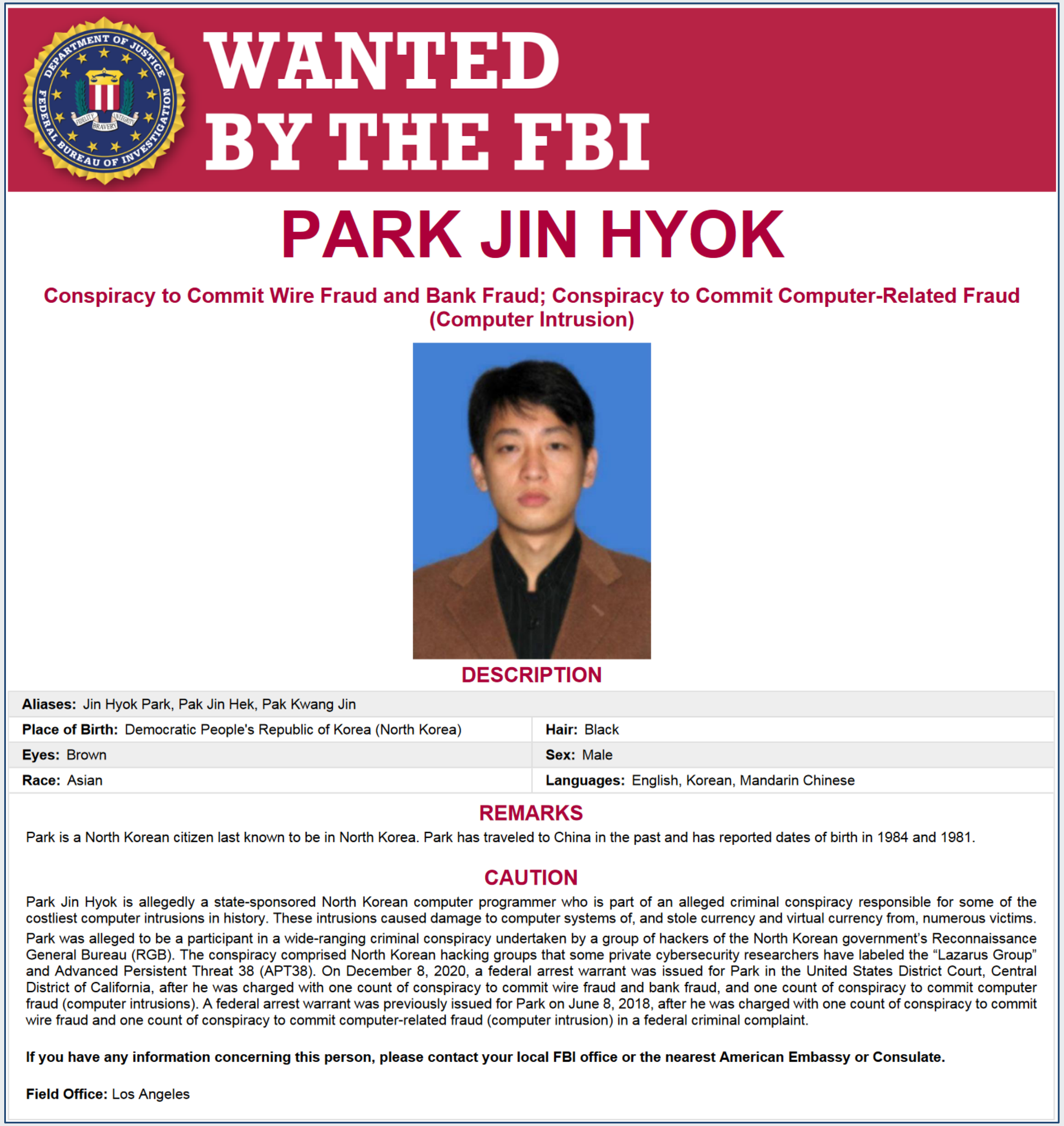
Lazarus Group Overview

- Attributed names/affiliated groups: APT38, Guardians of Peace, Whois Team, Labyrinth Chollima, Hidden Cobra, NICKEL ACADEMY, Diamond Sleet (ZINC)
- Active since at least 2009
- Purpose: Espionage, intellectual property theft, financial fraud, geopolitical goals; aligned under Lab 110 (formerly Bureau 121)
- Major cyber operations
  - Operation Troy
  - Sony Picture/Operation Blockbuster
  - GHOSTRAT
  - Bangladeshi Bank
  - Wannacry
  - Various cryptocurrency exchanges/companies
  - COVID-19 vaccine data

- Major tools and TTPs: VSingle, MagicRAT, WannaCry and other ransomware

Indictments

- Several members of Lazarus have been indicted by the U.S. government
- 2018 – Park Jin Hyok for Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)
- Added Jon Chang Hyok to indictment in 2021
- These groups have been described as:
  - “the world's leading bank robbers’
  - “a criminal syndicate with a flag”



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Jin Hyok Park, Pak Jin Hek, Pak Kwang Jin

Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean, Mandarin Chinese

REMARKS

Park is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and has reported dates of birth in 1984 and 1981.

