Assessed Cyber Structure and Alignments of North Korea in 2023 | Mandiant

By Mandiant

Published: 2023-10-10 · Archived: 2026-04-05 13:40:25 UTC

Written by: Michael Barnhart, Austin Larsen, Jeff Johnson, Taylor Long, Michelle Cantos, Adrian Hernandez

---

Executive Summary

- The DPRK's offensive program continues to evolve, showing that the regime is determined to continue using cyber intrusions to conduct both espionage and financial crime to project power and to finance both their cyber and kinetic capabilities.
- Latest DPRK nexus operations hint at an increase in adaptability and complexity, including a cascading software supply chain attack seen for the first time, and consistently targeting blockchain and fintech verticals.
- While different threat groups share tooling and code, North Korean threat activity continues to adapt and change to build tailored malware for different platforms, including Linux and macOS.
- Mandiant's continuous monitoring of DPRK aligned malicious cyber actors highlights a significant multiyear shift and blend in the country's cyber posture.
- Overlaps in targeting and shared tooling muddles attribution attempts for investigators while streamlining adversarial activities.
- Historical examples of activity and uncategorized clustering represent a way forward for maintaining visibility on separate groups.

Summation of North Korea's Cyber Program

Historically Mandiant has made assessments on the Democratic People's Republic of Korea's (DPRK) cyber program based on Mandiant responses to intrusions, defector accounts, and OSINT reporting, in conjunction with government disclosures of DPRK units and motivation information. These assessments were generalizations and as new activity, such as cryptocurrency-focused units, emerged it blended the efforts from DPRK aligned cyber operators, and updates were needed for the now historic chart seen in Figure 1.

