North Korean and Chinese Cyber Crime Threats to the HPH

September 21, 2023
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.

<table>
<thead>
<tr>
<th></th>
<th>Number of staff and affiliates</th>
<th>Annual revenue</th>
<th>Management layers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1 - 5</td>
<td>Under US$500,000</td>
<td>1</td>
</tr>
<tr>
<td>Medium</td>
<td>6 - 49</td>
<td>Up to US$50 million</td>
<td>2</td>
</tr>
<tr>
<td>Large</td>
<td>50+</td>
<td>US$50 million+</td>
<td>3</td>
</tr>
</tbody>
</table>

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

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

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
Cyber Threat Actor Characterization/Categorization

What are the different types of threat actors?

<table>
<thead>
<tr>
<th>STATE/NON-STATE</th>
<th>TYPE</th>
<th>MOTIVATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Advanced Persistent Threat</td>
<td>Political agenda</td>
</tr>
<tr>
<td>Non-state</td>
<td>Cybercriminal groups</td>
<td>Financial fraud/theft</td>
</tr>
<tr>
<td>Non-state</td>
<td>Contractors</td>
<td>Political agenda (host)</td>
</tr>
<tr>
<td>Non-state</td>
<td>Hacktivists</td>
<td>Political activism</td>
</tr>
<tr>
<td>Non-state</td>
<td>Individuals</td>
<td>Any</td>
</tr>
</tbody>
</table>

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
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.
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: [hrs0n59 @ gmail.com] is used in both state-directed and criminal attacks.
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
### APT41 Targeting by Industry

<table>
<thead>
<tr>
<th>Industries Targeted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive</td>
</tr>
<tr>
<td>Financial</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
</tr>
<tr>
<td>Business Services</td>
</tr>
<tr>
<td>Healthcare</td>
</tr>
<tr>
<td>Retail</td>
</tr>
<tr>
<td>Cryptocurrency</td>
</tr>
<tr>
<td>High-Tech</td>
</tr>
<tr>
<td>Telecommunications</td>
</tr>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Intergovernmental</td>
</tr>
<tr>
<td>Travel</td>
</tr>
<tr>
<td>Energy</td>
</tr>
<tr>
<td>Media and Entertainment</td>
</tr>
</tbody>
</table>

*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.

<table>
<thead>
<tr>
<th>Year</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Video Game, Hi-Tech, Intergovernmental</td>
</tr>
<tr>
<td>2013</td>
<td>Video Game, Hi-Tech, Media</td>
</tr>
<tr>
<td>2014</td>
<td>Video Game, Hi-Tech, Media</td>
</tr>
<tr>
<td>2015</td>
<td>Video Game, Hi-Tech, Media</td>
</tr>
<tr>
<td>2016</td>
<td>Video Game, Hi-Tech, Automotive, Energy</td>
</tr>
<tr>
<td>2017</td>
<td>Retail, Telecom, Finance, Travel</td>
</tr>
<tr>
<td>2018</td>
<td>Video Game, Telecom, Travel</td>
</tr>
<tr>
<td>2019</td>
<td>Video Game, Telecom, Travel</td>
</tr>
</tbody>
</table>

*Image courtesy of Mandiant*
APT41 geographic targeting

Image courtesy of Mandiant
APT41 targeting in 2019

Image courtesy of CrowdStrike
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

**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

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

Image courtesy of Mandiant
Cryptocurrency Laundering

APT43’s cryptocurrency laundering techniques – purchasing mining power – makes on-chain transaction tracing impossible.
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
- GOLDORAGON POWERSHELL
- LATE3P
- LOGBABIN
- DNEJUGGER
- SPICYTUNA

