North Korean Cyber Activity

03/25/2021
• DPRK National Interests
• Timeline of Recent Activity
• Overview of DPRK APT Groups
• APT Threat Actor Profiles
  o HIDDEN COBRA
  o Andariel
  o APT37
  o APT38
  o TEMP.Hermit
  o TEMP.Firework
  o Kimsuky
  o Bureau 121
  o Bureau 325
• Recommendations
• Outlook

Slides Key:

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

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

• North Korea, officially the Democratic People’s Republic of Korea (DPRK)
• Supreme leader: Kim Jong-un (since 2011)
• Primary strategic goal: perpetual Kim family rule via development of economy and nuclear weapons
• Primary drivers of security strategy:
  o Deterring foreign intervention by obtaining nuclear capabilities
  o Eliminating perceived threats to Kim regime
  o Belief that North Korea is entitled to respect as a world power

• “Cyberwarfare is an all-purpose sword that guarantees the North Korean People’s Armed Forces ruthless striking capability, along with nuclear weapons and missiles.” – Kim Jong-un (2013)
• Reportedly has 7,000 cyber warriors
• 300% increase in the volume of activity to and from North Korean networks since 2017
Timeline of Recent Activity

**Jan 2020**
Two distinct clusters of DPRK cyber activity begin targeting healthcare & pharma

**Aug 2020**
USG exposed DPRK malware used in fake job posting campaign

**Nov 2020**
North Korean hackers targeted a major COVID-19 vaccine developer

**Feb 2021**
South Korean Intelligence claims DPRK targeted COVID-19 data at major pharma org

**Feb 2021**
North Korean Lazarus Group hackers indicted in the US

**June 2020**
North Korean state hackers sent COVID-19-themed phishing emails to 5 million entities in an attempt to steal personal and financial data

**Oct 2020**
Russian and North Korean hackers targeted seven major companies involved in COVID-19 research

**Jan 2021**
North Korean social engineering campaign against cybersecurity researchers

**Feb 2021**
Media reports on creation of North Korean hacking group specialized in stealing COVID-19 info
• HIDDEN COBRA is the general term that the US Government uses to refer to malicious cyber activity by the North Korean government

• North Korean APT groups are known to leverage cyberattacks to finance nuclear development, as well as for intelligence collection and espionage purposes

• DPRK cyber operators known to have previously supported operations for multiple APT groups

• North Korean APT groups likely share malware and resources, making attribution difficult

o HIDDEN COBRA
o Andariel
o APT37
o APT38
o TEMP.Hermit
o TEMP.Firework
o Kimsuky
o Bureau 121
o Bureau 325
HIDDEN COBRA

Also known as: Lazarus Group, Guardians of Peace, ZINC, NICKEL ACADEMY

Suspected attribution: Democratic People’s Republic of Korea

Target sectors: Finance, aerospace and defense, manufacturing, healthcare, banking, telecommunications, media

Overview: Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims, some resulting in the exfiltration of data while others have been disruptive in nature. HIDDEN COBRA actors are likely to continue to use cyber operations to advance their government’s military and strategic objectives. HIDDEN COBRA is known for a campaign of coordinated DDoS attacks on South Korean media, financial, and critical infrastructure in 2011, as well as the Sony Breach in 2014 and various cryptocurrency attacks in 2017.

Associated malware: Copperhedge, Taintedscribe, Pebbledash, Destover, Wild Positron/Duuzer, Hangman, DeltaCharlie, WannaCry, RawDisk, Mimikatz, BADCALL, Volgmer, FALLCHILL, HOPLIGHT, FASTCash

Attack vectors: Adobe Flash player and Hangul Word Processor (HWP) vulnerabilities, social engineering and phishing with fake job offers via LinkedIn and WhatsApp, spear phishing emails containing malicious Microsoft Word vulnerabilities, zero day vulnerabilities.
Andariel

**Also known as:** Silent Chollima, Dark Seoul, Rifle, Wassonite

**Suspected attribution:** DPRK, Bureau 121

**Target sectors:** South Korean government and military, foreign businesses, government agencies, financial services infrastructure, private corporations, and businesses

**Overview:** Andariel is a sub-group of the Lazarus Group mainly focused on cyber espionage. The group was first seen around 2009 and has carried out numerous operations against the defense industry, mainly in South Korea. Andariel also focuses on conducting malicious cyber operations on foreign businesses, government agencies, financial services infrastructure, private corporations, and businesses. Andariel is also believed to conduct financially-motived computer intrusions.