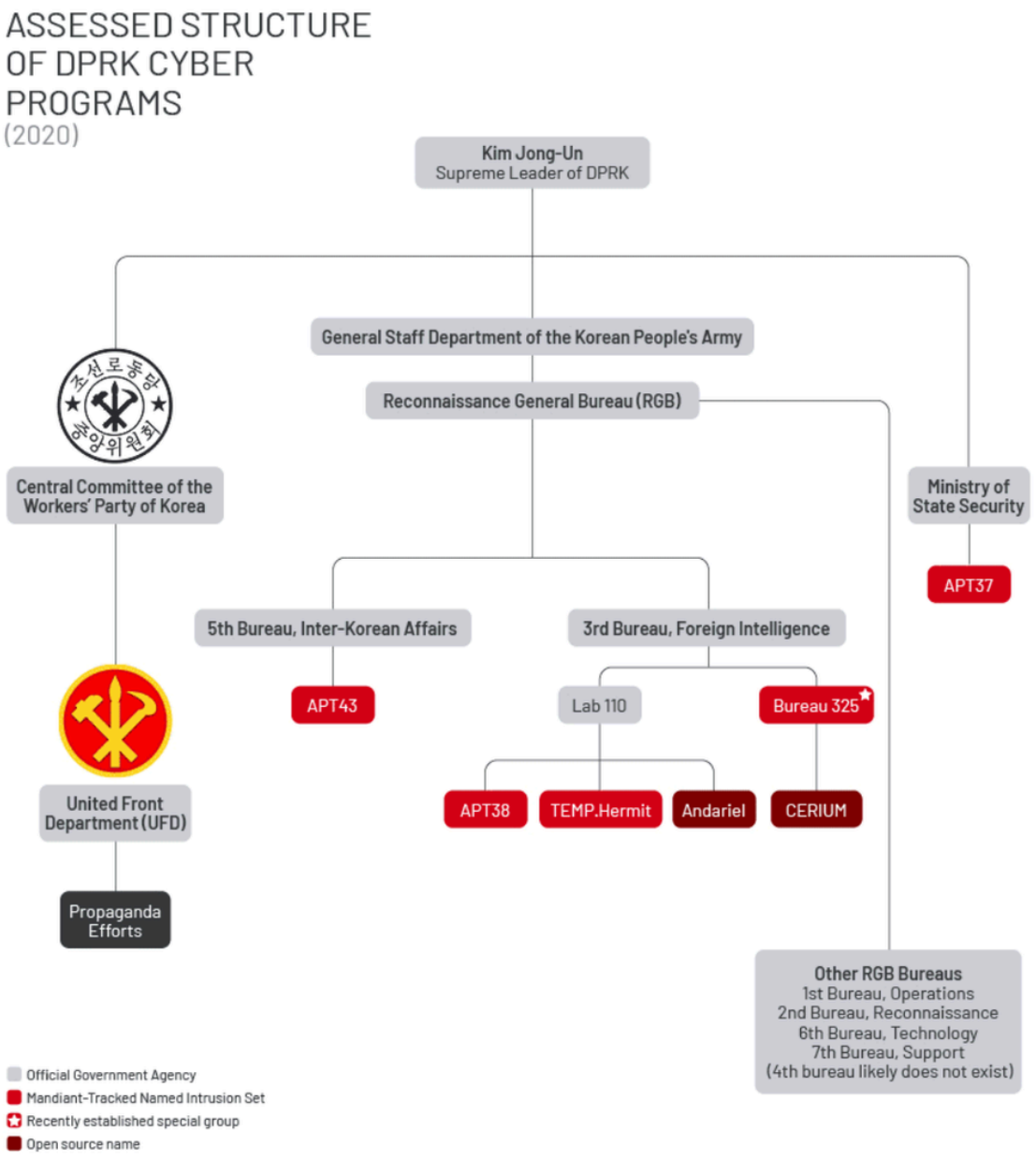


Figure 1: Previously assessed DPRK cyber organizational chart for 2020

Since 2009, the DPRK cyber landscape has changed tremendously, and overlapping indicators, which would traditionally be tracked individually to these separate organizations, seemingly signal a growing adaptability and collaboration between the threat actors. Instances of overlap and "sharing" of tools and targeting, which are detailed throughout this product, have occurred in the past, but the 2020 COVID-19 Pandemic marked a significant shift in DPRK's operations.

Prior to the pandemic, the following groups and their assessed unit alignments represented the overarching DPRK cyber organization:

- UNC614 (Andariel) – Reconnaissance General Bureau (RGB)
- APT37 – Ministry of State Security (MSS)

- APT38 – RGB
- APT43 – RGB (publicly referred toas Kimsuky)
- TEMP.Hermit – RGB
- IT Workers – Workers Party of Korea (KWP)

DPRK conducts offensive operations relying on their military units and proxies located inside and outside the Peninsula, however, the regime was forced to modify their operations in 2020 as the COVID-19 pandemic hardened borders around the world; most notably within the Korean Peninsula and China.

It is assessed that an unknown number of DPRK operators were cut off from the support of the regime during this period, as Mandiant observed signs of "self-funding" operations grow, such as the publicly reported ransomware activities of the Andariel group involving MAUI and HolyGh0st ransomware. This is also known as Ransomware as a Service (RaaS,) such as Lockbit 2.0 or Ryuk, and the cryptocurrency theft activities of APT43.

During this same time, Mandiant began discovering campaigns that indicated newly assembled groups, or task forces, consisting of tooling and suspected personnel from multiple groups being created. One such suspected operation was a temporary. COVID-19-focused grouping of clusters active during the pandemic that targeted healthcare and research entities investigating COVID-19 treatments.

These operations had overlaps with APT43 and TEMP.Hermit activities, as well as an unverified link to Andariel signaling an unprecedented shift in collaborations. We believe that this reflected an increase in adaptability among the threat actors, moving resources to these task force-like groups in moments of necessity, much like the level of organizations from very mature cyber threat groups such as Chinese APTs. Tracking APT43 actors during this time proved difficult as tactics and tooling from the threat actors were utilized for both efforts supporting the nuclear and strategic policy Priority Intelligence Requirements (PIR), and new PIRs regarding COVID-19 vaccine information. Mandiant assesses that DPRK's cyber organizational structure, post-pandemic, likely resembles Figure 2.