ESTABLISH FOOTPRINT
- Keylogging
- Scheduled task
- PowerShell
- Scripting
- Command-line interface
- Visual Basic Scripts
- Metasploit
- APADAD
- BISHON
- BITTERSWEET
- BRAVAFRINE
- COMTOSS
- GOMFLOSS ALM
- DRIVEDOWN
- EGG247CH
- Ghoul RAT
- GOLDORAGON
- GOLDORAGON POWERSHELL
- GOLDOROP
- GRAYZONE
- HANDMAN v2
- Landmark
- LATE3P
- LNEJUGGER
- PASSMARK
- PENCOLOW
- PENDOWN
- PHANTOMBAR
- QUASARRAT
- SL INCUR
- SOURDOUGH
- SPICYTUNA
- SWEETIROP
- TROJAN
- VENOMITE
- XRAT

ESCALATE PRIVILEGE
- Scheduled task
- Registry modifications
- Stolen credentials
- Windows service
- Shortcut modification
- Access token manipulation
- Bypass user access control
- Process injection
- GOLDORAGON
- GRAYZONE
- LATE3P
- PENCOLOW
- TROJAN
- VENOMITE

MAINTAIN PRESENCE
- Built-in Windows commands (planexec, ipconfig, etc.)
- FASTFIRE
- GOLDORAGON
- GOLDORAGON POWERSHELL
- GRAYZONE
- HANDMAN v2
- LATE3P
- LOGBABIN
- QUASARRAT
- SOURDOUGH
- SPICYTUNA
- TROJAN
- VENOMITE
- XRAT

MOVE LATERALLY
- Team Viewer
- Data compression
- Automated exfiltration
- SIKOLAG
- GOLDORET
- JURASSICSHIELD
- METASPLOT

COMPLETE MISSION

Image courtesy of Mandiant
# APT43 tradecraft mapped to MITRE ATT&CK framework

<table>
<thead>
<tr>
<th><strong>Initial Access</strong></th>
<th><strong>Command and Control</strong></th>
<th><strong>Defence Evasion</strong></th>
<th><strong>Impact</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>T1566 Phishing</td>
<td>T1671 001 Web Protocols</td>
<td>T1097 Evasive Files or Information</td>
<td>T1110 Brute Force</td>
</tr>
<tr>
<td>T1566.001 Spearphishing Attachment</td>
<td>T1671 004 DNS</td>
<td>T1627 Obfuscated Files or Information</td>
<td>T1110.003 Credentials from Web Browsers</td>
</tr>
<tr>
<td>T1566.002 Spearphishing Link</td>
<td>T1100 003 Multi-hop Proxy</td>
<td>T1627.001 Binary Padding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1100 002 Non-Application Layer Protocol</td>
<td>T1627.002 Software Packing</td>
<td></td>
</tr>
<tr>
<td><strong>Resource Development</strong></td>
<td>T1100 003 Web Service</td>
<td>T1627.005 Indicator Removal from Tools</td>
<td></td>
</tr>
<tr>
<td>T1583 003 Virtual Private Server</td>
<td>T1102 002 Bidirectional Communication</td>
<td>T1627.009 Embedded Payloads</td>
<td></td>
</tr>
<tr>
<td>T1584 Compromise Infrastructure</td>
<td>T1102 001 Ingress Tool Transfer</td>
<td>T1638 Pass the Bait</td>
<td></td>
</tr>
<tr>
<td>T1588 003 Code Signing Certificates</td>
<td>T1102 001 Standard Encoding</td>
<td>T1638.001 Invalid Code Signature</td>
<td></td>
</tr>
<tr>
<td>T1588 004 Digital Certificates</td>
<td>T1102 001 Asymmetric Cryptography</td>
<td>T1638.007 Double File Extension</td>
<td></td>
</tr>
<tr>
<td>T1608 003 Install Digital Certificate</td>
<td></td>
<td>T1641 Process Injection</td>
<td></td>
</tr>
<tr>
<td>T1608 005 Link Target</td>
<td></td>
<td>T1655 Dynamic Link Library Injection</td>
<td></td>
</tr>
<tr>
<td><strong>Execution</strong></td>
<td></td>
<td>T1655.001 Thread Execution Hijacking</td>
<td></td>
</tr>
<tr>
<td>T1647 Windows Management Instrumentation</td>
<td>T1107 System Service Discovery</td>
<td>T1655.003 File Delete</td>
<td></td>
</tr>
<tr>
<td>T1653 005 Scheduled Task</td>
<td>T1107 001 Application Window Discovery</td>
<td>T1670 006 Timestamp</td>
<td></td>
</tr>
<tr>
<td>T1659 001 Command and Scripting Interceptor</td>
<td>T1107 002 System Networking Discovery</td>
<td>T1670.002 Modify Registry</td>
<td></td>
</tr>
<tr>
<td>T1659.002 PowerShell</td>
<td>T1107 003 System Owner/Owner Discovery</td>
<td>T1670.003 Access Token Manipulation</td>
<td></td>
</tr>
<tr>
<td>T1659.003 Windows Command Shell</td>
<td>T1107 004 Process Discovery</td>
<td>T1670.004 Infect</td>
<td></td>
</tr>
<tr>
<td>T1659.005 Visual Basic</td>
<td>T1107 005 File and Directory Discovery</td>
<td>T1670.005 Get Code from Injected Malware</td>
<td></td>
</tr>
<tr>
<td>T1659.007 JavaScript</td>
<td>T1107 006 Account Discovery</td>
<td>T1671 001 Staged Code</td>
<td></td>
</tr>
<tr>
<td>T1129 Shared Modules</td>
<td>T1107 007 Software Discovery</td>
<td>T1671.002 Get Code from Injected Malware</td>
<td></td>
</tr>
<tr>
<td>T1203 Exploitation for Client Execution</td>
<td>T1107 008 System Language Discovery</td>
<td>T1671.003 API Hook</td>
<td></td>
</tr>
<tr>
<td>T1204 001 Malicious Link</td>
<td></td>
<td>T1671.004 Reflective Code Loading</td>
<td></td>
</tr>
<tr>
<td>T1204.002 Malicious File</td>
<td></td>
<td>T1671.005 Debugger Evasion</td>
<td></td>
</tr>
<tr>
<td>T1668 002 Service Execution</td>
<td></td>
<td>T1671.006 Data Execution</td>
<td></td>
</tr>
</tbody>
</table>