**Associated malware:** Aryan, Gh0st RAT, Rifdoor, Phandoor, Andarat

**Attack vectors:** ActiveX, vulnerabilities in software local to South Korea, watering hole attacks, spear phishing (macro), IT management products (antivirus, PMS), supply chain (installers and updaters)
APT37

Also known as: Ricochet Chollima, Group 123, Reaper, THALLIUM, ScarCruft

Suspected attribution: Democratic People’s Republic of Korea (DPRK)

Target sectors: Primarily South Korea – though also the U.S., Japan, Vietnam, and the Middle East – in various industry verticals, including chemicals, electronics, manufacturing, banking, aerospace, automotive, and healthcare.

Overview: APT37 is a suspected North Korean state-sponsored cyber espionage group active since at least 2012. The group has previously used a range of zero day exploits to carry out attacks against victims of interest to the North Korean government, aligning with counterintelligence priorities.

Associated malware: APT37 employs a diverse suite of malware for initial intrusion and exfiltration. Their malware is characterized by a focus on stealing information from victims, with many set up to automatically exfiltrate data of interest. APT37 also has access to destructive malware. Some include DOGCALL, RUHAPPY, CORALDECK, SHUTTERSPEED, WINERACK, and several 0-day Flash and MS Office exploits.

Attack vectors: Social engineering tactics tailored specifically to desired targets, strategic web compromises typical of targeted cyberespionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately.
APT38

Also known as: BlueNoroff, Stardust Chollima, BeagleBoyz, NICKEL GLADSTONE

Suspected attribution: DPRK, Reconnaissance General Bureau

Target sectors: Banks, financial institutions, cryptocurrency exchanges

Overview: APT38 is a financially-motivated threat group that is backed by the North Korean regime. The group mainly targets banks and financial institutions, and has targeted more than 16 organizations in at least 13 countries since at least 2014. The funds stolen by APT38 are likely channeled into the DPRK’s missile and nuclear development programs. APT38 is known to share malware and other resources with TEMP.Hermit. In February 2021, three members of APT38 were indicted by the US DOJ.

Associated malware: DarkComet, Mimikatz, Net, NESTEGG, MACKTRUCK, WANNACRY, WHITEOUT, QUICKCAFE, RAWHIDE, SMOOTHRIDE, TightVNC, SORRYBRUTE, KEYLIME, SNAPSHOT, MAPMAKER, net.exe, sysmon, BOOTWRECK, CLEANTOAD, CLOSESHAVE, DYEPACK, Hermes, TwoPence, ELECTRICFISH, PowerRatankba, PowerSpritz

Attack vectors: Drive-by compromise, watering hole schemes, exploit insecure out-of-date version of Apache Struts2 to execute code on a system, strategic web compromise, access Linux servers
WannaCry Global Ransomware Attack in 2017

- WannaCry ransomware attack infected a quarter million machines in more than 150 countries in 2017
- Largest ransomware attack to date
- Impacted a national health service as well as a multinational pharmaceutical company’s medical devices
- Affected hospitals, GP surgeries across England and Scotland
- Resulted in cancellation of thousands of appointments and operations
- Frantic relocation of emergency patients
- Reverted to pen and paper
- Most of the health service’s devices infected with the ransomware were found to have been running the supported, but unpatched, Microsoft Windows 7 operating system
- Leveraged EternalBlue exploit
- Indictment of North Korean citizen Park Jin Hyok in 2018 worked for a front company
- Indicted again in February 2021
- Tied to Lazarus Group / APT38
**TEMP.Hermit**

*Also known as*: N/A

*Suspected attribution*: DPRK, Lab 110, 6th Technical Bureau of the Reconnaissance General Bureau (RGB)

*Target sectors*: Primarily government, defense, energy, and financial institutions in South Korea as well as targets worldwide aligned with DPRK affairs, including the United States

*Overview*: TEMP.Hermit is a cluster of cyber espionage activity tracked by FireEye that has been active since at least 2013. The group primarily targets the government, defense, energy, and financial sectors in South Korea, but also conducts operations against targets worldwide aligned with North Korean affairs. TEMP.Hermit is believed to share significant development resources with APT38.

*Associated malware*: MONKEYCHERRY, FALLCHILL

*Attack vectors*: Spear phishing, front organizations mainly located in northeast China
TEMP.Firework

Also known as: N/A

Suspected attribution: DPRK

Target sectors: Governments, think tanks, and universities; primarily in the U.S. and South Korea, but also Australia, Italy, India, Japan, Hong Kong, Hungary, and the Philippines.

