FireEye

APT38

Un-usual Suspects

EXECUTIVE SUMMARY

APT38 is a financially motivated North Korean regime-backed group responsible for conducting destructive attacks against financial institutions, as well as some of the world's largest cyber heists. Based on widely publicized operations alone, the group has attempted to steal more than $1.1 billion.

Instead of simply obtaining accesses and moving to transfer funds as quickly as possible, APT38 is believed to operate more similarly to an espionage operation, carefully conducting reconnaissance within compromised financial institutions and balancing financially motivated objectives with learning about internal systems.

APT38 shares malware code and other development resources with TEMP.Hermit North Korean cyber espionage activity, although we consider APT38's operations more global and highly specialized for targeting the financial sector.

The group has compromised more than 16 organizations in at least 11 different countries, sometimes simultaneously, since at least 2014.

Since the first observed activity, the group's operations have become increasingly complex and destructive. APT38 has adopted a calculated approach, allowing them to sharpen their tactics, techniques, and procedures (TTPs) over time while evading detection.

Table of Contents

●●●

Re-evaluation of North Korean State-Sponsored Activities

In 2018, we began an intensive review of North Korean state-sponsored cyber operations based on activity that we had previously attributed to TEMP.Hermit, related data derived from Mandiant forensic investigations, FireEye appliances, FireEye iSIGHT Intelligence collections, and public reporting associated with the "Lazarus" (aka Hidden Cobra) group. Investigating intrusions of many victimized organizations has provided us with a unique perspective into the entire attack lifecycle. As a result of this review, we are separating a cluster of activity distinct enough to be tracked separately from TEMP.Hermit. We now refer to this financially motivated group as APT38.

- APT38 is a financially motivated group linked to North Korean cyber espionage operators, renown for attempting to steal hundreds of millions of dollars from financial institutions and their brazen use of destructive malware.

- APT38 executes sophisticated bank heists typically featuring long planning, extended periods of access to compromised victim environments preceding any attempts to steal money, fluency across mixed operating system environments, the use of custom developed tools, and a constant effort to thwart investigations capped with a willingness to completely destroy compromised machines afterwards.

- A 2016 Novetta report detailed the work of security vendors attempting to unveil tools and infrastructure related to the 2014 destructive attack against Sony Pictures Entertainment. This report detailed malware and tactics, techniques, and procedures (TTPs) that the researchers believed were linked to a set of developers and operators they dubbed "Lazarus," a name that has become largely synonymous with aggressive North Korean cyber operations. We tracked many of these indicators and campaigns as TEMP.Hermit.

- Attribution to both the "Lazarus" group and TEMP.Hermit was made with varying levels of confidence primarily based on similarities in malware being leveraged in identified operations. Over time these malware similarities diverged, as did targeting, intended outcomes, and TTPs, almost certainly indicating that TEMP.Hermit activity is made up of multiple operational groups primarily linked together with shared malware development resources and North Korean state sponsorship.

- Because APT38 is backed by (and acts on behalf of) the North Korean regime, we opted to categorize the group as an "APT" instead of a "FIN." This also reflects that APT38's operations closely resemble espionage-related activity.

- We will continue to refer to TEMP.Hermit and related North Korea-sponsored activity as appropriate, minus the distinct operations we are now attributing to APT38.

Targeting and Mission

Based on observed activity, we judge that APT38's primary mission is targeting financial institutions and manipulating inter-bank financial systems to raise large sums of money for the North Korean regime. Increasingly heavy and pointed international sanctions have been levied on North Korea following the regime's continued weapons development and testing. The pace of APT38 activity probably reflects increasingly desperate efforts to steal funds to pursue state interests, despite growing economic pressure on Pyongyang. Since 2015, APT38 has attempted to steal hundreds of millions of dollars from financial institutions. Some of the publicly reported attempted heists attributable to APT38 include:

- Vietnam TP Bank in December 2015
- Bangladesh Bank in February 2016
- Far Eastern International Bank in Taiwan in October 2017
- Bancomext in January 2018
- Banco de Chile in May 2018

Bank Targeting

APT38 has pursued their main objective of targeting banks and financial entities since at least 2014[1]. In late 2015, their operations escalated as they attempted to conduct fraudulent transactions for the first time. Throughout 2016, APT38 pursued geographically diverse targets at a notable rate. While APT38 is financially motivated, we believe that in certain instances, they targeted entities solely for infrastructure to facilitate follow-on operations or help evade detection.
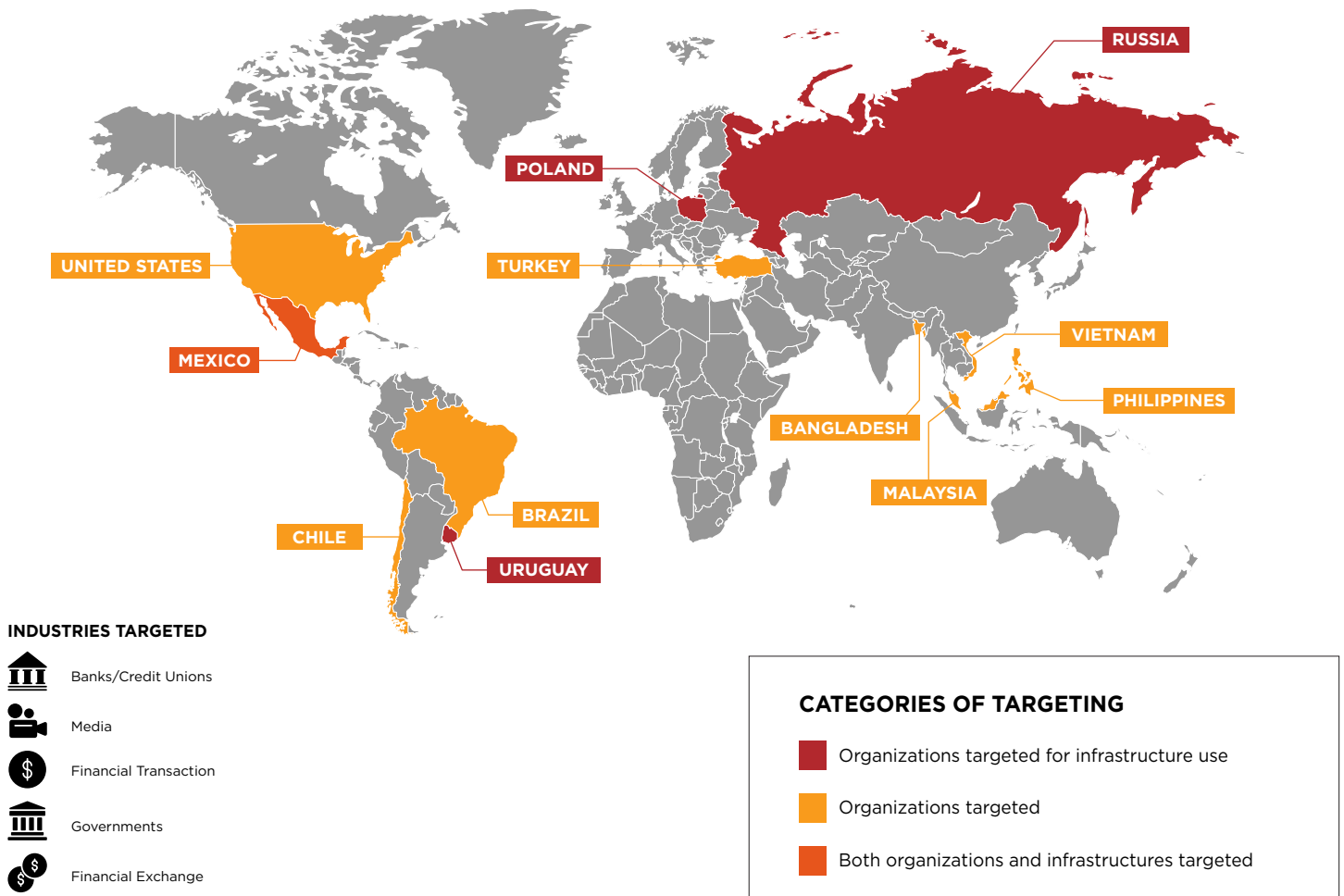
During our review, multiple public incidents have been reportedly linked to this body of activity based largely on their targeting of SWIFT systems. We are currently tracking a variety of suspected events that have varying degrees of associations to APT38. Although we cannot confirm these instances were conducted by APT38, we have observed some overlaps between these publicly reported events and APT38 based on the timing and location of targeting, malware, and general TTPs used.

- A recent criminal complaint, unsealed on Sept. 6, 2018, by the U.S. Department of Justice (DOJ) detailing links between APT38, additional TEMP.Hermit activity, and the North Korean regime, named an African bank that appears to have been targeted in early 2016. The bank was allegedly targeted with the NESTEGG backdoor and involved an attempted theft of approximately $100 million. This compromise overlaps with APT38's use of NESTEGG and the general timing of APT38 operations in early 2016.

- The DOJ complaint detailed a Southeast Asian bank targeted in late 2015 and 2016. This coincides with APT38's targeting of organizations in Southeast Asia, including entities located in Vietnam, Malaysia, and the Philippines throughout 2016. The DOJ complaint also detailed adversary use of a shared password between Bangladesh Bank, the African bank and Southeast Asian bank, providing evidence of further TTP overlap with APT38.

- Per public reporting, threat actors targeted Banco del Austro in Ecuador with fraudulent SWIFT transactions in 2015. While we have limited insight into this targeting, we have identified APT38 targeting South American entities previously.

- In August 2018, threat actors targeted Cosmos Bank in India using both fraudulent ATM and SWIFT transactions. Public reports have indicated that individuals located in India were used to assist in withdrawing fraudulent funds. While we have not observed APT38 target ATMs, the use of individuals in country to carry out attacks is similar to public reporting of APT38 leveraging individuals to launder money after SWIFT attacks.