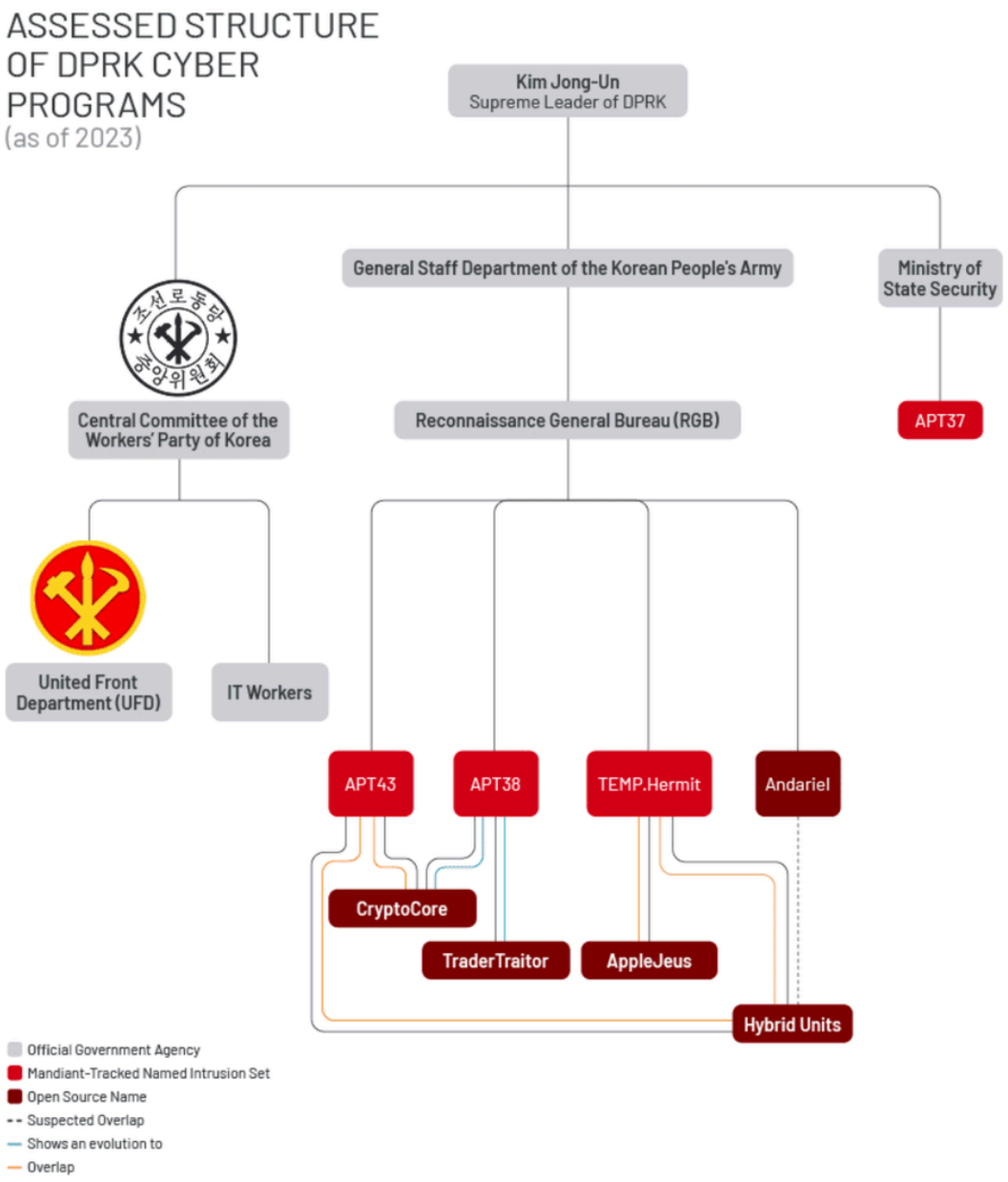


Figure 2: New organizational chart factoring in evolved, overlapped groups and removing Bureau alignment due to fluidity realignment of DPRK cyber organizations

Current Assessment

Based on the history the details that follow, Mandiant assesses that the DPRK's cyber landscape has evolved to a streamlined organization with shared tooling and targeting efforts.

Operators within these units quickly change their current focus and begin working on separate, unrelated efforts such as ransomware, collecting information on conventional weapons, nuclear entity targeting, blockchain and fintech targeting efforts, among various others. This flexible approach to tasking makes it difficult for defenders to track, attribute, and thwart malicious activities, while enabling this now collaborative adversary to move stealthily with greater speed and adaptability.

The level of shared targeting and tooling leads Mandiant to believe that shifts are continuing to occur throughout all parts of the DPRK's cyber apparatus. Investigations regarding the cooperation between groups not assessed to be RGB continue to produce information, but are still largely unknown.

At this time, it is unknown whether APT37 remains focused on MSS intelligence requirements or if its priorities have shifted. Throughout 2023, APT37 has increased activity, targeting a variety of victims, some of which align with our current understanding of MSS PIRs, while others do not. The MSS role in monitoring business dealings with the North Korean government and defectors, or entities outside of the country, suggest it is likely that the MSS would have some involvement in supervision of the forward deployed IT workers.

In late March 2023, public reporting described the exposure of a suspected APT37 GitHub repository containing samples, files, and additional tooling. The repository is reportedly linked to one member of APT37 and has been used for staging infrastructure since at least 2021.

- The decoy documents and files identified in the repository focused on a variety of themes, but appeared to be focused on organizations in the education, government, and financial sectors. Many of the victims and targets appear to be based in South Korea, based on the usage of HWP files and themes.
- Additionally, several of the documents focused on resumes, CVs and references, which may be leveraged to apply to various job openings, or used to target journalists. This is prominent activity Mandiant has observed several other actors, like APT43, conducting.
- In February 2023, open-source reporting identified APT37 allegedly disguising malware as a password file and distributing it as a compressed file. Open-source reporting mentions LOGCABIN as the delivered payload, a malware Mandiant attributes to APT43.

Also in March, Mandiant responded to a series of North Korean operations we track as UNC4736 (which overlaps with public AppleJeus reporting) that leveraged software supply chain attacks against 3CX and Trading Technologies to steal credentials and gain access to multiple networks.

The UNC4736 supply chain attacks were sophisticated and involved the use of a variety of tools, including both open source projects, such as DAVESHELL and SIGFLIP, and custom malware with more advanced capabilities.

In July 2023 Mandiant responded to additional North Korea nexus supply chain attacks, again tracked under UNC4899. We believe this activity was likely conducted by the same actor that has been publicly reported as TraderTraitor. Both UNC4899 and UNC4736 operations show a high level of sophistication and consistency targeting supply chain providers as a means to gain access to arbitrary networks to expand the potential foothold of their operators in order to select networks of interest.

These most recent events suggest that DPRK operations may be evolving towards more aggressive and broader intrusions and that these threat actors are able to conduct multiple intrusions to multiple networks, leveraging the supply chain vector.

Current Groups

Mandiant maintains, tracks, and reports campaign history on North Korea's offensive cyber operations. The following are the most prevalent groups Mandiant currently tracks, along with a brief summary of each threat

group, and primary targeting priority/priorities. Note: The groups that follow are referred to with their Mandiant designations (UNC numbers) alongside the names that have been used publicly to identify activity we attribute to the underlying group. While we believe that these definitions are largely congruent, differences in visibility and analytic tradecraft mean that an exact match is unlikely.