CAUTION

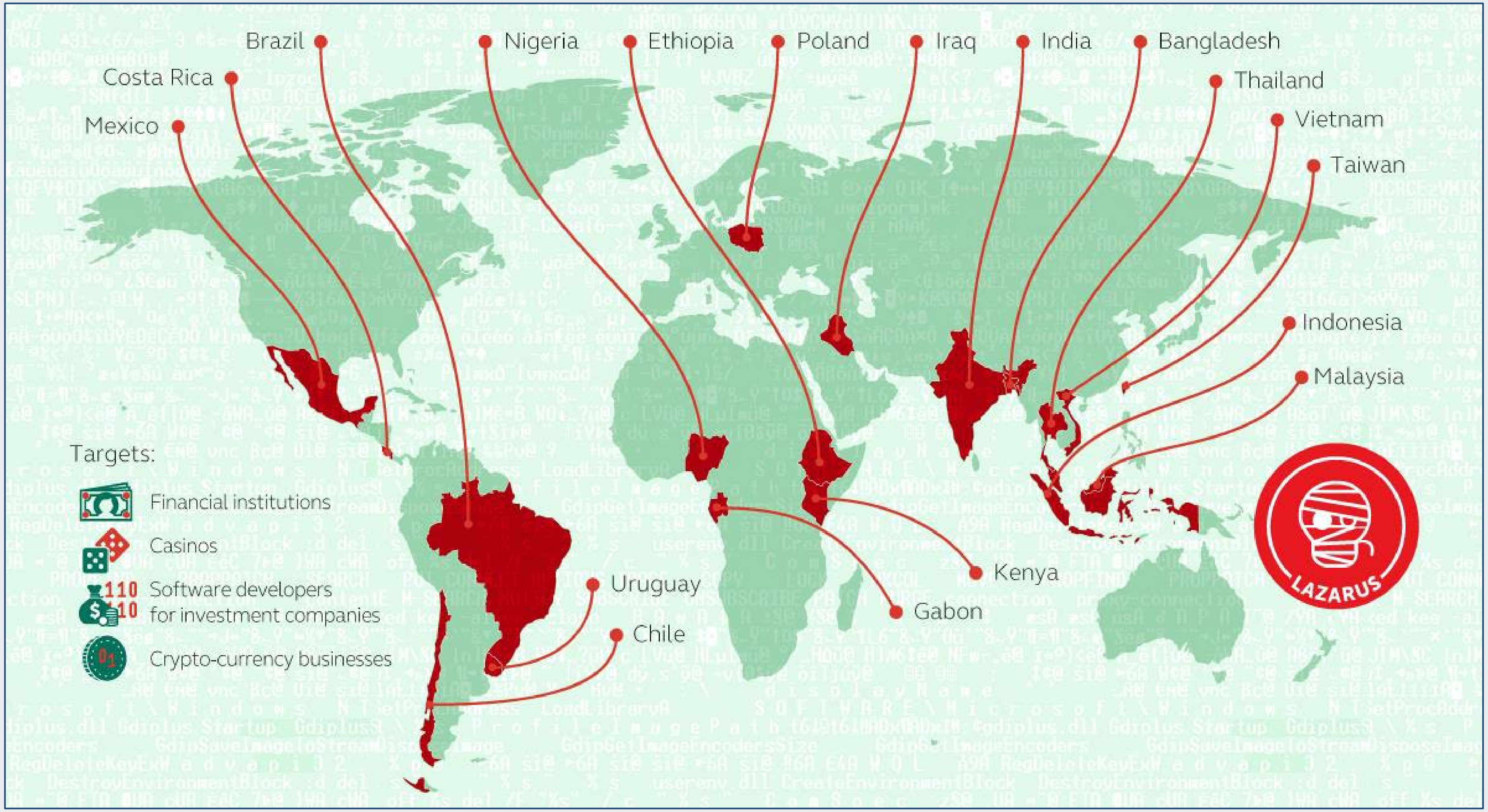
Park Jin Hyok is allegedly a state-sponsored North Korean computer programmer who is part of an alleged criminal conspiracy responsible for some of the costliest computer intrusions in history. These intrusions caused damage to computer systems of, and stole currency and virtual currency from, numerous victims.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers of the North Korean government’s Reconnaissance General Bureau (RGB). The conspiracy comprised North Korean hacking groups that some private cybersecurity researchers have labeled the “Lazarus Group” and Advanced Persistent Threat 38 (APT38). On December 8, 2020, a federal arrest warrant was issued for Park in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and bank fraud, and one count of conspiracy to commit computer fraud (computer intrusions). A federal arrest warrant was previously issued for Park on June 8, 2018, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion) in a federal criminal complaint.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

Screenshot courtesy of the FBI

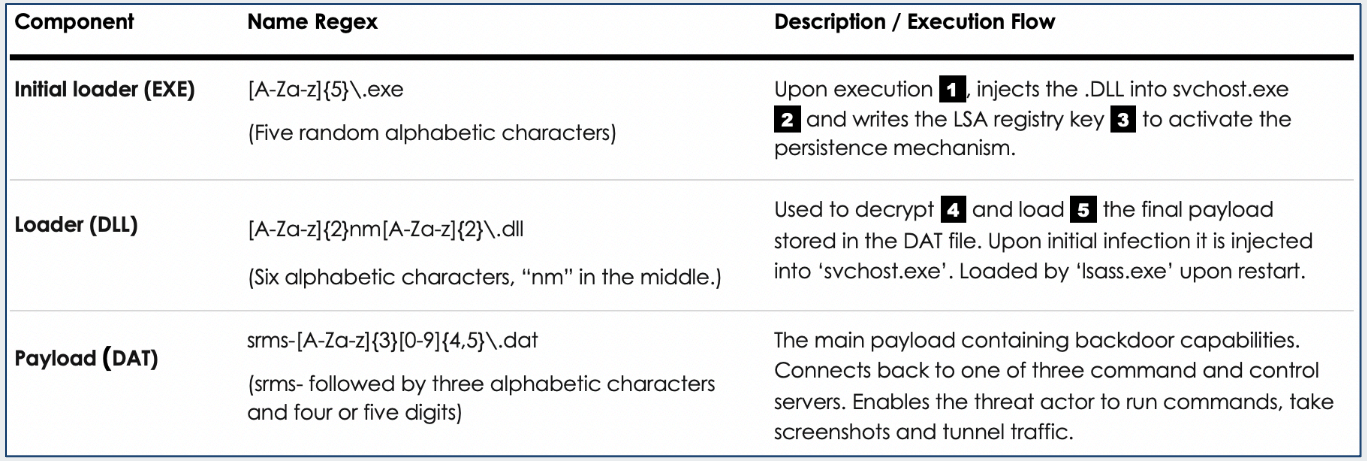


The geographic distribution of Lazarus' financial attacks (map from 2017)

MATA Framework

The MATA framework:

- A cross-platform malware framework often used to deploy ransomware
- Consists of three components:
  - Initial Loader (.exe file which injects .DLL into svchost.exe)
  - Loader (executes payload in .DAT file, loaded by lsass.exe upon reboot)
  - Payload implements full backdoor capability



Component	Name Regex	Description / Execution Flow
Initial loader (EXE)	[A-Za-z]{5}\.exe (Five random alphabetic characters)	Upon execution 1, injects the .DLL into svchost.exe 2 and writes the LSA registry key 3 to activate the persistence mechanism.
Loader (DLL)	[A-Za-z]{2}nm[A-Za-z]{2}\.dll (Six alphabetic characters, "nm" in the middle.)	Used to decrypt 4 and load 5 the final payload stored in the DAT file. Upon initial infection it is injected into 'svchost.exe'. Loaded by 'lsass.exe' upon restart.
Payload (DAT)	srms-[A-Za-z]{3}[0-9]{4,5}\.dat (srms- followed by three alphabetic characters and four or five digits)	The main payload containing backdoor capabilities. Connects back to one of three command and control servers. Enables the threat actor to run commands, take screenshots and tunnel traffic.