---

1   The characterizations in this report are based upon our visibility and public reporting of activity. There are potentially additional banks and financial entities affected by APT38 that have not been publicized due to sensitivities and a lack of open reporting about such events. Reports or investigations of future incidents may expand our understanding of APT38's targeting.

Figure 1. APT38 global targeting.

INDUSTRIES TARGETED

🏛 Banks/Credit Unions

📹 Media

$ Financial Transaction

🏛 Governments

$ Financial Exchange

CATEGORIES OF TARGETING

■ Organizations targeted for infrastructure use

■ Organizations targeted

■ Both organizations and infrastructures targeted

Other Targeting

Although the group's primary targets appear to be banks and other financial organizations, they have also targeted countries' financial governing bodies as well as media organizations with a focus on the financial sector. We surmise that the targeting of banks, media, and government agencies is conducted in support of APT38's primary mission.

• In late 2016, APT38 most likely deployed strategic web compromises (watering holes) at cryptocurrency-focused media organizations during the cryptocurrency bubble. These sites attracted significant traffic from financial institutions as they were seeking more

information on different cryptocurrencies and initial coin offering. This incident was previously reported under TEMP.Hermit.

• The group targeted news outlets known for their business and financial sector reporting, probably in support of efforts to identify and compromise additional financial institutions. These incidents were previously reported under TEMP.Hermit.

• APT38 also targeted financial transaction exchange companies likely because of their proximity to banks.

Figure 1 displays a map of countries associated with organizations that we can confirm were targeted by APT38.

Figure 2. North Korean operator posting in an underground forum.

looking for a silent doc exploit

[closed@HF:]

Posts:	13
Threads:	3
Reputation:	0
Bytes:	0

12-04-2015, 09:01 AM

I am looking for a silent doc exploit that runs on latest versions of office and Windows.

If any one send me a sample doc and it runs successfully I will buy.

Contact

campbelldavid793@gmail.com
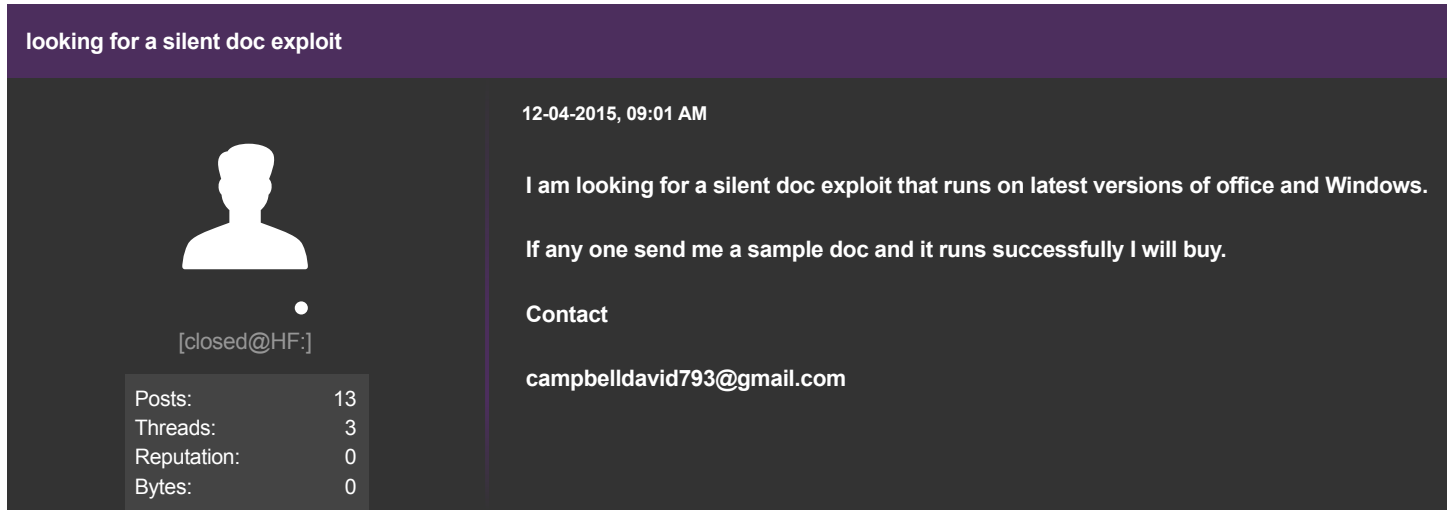
Relationship to other North Korean State-Sponsored Activities

While the DOJ complaint highlighted potential links between major incidents associated with the North Korean regime, we believe these links provide insight to the much larger cyber initiatives conducted by the regime and are not bound by motivation or operation. The complaint details a complex web of social media accounts, infrastructure, links to a North Korean government front organization, developers and operators associated with initial reconnaissance of victim organizations, as well as malware similarities observed between intrusions. These links provide support for the operations being carried out under the direction of the North Korean government, as well as giving insight into the scale and scope required to carry out these large-scale operations.

- The details provided in the DOJ allegations include specifics about the email accounts and infrastructure that were leveraged across multiple operations, such as:

  — In December 2015, a North Korean operator associated with the email account (campbelldavid793@gmail.com) was observed posting in underground forums (as shown in Figure 2) asking for a "silent doc exploit."

  — This email account was later observed sending spear-phishing emails to a U.S. defense contractor.

  — The North Korean IP address that was used to access the email account was also used to access another account (wangchung01@gmail.com).

  — This email account was associated with testing content in spear-phishing emails that was later observed in spear-phishing emails sent to Bangladesh Bank.

- The DOJ complaint provided insight into overlaps in operator accounts used to conduct reconnaissance against a U.S. defense contractor, Sony Pictures Entertainment, and actors associated with their movie *The Interview*, Bangladesh Bank, and other related organizations. It stated that the operators conducted online research on the targeted organizations and individuals related to those organizations. The operator accounts purportedly sent out LinkedIn invitations to the related individuals, and operators later sent spear-phishing messages to many of these individuals.

- The complaint also detailed similarities in malware observed in targeting different organizations.

  — Allegations against the subject of the complaint, Park Jin Hyok, tie him to multiple campaigns, including the SWIFT fraud incidents we now attribute to APT38, targeting of aerospace and defense contractors we still attribute to TEMP.Hermit, and the release of WANNACRY ransomware.

  — Specific technical details regarding some of these overlaps are outlined in the Malware section of this report.

We assess with high confidence that the concurrent targeting of multiple organizations in the entertainment, defense, and financial industries would require a significant amount of resources and multiple teams dedicated to achieving specific objectives.

• The overlapping accounts used to research the affected organizations provides some indication that the same ultimate sponsor ordered the reconnaissance activity of the targeted organizations.

• Most likely, the skillset of those conducting phishing and post-compromise operations are different and those job functions may also be separated. At one victim, for example, there was a significant time gap between the observed spear-phishing associated with operators outlined in the complaint and the observed activity associated with the attempted heists, providing some indication that the spear-phishing was not necessarily conducted by the same actor attempting the heist.

— Given the lapse in time between the spear-phishing and the heist activity in the above example, we suggest two separate but related groups under the North Korean regime were responsible for carrying out missions; one associated with reconnaissance (TEMP.Hermit or a related group) and another for the heists (APT38).

— Another potential explanation is that in many cases it was difficult to identify the original method of infection at the affected financial institutions (APT38 is adept in covering their tracks), making it difficult for forensic analysts to trace operations back to the original source.

• Similarities in malware observed at the victim organizations is a likely indication that the attackers had access to either shared development resources or the same code repository.

Connections between APT38, TEMP.Hermit, and additional linked incidents and organizations are notionally depicted in Figure 3 below. Park Jin Hyok's involvement as detailed in the DOJ complaint most likely indicates that he had a malware and/or operational development role and that his work was shared with multiple North Korean operations across different motivations.

• Park's connections to Lab 110, a cyber-focused North Korean military unit, and its front organizations were summarized in the DOJ complaint. These ties are detailed further in the section Links to North Korean Military Units.

• Park's activities are linked to multiple incidents typically described in public reporting as broadly linked to "Lazarus," including WANNACRY and the targeting of the entertainment industry. Although malware similarities and common sponsorship link these incidents to Park, there is significant differentiation between APT38 and these other related clusters of activity.

• APT38, in particular, is strongly distinguishable because of its specific focus on financial institutions and operations that attempt to use SWIFT fraud to steal millions of dollars at a time. Despite toolset overlap, this is significantly different from TEMP.Hermit's more traditional espionage-driven activity and distinct from other operations publicly lumped together as "Lazarus."