Andariel (UNC614): This actor targets foreign businesses, government agencies, financial services infrastructure, private corporations, and the defense industry. UNC614 also engages in cyber crime as an extra source of income to fund their operations, including the ransoming of hospitals, using their own ransomware malware dubbed MAUI. However, their primary focus is on targeting military and government personnel.

This cyber group stands apart from the other DPRK aligned groups and typically does not fall into the blending and targeting that the others may do. Some groups have espionage and financial focuses, but Andariel is tasked to acquire information to “build” the weapons of mass destruction or research and development programs in other targeted fields, like pharmaceuticals.

The targeting trends, such as nuclear, aerospace, high heat molds, etc. and overall successful compromises of this actor make it quite possibly the scariest of all the DPRK affiliated groups.

- Primary targeting: Defense, Aerospace, Healthcare (when self-funding operations), Nuclear

TEMP.Hermit: TEMP.Hermit, is an actor that has been active since at least 2013. Their operations since that time are representative of Pyongyang's efforts to collect strategic intelligence to benefit North Korean interests. This actor targets government, defense, telecommunications, and financial institutions worldwide and the term “Lazarus Group” refers most often to this cluster of activities. AppleJeus maintains overlap with this organization, but TEMP.Hermit’s targeting continues to focus on espionage related activities and not cryptocurrency as its primary focus.

- Primary targeting: Government, Defense, Telecommunications

AppleJeus (UNC1720): A threat group that has been active since at least 2018. It is assessed to primarily target the cryptocurrency industry with the goal of stealing digital assets to fund the regime’s priorities. The group uses a variety of tactics, including spear-phishing emails and fake cryptocurrency trading software, to infiltrate target systems and steal cryptocurrency. Like TraderTraitor, this crypto-focused group appeared to emerge after the notoriety that came with the Bangladesh heist and issues with stealing and laundering traditional currency. This group’s tools overlap with TEMP.Hermit, but is not focused on the same targeting profiles, potentially indicating shared resources.

- Primary targeting: Cryptocurrency

APT37: APT37's assessed primary mission is covert intelligence gathering in support of DPRK's strategic military, political, and economic interests. The group has been observed targeting a wide range of industries, primarily in South Korea. This organization is most closely aligned with the efforts of the MSS and its overarching cyber activities highlight the monitoring of defectors abroad and foreign elements interacting with DPRK.

- Primary targeting: Defectors, Governments

APT38: APT38 is a financially motivated group, known for significant financial compromises and its use of destructive malware against financial institutions. The group has been attributed to sophisticated compromises targeting Interbank Fund Transfer Systems to steal millions of dollars at a time across multiple countries worldwide. Current activity from this group is conducted by associated subgroups. Mandiant identified a long hiatus of activity attributed to APT38, which may be indicative of modifications and regrouping of APT38 operators to other units aligned with new priorities and needs.

- Primary targeting: Financials

APT43: APT43 is a prolific cyber operator that directly supports intelligence gathering interests of the North Korean regime. The group combines moderately sophisticated technical capabilities with aggressive social engineering tactics, especially against South Korean and US-based government organizations, academics, and think tanks focused on Korean peninsula geopolitical issues.

This organization acts as an intelligence arm and seeming embassy replacement for the RGB and DPRK leadership writ large.

- Primary targeting: Governments, Nuclear, Foreign Relations

CryptoCore (UNC1069): A threat actor that has been active since at least 2018. UNC1069 is a cryptocurrency focused group that may include individuals or units previously tracked as APT38, and while it has minor overlaps with APT43, we belive it is distinct. UNC1069 has targeted a variety of financial services firms and cryptocurrency exchanges, commonly employing spear-phishing techniques that result in LONEJOGGER malware infections. This organization appears to maintain a revenue generation priority, like its overarching APT38 subunits, however on a much smaller financial scale.

- Primary Targeting: Financials, Cryptocurrency

Hybrid Operations: Mandiant has observed operations that include tactics and tools from multiple groups, which suggests that in certain cases, operations may be undertaken by multiple groups that fluidly perform ad hoc tasks in support of another group, or due to temporary tasking. This is consistent with public reporting that identified a group that aligns with an alleged RGB Bureau, designated ‘325’, which was publicly announced in January 2021, when the structure of the RGB likely shifted in response to the COVID-19 pandemic.

Mandiant assesses that UNC2226 is one of the collections of activity supporting the aforementioned mission. UNC2226, like other seemingly ad hoc created efforts, appears to have changed or even expanded targeting to fulfill intelligence gathering efforts. Other clusters, such as UNC3782, have a similar composition and are focused on cryptocurrency theft among other seemingly ad hoc tasks.

The operations initially appeared to focus almost exclusively on intelligence gathering operations against COVID-19 research and vaccine development/manufacturing organizations. Over time, Mandiant perceived these operations shift from strictly COVID-19 efforts to the targeting of defectors, defense and governments, bloggers, media, cryptocurrency services, and financial institutions.

IT Workers: DPRK’s IT Workers, which according the the US Treasury department, primarily fall under the KWP’s Munitions Industry Department, are made up of thousands of highly skilled IT workers from North Korea.

They are reportedly deployed both domestically and abroad to generate revenue and finance the country's weapons of mass destruction and ballistic missile programs. These workers acquire freelance contracts from clients around the world and sometimes pretend to be based in the US or other countries to secure employment. Although they mainly engage in legitimate IT work, they have misused their access **to enable malicious cyber intrusions** carried out by North Korea.