Overview: TEMP.Firework primarily targets governments, think tanks, and universities focused on DPRK strategic issues such as nuclear security, nonproliferation, and U.S.-South Korea military capabilities. The group typically operates between 0700 and 1900 KST (GMT +9) Monday to Friday and has only once been observed operating outside of this schedule. In some recent operations, TEMP.Firework was called out for cyber campaigns leading up to the US 2020 Election and conducted spear phishing to gain access to multiple pharmaceutical companies and medical centers.

Associated malware: LATEOP, TROIBOMB, Mshta, TeamViewer, Mimikatz, LOGCABIN, and built-in Windows commands

Attack vectors: Spear phishing emails, stolen credentials
Kimsuky

Also known as: Velvet Chollima, Group G0094

Suspected attribution: North Korea (DPRK)

Target sectors: Individuals and experts in various fields, think tanks, government entities in South Korea, Japan, and the United States as well as universities with biomedical engineering expertise

Overview: The Kimsuky APT group has most likely been active since 2012 and is most likely tasked by the North Korean regime with a global intelligence gathering mission. Kimsuky has reused infrastructure from previous campaigns in the past.

Associated malware: BabyShark, GREASE, Win7Elevate, HWP document malware, malicious Google Chrome extension

Attack vectors: Kimsuky employs common social engineering tactics, spear phishing, and watering hole attacks to exfiltrate desired information from victims.
Bureau 121

Also known as: N/A

Suspected attribution: DPRK, Reconnaissance General Bureau

Target sectors: Major biotechnology companies, pharmaceutical manufacturers, research institutions, IT companies and government organizations in South Korea, China, and the United States.

Overview: Bureau 121 is considered the cyber warfare guidance unit of the DPRK. Most cyber operations take place, or are coordinated, within this unit. There are reportedly over 6,000 members in Bureau 121, with many of them operating in other countries, such as Belarus, China, India, Malaysia, and Russia. There are four subordinate units below Bureau 121: the Andariel Group, The Bluenoroff Group, an Electronic Warfare Jamming Regiment, and the Lazarus Group.

Associated malware: N/A

Attack vectors: N/A
Bureau 325

Also known as: 325 국 (possibly related to Cerium)

Suspected attribution: DPRK, Reconnaissance General Bureau

Target sectors: Major biotechnology companies, pharmaceutical manufacturers, research institutions, IT companies and government organizations in South Korea, China, and the United States.

Overview: Bureau 325 was allegedly established on January 3, 2021 under the Reconnaissance General Bureau (RGB) (Korean: 정찰총국) and receives direct instructions from Kim Jong Un. The group is mainly focused on stealing information on vaccine technology related to COVID-19, and is composed of hackers from various existing DPRK cyber units plus recent grads in IT and computer science. The unit reportedly consists of five teams: with three research institutes overseas (charged with stealing information) and two research centers inside the country (analyzing the hacked data).

Associated malware: Unknown

Attack vectors: Unknown
• Assume press attention affiliating your organization with COVID-19 research will lead to increased interest and activity by nation state and cyber criminal actors to penetrate your network.

• Patch critical vulnerabilities on all systems. Prioritize patching of Internet-connected servers for known vulnerabilities as well as software that processes Internet data, such as web browsers, browser plugins, and document readers.

• Actively scan and monitor web applications for unauthorized access, modification, and anomalous activities.

• Strengthen credential requirements and implement multi-factor authentication to protect individual accounts. Change passwords and do not use the same passwords for multiple accounts.

• Identify unusual activity and suspend access of users exhibiting illicit, potentially compromising, or uniquely suspicious behavior.

• Network device management interfaces such as Telnet, SSH, Winbox, and HTTP should be turned off for wide-area network (WAN) interfaces, and secured with strong passwords and encryption when enabled.

• When possible, store critical information on air-gapped systems. Use strict access control measures for critical data.

• Be mindful of new and existing information technology systems for work and bioscience collaborations.
Outlook

• It is highly likely that multiple North Korean cyber espionage operators have expanded targeting to pharmaceutical research and organizations involved in the COVID-19 response.

• Continue to leverage common spear phishing and social engineering techniques (fake job lures) as well as custom (even destructive) and publicly available tools.


References
References


Questions

Upcoming Briefs

• New Ryuk Variant (4/8)
• TBD (4/22)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Product Evaluations

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

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. HHS does not endorse any specific person, entity, product, service, or enterprise.
HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

About Us

Products

Sector & Victim Notifications
Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar
Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3