Figure 3. Notional depiction of APT38's connections to other North Korean state-sponsored operations
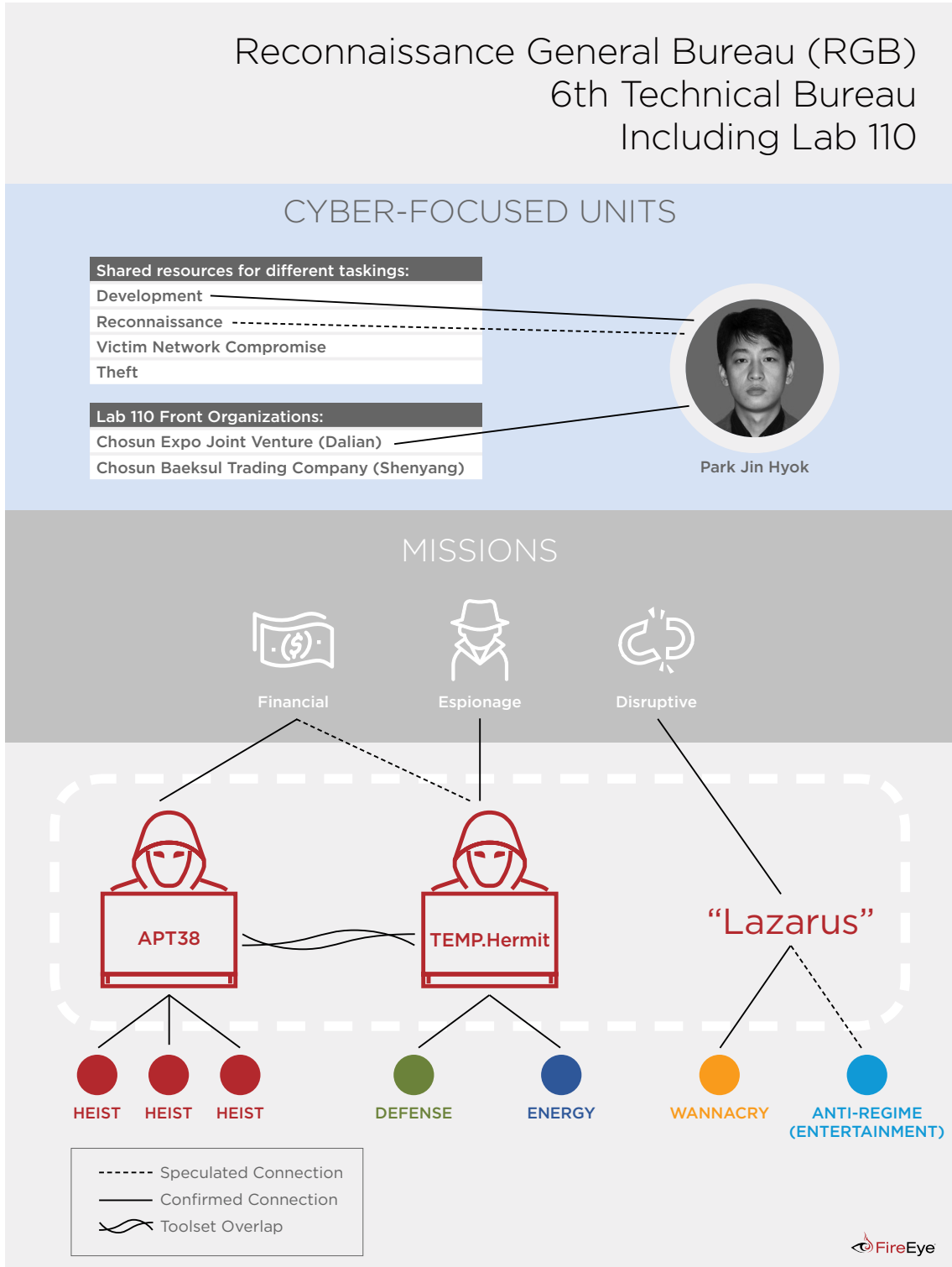
We can confirm that the APT38 operator activity is linked to the North Korean regime, but maintains a set of common characteristics, including motivation, malware, targeting, and TTPs that set it apart from other state-sponsored operations.

- APT38's operations, malware, and motivations are distinct from TEMP.Hermit.

  — As previously mentioned, we assess with high confidence that APT38's mission is focused on targeting financial institutions and financial systems to raise money for the North Korean regime. In contrast, TEMP.Hermit is a cluster of North Korean-sponsored cyber espionage activity that has primarily targeted defense and government entities; we believe its mission is to collect strategic intelligence against countries that would benefit North Korean interests and dissident activity deemed a threat to the regime. TEMP.Hermit's scope is broader in general as well, also targeting energy research in 2015 and electrical utilities in 2017.

  — Since at least the beginning of 2014, APT38 operations have focused almost exclusively on developing and conducting financially motivated campaigns targeting international entities, whereas TEMP.Hermit is generally linked to operations focused on South Korea and the United States. For example, TEMP.Hermit's July 2017 targeting of U.S. aerospace defense contractors was likely a result of political conflicts concerning North Korea's missile program and South Korea's missile-defense plans.

- Public reporting typically reports the financially motivated activities associated with the heists as a subgroup of Lazarus, such as "Bluenoroff" by Kaspersky and "Stardust Chollima" by CrowdStrike.

- Further, APT38's toolset is significantly more specialized. Malware such as DYEPACK (a suite of tools that manipulates local data from SWIFT servers) is specifically designed to consider the intricacies and complex nature of banking transaction systems, such as SWIFT.

It is important to note that not all financially motivated North Korean activity is attributable to APT38.

- While the broader TEMP.Hermit group has been observed targeting other financial-related organizations associated with cryptocurrency, our data did not demonstrate these incidents had infrastructure, malware, targeting, or timing overlap with other APT38-attributed operations.

- APT37 (Reaper), another North Korean state-sponsored group, targeted a Middle Eastern financial company, but there was no evidence of financial fraud.

  — This organization was likely targeted by APT37 because it pulled operations out of North Korea.

  — There are no apparent overlaps between APT37 and APT38's infrastructure and focus on targeting financial organizations. Although APT37 has previously targeted the financial sector, it does not focus specifically on stealing money as APT38 does.

Effect of Sanctions

While North Korean cyber operations against specific countries may have been driven by diplomatic factors and perceived insults against Pyongyang, the application of increasingly restrictive and numerous financial sanctions against North Korea probably contributed to the formation of APT38's core mission and operations.
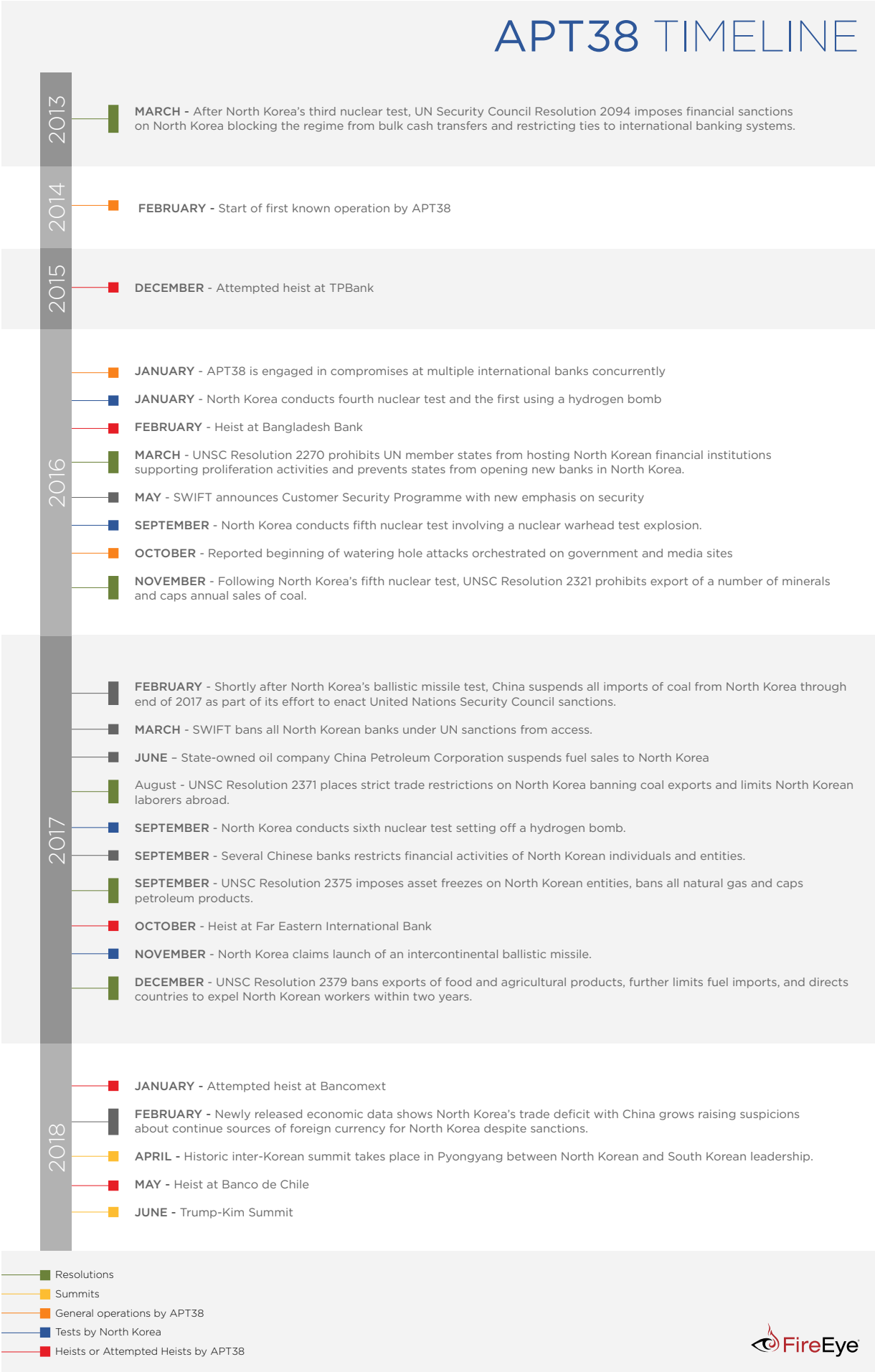
- APT38's operations began in February 2014 and were likely influenced by financial sanctions enacted in March 2013 that blocked bulk cash transfers and restricted North Korea's access to international banking systems.

- Sanctions enacted in 2016 in March and November broadened limitations and further curtailed North Korea's access to both funds and the international financial system by terminating joint ventures and prohibiting states from opening new bank branches in North Korea. Multiple rounds of sanctions in a single year likely increased pressure for North Korea to come up with funds quickly as evinced by their attempted heist in February 2016 only two months after a foiled attempt in December 2015. Despite being engaged in multiple active compromises in January 2016, new sanctions may have contributed to APT38's escalation in targeting via watering hole attacks in October 2016.

- Multiple sanctions were enacted again in 2017, and they may have continued to influence the speed of APT38's attempted heists with sanctions occurring in September and December 2017, and attempted heists taking place the following month in October 2017 and January 2018, respectively.