### Defence Evasion

- **T1097** Evasive Files or Information
- **T1627** Obfuscated Files or Information
- **T1627.001** Binary Padding
- **T1627.002** Software Packing
- **T1627.005** Indicator Removal from Tools
- **T1627.009** Embedded Payloads
- **T1638** Pass the Bait
- **T1638.001** Invalid Code Signature
- **T1638.007** Double File Extension
- **T1641** Process Injection
- **T1655** Dynamic Link Library Injection
- **T1655.001** Thread Execution Hijacking
- **T1670** File Delete
- **T1670.006** Timestamp
- **T1670.002** Modify Registry
- **T1670.003** Access Token Manipulation
- **T1671** Infect
- **T1671.001** Staged Code
- **T1671.002** Get Code from Injected Malware
- **T1671.003** API Hook
- **T1671.004** Reflective Code Loading
- **T1671.005** Debugger Evasion
- **T1671.006** Data Execution

### Impact

- **T1110** Brute Force
- **T1110.003** Credentials from Web Browsers

### Credential Access:

- **T1110** Brute Force
- **T1110.003** Credentials from Web Browsers
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”
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

<table>
<thead>
<tr>
<th>Component</th>
<th>Name Regex</th>
<th>Description / Execution Flow</th>
</tr>
</thead>
</table>
| Initial loader (EXE) | ![Pattern](image) \.(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)   | ![Pattern](image) \.(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)  | ![Pattern](image) \.(dot)  
(sms- 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.