Image courtesy of Sygna

MATA Framework (Part 2)

Windows version of MATA:

- Loader
- Orchestrator
- Command and Control (C2)

Plugin functionality

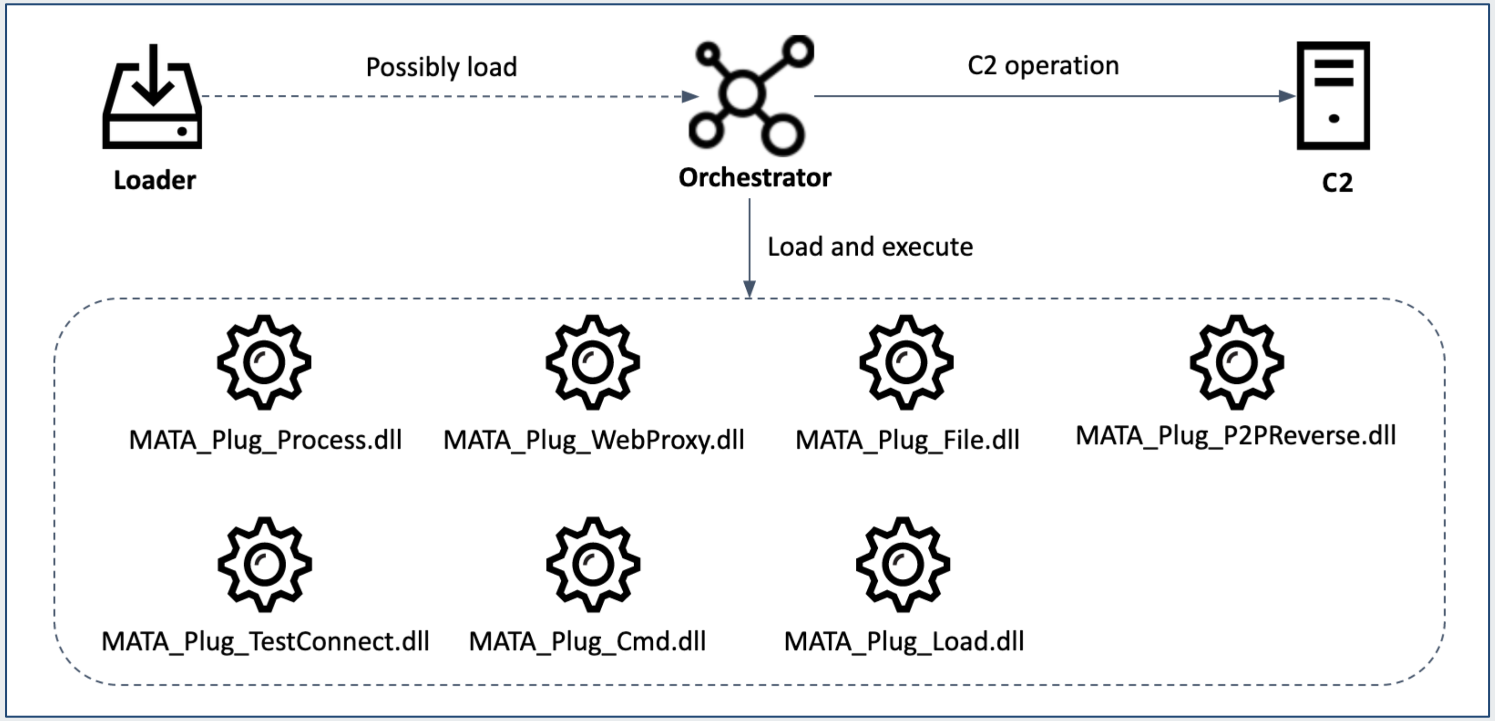
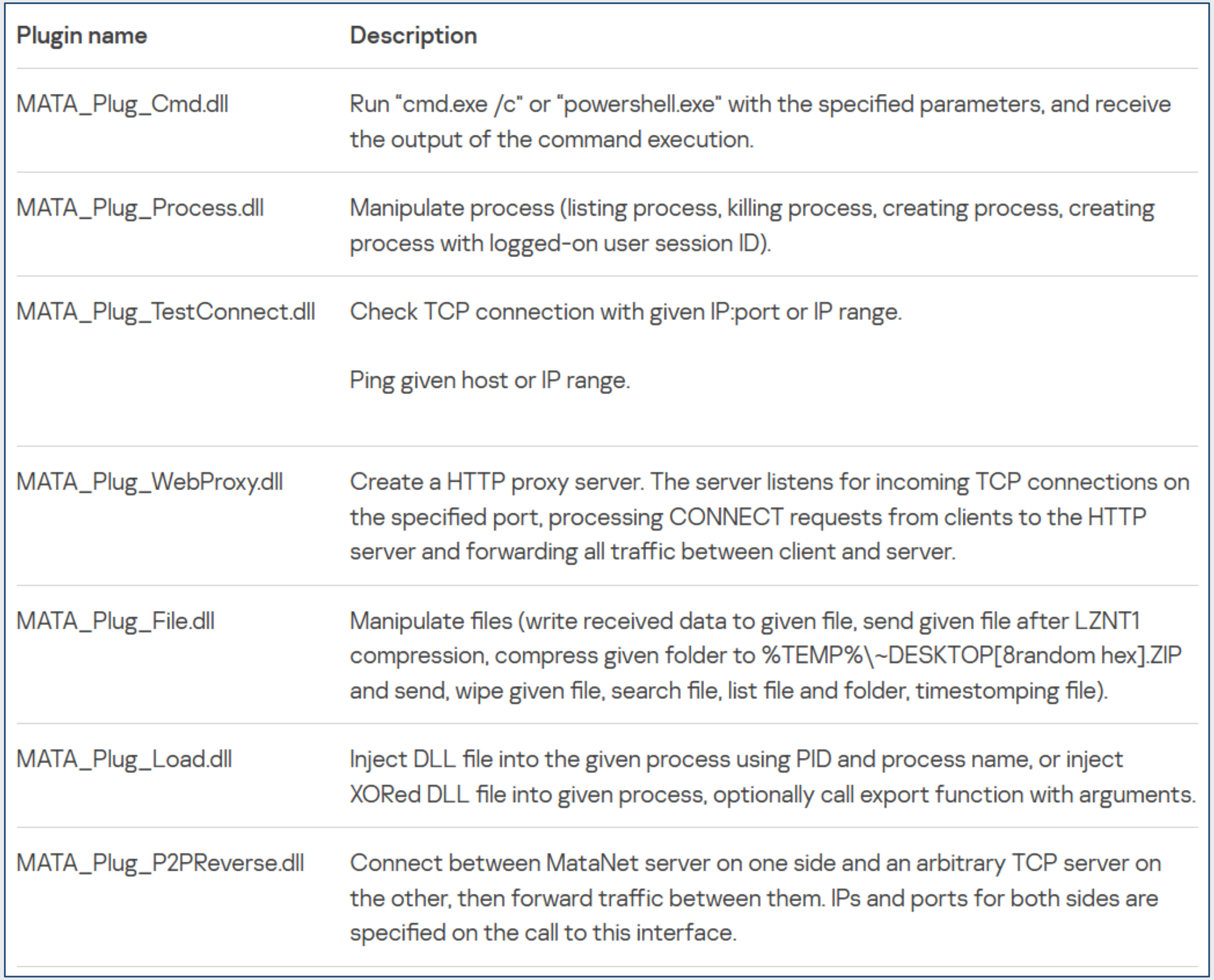