A detailed listing of these and other significant events surrounding the major attempted heists by APT38 is outlined in Figure 4 below.

---

2 It was widely reported that North Korean operators carried out a destructive attack against Sony Pictures Entertainment for the movie The Interview due the perception that it was directly insulting to the North Korean regime.

APT38 TIMELINE

Figure 4.
APT38 operations and North Korea's worsening financial situation

2013

MARCH - After North Korea's third nuclear test, UN Security Council Resolution 2094 imposes financial sanctions on North Korea blocking the regime from bulk cash transfers and restricting ties to international banking systems.

2014

FEBRUARY - Start of first known operation by APT38

2015

DECEMBER - Attempted heist at TPBank

2016

JANUARY - APT38 is engaged in compromises at multiple international banks concurrently

JANUARY - North Korea conducts fourth nuclear test and the first using a hydrogen bomb

FEBRUARY - Heist at Bangladesh Bank

MARCH - UNSC Resolution 2270 prohibits UN member states from hosting North Korean financial institutions supporting proliferation activities and prevents states from opening new banks in North Korea.

MAY - SWIFT announces Customer Security Programme with new emphasis on security

SEPTEMBER - North Korea conducts fifth nuclear test involving a nuclear warhead test explosion.

OCTOBER - Reported beginning of watering hole attacks orchestrated on government and media sites

NOVEMBER - Following North Korea's fifth nuclear test, UNSC Resolution 2321 prohibits export of a number of minerals and caps annual sales of coal.

2017

FEBRUARY - Shortly after North Korea's ballistic missile test, China suspends all imports of coal from North Korea through end of 2017 as part of its effort to enact United Nations Security Council sanctions.

MARCH - SWIFT bans all North Korean banks under UN sanctions from access.

JUNE – State-owned oil company China Petroleum Corporation suspends fuel sales to North Korea

August - UNSC Resolution 2371 places strict trade restrictions on North Korea banning coal exports and limits North Korean laborers abroad.

SEPTEMBER - North Korea conducts sixth nuclear test setting off a hydrogen bomb.

SEPTEMBER - Several Chinese banks restricts financial activities of North Korean individuals and entities.

SEPTEMBER - UNSC Resolution 2375 imposes asset freezes on North Korean entities, bans all natural gas and caps petroleum products.

OCTOBER - Heist at Far Eastern International Bank

NOVEMBER - North Korea claims launch of an intercontinental ballistic missile.

DECEMBER - UNSC Resolution 2379 bans exports of food and agricultural products, further limits fuel imports, and directs countries to expel North Korean workers within two years.

2018

JANUARY - Attempted heist at Bancomext

FEBRUARY - Newly released economic data shows North Korea's trade deficit with China grows raising suspicions about continue sources of foreign currency for North Korea despite sanctions.

APRIL - Historic inter-Korean summit takes place in Pyongyang between North Korean and South Korean leadership.

MAY - Heist at Banco de Chile

JUNE - Trump-Kim Summit

■ Resolutions
■ Summits
■ General operations by APT38
■ Tests by North Korea
■ Heists or Attempted Heists by APT38

FireEye

Tactics, Techniques and Procedures

Early Activities and Operations Development
Early APT38 operations suggest that the group began targeting financial institutions with an intent to manipulate financial transaction systems at least as early as February 2014, although we did not observe fraudulent transactions until 2015. These activities provide some indication of a learning period that would inform the development of TTPs later definitive of APT38 activity.

• We do not have evidence that the earliest targeted financial institutions were victimized by fraudulent transactions before APT38 left the compromised environments, possibly indicating that APT38 was conducting reconnaissance-only activity at that time.

• Initial operations targeted Southeast Asian financial institutions most likely because North Korea had better access to money laundering network in these countries.

• In early 2014, the group deployed NESTEGG (a backdoor) and KEYLIME (a keylogger) malware designed to impact financial institution-specific systems at a Southeast Asian bank. There is no evidence that these tools were used to target SWIFT systems at the time, even though the victimized bank used SWIFT. These factors most likely indicate that APT38 was still learning about various systems related to financial transactions.

• Details published by DOJ indicate that malware developers read user manuals for SWIFT systems, providing some indication of initial efforts to develop SWIFT-specific malware, such as DYEPACK. The earlier observed deployment of DYEPACK was in December 2015.

Based on observed incidents, we believe APT38 activities were initially clustered in Southeast Asia as the group built up its capabilities before expanding globally shortly after.

• Targeting in Southeast Asia likely spanned from February 2014 to late 2017.

• Expansion into other regions, such as Latin America and Africa, began in early to mid-2016. Latin American organizations have continued to be targeted into at least May 2018.

• APT38 operations extended to Europe and North America from approximately October 2016 to October 2017.

Scale of Operations

Based on the frequency and number of concurrent active operations, we have some indication that APT38 is a large operation with significant resources at its disposal. Furthermore, APT38 appears to have access to shared resources linked to TEMP.Hermit, most likely greatly increasing the number of personnel available to the group and the pace of malware development.

- From November 2015 through the end of 2016, APT38 was involved in at least nine separate compromises against banks. This is a large number of compromises for one group to conduct concurrently. The total number of concurrent compromises is likely to be even higher than this, especially when factoring in targeting outside of the financial industry as well as suspected APT38 activity detailed in the targeting section above. In addition, many of the operations were at different stages of the attack lifecycle throughout this time, adding to the complexity and effort required to manage all the operations simultaneously.

- The group conducted extremely thorough and time-consuming reconnaissance activities, demonstrating that it had both large numbers of personnel and the time to dedicate to lengthy operations. For example, in multiple instances, APT38 dedicated time to observing network activity and gathering critical information about users and systems that had access to SWIFT servers.

- APT38 maintained a large library of unique non-public backdoors and other utilities, detailed in the Malware section below. Additionally, APT38 continued to refine tools over time to incorporate additional tactics, including measures to evade detection. For example, threat actors modified DYEPACK to avoid writing the malware to disk by modifying the original stand-alone version to be used in memory inline.

- In addition to cyber operations, public reporting has detailed recruitment and cooperation of individuals located in-country to support with the tail end of APT38's thefts, including persons responsible for laundering funds and interacting with recipient banks of stolen funds. This adds to the complexity and necessary coordination amongst multiple components supporting APT38 operations.

A Modern Bank Heist at a Glance

At a high level, APT38's targeting of financial organizations and subsequent heist attempts have followed the same general pattern, as depicted in Figure 5 and explained below.

Figure 5. An APT38 cyber bank robbery

●●●
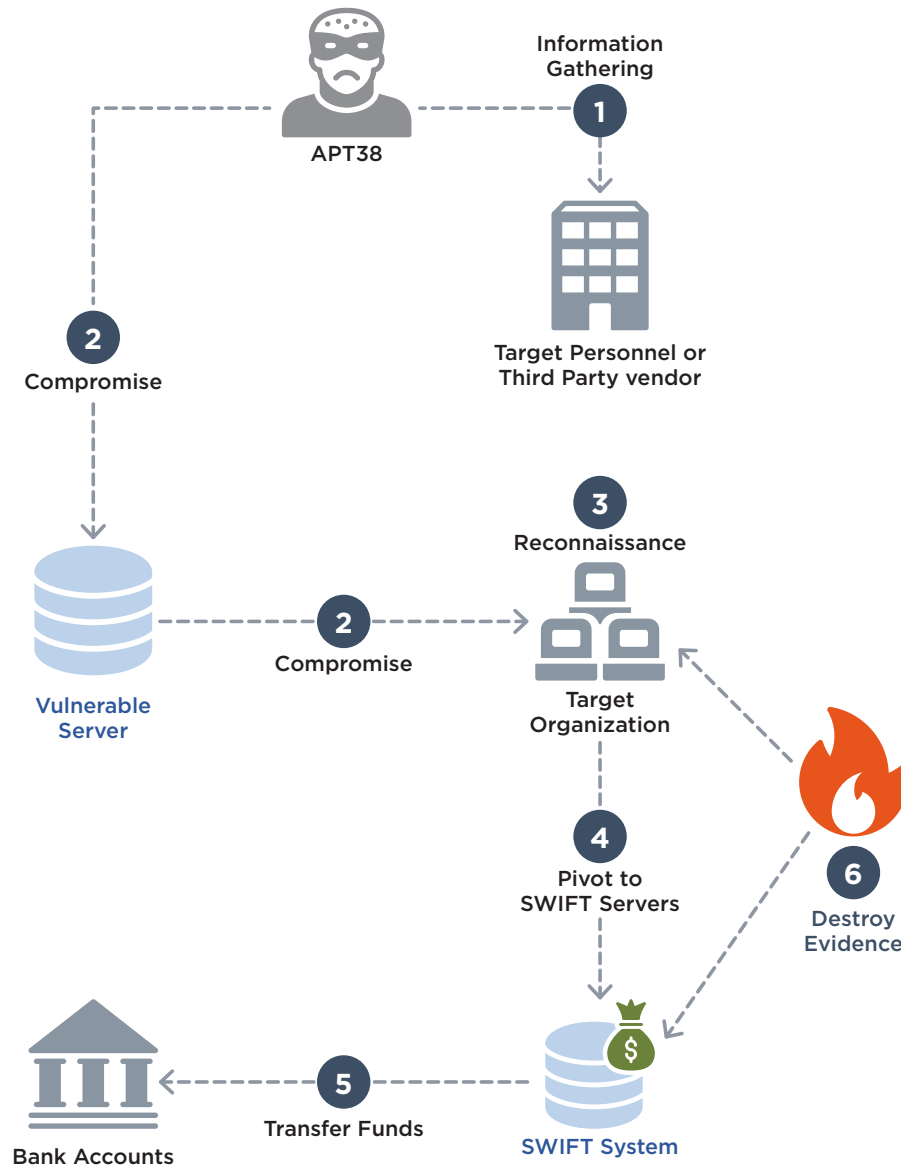
Heist Stages and Operational Characteristics

1

Information gathering

Characteristics:
- Research into a targeted organization's personnel.
- Research into a targeted organization's third-party vendors with likely SWIFT system access to understand the mechanics of SWIFT transactions.