TraderTraitor (UNC4899): TraderTraitor targets blockchain companies through spear-phishing messages. The group sends these messages to employees, particularly those in system administration or software development roles, on various communication platforms, intended to gain access to these start-up and high-tech companies. TraderTraitor may be the work of operators previously responsible for APT38 activity.

- Primary targeting: Cryptocurrency

Overlaps Emerge Over Time

APT38, Andariel, and TEMP.Hermit have historically been closely associated with each other and are assessed to be within the RGB. Sharing of resources is believed to be within the normal course of business for select factions that are likely in close proximity in Sinuiju, DPRK. However, the spike in overlapping infrastructure and tooling between these, and other groups, such as APT43, in addition to targeting overlaps amongst all groups, signals a shift in the DPRK cyber landscape. We believe that operators within North Korea may be co-located, or even sharing workstations, which can complicate attribution, as traditional tracking can potentially become misleading.

Procurement of infrastructure and domain registrants are also likely shared, further complicating clustering. For example, at the onset of the pandemic, Mandiant observed APT43 operations focusing on nuclear espionage and on COVID-19 treatment espionage. Andariel operators are now observed using the same infrastructure for exfiltration of pharmaceutical research and development, along with weapons development.

Cryptocurrency-Related Activity

The following have been observed as part of DPRK cyber operators' cryptocurrency usage and targeting

- Cryptocurrency usage in ransomware operations
- Cryptocurrency usage in hash rentals, self-funding of own operations
- Cryptocurrency themes used as lures and weaponized documents
- Theft of cryptocurrency from wallets, targeting cross chain bridges (Axie Infinity), targeting of cross chain bridges (Harmony), etc.

All assessed RGB-aligned groups maintain at least some interest in the cryptocurrency industry. Andariel and APT43 appear to have the least amount of focus on cryptocurrency efforts and have been identified using it primarily as a means to an operational end.

APT43 has targeted cryptocurrency and cryptocurrency-related services, using crafty and stealthy techniques to fund and sustain its own operations. Mandiant identified APT43 using cryptocurrency services to launder stolen currency. Associated activity included identified payment methods, aliases, and addresses used for purchases. APT43 operators also likely used hash rental and cloud mining services to launder stolen cryptocurrency into clean cryptocurrency.

- For a fee, these hash rental and cloud mining services provide hash power, which is used to mine cryptocurrency to a wallet selected by the buyer without any blockchain-based association to the buyer's original payments.
- Several payment methods were used for infrastructure and hardware purchases including PayPal, American Express cards, and Bitcoin likely derived from previous operations.

Throughout 2022 Mandiant identified Andariel using ransomware campaigns to fund additional malicious activity, especially cyber espionage operations. These activities are part of a larger ecosystem of money making schemes, including cryptocurrency targeting and freelancing work. The shift to ransomware to fund operations highlights the isolation of some groups from the rest of the regime, and the pressure to self-fund their operations.

Mandiant observed DPRK conducting a large-scale cryptocurrency phishing campaign targeting users of the Bitcoin, Arbitrum, Binance Smart Chain, Cronos, Ethereum, and Polygon blockchains during the latter half of 2022 and into 2023. This escalation in activity occurred after the DPRK successfully converted over $1 million in Ethereum assets to Bitcoin via the cross-chain bridge Ren Project. Mandiant assesses that the success of this hybrid cluster's operations likely have influenced APT43's expansion into Web3 operations.

In line with the increased focus on cryptocurrency targeting, CryptoCore was also observed targeting financial institutions and cryptocurrency entities throughout 2022. This group has targeted multiple financial verticals (including investing, transaction processing, and cryptocurrency) across North America, Europe, and East Asia with LONEJOGGER malware. In August 2022, Mandiant discovered new LONEJOGGER samples and decoy files that reinforced the group's interest in cryptocurrency. In the samples and malware laden decoy documents were entities like a legitimate American hedge fund specializing in cryptocurrency and digital asset platform that deals in the holding, investing, and infrastructure of cryptocurrency and cryptocurrency products.

In late 2022, the group was identified leveraging several lure documents relating to cryptocurrency, as well as other financial entities including investment firms and banks. In addition to targeting crypto and leveraging lure material, the CryptoCore grouping of clusters has been observed masquerading as crypto institutions from around the globe.


cogent economics & finance

Taylor & Francis

Cogent Economics & Finance

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/oaef20

A Bitcoin price prediction model assuming oscillatory growth and lengthening cycles

Guizhou Wang & Kjell Hausken |

To cite this article: Guizhou Wang & Kjell Hausken | (2022) A Bitcoin price prediction model assuming oscillatory growth and lengthening cycles, Cogent Economics & Finance, 10:1, 2087287, DOI: 10.1080/23322039.2022.2087287

To link to this article: https://doi.org/10.1080/23322039.2022.2087287

Figure 3: Bitcoin Bull Prediction.pdf, lure document

Defector Targeting Highlights Consistency Across Groups and Time

Lee Min-Bok (LMB) is an example that highlights shared targeting between groups. Mandiant has observed APT37, APT43, and both of DPRK's hybrid clusters targeting Lee. Lee Min-bok is a North Korean defector who previously worked for the Agricultural Research Institute in Pyongyang until 1991, when he began efforts to defect to South Korea. Until 2018 Lee had sent information attached to balloons along with anti-Pyongyang leaflets into North Korea.