Image courtesy of Kaspersky

MATA Framework (Part 3)

MATA plugins allow for a variety of file searching, manipulation, modification and transfer. They also can conduct basic reconnaissance and communicate externally.

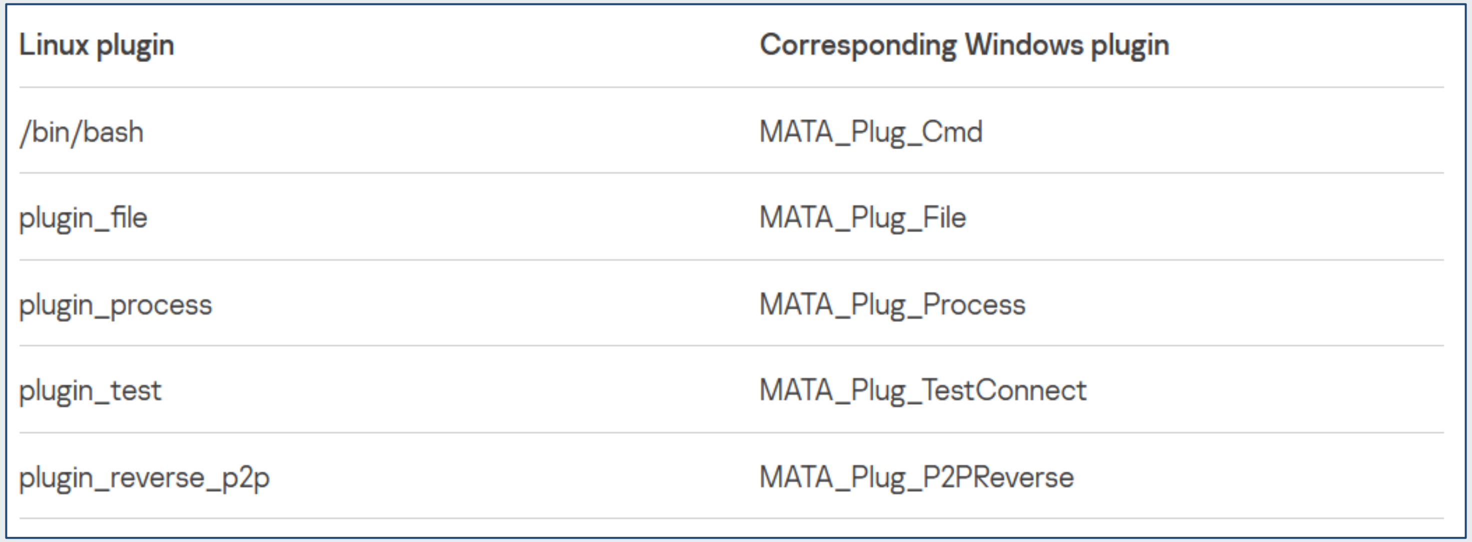


Plugin name	Description
MATA_Plug_Cmd.dll	Run "cmd.exe /c" or "powershell.exe" with the specified parameters, and receive the output of the command execution.
MATA_Plug_Process.dll	Manipulate process (listing process, killing process, creating process, creating process with logged-on user session ID).
MATA_Plug_TestConnect.dll	Check TCP connection with given IP:port or IP range. Ping given host or IP range.
MATA_Plug_WebProxy.dll	Create a HTTP proxy server. The server listens for incoming TCP connections on the specified port, processing CONNECT requests from clients to the HTTP server and forwarding all traffic between client and server.
MATA_Plug_File.dll	Manipulate files (write received data to given file, send given file after LZNT1 compression, compress given folder to %TEMP%\~DESKTOP[8random hex].ZIP and send, wipe given file, search file, list file and folder, timestomping file).
MATA_Plug_Load.dll	Inject DLL file into the given process using PID and process name, or inject XORed DLL file into given process, optionally call export function with arguments.
MATA_Plug_P2PReverse.dll	Connect between MataNet server on one side and an arbitrary TCP server on the other, then forward traffic between them. IPs and ports for both sides are specified on the call to this interface.