Operational specifics:

Based on observed intrusions, we believe the group is diligent in targeting individuals with accounts that can enable further accesses into targeted organizations. Additional details released by DOJ give us insight into the significant time and resources allocated to gathering information. This information gathering likely supported APT38 activity.

- APT38 operators made multiple attempts to target a mailbox of an account manager, possibly to conduct research to determine which employees have access to SWIFT-related systems.

- The DOJ complaint detailed targeting research as well as social media activity that may have supported APT38 operations based on targeting and timing overlaps.

  — In at least one instance, reconnaissance activity of a victim bank was conducted from North Korean IP space. This research identified that the targeted bank's connection to the SWIFT network was managed by a third party and that the bank's employees remotely connected to the third party's server to review SWIFT messages. APT38 leveraged this information a month later by incorporating this information into malware development.

  — Per the complaint, the email account watsonhenny@gmail.com was used to send LinkedIn invitations to employees of a bank later targeted by APT38. The same account had a contact list with email addresses for 37 employees of the same targeted bank, suggesting a wider effort to establish connections and potential intrusion vectors.

2

Initial Compromise

Characteristics:
- Watering holes
- Searching for and compromising Linux servers, such as those with Apache Struts2 vulnerabilities.

Operational specifics:

While the initial infection vectors at each attributed incident were not always discovered, APT38 relied on watering holes to gain initial access to at least some of the organizations. In at least one instance, APT38 actors also exploited an insecure out-of-date version of Apache Struts2 to execute code on a targeted system. Further, the recent DOJ complaint provides insight into initial compromise techniques conducted by North Korean operators against APT38 targets, which may have been leveraged as part of the initial compromise into the targeted organizations.

- A watering hole campaign hosted on the website of a Polish financial governing body (Komisja Nadzoru Finansowego, or KNF) was linked to multiple additional watering holes in Latin America as well as a cryptocurrency news page. These strategic web compromises are believed to have been used to infect multiple organizations, including some in Europe and North America when victims visited the site.

- At one victim, APT38 compromised a subsidiary organization's environment before moving into the parent organization.

- Details released in the DOJ complaint indicate that North Korean operators conducted a spear-phishing campaign against a specific bank using résumé-themed lure documents in early 2015. This is corroborated by our identification of TEMP.Hermit's use of MACKTRUCK at a bank, preceding the APT38 operation targeting the bank's SWIFT systems in late 2015. This activity is noteworthy and while we acknowledge the operators detailed in the complaint share resources and ultimate sponsorship with APT38, we do not have the evidence at this time to attribute this spear-phishing activity to APT38.

3

Internal Reconnaissance

Characteristics:
- Deploy malware in a target environment to gather credentials and map the victim's network topology.
- Use internal tools, such as Sysmon and the net.exe Windows command-line tool, to scan systems.

Operational specifics:
APT38 operators put significant effort into understanding their environments and ensuring successful deployment of tools against targeted systems. The group has demonstrated a desire to maintain access to a victim environment for as long as necessary to understand the network layout, necessary permissions, and system technologies to achieve its goals. APT38 also takes steps to make sure they remain undetected while they are conducting their internal reconnaissance. **On average, we have observed APT38 remain within a victim network approximately 155 days, with the longest time within a compromised victim believed to be 678 days (almost two years)**.

- The length of time between APT38's first interaction with the SWIFT system and the observed malicious transactions has varied significantly between operations.
  - In one case, we observed malicious transactions were being made less than a month after initial reconnaissance of the SWIFT server.
  - In another case, we observed that APT38 compromised a SWIFT system and waited almost two years before conducting fraudulent transactions. During that two-year period, APT38 maintained access to the environment, installed and updated backdoors, and monitored activity to learn more about individual users, administrators, and SWIFT systems.
  - It is possible that additional SWIFT interactions occurred that were not observed.

- The group leverages internal tools when possible throughout their operations. For example, APT38 has leveraged the Windows Sysinternals utility, Sysmon, in multiple instances to monitor systems; and in another observed case, the group relied on internal file transfer software already present in the environment to move and delete malware.

- APT38 operators also try to match naming conventions that already exist on compromised systems to mask their activities. This includes mimicking file naming conventions in a victim network and hiding these malicious files amongst legitimate files.

- The group understands compromised environments well enough that in at least one instance, they incorporated hard-coded internal proxy IP addresses specific to the victim environment in their malware.

4

Pivot to SWIFT Servers

Characteristics:

- Install reconnaissance malware and internal network monitoring tools on SWIFT systems to further understand how SWIFT is configured and being used.

- Deploy active and passive backdoors on SWIFT systems operating at the target organization.

Operational specifics:

APT38 closely monitors SWIFT systems, deploying a variety of tools to observe both related applications and the users that interact with them.

- APT38 demonstrated knowledge of compromised environments, including leveraging existing legitimate tools in an environment for their benefit. APT38 deployed Sysmon on SWIFT systems to understand the processes, services, and users that use SWIFT at each organization.

- APT38 installed MAPMAKER, a port monitoring tool, on SWIFT systems. MAPMAKER is a reconnaissance tool that enumerates and prints active TCP connections on the local system. APT38 has used Sysmon and MAPMAKER together to gain a better understanding of the configuration and use of SWIFT systems within victim environments.

- APT38 has been observed actively testing their tools within victim environments to further their understanding of the SWIFT systems. According to public reporting, APT38 replaced the legitimate "nroff. exe," a printer utility associated with the SWIFT software suite, with a test version of DYEPACK's print job interception component. APT38 allowed the utility to run for more than hour, processing and gathering information on hundreds of local SWIFT transaction messages.

5 Transfer Funds

Characteristics:
- Deploy and execute malware that allows APT38 to insert fraudulent SWIFT transactions and alter transaction history
- Transfer funds to accounts set up in other banks, usually located in separate countries where little oversight enables money laundering.
- Typically, multiple transactions are initiated.

Operational specifics:

APT38 relies on DYEPACK, a SWIFT transaction-hijacking framework, to initiate transactions, steal money, and hide any evidence of the fraudulent transactions from the victimized bank. The group uses DYEPACK to manipulate the SWIFT transaction records and hide evidence of the malicious transactions, so bank personnel are none the wiser when they review recent transactions.

- SQL statements identified at multiple victims deleting fraudulent SWIFT messages provide some evidence of how DYEPACK modifies transaction records.
- If the DYEPACK processor manipulates a record of a SWIFT message destined for a file or printer, it also modifies the raw record in the Alliance Access Oracle SQL database. It does this using a series of steps:
  - First, it serializes the data extracted from the print job into an appropriate format.
  - It then invokes a legitimate Oracle command-line SQL utility to update the database. These updates may delete rows containing local records of SWIFT messages or update the body text of a local record of a SWIFT message. (Figure 6 shows an example SQL statement used to query for SWIFT records.)
  - When an employee goes to review the local records of the SWIFT messages, they will see the falsified data planted by the attacker using DYEPACK.

  - Because these techniques manipulate the SQL database directly, the transaction data is changed outside of the SWIFT framework.
- APT38 modified their malware to better suit the specifics of how SWIFT was used in at least one victimized organization, indicating the group has access to custom development capabilities. The targeted victim uses Foxit PDF Reader, a legitimate program, to review SWIFT message records as opposed to relying on printed paper copies. To accommodate for this, APT38 updated DYEPACK to modify PDF files opened with Foxit PDF Reader to remove traces of the fraudulent transactions. We refer to this variant of DYEPACK as DYEPACK.FOX.
- APT38 transferred funds to banks in a separate country, most likely to facilitate money laundering activity. Public information reports that fictitious names and fraudulently opened accounts are used to quickly transfer the funds to additional accounts, often under the guise of government account payments, non-governmental organizations (NGOs), foundations, and similar organizations.

  - According to public reporting, funds stolen from Bangladesh Bank were sent to four bank accounts in the Philippines and one account associated with an NGO in Sri Lanka via multiple transactions. Further reporting indicates that two individuals were associated with allegedly laundering tens of millions of dollars in an illegal gambling operation. During this heist, APT38 waited for a holiday weekend in the respective countries to increase the likelihood of hiding the transactions from banking authorities.
  - The use of an NGO for transferring money was also mirrored in a separate operation, where APT38 attempted to transfer multiple transactions totaling more than $100 million to a South Korean bank account for a South Korean NGO.

```
select * from saaowner.appe_<date> where appe_s_umid = '<id>';
```

Figure 6. Example SQL statement requesting SWIFT transactions

6 Destroy Evidence

Characteristics:

- Securely delete logs and files using non-public malware.

- Deploy and execute disk-wiping malware to cover tracks and disrupt later forensic analysis.

- Use publicly available ransomware on the organization's systems to delay SWIFT investigations and destroy remaining evidence of activity.

Operational specifics:

APT38 is unique in that it is not afraid to aggressively destroy evidence or victim networks as part of their operations. The group, like many of the APT groups we track, uses various methods to cover its tracks and misdirect investigators. However, APT38 is also one of the more brazen groups in that it is not afraid to cause enough damage to render entire networks inoperable. This attitude toward destruction is probably a result of the group trying to not only cover its tracks, but also to provide cover for money laundering operations.

- Some functionality to remove traces of malware were built into the malware itself. For example, DYEPACK includes the ability to uninstall itself by removing its service entry and calling a utility specifically used for secure deletion. Once the file has been removed, it executes a Windows batch script to also remove the secure deletion utility. In one instance, DYEPACK was configured to self-destruct on a preconfigured date.