This consistency in targeting is mirrored by the consistency over time between the current and historic organization of DPRK cyber operations. While little is publicly reported about the North Korea's cyber organziation, referred to as "Room 35", and their operations prior to the 2009 reorganization, which is an organization that allegedly develops malware and intrusion tools to collect information on its targets and build intelligence reports for senior DPRK officials. The information that is available about this organization directly corresponds to operations observed by Mandiant, and when supplemented with Mandiant intelligence, does show hints at the "why" and "how" in some instances, such as the case for LMB's targeting. Reorganizations may take place, tools and infrastructure may be shared, but targeting and fulfillment of PIRs remain intact at this time.

Table 1 shows the identified overlaps and similarities between reported Room 35's operations and activities, with observed APT43 characteristics and activities.

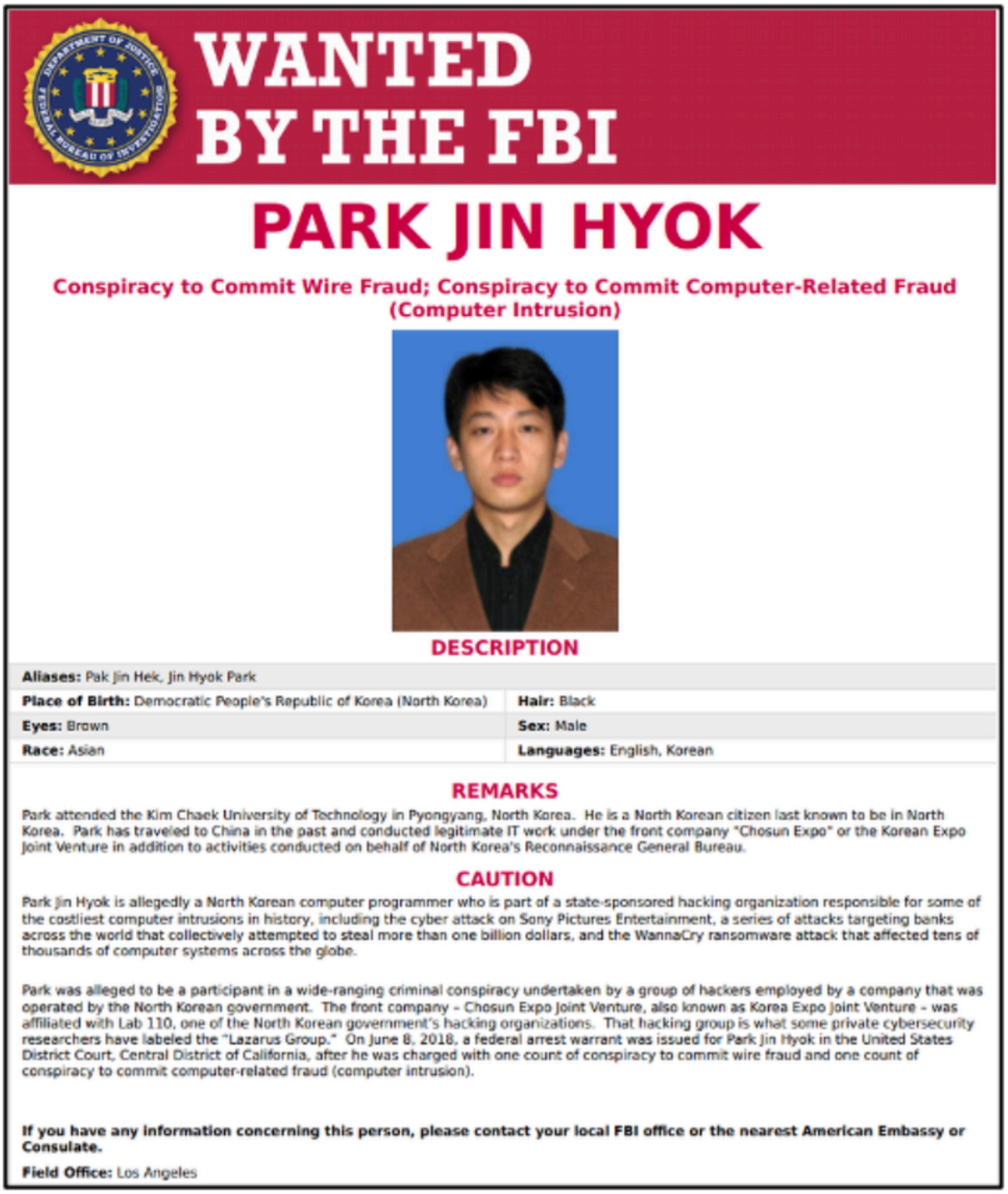
Room 35	**APT43**
Gathers data to generate internal briefs and reports that provide insights and recommendations to the higher echelons of leadership in the government.	Appears to gather information to answer leadership and regime level PIRs.
The main focus of its mission is directed towards several nations in Europe, along with the Republic of Korea (ROK), the United States, and Japan.	Consists of sub teams focusing on ROK, US, and Japan, with sporadic targeting throughout Europe.
The group enables a small skilled and efficient team of hackers to create malware and hacking tools for gathering information on their targets, which is then used to compile intelligence reports.	APT43's efforts rely on social engineering in addition to some malware that appears to be created within the organization. APT does not appear to be as large as other units such as APT38, Andariel, and TEMP.Hermit.