Image courtesy of Kaspersky

MATA Framework (Part 4)

As previously noted, MATA can run on a Linux system as well. Here are some of its Linux capabilities mapped to its Windows counterpart.

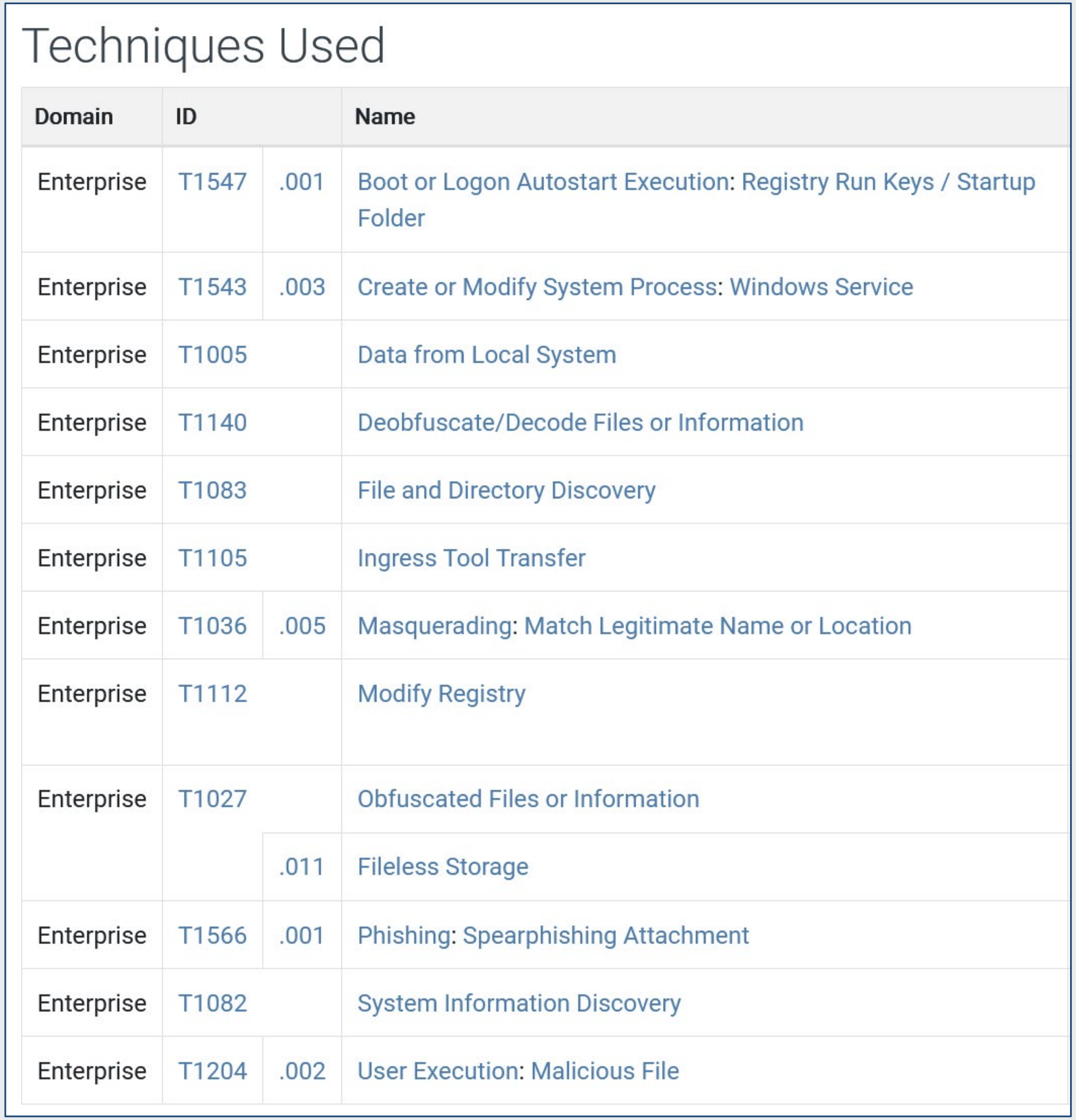


Linux plugin	Corresponding Windows plugin
/bin/bash	MATA_Plug_Cmd
plugin_file	MATA_Plug_File
plugin_process	MATA_Plug_Process
plugin_test	MATA_Plug_TestConnect
plugin_reverse_p2p	MATA_Plug_P2PReverse

Image courtesy of Kaspersky

ThreatNeedle

- Backdoor malware, operated by Lazarus since 2019 and believed to be derived from Manuscrypt
- Runs on Windows
- Persistence, file manipulation and registry modification capabilities, in addition to reconnaissance and phishing