<table>
<thead>
<tr>
<th>Plugin name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MATA_Plug_Cmd.dll</td>
<td>Run &quot;cmd.exe /c&quot; or &quot;powershell.exe&quot; with the specified parameters, and receive the output of the command execution.</td>
</tr>
<tr>
<td>MATA_Plug_Process.dll</td>
<td>Manipulate process (listing process, killing process, creating process, creating process with logged-on user session ID).</td>
</tr>
<tr>
<td>MATA_Plug_TestConnect.dll</td>
<td>Check TCP connection with given IP port or IP range. Ping given host or IP range.</td>
</tr>
<tr>
<td>MATA_Plug_WebProxy.dll</td>
<td>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.</td>
</tr>
<tr>
<td>MATA_Plug_File.dll</td>
<td>Manipulate files (write received data to given file, send given file after LZNT1 compression, compress given folder to %TEMP%\DESKTOP[random hex]\ZIP and send, wipe given file, search file, list file and folder, timestamping file).</td>
</tr>
<tr>
<td>MATA_Plug_Load.dll</td>
<td>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.</td>
</tr>
<tr>
<td>MATA_Plug_P2PReverse.dll</td>
<td>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.</td>
</tr>
</tbody>
</table>
As previously noted, MATA can run on a Linux system as well. Here are some of its Linux capabilities mapped to its Windows counterpart.

<table>
<thead>
<tr>
<th>Linux plugin</th>
<th>Corresponding Windows plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bin/bash</td>
<td>MATA_Plug_Cmd</td>
</tr>
<tr>
<td>plugin_file</td>
<td>MATA_Plug_File</td>
</tr>
<tr>
<td>plugin_process</td>
<td>MATA_Plug_Process</td>
</tr>
<tr>
<td>plugin_test</td>
<td>MATA_Plug_TestConnect</td>
</tr>
<tr>
<td>plugin_reverse_p2p</td>
<td>MATA_Plug_P2PReverse</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1547</td>
<td>.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1543</td>
<td>.003 Create or Modify System Process: Windows Service</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1005</td>
<td>Data from Local System</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1140</td>
<td>Deobfuscate/Decode Files or Information</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1083</td>
<td>File and Directory Discovery</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1105</td>
<td>Ingress Tool Transfer</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1036</td>
<td>.005 Masquerading: Match Legitimate Name or Location</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1112</td>
<td>Modify Registry</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1027</td>
<td>Obfuscated Files or Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.011 Fileless Storage</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1566</td>
<td>.001 Phishing: Spearphishing Attachment</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1082</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1204</td>
<td>.002 User Execution: Malicious File</td>
</tr>
</tbody>
</table>
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](https://www.cisa.gov/stopransomware)
  - FBI Cybercrime: [https://www.fbi.gov/investigate/cyber](https://www.fbi.gov/investigate/cyber)
  - H-ISAC White Papers: [https://h-isac.org/category/h-isac-blog/white-papers/](https://h-isac.org/category/h-isac-blog/white-papers/)
  - 405(d) Resource Library: [https://405d.hhs.gov/resources](https://405d.hhs.gov/resources)
  - HC3 Products: [https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html](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

GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation

ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World

APT41 - A Dual Espionage and Cyber Crime Operation

CrowdStrike 2020 Global Threat Report

CrowdStrike 2023 Global Threat Report

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

HIDDEN COBRA – North Korea’s 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

North Korean Cyber Capabilities: In Brief

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

North Korean Hackers May Be Dabbling in Ransomware Again
References

North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign

Lazarus hackers use Windows Update to deploy malware

UN Security Council: Note by the President of the Security Council

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

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

MATA: Multi-platform targeted malware framework

Coronavirus: North Korea and Russia hackers ‘targeting vaccine’

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

Wanted by the FBI: JON CHANG HYOK

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

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

North Korean hackers targeting hospitals and healthcare providers, U.S. agencies warn

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

North Korea Targets—and Dupes—a Slew of Cybersecurity Pros

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

The 5x5—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

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

F-Secure: Lazarus Group Campaign Targeting the Cryptocurrency Vertical

APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION
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.