A secondary mission for Room 35 is allegedly "to generate profit to support and fund the tools and resources used in their primary mission."	APT43 conducts smaller financially focused side efforts such as cryptojacking and crypto theft likely in order to fund their own operations.
Chain of command is grouped with KWP Operations Department, CC KWP United Front Department (UFD), and the MSS.	Mandiant and open source reporting highlight the constant and common targeting overlaps between APT43 and mission mandates of the UFD and MSS.

Table 1: Similarities between alleged units prior to 2009 and related interests by APT43

DPRK Operator Activity Examples

Some of the DPRK-aligned cyber operators Mandiant tracks are highly skilled across numerous cyber endeavors. Operators have demonstrated the ability to conduct activities at high levels of sophistication and execution, then immediately pivot to separate tasks and maintain that same level of execution (i.e. blockchain and cryptocurrency targeting, espionage, ransomware, supply chain targeting). Highlighting past Department of Justice indictments (see Figure 4 and Figure 5) illustrates how a single individual can supplement vastly different efforts.



WANTED BY THE FBI

PARK JIN HYOK

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

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company – Chosun Expo Joint Venture, also known as Korea Expo Joint Venture – was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, 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).

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

Figure 4: Park Jin Hyok FBI Wanted Poster highlighting the range of skillsets within his RGB cyber role

Figure 5: Kim Il, RGB hacker, detailed in USG Indictment

Park Jin Hyok's (PJH) identified activities show adaptability and flexibility, based on mission requirements:

- In 2014, PJH was involved in the attack on Sony Pictures Entertainment in retaliation for the release of "The Interview," which depicted the assassination of the DPRK's leader. Operator then targeted other victims in the entertainment industry and stole confidential data, threatened executives and employees, and damaged thousands of computers.
- In 2016, he was involved in stealing $81 million from Bangladesh Bank by compromising their computer network with spear-phishing emails and sending fraudulently authenticated SWIFT messages to transfer funds to other countries.
- In 2017, he was connected to the development of the ransomware WannaCry 2.0, which infected hundreds of thousands of computers around the world.
- In 2016 and 2017, he was involved in targeting US defense contractors, including Lockheed Martin, using spear-phishing emails.

- In the time between the Sony attack and the arrest warrant issued, PJH was observed on job seeker platforms alongside DPRK's IT workers.

Identified Malware Sharing Supports Public Reports of Combined Task Forces

As stated previously, open-source reporting in early 2021 described the creation of "Bureau 325," a collaborative effort between separate North Korean cyber operations targeting COVID-19-related information. According to Daily NK, a new organization dubbed Bureau 325 was formalized just before North Korea's Eighth Party Congress in January 2021, and, unlike prior cyber operations, reported its COVID-19-focused efforts directly to Kim Jong Un. Notably, Bureau 325 reportedly includes individuals previously assigned to existing groups.

- According to Reuters, in mid-November 2020, Microsoft observed North Korean espionage activity at vaccine makers in multiple countries. This observation match our assessment about targeting and corresponded to CUTELOOP and PENDOWN activity Mandiant detected targeting pharmaceuticals.
- In some instances, defense job related lures were used against pharmaceutical entities, suggesting that a shift toward healthcare and pandemic-related targeting was abrupt and unexpected. Later, more relevant social engineering lures and new malware were employed suggesting a more complete shift toward the focus on COVID-19.
- Mandiant observed domain registrants overlap between APT43 and the COVID centric cyber campaigns. This is further evidence that these organizations are close bureaucratically and share resources.

Malware and Tooling

Cyber groups within the DPRK ecosystem continue sharing tooling and malware. Figure 6 is a visual breakdown of malware families and their associated actors. These malware families seem to be given in order for the newer units to create their own group-tailored family. For example, APT43's PENCILDOWN malware changed to the new group's PENDOWN malware family.