- APT38 deployed other tools (including CLEANTOAD and CLOSESHAVE) that were specifically designed to clean up other malware used during the operation. In multiple intrusions, APT38 cleared Windows Event logs and Sysmon logs probably to thwart forensic analysis. In early intrusions, this was done manually, but as the group's activities progressed, they developed and deployed SCRUBBRUSH, a tool that deletes event logs and prefetch files, and may attempt to clean up master file table (MFT) records.

- APT38's operations demonstrate the group's intent to disrupt victim operations. The group carefully identified all systems within an environment (along with the credentials needed to access those systems) and then pushed wiper malware to the selected systems before initiating a massive wipe event. This is more calculated and time-consuming than relying on malware that uses self-replication to identify and wipe systems. Further, BOOTWRECK (one of the wipers used by APT38) was configured to destroy critical sections of the victim machines and then initiate a system reboot, demonstrating an intention to knock the majority of workstations and servers offline. An example disk boot failure screen observed at one affected Latin American organization is depicted in Figure 7.

- APT38 has disrupted organizations' daily operations, including causing website outages, phone inaccessibility, and inoperability of important systems. During one reported incident, APT38 rendered close to 10,000 workstations and servers completely inoperable, causing an outage in the bank's telephone service and other essential services.
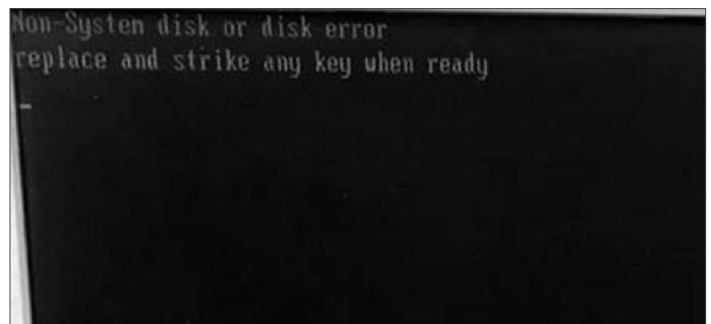
Figure 7. Example system knocked offline by APT38 (Source: Twitter)
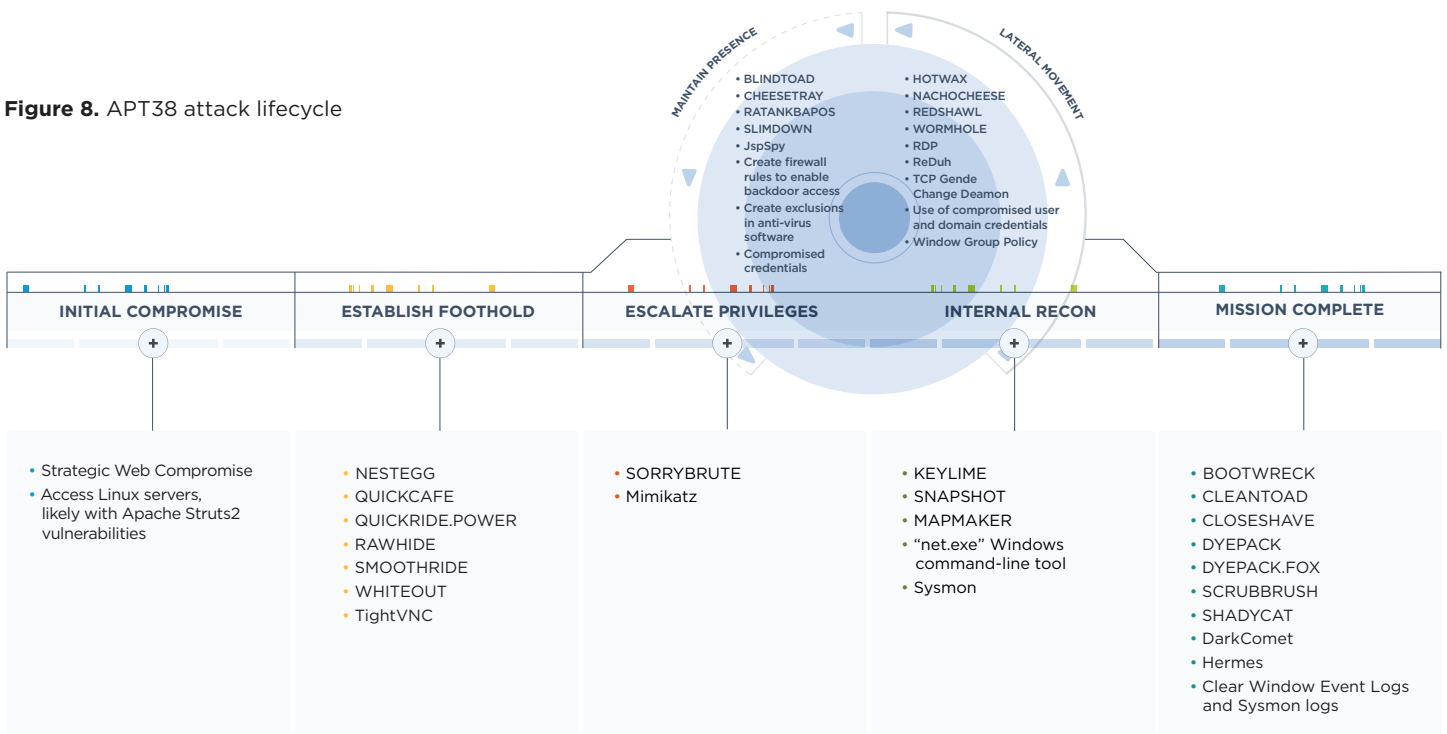
●●●
Malware

APT38 has leveraged a large number of customized tools, almost certainly indicating access to significant resources, including a large development team. Several tools unique to APT38 contain functions and code overlap with malware used by TEMP.Hermit, almost certainly indicating that these groups share a common developer.

- As of this writing, we have attributed at least 26 unique non-public malware families to APT38 and have observed the group using at least two publicly available malware families. This tool set includes a variety of backdoors, disruptive tools, tunnelers, and data miners.

- NESTEGG and MACKTRUCK share an identical hard-coded byte array, although this is not used in MACKTRUCK and appears to be an artifact from development.

- 260 bytes of functionality are shared between WANNACRY and WHITEOUT; the specific function generates a random selection of cipher suites for a Transport Layer Security (TLS) handshake.

Figure 8 provides the breakdown of all the observed malware families used by APT38, broken down by stages of the attack life cycle. The Technical Annex contains additional details on each malware family.

Figure 8. APT38 attack lifecycle

MAINTAIN PRESENCE
- BLINDTOAD
- CHEESETRAY
- RATANKBAPOS
- SLIMDOWN
- JspSpy
- Create firewall rules to enable backdoor access
- Create exclusions in anti-virus software
- Compromised credentials

LATERAL MOVEMENT
- HOTWAX
- NACHOCHEESE
- REDSHAWL
- WORMHOLE
- RDP
- ReDuh
- TCP Gende Change Deamon
- Use of compromised user and domain credentials
- Window Group Policy

INITIAL COMPROMISE
- Strategic Web Compromise
- Access Linux servers, likely with Apache Struts2 vulnerabilities

ESTABLISH FOOTHOLD
- NESTEGG
- QUICKCAFE
- QUICKRIDE.POWER
- RAWHIDE
- SMOOTHRIDE
- WHITEOUT
- TightVNC

ESCALATE PRIVILEGES
- SORRYBRUTE
- Mimikatz

INTERNAL RECON
- KEYLIME
- SNAPSHOT
- MAPMAKER
- "net.exe" Windows command-line tool
- Sysmon

MISSION COMPLETE
- BOOTWRECK
- CLEANTOAD
- CLOSESHAVE
- DYEPACK
- DYEPACK.FOX
- SCRUBBRUSH
- SHADYCAT
- DarkComet
- Hermes
- Clear Window Event Logs and Sysmon logs

Evading Detection

APT38 has employed multiple techniques for avoiding detection, including use of passive and active backdoors, modular malware, active testing, and agile response to AV. Additionally, APT38 regularly timestomps their files to blend in with other files in the victim environment

Backdoors that are configured to operate in "passive" mode indicate that the attacker intends to access the system with the backdoor from other internally compromised systems. APT38 consistently leverages "passive" backdoors to provide ease of access to segmented internal systems.

- The NESTEGG and CHEESETRAY backdoors have been identified being used in passive mode.
- At one victim, CHEESETRAY was configured to operate in passive mode on SWIFT servers, but in active mode on SWIFT workstations.
- Figure 9 contains an example of how APT38 used a tunneler to relay commands from an active CHEESETRAY backdoor on a SWIFT workstation to a passive CHEESETRAY backdoor listening on port 8443 on a SWIFT Alliance application server.