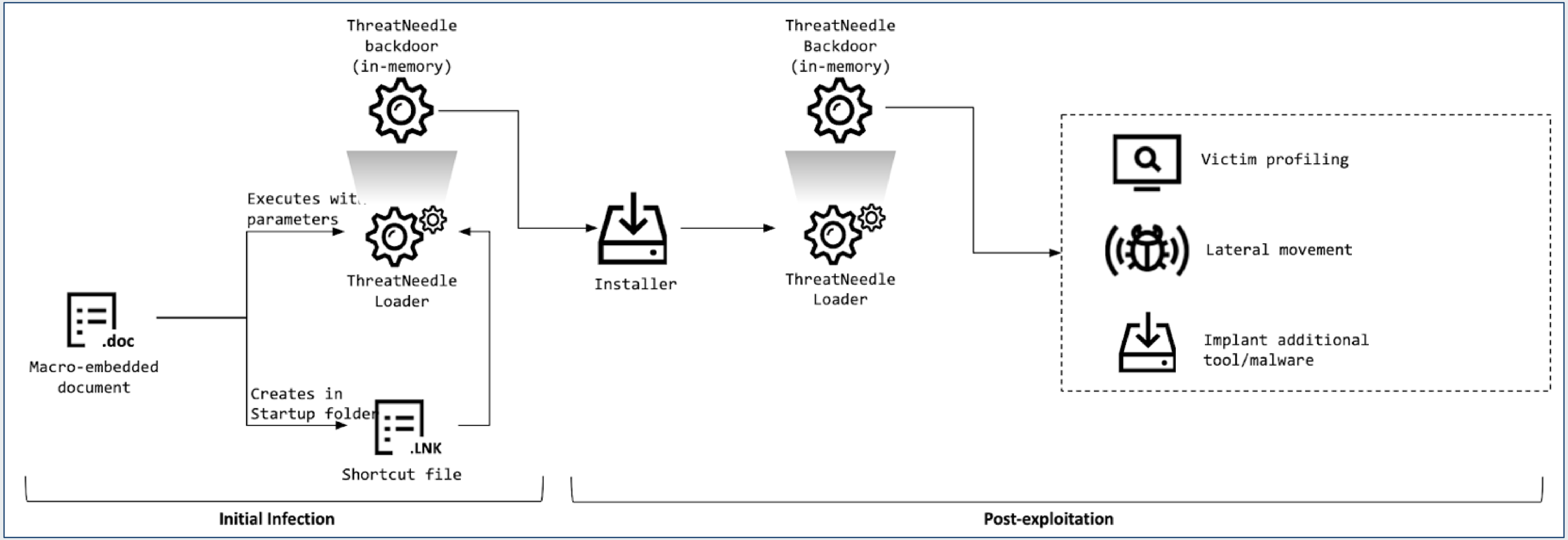


Techniques Used

Domain	ID		Name
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Enterprise	T1543	.003	Create or Modify System Process: Windows Service
Enterprise	T1005		Data from Local System
Enterprise	T1140		Deobfuscate/Decode Files or Information
Enterprise	T1083		File and Directory Discovery
Enterprise	T1105		Ingress Tool Transfer
Enterprise	T1036	.005	Masquerading: Match Legitimate Name or Location
Enterprise	T1112		Modify Registry
Enterprise	T1027		Obfuscated Files or Information
		.011	Fileless Storage
Enterprise	T1566	.001	Phishing: Spearphishing Attachment
Enterprise	T1082		System Information Discovery
Enterprise	T1204	.002	User Execution: Malicious File

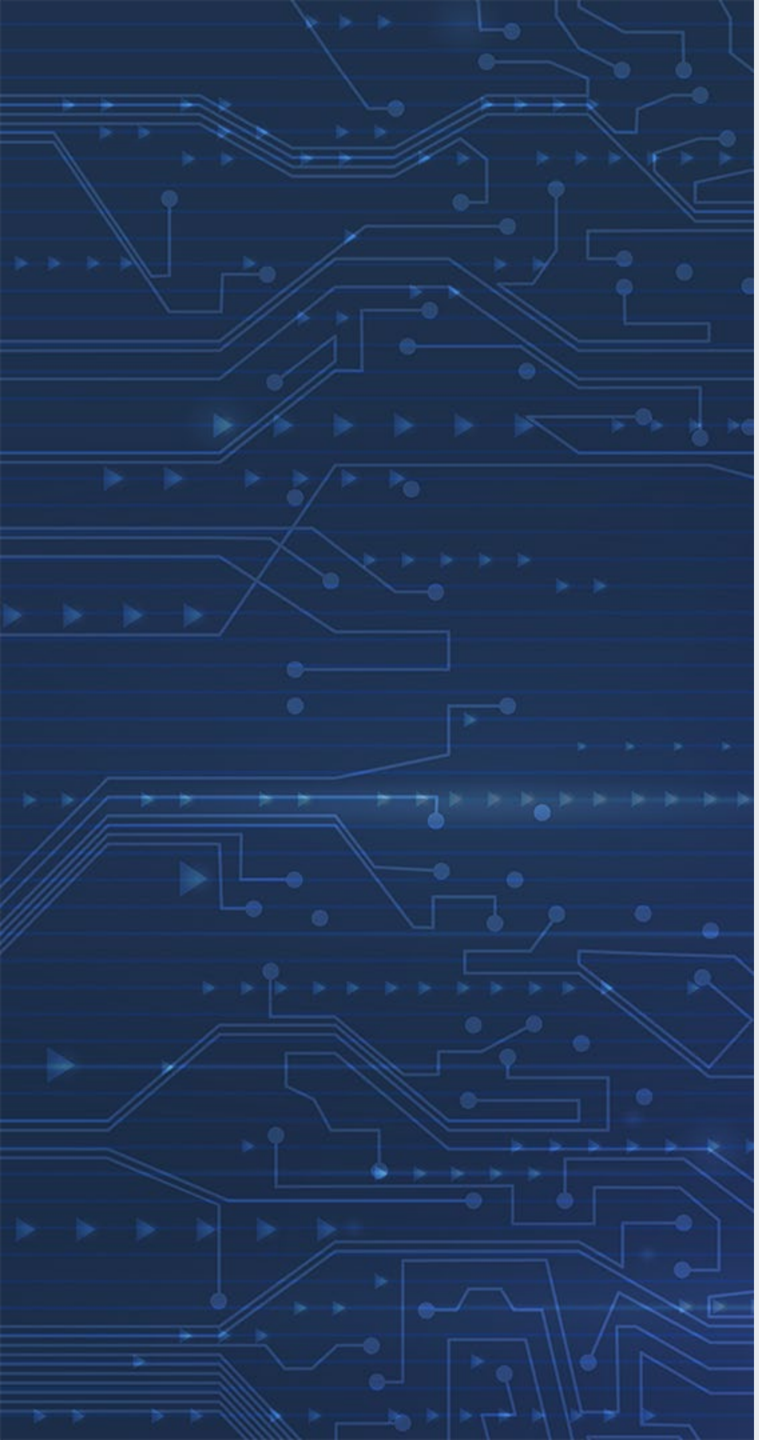
Image courtesy of MITRE

ThreatNeedle (Part 2)



Malware Used by Lazarus Group

- The following is a sample of malware variants leveraged by Lazarus Group:
- BISTROMATH – A multi-functional remote access trojan; part of the HotCroissant malware family
- SLICKSHOES – Dropper with beaconing, reconnaissance, file transfer and other capabilities
- CROWDEDFLOUNDER – Remote Access Trojan capable of receiving and initiating connections
- HOTCROISSANT – Remote Access Trojan can collect usernames, administrative and system data, as well as transfer files, execute commands and capture screens
- ARTFULPIE – Implant that can transfer files and load and execute files into memory
- BUFFETLINE – Implant that can conduct beaconing, file transfers and execution, as well as Windows command line access, process creation/termination and system enumeration



Defense and Mitigations

What can the U.S. health sector do about these cybercriminal threats?