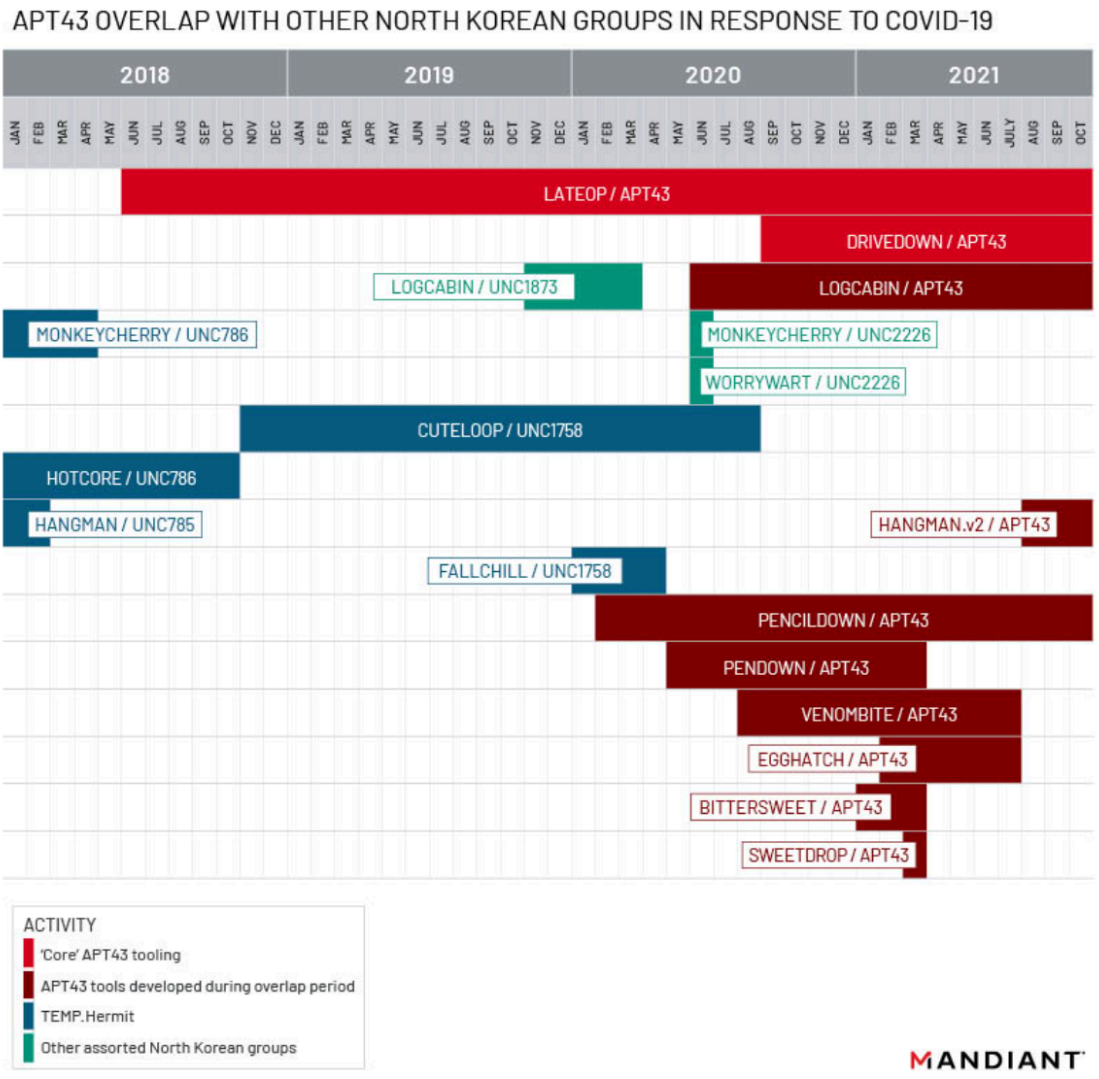


Figure 6: Malware tools leveraged by TEMP.Hermit and linked groups (green), APT43, and suspected linked groups (red), and those overlapping with COVID-19 -focused operations (blue)

Another instance where resources were likely shared between groups was with ROCKHATCH malware (bcac28919fa33704a01d7a9e5e3ddf3f). ROCKHATCH was discovered being used as part of a suspected Andariel operation.

- The malware uses the key 74 61 51 04 77 32 54 45 89 95 12 52 12 02 32 73, which was also used in samples of , a HANGMAN.V2 (21cffaa7f9bf224ce75e264bfb16dd0d) malware used by APT43, and, CAKETEARS malware (1ecd83ee7e4cfc8fed7ceb998e75b996) which is primarily associated with TEMP.Hermit
    - HANGMAN.V2 itself is a variant of TEMP.Hermit's HANGMAN malware, but has only been observed used with APT43 infrastructure
- ROCKHATCH uses the same uninstall script seen in TEMP.Hermit’s FALLCHILL and HANGMAN malware.

While Mandiant have observed DPRK operators share tools and resources, different threat actors have used tailored tools including multi-platform malware such as POOLRAT, a backdoor that allowed threat actors to

collect system data and to execute commands and that has Windows, Linux and macOS variants as well as dedicated implants for macOS like FULLHOUSE.DOORED, which shows an increased interest in the development of macOS malware to backdoor platforms of high value targets within the cryptocurrency and the blockchain industries.

Outlook and Way Ahead

The years of public reporting on multiple DPRK aligned cyber units as “Lazarus Group" moniker have come full circle. The shifting DPRK cyber landscape is increasingly characterized by resource sharing and temporary collaboration. We believe that this will make precise attribution more difficult.

Some increased fidelity is likely to arrive as additional data is collected, and may help better scope groups and identify any specialized in targeting specific industries or sectors.

Malware infrastructure overlaps indicating resources and attribution muddled by shifting assignments show how DPRK cyber operations are changing. However, operations conducted to fulfill regime requirements remain steadfast and we believe they will continue. While defenders may not be able to easily sort new DPRK activity into a previously identified bucket, the malware reuse and shared resources creates opportunities for detection and country level attribution.

Posted in

- Threat Intelligence