Figure 9. Active versus passive backdoors
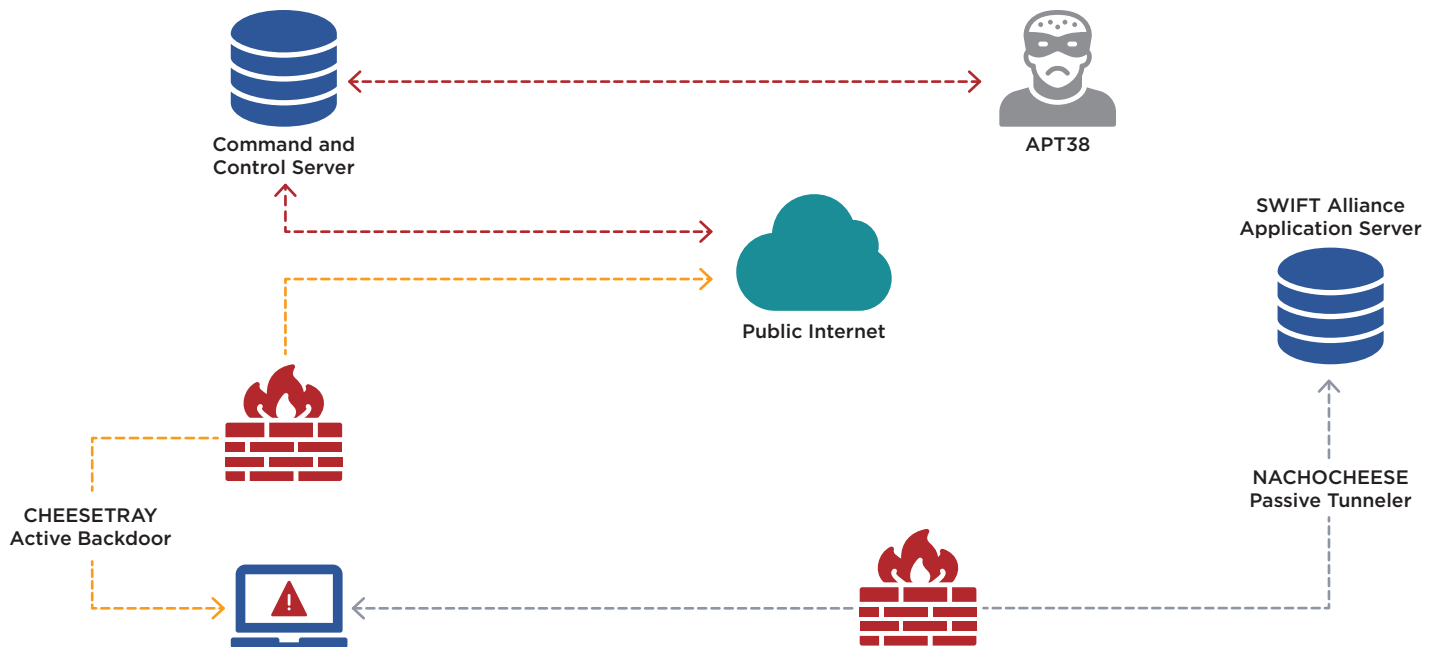
Evading Antivirus

APT38 uses several measures to evade anti-virus and thwart investigator analysis, including the use of multiple code packing methods and encrypting files on the system and in the registry.

- Of the 26 unique custom malware families used by APT38, at least nine malware families use a publicly available method of code packing, such as Themida, Enigma, VMProtect, and Obsidium.

- APT38 has demonstrated a quick response when its backdoors are detected by anti-virus. In one victim network, an anti-virus program began identifying the BLINDTOAD loader and subsequently detected it on the multiple systems. In response, APT38 operators returned to the environment and installed new undetected versions of BLINDTOAD and CHEESETRAY.

- In one instance, the group purposefully ran an anti-virus scan on a victim system, potentially to determine if its backdoors were detected.

Modular Malware

Some tools used by APT38 are composed of multiple components that load each other and are positioned in different places within a compromised environment. The use of modular components is useful both in its extensibility, in that it's easy for the programmer to build out additional functionality in the future, and the distribution of functionality among components assists in evading detection.

- DYEPACK, for example, is comprised of separate processor, interceptor, and encrypted configuration components.

- BLINDTOAD, another APT38 tool, is a loader that provides a framework to load an encrypted resource, decode it in memory, and execute it. This typically bypasses traditional anti-virus detection.

Use of False Flags

APT38 has incorporated several false flags during their operations to further mislead investigators, including:

- In one case, APT38 dropped a variant of DARKCOMET (a publicly available backdoor) at the end of their operations. The configured command and control (C&C) server for this sample was a legitimate bank in Africa. We surmise that APT38 possibly deployed this tool to distract investigators.

- APT38 has also deployed the HERMES ransomware, which has been used by other financially motivated cyber crime actors. In this case, the ransomware was not correctly configured to collect ransom. We suspect this was another technique employed by APT38 to distract investigators and destroy evidence.

- Additionally, the NACHOCHEESE malware used by APT38 contained poorly translated Russian-language strings, which were likely included to misdirect investigators.

Attribution

North Korean Infrastructure

We attribute APT38 to North Korean state-sponsored operators based on a combination of technical indicators linking the activity to Pyongyang and details released by DOJ implicating North Korean national Park Jin Hyok in a criminal conspiracy. We assess with high confidence that these activities were directed and sponsored by the North Korean government. Because the North Korean regime keeps strict control over communications and internet infrastructure in the country, it is highly improbable that these operations could be conducted without the knowledge or explicit sponsorship of the government.

- The DOJ complaint also detailed two blocks of IP addresses used by Park in APT38 and other North Korean operations:

Table 1. North Korean IP address ranges

North Korean IP Address Range	Description
175.45.176.0 – 175.45.179.255	IP range registered to a company in Pyongyang
210.52.109.0 – 210.52.109.255	IP range registered to a company in China but leased to North Korea

- The use of these ranges by APT38 for their operations has been corroborated by third-party reporting:

  — A public report by Group-IB indicated APT38 logged into watering hole domains associated with (brou.com[.]uy, cnbv.gob[.]mx knf.gov[.]pl) from two IPs (210.52.109.22 and 175.45.178.222) within the same North Korean IP ranges.

  — A report by Kaspersky indicates APT38 also logged into an Apache Tomcat server used to host its malicious files from the same IP range (175.45.176.0 -175.45.179.255) in January 2017.

- As detailed in the DOJ complaint, a sample of WHITEOUT (aka Contopee) malware we attribute to APT38 was used between 2015 and 2016 against a Southeast Asian bank. The sample used a specific DDNS domain, onlink.epac[.]to, which was managed by an account at a DDNS provider. The same account was accessed on October 6, 2015 from a North Korean IP address.

- As detailed in the DOJ complaint, the North Korean operators conducted reconnaissance on a Southeast Asian bank, including visiting its website, researching the business identifier code (BIC) used by the SWIFT system to uniquely identify the bank, and the BIC code for a corresponding bank needed to carry out the intended fraudulent transactions. This is evidence of shared motivation and intent to target the SWIFT system by the North Korean operators performing the reconnaissance and APT38 which later targeted that organization.
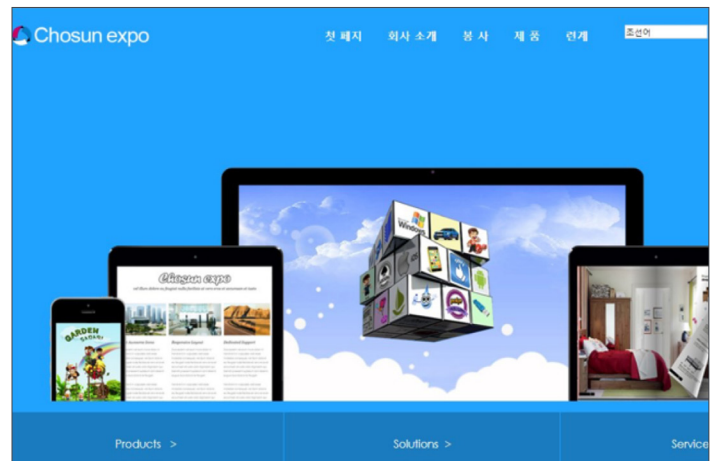
Shared Resources, Motivation

Malware overlaps between APT38 and TEMP.Hermit highlight the shared development resources accessible by multiple operational groups linked to North Korean state-sponsored activity. Although these are disparate operations against different targets and rely on distinct TTPs, the malware tools being used either overlap or exhibit shared characteristics indicating a shared developer or access to the same code repositories. Although APT38 is distinct from other TEMP.Hermit activity, both groups operate consistently within the interests of the North Korean state.

- Malware similarities, including code overlap and shared functions, are a primary connection between APT38 and other operations still attributed to TEMP.Hermit. For additional malware similarity details, please see the preceding section.

- APT38's increasingly aggressive targeting against banks and other financial institutions has paralleled North Korea's worsening financial condition (Figure 4). Similarly, TEMP.Hermit campaigns against U.S. defense contractors and South Korean government offices and companies is consistent with other North Korean objectives.

Links to North Korean Military Units

Based on details published in the DOJ complaint against North Korean programmer Park Jin Hyok, we know that APT38 and other cyber operators linked to TEMP.Hermit are associated with Lab 110, an organization subordinate to or synonymous with the 6th Technical Bureau in North Korea's Reconnaissance General Bureau (RGB). The organization is believed to leverage front organizations to mask their activities, including infiltrating networks and gathering intelligence. These relationships are outlined in Figure 3.

- The DOJ complaint and open sources report that Lab 110 operates out of front companies typically based in northeast China. Identified fronts include Chosun Expo Joint Venture in Dalian and Chosun Baeksul Trading Company in Shenyang.

- Firsthand accounts, information provided by a foreign investigative agency, and common IP addresses used to access the company website and associated accounts while connecting to and from North Korea corroborate reports that Chosun Expo was a front company operated by authorities in Pyongyang.

- Similar units reportedly operate in other regions around the world, including Southeast Asia, Eastern Europe, and other parts of China.

- Malware developers and other adversary actors are believed to be recruited out of North Korea's universities and directly into military units, such as Lab 110. Schools reportedly feeding into these units include Kim Chaek University of Technology and Kim Il Sung Military Science University.

Figure 10. Archived website for Chosun Expo Joint Venture (Source: archive.fo)

●●●
Outlook and Implications

APT38's targeting of financial institutions is most likely an effort by the North Korean government to supplement their heavily-sanctioned economy. Stricter and more targeted sanctions which expanded from restricting access to international banking systems to focusing on specific exports have most likely increased pressure significantly and emboldened operations. Public reporting suggests North Korea has previously engaged in illicit activities such as smuggling and drug trade to raise currency and keep its economy afloat. We judge APT38's cyber heists are extensions of these illicit activities. Published reports from North Korean defectors additionally provide details on cyber-focused military units being tasked to generate income for the regime, generally by engaging in various cybercriminal schemes including piracy and freelance programming work.

While it is unclear how APT38's operations will be affected by the recent DOJ complaint, it is notable that North Korean operators appear to be undeterred by public outings in the past. Furthermore, the timing of recent APT38 operations provides some indication that even diplomatic re-engagement will not motivate North Korea to rein in its illicit financially-motivated activities. Based on the large scale of resources and vast network dedicated to compromising targets and stealing funds over the last few years, we believe APT38's operations will continue in the future. In particular, the number of SWIFT heists that have been ultimately thwarted in recent years coupled with growing awareness for security around the financial messaging system could drive APT38 to employ new tactics to obtain funds especially if North Korea's access to currency continues to deteriorate.

Technical Annex: Malware Used by APT38

Table 2. Malware used by APT38.

Malware	Description	Detected as
BLINDTOAD	BLINDTOAD is 64-bit Service DLL that loads an encrypted file from disk and executes it in memory.	• FE_APT_BLINDTOAD • FE_APT_FIN_BLINDTOAD_1 • FE_APT_FIN_BLINDTOAD_2 • FE_APT_Loader_Win64_BLINDTOAD_1
BOOTWRECK	BOOTWRECK is a master boot record wiper malware.	• FE_APT_Wiper_Win32_BOOTWRECK_1
CHEESETRAY	CHEESETRAY is a sophisticated proxy-aware backdoor that can operate in both active and passive mode depending on the passed command-line parameters. The backdoor is capable of enumerating files and processes, enumerating drivers, enumerating remote desktop sessions, uploading and downloading files, creating and terminating processes, deleting files, creating a reverse shell, acting as a proxy server, and hijacking processes among its other functionality. The backdoor communicates with its C&C server using a custom binary protocol over TCP with port specified as a command-line parameter.	• FE_APT_Backdoor_Win64_CHEESETRAY_1 • FE_APT_Backdoor_Win_CHEESETRAY_1 • APT.Backdoor.Win.CHEESETRAY
CLEANTOAD	CLEANTOAD is a disruption tool that will delete file system artifacts, including those related to BLINDTOAD, and will run after a date obtained from a configuration file. The malware injects shellcode into notepad.exe and it overwrites and deletes files, modifies registry keys, deletes services, and clears Windows event logs.	• FE_APT_HackTool_Win_CLEANTOAD_1
CLOSESHAVE	CLOSESHAVE is a secure deletion utility that expects single command line parameter that is a path to an existing file on the system. It overwrites the file with null bytes, changes the file name, and deletes the file.	• FE_APT_Hacktool_CLOSESHAVE

Table 2. Malware used by APT38.

Malware	Description	Detected as
DarkComet	DarkComet is a publicly available remote access Trojan (RAT) capable of more than 60 different functions, including collecting system information, controlling all processes currently running on an infected system, viewing and modifying registries, creating a reverse shell, modifying or adding start-up processes and services, keylogging, stealing credentials, recording audio, scanning networks, locking, restarting and shutting down infected systems, updating malware with a new command and control (C&C) server or new functionality, and downloading, modifying, and uploading files.	• Backdoor.DarkComet Trojan.DarkComet • Backdoor.Fynloski • Trojan.Fynloski
DYEPACK	DYEPACK is a malware suite that manipulates local information regarding SWIFT transaction activity. DYEPACK would most likely be used to cover the traces of fraudulent SWIFT transactions that were performed via other tools or tactics. Variants of this malware may have been intended for deployment within multiple financial institutions targeted by likely related malicious activity. However, its actual deployment has not been confirmed in all of these cases.	• Hacktool.APT.DYEPACK
DYEPACK.FOX	Variant of DYEPACK utility. DYEPACK.FOX has the ability to manipulate PDF documents containing records of SWIFT messages.	• Hacktool.APT.DYEPACK
HERMES	HERMES is a multi-threaded ransomware that enumerates all logical drives on a system and starts a new encryption thread for each drive. It attempts to encrypt all files using AES256 encryption that return FILE_ATTRIBUTE_NORMAL for GetFileAttributes requests. HERMES will attempt to create and display a file on the desktop called DECRYPT_INFORMATION.txt containing the ransom instructions.	• FE_APT_Ransomware_HERMES_1 • FE_APT_Ransomware_Win_HERMES_1 • FE_APT_FIN_Ransomware_HERMES • FE_Ransomware_Win32_HERMES_1 • Ransomware.Hermes.DNS • Ransomware.Hermes • RansomDownloader.Hermes
HOTWAX	HOTWAX is a module that upon starting imports all necessary system API functions, and searches for a .CHM file. HOTWAX decrypts a payload using the Spritz algorithm with a hard-coded key and then searches the target process and attempts to inject the decrypted payload module from the CHM file into the address space of the target process.	• FE_APT_Trojan_Win64_HOTWAX_1
JspSpy	JspSpy is a publicly available web shell that has been posted on github.com. One publicly available version says "Code By Ninty"	• FE_Webshell_JSP_JSPSPY_1 • FE_Webshell_Java_JSPSPY_1 • Webshell.JSP.JSPSPY • JSPSPY WEBSHELL
KEYLIME	KEYLIME is a keylogger and clipboard logger that encodes the results to a log file.	• FE_Hacktool_KEYLIME • FE_APT_Trojan_KEYLIME • FE_Trojan_KEYLIME
MAPMAKER	MAPMAKER is a reconnaissance tool that enumerates and prints active TCP connections on the local system. It queries the operating system for the IPv4 TCP connection table, and writes lines like "<ip>:<port> -> <ip>:<port>" to a log file.	• FE_APT_HackTool_Win32_MAPMAKER_1
NACHOCHEESE	NACHOCHEESE is a command-line tunneler that accepts delimited C&C IPs or domains via command-line and gives actors shell access to a victim's system.	• FE_APT_FIN_Trojan_NACHOCHEESE • FE_APT_FIN_Backdoor_NACHOCHEESE
NESTEGG	NESTEGG is a memory-only backdoor that can proxy commands to other infected systems using a custom routing scheme. It accepts commands to upload and download files, list and delete files, list and terminate processes, and start processes. NESTEGG also creates Windows Firewall rules that allows the backdoor to bind to a specified port number to allow for inbound traffic.	• FE_APT_Backdoor_NESTEGG • FE_APT_Backdoor_NESTEGG_2 • FE_APT_Backdoor_NESTEGG_3 • FE_Backdoor_NestEgg_DLL

Table 2. Malware used by APT38.

Malware	Description	Detected as
QUICKCAFE	QUICKCAFE is an encrypted JavaScript downloader for QUICKRIDE.POWER that exploits the ActiveX M2Soft vulnerabilities. QUICKCAFE is obfuscated using JavaScript Obfuscator.	• FE_APT_Downloader_JS_QUICKCAFE_1
QUICKRIDE	QUICKRIDE is a backdoor that establishes persistence using the Startup folder. It communicates to its C&C server using HTTPS and a static HTTP User-Agent string. QUICKRIDE is capable of gathering information about the system, downloading and loading executables, and uninstalling itself. It was leveraged against banks in Poland.	• Backdoor.APT.QUICKRIDE
QUICKRIDE.POWER	QUICKRIDE.POWER is a PowerShell variant of the QUICKRIDE backdoor. Its payloads are often saved to C:\windows\temp\	• FE_APT_Backdoor_PS1_QUICKRIDE_1 • FE_APT_Backdoor_PS1_QUICKRIDE_2
RATANKBAPOS	RatankbaPOS is a backdoor that targets a payment card application platform. exe, scrapes track2 data, and sends it to a remote C&C. RATANKBAPOS is also capable of running arbitrary commands and deleting itself. This tool was linked to APT38-attributed infrastructure, suggesting that the group may have considered other tactics for intercepting transaction data.	• Trojan.POS.RatankbaPOS • Trojan.RatankbaPOS
RAWHIDE	RAWHIDE is a rootkit variant of the ProcessHider rootkit. ProcessHider is a post-exploitation tool that hides processes from monitoring tools such as Task Manager and Process Explorer.	• FE_HACKTOOL_RAWHIDE • Exploit.APT.RAWHIDE
REDSHAWL	REDSHAWL is a session hijacking utility that starts a new process as another user currently logged on to the same system via command-line.	• FE_APT_HackTool_Win64_REDSHAWL_1
SCRUBBRUSH	SCRUBBRUSH is a disruption utility that can delete event logs, prefetch files, and may attempt to clean up MFT file records.	• FE_APT_Tool_Win32_SCRUBBRUSH_1
SHADYCAT	SHADYCAT is a dropper and spreader component for the HERMES 2.1 RANSOMWARE radical edition.	• FE_APT_Dropper_SHADYCAT_1 • FE_APT_FIN_Trojan_SHADYCAT_Dropper
SLIMDOWN	SLIMDOWN is a downloader that fetches PE executables via a custom encrypted binary protocol.	• FE_APT_Backdoor_SLIMDOWN
SMOOTHRIDE	SMOOTHRIDE is a Flash loader that contains three different exploits embedded within it. SMOOTHRIDE acts an exploit dispatcher and delivers one of three exploits (CVE-2016-4119, CVE-2016-1019, or CVE-2015-8651) based on the affected operating system. SMOOTHRIDE has been observed being delivered via a watering hole.	• Trojan.SMOOTHRIDE.Profiler
SORRYBRUTE	SORRYBRUTE is an SMB brute-forcer that accepts target IPs, usernames, and passwords to try, as well as runtime parameters on the command-line and is used for lateral movement	• FE_APT_HackTool_Win32_SORRYBRUTE_1
WHITEOUT	WHITEOUT is a proxy-aware backdoor that communicates using a custom-encrypted binary protocol. It may use the registry to store optional configuration data. The backdoor has been observed to support 26 commands that include directory traversal, file system manipulation, data archival and transmission, and command execution.	• FE_APT_Backdoor_WHITEOUT
WORMHOLE	WORMHOLE is a TCP tunneler that is dynamically configurable from a C&C server and can communicate with an additional remote machine endpoint for a relay.	• FE_APT_Tunneler_Win32_WORMHOLE_1

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.