Staying Secure

- Government resources:
  - DHS/CISA Stop Ransomware: https://www.cisa.gov/stopransomware
  - FBI Cybercrime: https://www.fbi.gov/investigate/cyber
  - FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
  - FDA: Medical Device Information: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
  - H-ISAC White Papers: https://h-isac.org/category/h-isac-blog/white-papers/
  - 405(d) Resource Library: https://405d.hhs.gov/resources
  - HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

Ransomware Mitigations and Defense (Source: FBI)

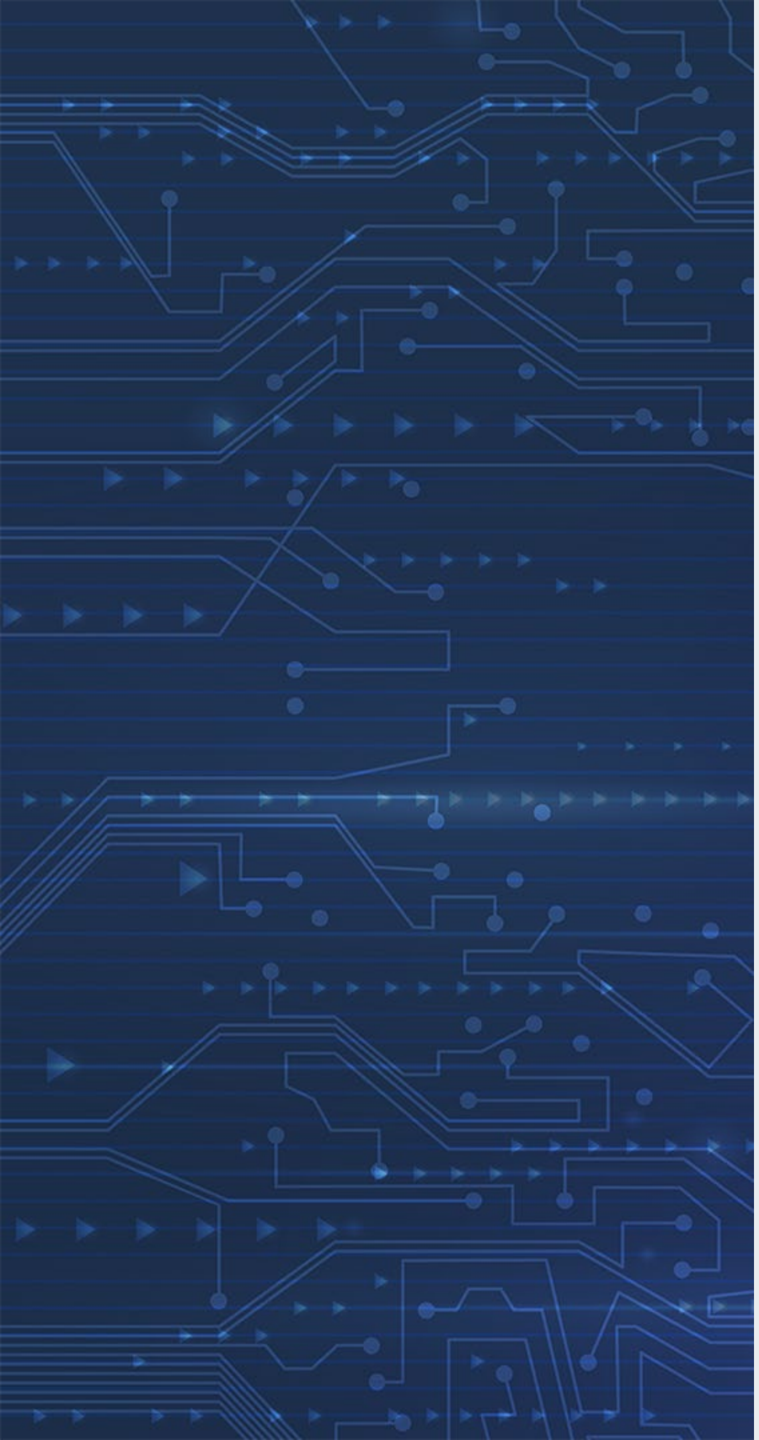
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system-defined or -recognized scheduled tasks for unrecognized "actions" (for example: review the steps each scheduled task is expected to perform).
- Review anti-virus logs for indications that they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).

Ransomware Mitigations and Defense (Part 2)

- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Recommendations

In addition to following the mitigations, HC3 recommends organizations review and utilize CISA's Free Cybersecurity Services and Tools, which can be accessed by visiting https://www.cisa.gov/free-cybersecurity-services-and-tools.



Conclusions

What do these threats mean for U.S. healthcare?

What Are the Takeaways?

Chinese and North Korean "cybercriminal groups" act as unique threats to the U.S. health sector.

- China and North Korea are both significant cyber powers – China in absolute terms and North Korea in relative terms.
- Domestic politics in both nations has created a unique cybercriminal ecosystem, where the only significant cybercriminals that exist as a threat to the U.S. health sector are state-sponsored.
- The most significant point is that groups originating in North Korea and China that act as cyber criminal gangs (i.e. are financially motivated) have all the sophistication of many other cybercriminal gangs, but also have the resources (technological, financial and diplomatic) of a state behind them.
  - They are state-backed criminals and they target a number of industries, including the U.S. health sector.

Reference Materials

References

GOZNYM MALWARE: CYBERCRIMINAL NETWORK DISMANTLED IN INTERNATIONAL OPERATION
https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation
https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled

ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World
https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world

APT41 - A Dual Espionage and Cyber Crime Operation
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

CrowdStrike 2020 Global Threat Report
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

CrowdStrike 2023 Global Threat Report
https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf

Threat Trends: How APT43 Targets Security Policy Experts Focused on North Korea
https://www.mandiant.com/resources/podcasts/threat-trends-apt43-security-policy

APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations
https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

References

Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups
https://home.treasury.gov/news/press-releases/sm774

HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure
https://www.cisa.gov/news-events/alerts/2017/06/13/hidden-cobra-north-koreas-ddos-botnet-infrastructure

Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations
https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government

North Korean threat actor APT43 pivots back to strategic cyberespionage
https://www.csoonline.com/article/3692288/north-korean-threat-actor-apt43-pivots-back-to-strategic-cyberespionage.html

North Korean Cyber Capabilities: In Brief
https://sgp.fas.org/crs/row/R44912.pdf

Lazarus Group Brings APT Tactics to Ransomware
https://threatpost.com/lazarus-group-apt-tactics-ransomware/157815/

Lazarus on the hunt for big game
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/

Kaspersky finds Lazarus is now operating its own ransomware
https://usa.kaspersky.com/about/press-releases/2020_kaspersky-finds-lazarus-is-now-operating-its-own-ransomware

North Korean Hackers May Be Dabbling in Ransomware Again
https://www.pcmag.com/news/north-korea-hackers-ransomware-vhd-lazarus-kaspersky

References

North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign
https://www.malwarebytes.com/blog/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign

Lazarus hackers use Windows Update to deploy malware
https://www.bleepingcomputer.com/news/security/lazarus-hackers-use-windows-update-to-deploy-malware/

UN Security Council: Note by the President of the Security Council
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/028/82/PDF/N1902882.pdf?OpenElement

UN Report: N. Korea Targets Cryptocurrency Exchanges, Banks
https://www.bankinfosecurity.com/un-report-n-korea-targets-cryptocurrency-exchanges-banks-a-12192

US charges two more members of the 'Lazarus' North Korean hacking group
https://www.zdnet.com/article/us-charges-two-more-members-of-the-lazarus-north-korean-hacking-group/

Lazarus and the tale of three RATs
https://blog.talosintelligence.com/lazarus-three-rats/

Lazarus Group’s Mata Framework Leveraged To Deploy TFlower Ransomware
https://blog.sygnia.co/lazarus-groups-mata-framework-leveraged-to-deploy-tflower-ransomware

References

Lazarus Group’s Mata Framework Leveraged To Deploy TFlower Ransomware
https://blog.sygnia.co/lazarus-groups-mata-framework-leveraged-to-deploy-tflower-ransomware

Lazarus targets defense industry with ThreatNeedle
https://ics-cert.kaspersky.com/publications/reports/2021/02/25/lazarus-targets-defense-industry-with-threatneedle/#_Toc64638330

MATA: Multi-platform targeted malware framework
https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/

Coronavirus: North Korea and Russia hackers 'targeting vaccine’
https://www.bbc.com/news/technology-54936886

Lazarus on the hunt for big game
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/

Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe
https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

Wanted by the FBI: JON CHANG HYOK
https://www.justice.gov/opa/press-release/file/1367706/download

FBI Most wanted: PARK JIN HYOK
https://www.fbi.gov/wanted/cyber/park-jin-hyok

APT41
https://attack.mitre.org/groups/G0096/

References

A Look into the Lazarus Group’s Operations
https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations

US charges two more members of the 'Lazarus' North Korean hacking group
https://www.zdnet.com/article/us-charges-two-more-members-of-the-lazarus-north-korean-hacking-group/

Council on Foreign Relations: Lazarus Group
https://www.cfr.org/cyber-operations/lazarus-group

Lazarus Group
https://attack.mitre.org/groups/G0032/

North Korea Targets—and Dupes—a Slew of Cybersecurity Pros
https://www.wired.com/story/north-korea-hackers-target-cybersecurity-researchers/

North Korean hackers targeting hospitals and healthcare providers, U.S. agencies warn
https://www.upi.com/Top_News/World-News/2022/07/07/ransomware-cybersecurity-FBI-hack-hospitals-healthcare/8991657180214/

Lazarus Group
https://attack.mitre.org/groups/G0032/

North Korea Targets—and Dupes—a Slew of Cybersecurity Pros
https://www.wired.com/story/north-korea-hackers-target-cybersecurity-researchers/

MagicRAT: Lazarus’ latest gateway into victim networks
https://blog.talosintelligence.com/lazarus-magicrat/

References

Public Key Episode 8 preview: Sony Productions Sabotage, Largest DeFi Hack in the world and ongoing cryptocurrency related stolen funds
https://blog.chainalysis.com/reports/chainalysis-podcast-episode-8-lazarus-group-north-korea/

New Threat Activity by Lazarus Group Spells Trouble for Orgs
https://www.darkreading.com/threat-intelligence/new-threat-activity-by-lazarus-group-spells-trouble-for-orgs

The 5×5—China's cyber operations
https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/

North Korean hackers targeting hospitals and healthcare providers, U.S. agencies warn
https://www.upi.com/Top_News/World-News/2022/07/07/ransomware-cybersecurity-FBI-hack-hospitals-healthcare/8991657180214/

FBI links largest crypto hack ever to North Korean hackers
https://www.bleepingcomputer.com/news/security/fbi-links-largest-crypto-hack-ever-to-north-korean-hackers/

Lazarus Attackers Turn to the IT Supply Chain
https://threatpost.com/lazarus-apt-it-supply-chain/175772/

THREAT ANALYSIS REPORT: PlugX RAT Loader Evolution
https://www.cybereason.com/blog/threat-analysis-report-plugx-rat-loader-evolution

F-Secure: Lazarus Group Campaign Targeting the Cryptocurrency Vertical
https://labs.withsecure.com/content/dam/labs/docs/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf//www.zdnet.com/article/us-treasury-links-north-korean-hacker-group-lazarus-to-600m-axie-infinity-heist/

APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION
https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

? Questions

FAQ

Upcoming Briefing

- October 12 – Incident Response Plans

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV