APT38: Unusual Suspects

Operational (OP)	Fusion (FS)
Strategic (ST)	Vulnerability (VU)
Cyber Physical (CP)	Cyber Espionage (CE)
Hacktivism (HK)	Cyber Crime (CC)

October 05, 2018 08:15:00 PM, 18-00016353, Version: 3

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 13 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.

Threat Detail

New Version Details

Version 2, Oct. 5, 2018: Executive summary updated to be consistent with published graphics (Figure 1)

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.

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.

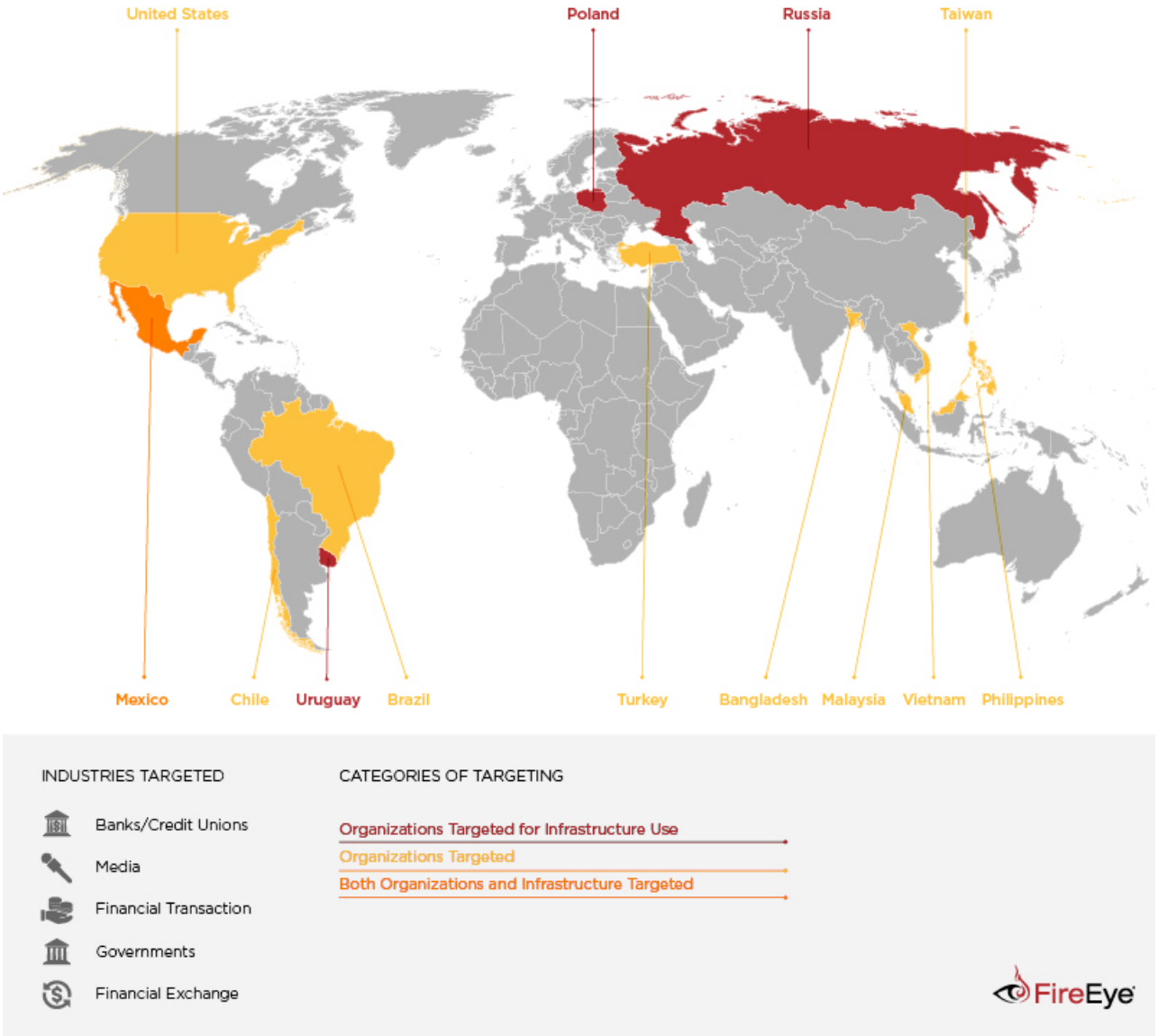

Figure 1: APT38 global targeting

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.

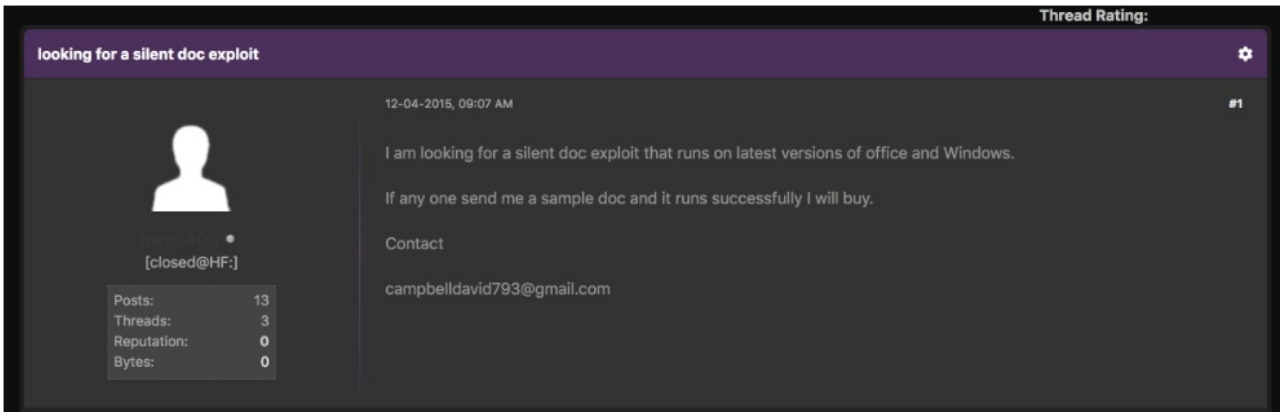

Figure 2: North Korean operator posting in an underground forum

- 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."

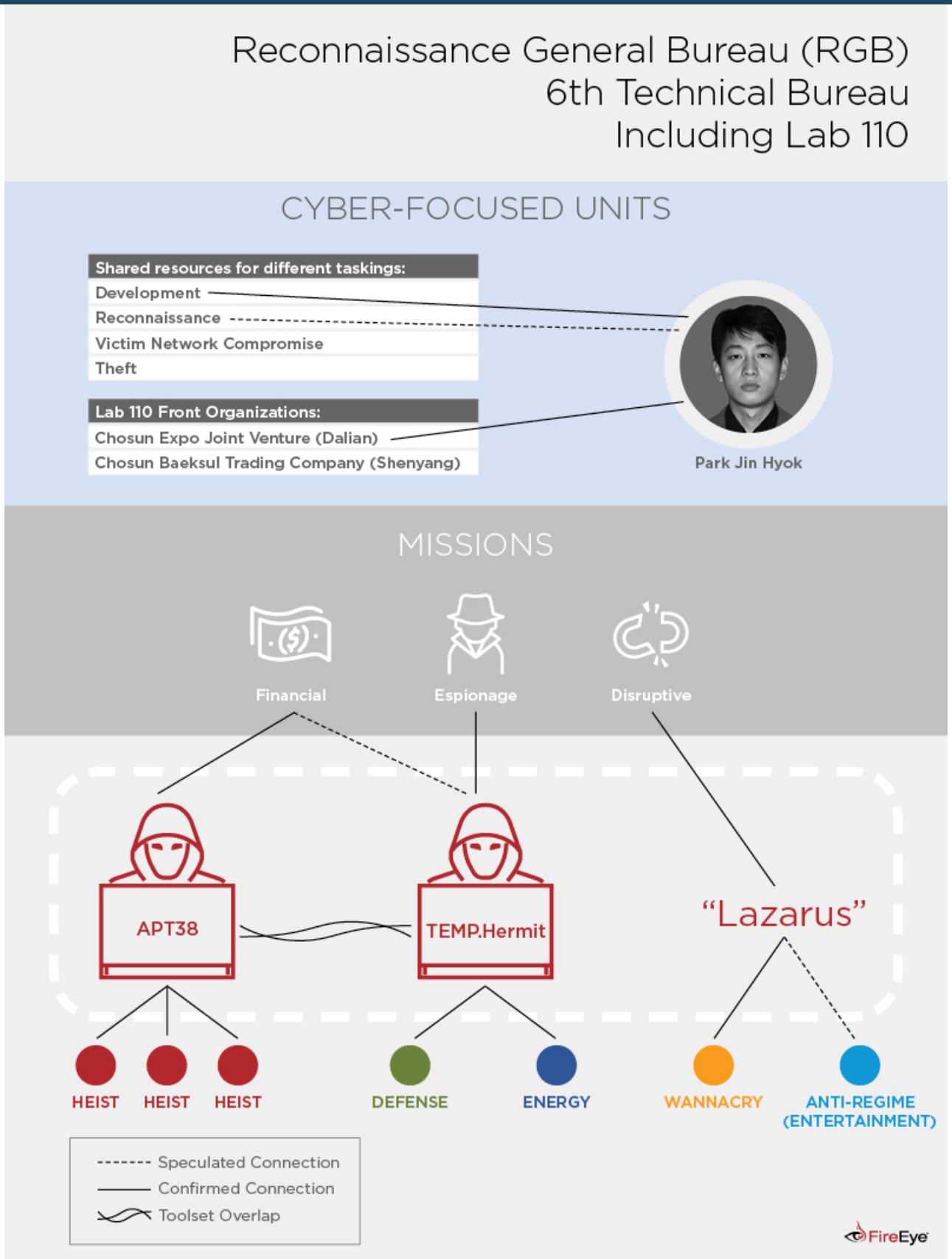

Figure 3: Notional depiction of APT38's connections to other North Korean state-sponsored operations

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, targeteda 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[2] 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.

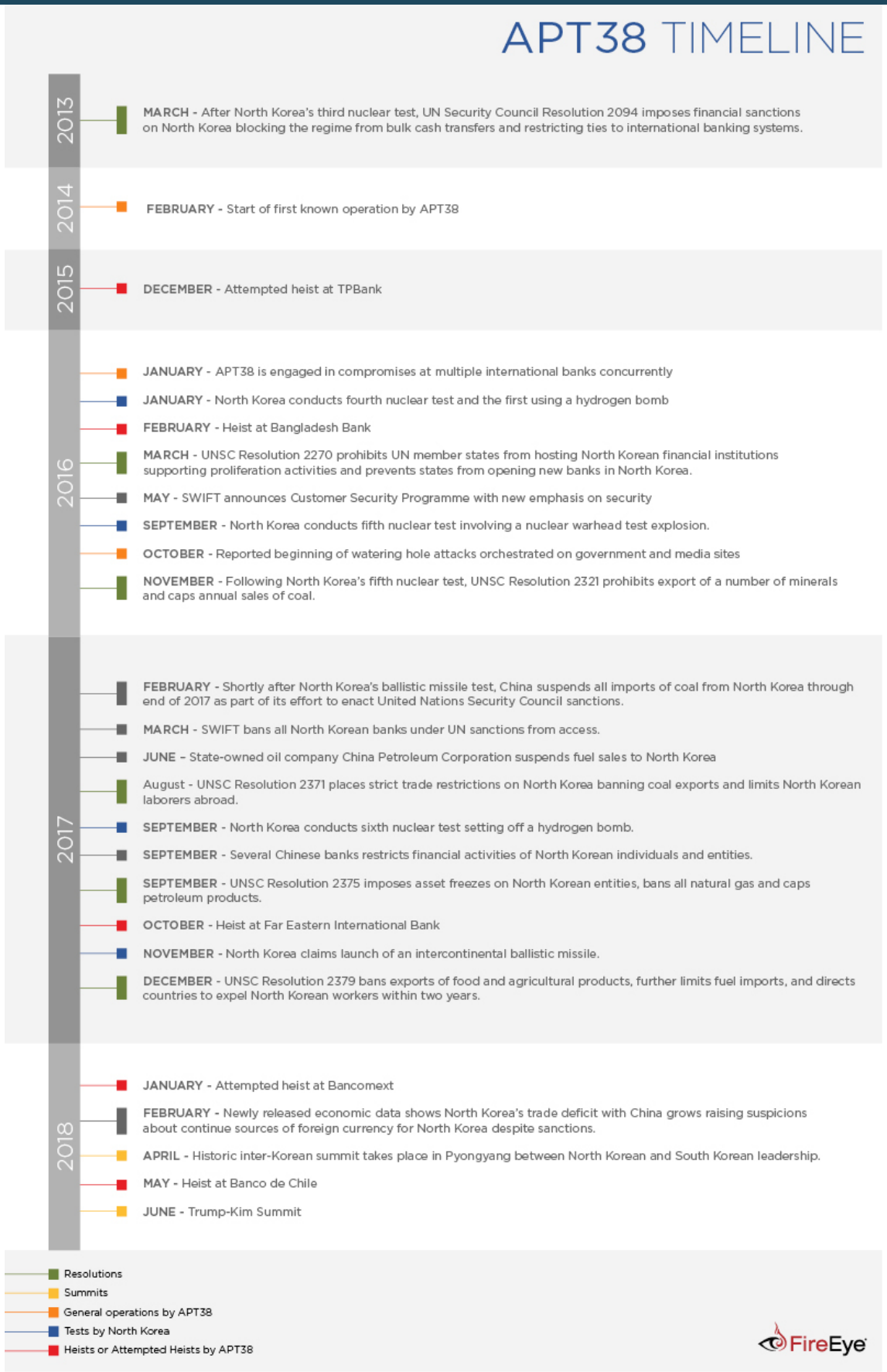

Figure 4: APT38 operations and North Korea's worsening financial situation

Tactics, Techniques, and Procedures (TTPs)

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.

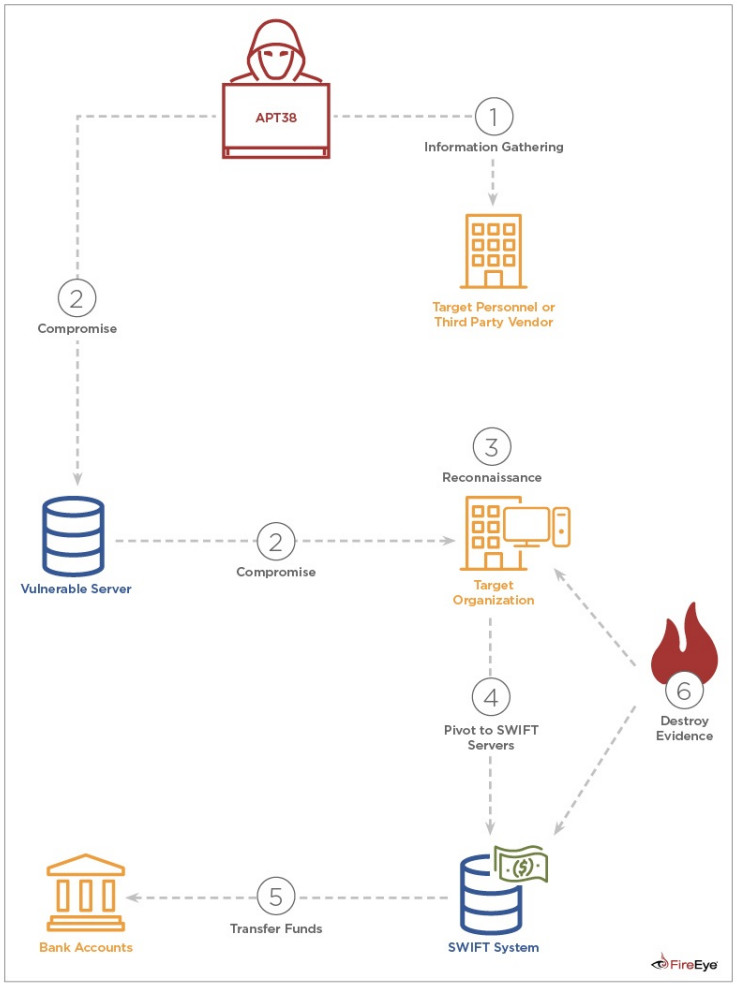

Figure 5: An APT38 cyberbank robbery

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

a. Deploy malware in a target environment to gather credentials and map the victim's network topology.
b. Use internal tools, such as Sysmon and the net1.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 system 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.

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

Figure 6: Example SQL statement requesting SWIFT transactions

- 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.

(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.

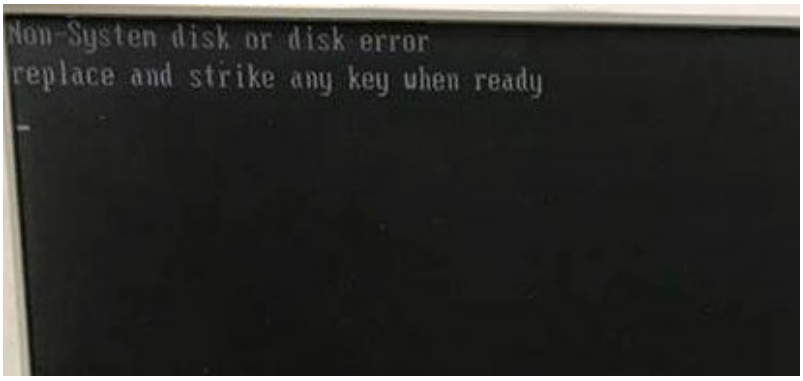

Figure 7: Example system knocked offline by APT38
(Source: Twitter)

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.

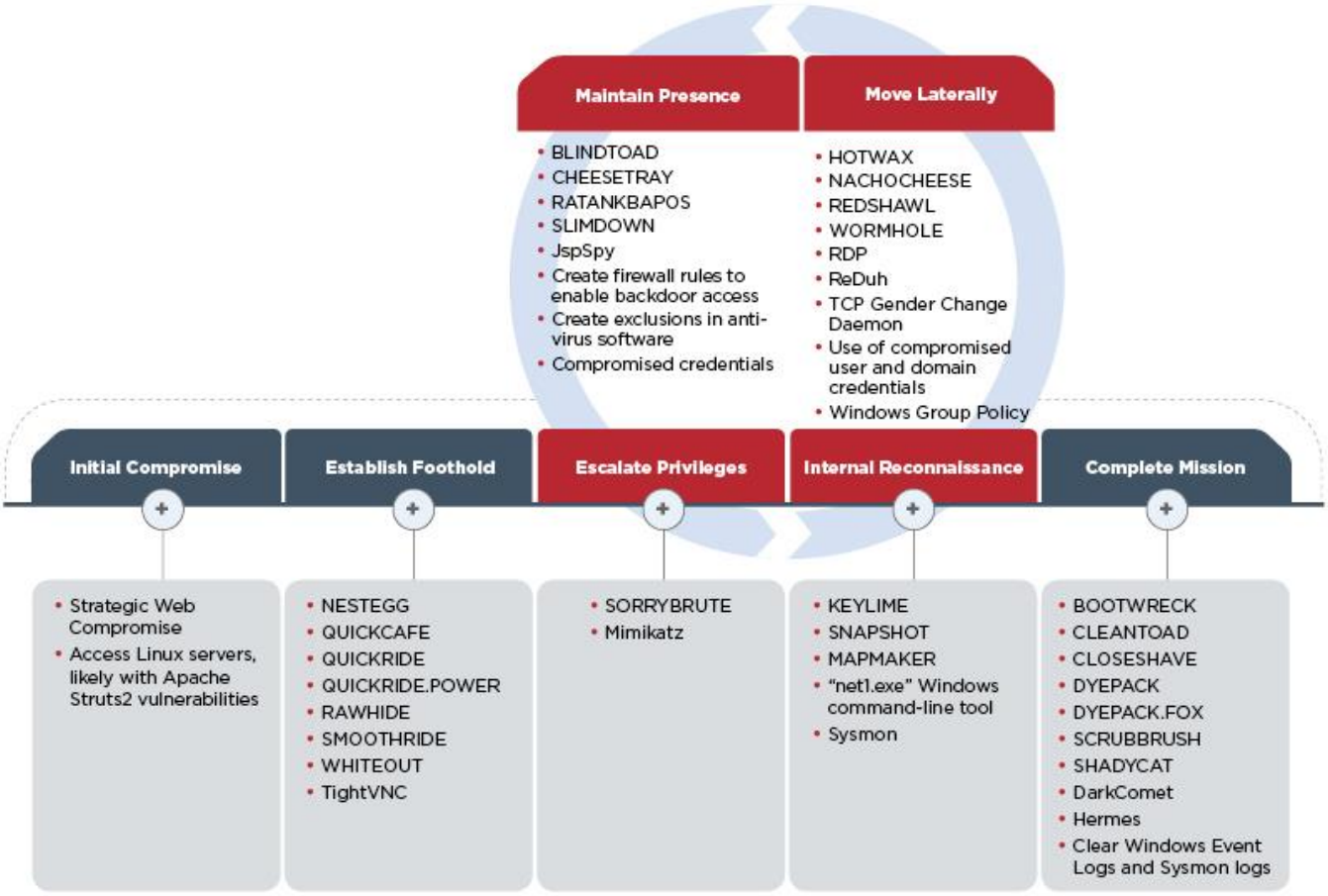

Figure 8: APT38 attack lifecycle

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.

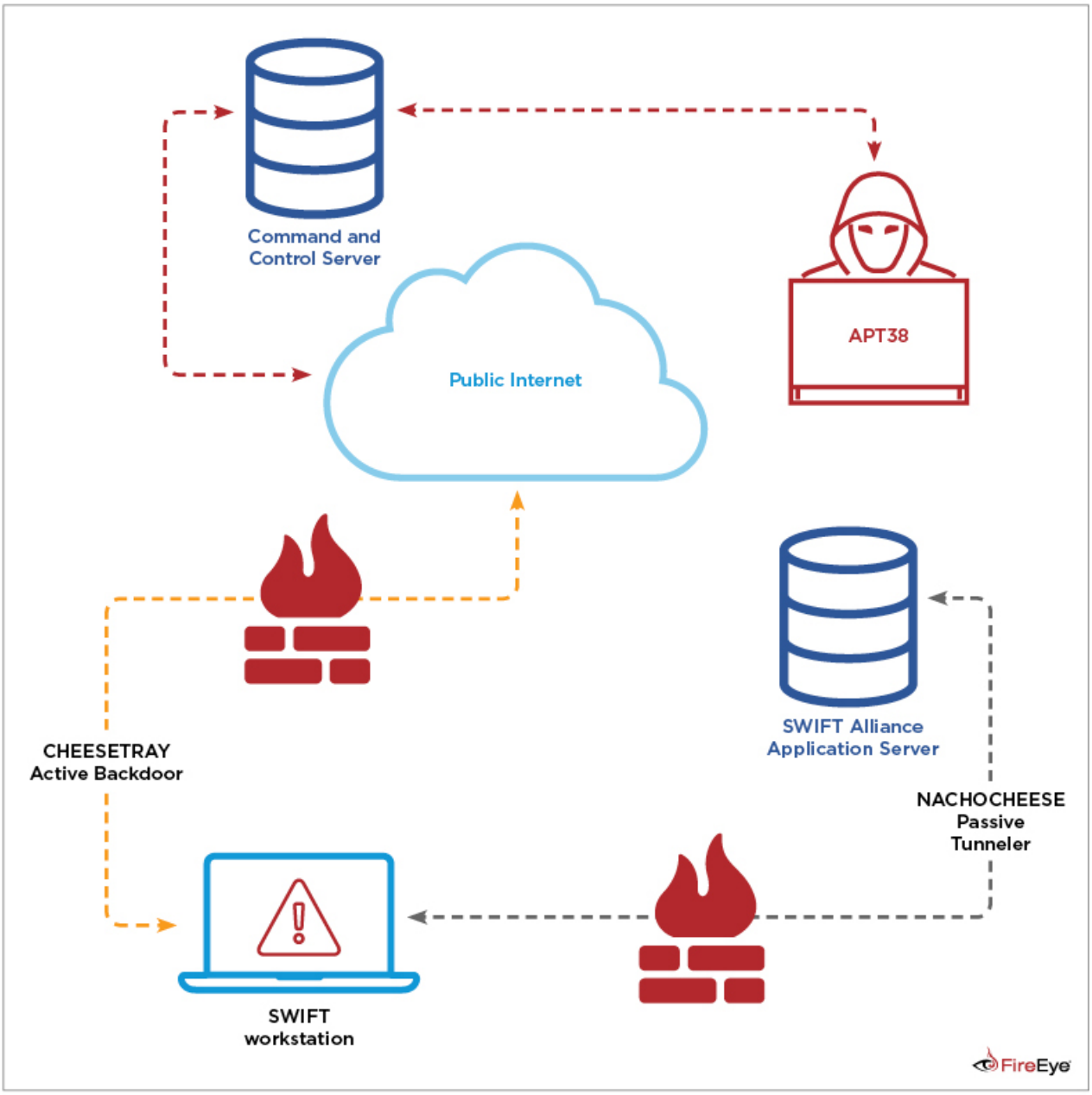

Figure 9: Active versus passive backdoors

Evading Anti-Virus

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 the 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 government's knowledge or explicit sponsorship.

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

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

Table 1: North Korean IP address ranges

- The use of these ranges by APT38 for their operations has been corroborated by third-party reporting:
  - A public report by Group-IB indicated that APT38 logged into watering hole domains associated with brou.com.uy, cnbv.gob.mx, and 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 that 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 Oct. 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.

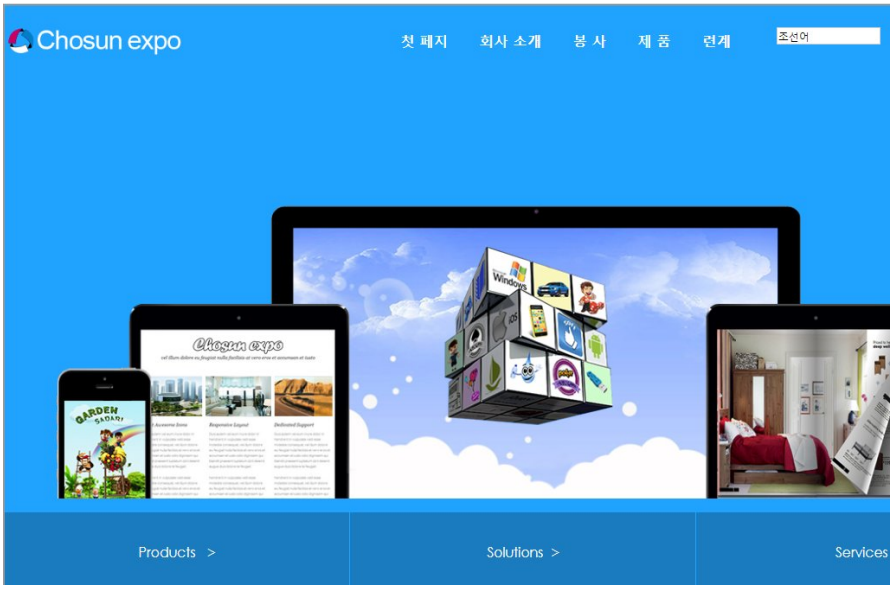

Figure 10: Archived website for Chosun Expo Joint Venture (Source: archive.fo)

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 that 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 cyber criminal schemes, including piracy and freelance programming work.

While it is unclear how APT38's operations will be affected by the DOJ complaint unsealed in September 2018, 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 during 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

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	FE_APT_Backdoor_Win64_CHEESETRAY_1 FE_APT_Backdoor_Win_CHEESETRAY_1 APT.Backdoor.Win.CHEESETRAY

	server using a custom binary protocol over TCP with port specified as a command-line parameter.	
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_CLEANTOD_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 filename, and deletes the file.	FE_APT_Hacktool_CLOSESHAVE
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	Backdoor.DarkComet Trojan.DarkComet Backdoor.Fynloski Trojan.Fynloski

	new functionality, and downloading, modifying, and uploading files.	
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 is a module that upon starting imports all	

HOTWAX	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	FE_APT_Backdoor_NESTEGG FE_APT_Backdoor_NESTEGG_2 FE_APT_Backdoor_NESTEGG_3 FE_Backdoor_NestEgg_DLL

	start processes. NESTEGG also creates Windows Firewall rules that allows the backdoor to bind to a specified port number to allow for inbound traffic.	
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

Table 2: Malware used by APT38

[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.

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

Please rate this product by taking a short four question survey

First Version Publish Date

September 27, 2018 11:52:00 AM

Threat Intelligence Tags

Motivation

- Financial or Economic

Affected System

- Users/Application and Software
- Third Party Services

Source Geography

- North Korea

Affected Industry

- Financial Services
- Media
- Banks
- Government - National
- Government - Subnational

Intended Effect

- Degradation
- Destruction
- Credential Theft/Account Takeover
- Financial Theft
- Denial and Deception
- Disruption

Tactics, Techniques And Procedures(TTPs)

- Monetization and Laundering
- Social Engineering
- Network Reconnaissance
- Communications
- Malware Propagation and Deployment
- Fraud
- Malware Research and Development
- Enabling Infrastructures

Target Geography

- Russian Federation
- United States
- Uruguay
- Philippines
- Malaysia
- Bangladesh
- Vietnam
- Turkey
- Taiwan
- Poland
- Brazil
- Mexico
- Chile

Actor

- APT38

Targeted Information

- Corporate Employee Info
- Financial Data
- Credentials

Malware Family

- CHEESETRAY
- RatankbaPOS
- SMOOTHRIDE
- NACHOCHEESE
- QUICKCAFE
- WORMHOLE
- NESTEGG
- DYEPACK
- SLIMDOWN
- SCRUBBRUSH
- HOTWAX
- WHITEOUT
- RAWHIDE
- SHADYCAT
- QUICKRIDE.POWER
- SNAPSHOT
- MAPMAKER
- QUICKRIDE
- HERMES
- CLEANTOAD
- SORRYBRUTE
- KEYLIME
- DYEPACK.FOX
- BOOTWRECK
- BLINDTOAD
- DarkComet
- CLOSESHAVE

Technical Indicators & Warnings

URL:	http://158[.]69[.]57[.]135/card[.]jsp?action=BaseInfo&u=
Network Type:	url
Identifier:	Attacker
Actor:	APT38
IP:	210.52.109.0
Identifier:	Attacker
Actor:	APT38
Network Type:	network
URL:	http://www.energydonate[.]com/files/download/bithumb.zip
Network Type:	url

Identifier:	Attacker
Actor:	APT38
URL:	http://sap.misapor[.]ch/vishop/include/cambio.swf
Network Type:	url
Identifier:	Attacker
Actor:	APT38
IP:	210.52.109.22
Identifier:	Attacker
Actor:	APT38
Network Type:	network
URL:	http://www.businesshop[.]net/theme.gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://trade.publicvm[.]com/server.jsp?action=%22BaseInfo%22&u=%22UkRRNlFVVTZOVEk2TmtZNk5UWTZNREE9%22
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://41[.]203[.]65[.]250/eshop/view[.]jsp
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://51[.]255[.]219[.]82/files/download/alchain[.]pdf
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://158[.]69[.]57[.]135/theme[.]gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://www.businesshop[.]net/card.jsp?action=BaseInfo&u=TURBNk1qQTZNVGc2TVRFNk1ERTZOalU9
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?action=BaseInfo&u=21632843515764

Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://92[.]222[.]106[.]229/card[.]jsp?action=BaseInfo&u=TURBNk1qQTZNVGc2TVRFNk1ERTZOalk9
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/dfbox/list.jsp?action=BaseInfo&u=10793128109959
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://onlink.epac[.]to:8080/onlink.epac[.]to:443
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://www.energydonate[.]com/images/character.gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://sap.misapor[.]ch/vishop/view.jsp?pagenum=1
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://41[.]203[.]65[.]250/eshop/view[.]jsp?uid=68883194&pagenum=3&eid=00000002&s=2&data=
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/dfbox/list.jsp?action=What&u=10793128109959
Network Type:	url
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	tradeboard.mefound.com
Identifier:	Attacker
Actor:	APT38
IP:	180.235.133.121
Identifier:	Related

Actor:	APT38
Network Type:	network
URL:	http://trade.publicvm[.]com/images/top_bar.gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://51[.]255[.]219[.]82/card[.]jsp?action=BaseInfo&u=TURBNk1qQTZNVGc2TVRFNk1ERTZOalU9
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://apps.got-game[.]org/files/download/transaction.pdf
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://41[.]203[.]65[.]250/eshop/view[.]jsp?pagenum=1
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://92[.]222[.]106[.]229/theme[.]gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://www[.]btc-gold.us/images/top_bar.gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	webkingston.com
Identifier:	Related
Actor:	APT38
IP:	175.45.178.222
Identifier:	Attacker
Actor:	APT38
Network Type:	network
URL:	http://www.cnbv.gob.mx/Paginas/Informacion-Estadistica[.]aspx
Network Type:	url
Identifier:	Attacker
Actor:	APT38

Network Type:	network
Domain:	energydonate.com
Identifier:	Related
Actor:	APT38
URL:	http://www.energydonate[.]com/server.jsp?action=BaseInfo&u=TURBNk1qQTZNVGc2TVRFNk1ERTZOalU9
Network Type:	url
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	statis.ignorelist.com
Identifier:	Attacker
Actor:	APT38
URL:	http://www.knf[.]gov.pl/DefaultDesign/Layouts/KNF2013/resources/accordian-src.js?ver=11
Network Type:	url
Identifier:	Attacker
Actor:	APT38
IP:	92.222.106.229
Identifier:	Related
Actor:	APT38
Network Type:	network
URL:	http://www.knf[.]gov.pl/dla_rynku/PODMIOTY_rynku/index.htm
Network Type:	url
Identifier:	Attacker
Actor:	APT38
IP:	175.45.176.0
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Network Type:	network
Domain:	btc-gold.us
Identifier:	Related
Actor:	APT38
URL:	http://btc-gold.us/images/top_bar[.]gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://sap.misapor[.]ch/vishop/include/cambio.swf

Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://158[.]69[.]57[.]135/card[.]jsp?action=BaseInfo&u=TURBNk1qQTZNVGc2TVRFNk1ERTZOalU9
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://trade.publicvm[.]com/server.jsp?action=%22BaseInfo%22&u=%22TURBNk1qQTZNVGc2TVRFNk1ERTZOalU9%22
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?action=What&u=21632843515764
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?action=BaseInfo&u=28508632430582
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://51[.]255[.]219[.]82/files/download/falconcoin[.]zip
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://158[.]69[.]57[.]135/card[.]jsp?action=BaseInfo&u=TURBNk1qQTZNVGc2TVRFNk1ERTZOalk9
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://92[.]222[.]106[.]229/card[.]jsp?action=BaseInfo&u=
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://www.eye-watch[.]in/design/img/perfmon.dat
Network Type:	url
Identifier:	Attacker
Actor:	APT38

Network Type:	network
Domain:	update.toythieves.com
Identifier:	Attacker
Actor:	APT38
IP:	210.52.109.255
Identifier:	Attacker
Actor:	APT38
Network Type:	network
URL:	http://92[.]222[.]106[.]229/card[.]jsp?action=BaseInfo&u=TURBNk1qQTZNVGc2TVRFNk1ERTZOalU9
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://51[.]255[.]219[.]82/files/download/falconcoin[.]pdf
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://sap.misapor[.]ch/favicon.ico
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/fancybox/include/cambio.xap
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?action=What&u=23225812046875
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?u=30341549164209
Network Type:	url
Identifier:	Attacker
Actor:	APT38
IP:	158.69.57.135
Identifier:	Related
Actor:	APT38
Network Type:	network
URL:	http://sap.misapor[.]ch/vishop/view.jsp

Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://158[.]69[.]57[.]135/hide[.]gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://trade.publicvm[.]com/images/character.gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://sap.misapor[.]ch/vishop/view.jsp
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?u=12011128451612
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?action=What&u=28508632430582
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://brou[.]com.uy/uy[.]com.brou-Theme/javascript/javascript.js?t=1477112270358
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://sap.misapor[.]ch:443/vishop/include/cambio.swf
Network Type:	url
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	channel.jetos.com
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	apps.got-game.org
Identifier:	Attacker
Actor:	APT38

Network Type:	network
Domain:	trade.publicvm.com
Identifier:	Attacker
Actor:	APT38
IP:	175.45.179.255
Identifier:	Attacker
Actor:	APT38
Network Type:	network
URL:	http://www.eye-watch[.]in/jscroll/images/images.jsp?pagenum=1
Network Type:	url
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	eye-watch.in
Identifier:	Related
Actor:	APT38
URL:	http://180[.]235[.]133[.]121/images/img[.]gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/jscroll/board/list.jsp?action=BaseInfo&u=43523315087040
Network Type:	url
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	onlink.epac.to
Identifier:	Attacker
Actor:	APT38
URL:	http://www.energydonate[.]com/files/download/Bithumb.zip
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://www.energydonate[.]com/files/download/bithumb.pdf
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/jscroll/board/list.jsp?action=What&u=43523315087040

Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/fancybox/images.jsp?pagenum=1
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.knf[.]gov.pl/DefaultDesign/Layouts/KNF2013/resources/accordian-src.js?ver=11
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://apps.got-game[.]org/images/character.gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch.in/design/fancybox/Pnf[.]action
Network Type:	url
Identifier:	Attacker
Actor:	APT38
IP:	41.203.65.250
Identifier:	Related
Actor:	APT38
Network Type:	network
URL:	http://www.energydonate[.]com/list.jsp?action=up
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	http://www.coinfox[.]info/news/4316-guardtime-using-blockchain-to-guard-industries
Network Type:	url
Identifier:	Attacker
Actor:	APT38
URL:	https://www.eye-watch[.]in/design/img/list.jsp?action=BaseInfo&u=3739922337404
Network Type:	url
Identifier:	Attacker
Actor:	APT38
Network Type:	network
Domain:	repview.ignorelist.com
Identifier:	Attacker
Actor:	APT38

URL:	http://www.businesshop[.]net/hide.gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38

URL:	http://41[.]203[.]65[.]250/eshop/include/cambio[.]swf
Network Type:	url
Identifier:	Attacker
Actor:	APT38

URL:	http://www.webkingston[.]com/update.jsp?action=need_update
Network Type:	url
Identifier:	Attacker
Actor:	APT38

URL:	https://www.eye-watch[.]in/design/img/list.jsp?action=BaseInfo&u=23225812046875
Network Type:	url
Identifier:	Attacker
Actor:	APT38

IP:	51.255.219.82
Identifier:	Related
Actor:	APT38
Network Type:	network

URL:	http://sap.misapor[.]ch/vishop/view.jsp?pagenum=1
Network Type:	url
Identifier:	Attacker
Actor:	APT38

URL:	http://51[.]255[.]219[.]82/theme[.]gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38

URL:	http://51[.]255[.]219[.]82/hide[.]gif
Network Type:	url
Identifier:	Attacker
Actor:	APT38

URL:	http://www.eye-watch[.]in/design/fancybox/images.jsp?pagenum=1
Network Type:	url
Identifier:	Attacker
Actor:	APT38

URL:	http://trade.publicvm[.]com/server.jsp?action=%22What%22&u=%22UkRRNlFVVTZOVEk2TmtZNk5UWTZNREE9%22
Network Type:	url
Identifier:	Attacker
Actor:	APT38
SHA1:	40021a9779c3d75251fe50c833b917d5a73c9d01
Fuzzy Hash:	3072:b4N6zXn2iTGCoYrIvhOaR8X3dfE8VQKMVZJl:b4N6zXmCoZOaR8X3ZoKM7Jl
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	119877258d9e5ff6b4e1a70a3c8f3692.virus
Malware Family:	QUICKRIDE
SHA256:	52de4a4a2bdc7dc5c64bb5b6032df6ffd37c512c694993c337d6913eab316d78
File Size:	128512
File Compilation Date Time:	October 20, 2016 05:30:05 AM
Identifier:	Attacker
Type:	fileType
MD5:	119877258d9e5ff6b4e1a70a3c8f3692
SHA1:	bcf977fb959b7f553e2671c8d2810f6fd1976a49
Fuzzy Hash:	768:9NCQFaKISRuDusn0c7+iO2Ydly1taYIbISMmnco/iMLqwoDkA6RGq7yROhpSsKUk:9rFl6l0c7WwLWPcaqwoDbmyROzjKU9C
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	SCLGNTFY.DLL
Malware Family:	WHITEOUT
SHA256:	1c94fb4d340d8308be330a618f29ddee6c2a0f2de1518917960097d88c3b1dfc
File Size:	65536
File Compilation Date Time:	September 21, 2015 12:48:47 AM
Identifier:	Attacker
Type:	fileType
MD5:	26f66f775c92cb629647cbe1331dc439
SHA1:	b1ac9c3eca2ef12ff883652ac8dc3db883ee6f6e
Fuzzy Hash:	3072:+tHzTmKNTDEJ0t4anwbVSlibrvDjjI86ssTOy/qKJiuv5:czT/NT/tLnsVlvDjjCsKOyyVuv
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	944439b6693b0589ae73421c0a342d8a
Malware Family:	RatankbaPOS
SHA256:	b66624ab8591c2b10730b7138cbf44703abec62bfc7774d626191468869bf21c
File Size:	142848
File Compilation Date Time:	December 07, 2017 03:54:12 AM
Identifier:	Attacker
Type:	fileType

MD5:	944439b6693b0589ae73421c0a342d8a
SHA1:	d900ea051b082e9f04fe5a7ab533fca59c18a12b
Identifier:	Attacker
Actor:	APT38
File Name:	deobfuscated
Malware Family:	QUICKRIDE.POWER
File Size:	153462
SHA256:	cf65b421315c89f12adb11a14b2d407a2cf98e20d85871eb6711bb9c0531dace
Type:	fileType
MD5:	92dfa90dc5389e496f612f50ef9fe3b3
SHA1:	2ca8d615c553925b65a7d2639d08700e71044b42
Identifier:	Attacker
Actor:	APT38
File Name:	cambio.xap
File Size:	64677
SHA256:	00501384ff0a9b6c20f12961008ebe5d26858f65e89b59b14d26cb2d115e1833
Type:	fileType
MD5:	4cc10ab3f4ee6769e520694a10f611d5
SHA1:	88554b0b8066cb059f9fc06d2620d84737251a29
Identifier:	Attacker
Actor:	APT38
File Name:	ALCHAIN.chm
File Size:	1457953
SHA256:	d5f9a81df5061c69be9c0ed55fba7d796e1a8ebab7c609ae437c574bd7b30b48
Type:	fileType
MD5:	9e36b094d9769025699804f10c9a6523
SHA1:	65b41f52f51d5290143a8713c266605c76b022e3
Fuzzy Hash:	1536:qMthrt5owtjpEq220VofvctInHf/DQJpqV+MzV36Mqf0DK3TEyLixYfjZG/GIhw+:HniVTIHQWJgvG/GIh68
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	c090a91efdaf0627450b1b979dac26223a22917688800ff6c60a1710d38225f1
Malware Family:	KEYLIME
SHA256:	c090a91efdaf0627450b1b979dac26223a22917688800ff6c60a1710d38225f1
File Size:	69632
File Compilation Date Time:	May 02, 2011 10:46:55 PM
Identifier:	Attacker
Type:	fileType
MD5:	b846d47e539ccf36cdbc6bfc2e8a5e2e
SHA1:	50b4f9a8fa6803f0aabb6fd9374244af40c2ba4c

Fuzzy Hash:	12288:E30MB7N+man4IrT0qhPyRg8o//ND6lAMYqcl:i0YNwrT0qhPFtHN2lLYq
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	abc.txt.exe.bin
Malware Family:	NACHOCHEESE
SHA256:	a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118
File Size:	408576
File Compilation Date Time:	July 08, 2016 10:11:36 PM
Identifier:	Attacker
Type:	fileType
MD5:	40e698f961eb796728a57ddf81f52b9a
SHA1:	bdb632b27ddb200693c1b0b80819a7463d4e7a98
Fuzzy Hash:	24576:5gDgaE2r55ENJSOZ8jsAMZMF2kPupVevS6ieT17cZ/hJMIYO0:+D9vrrs8OZxZl+wvTTahqO
Identifier:	Attacker
Actor:	APT38
File Name:	msmpeng.exe
Malware Family:	NACHOCHEESE
File Size:	1637888
File Compilation Date Time:	February 20, 2017 10:09:30 AM
SHA256:	70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38
Type:	fileType
MD5:	3c9e71400b72cc0213c9c3e4ab4df9df
SHA1:	3ea1ebf0f626d914c4185e12740f84cc2d4aef22
Identifier:	Attacker
Actor:	APT38
File Name:	newmacros
File Size:	3668
SHA256:	8a6a86ca4da8f70227a8e0e0ec9793c0650e638bc0676a15c1793f0fcb323576
Type:	fileType
MD5:	e54e0087fb07a9015d77c520e94de1a2
SHA1:	d851ff7b371d15bf03a670e45ec5df327406ab45
Identifier:	Attacker
Actor:	APT38
File Name:	opt.ps1
Malware Family:	QUICKRIDE.POWER
File Size:	206329
SHA256:	f7f2dd674532056c0d67ef1fb7c8ae8dd0484768604b551ee9b6c4405008fe6b
Type:	fileType
MD5:	6c360e9a6f933bf172591a81881ca79b
SHA1:	ab141ea1fd5d2198033bf3847a00f37894667d90
Fuzzy Hash:	192:odrH8nT4ErAtkHPH+JmP1oynWsmOWl0Wi:Y8nT4ErA/Q1xmOWl0Wi

Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	taskeng.exe
Malware Family:	SLIMDOWN
SHA256:	5809bab3ea5e3feba27fc97586ad762c9c93f657f47c366b68de62ec8add21d2
File Size:	24578
File Compilation Date Time:	January 03, 2016 07:37:52 AM
Identifier:	Attacker
Type:	fileType
MD5:	556d54d7ab1f52c715f21058bd6fe268
SHA1:	97a3698ffffdb63df79faeaf58169f9755db1f90
Identifier:	Attacker
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	gpsvc.exe
Malware Family:	QUICKRIDE
File Size:	128512
SHA256:	200c0f4600e54007cb4707c9727b1171f56c17c80c16c53966535c57ab684e22
Type:	fileType
MD5:	1507e7a741367745425e0530e23768e6
SHA1:	3d34eb23728f443e930885e89485cfc78cc34e07
Identifier:	Attacker
Actor:	APT38
File Name:	b64.txt
Malware Family:	QUICKRIDE.POWER
File Size:	211328
SHA256:	41f155f039448edb42c3a566e7b8e150829b97d83109c0c394d199cdcfd20f9b
Type:	fileType
MD5:	cba175498af45dca6970aeee83a6d9f4
SHA1:	ef263466563037c4f358e6467157194eb0752bdf
Identifier:	Attacker
Actor:	APT38
File Name:	12d79a84-67ae-5a05-9616-b3f5a709b0a0
File Size:	2049761
SHA256:	b9cf1cba0f626668793b9624e55c76e2dab56893b21239523f2a2a0281844c6d
Type:	fileType
MD5:	157074713fc886e3632acc6f040982dd
SHA1:	0d6632694e16569fab115c842f510765794f0e5c
Identifier:	Attacker
Actor:	APT38
File Name:	dae1344b-59ca-561a-a9ae-9022ab74f766
File Size:	152268

SHA256:	21eac314a438610449d6062584a963f748fa564437663ceaf25927403d6f9865
Type:	fileType
MD5:	563db5fc71da5f3bfc216aa3ec52f074
SHA1:	f54fed3a1c34f09e4119caa79ae48a369bdd8e75
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	17920
SHA256:	10cbb5d0974af08b5d4aa9c753e274a81348da9f8bfcaa5193fad08b79650cda
Type:	fileType
MD5:	0f8e2736877648b22baecad61c52692d
SHA1:	325e27077b4a71e6946735d32224ca0421140ef4
Fuzzy Hash:	3072:plRipWFnsn297EBifyASgCLrCLiq7Fu5E9S7KvnMkIzeG7K5yEHhLNy3:d4f2944fyASXubpAEUExy
Packer:	Microsoft Visual C++ 8.0 (DLL),
Actor:	APT38
File Name:	svchost.exe
SHA256:	1750d7ae9fccf192a79386a589e2f9073611854b0d7a515584ade2870feff2cc
File Size:	165888
File Compilation Date Time:	April 20, 2017 11:57:30 PM
Identifier:	Attacker
Type:	fileType
MD5:	8641e90dd7a6bd2151fb02da3112dcf0
SHA1:	decbe1c57510b3ca8e0e63ebafeb18e806fbc768
Fuzzy Hash:	3072:ppoYt47tRgXuj8NXpqo1gkXhIy0Vs/35Y4:ppC2BNszkRBp
Packer:	Microsoft Visual C++ v6.0 DLL,Armadillo v1.xx - v2.xx,Microsoft Visual C++ 6.0,
Actor:	APT38
File Name:	wmvdec.dll
Malware Family:	NESTEGG
SHA256:	28bfc374c747549643b2f1c4758ee0572d3aeb900bd29bc0e5c88c2bee1adefa
File Size:	192512
File Compilation Date Time:	December 08, 2014 12:12:17 PM
Identifier:	Attacker
Type:	fileType
MD5:	268dca9ad0dcb4d95f95a80ec621924f
SHA1:	97936a1225622bf61f916c629882aab19ff1f1a6
Identifier:	Attacker
Actor:	APT38
File Name:	b8739333-b531-54eb-981f-6bde2bdc4a0d
Malware Family:	QUICKRIDE.POWER
File Size:	203871

SHA256:	d844777dcafcde8622b9472b6cd442c50c3747579868a53a505ef2f5a4f0e26a
Type:	fileType
MD5:	5d06ff8f43f631cd2a71a565dd10b7a5
SHA1:	53b079072c81f7c879ea1f808c18dcd6134afc5c
Identifier:	Attacker
Actor:	APT38
File Name:	FALCON.chm
File Size:	1755618
SHA256:	01b047e0f3b49f8ab6ebf6795bc72ba7f63d7acbc68f65f1f8f66e34de827e49
Type:	fileType
MD5:	7a27da13bbdfc34118a30ecd83a75614
SHA1:	b30daf74b25b8615ada10cca195270c32e6b343a
Fuzzy Hash:	3072:ONXMmD9wkpopLQuzWBNkEZvUl7Hltyq1c:sczkpcnIkEZ80q
Identifier:	Attacker
Actor:	APT38
File Name:	bitsran.exe
Malware Family:	SHADYCAT
File Size:	150528
File Compilation Date Time:	October 01, 2017 02:37:31 PM
SHA256:	9cc69d81613285352ce92ec3cb44227af5daa8ad4e483ecc59427fe23b122fce
Type:	fileType
MD5:	d08f1211fe0138134e822e31a47ec5d4
SHA1:	8eb5111c5447498f47958b7911f0976090d98f75
Identifier:	Attacker
Actor:	APT38
File Name:	cambio.swf
File Size:	88521
SHA256:	8a18cdb23d623f69daa3c7580eed064e9b99203dda14d634f8bb72ac14197a0c
Type:	fileType
MD5:	1f2cd85583a4a56b764ba6429c2155ec
SHA1:	b8f6454c802c511e818e0f6c4acd05415f3854f5
Identifier:	Attacker
Actor:	APT38
File Name:	decrypted_8e32fccd70cec634d13795bcb1da85ff.hlp
Malware Family:	WHITEOUT
File Size:	3696
SHA256:	2e3c040e778c8579242f9c3ea0de7084ea4d99ad91667aa914d80572853d03fc
Type:	fileType
MD5:	e5b43b414a3cc16b774db6318171c586
SHA1:	744aea014fbab6747acaf3997f1ed2f37c052748

Fuzzy Hash:	6144:hRVcnc5DXuPbXw6wqYeg5lvD+kWVK25UQzYxvi7gqg4IpSlX/0BV1WTBbKhu9:h3uDXw6wqTgfD3WVFHzoP0/GbWTZqu9
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	e97512d0-9949-5790-beee-fe05c02ed6f1
Malware Family:	WHITEOUT
SHA256:	c992e76a0af12bd88c97e6e5aecd0fd872e6ac79520aa8970203f1edb373d1ac
File Size:	487424
File Compilation Date Time:	October 05, 2016 01:36:48 AM
Identifier:	Attacker
Type:	fileType
MD5:	001d1750f5c7652673e781d73b9b3f67
SHA1:	92103c4010779fb4c382b2adec47fb2215c4d190
Identifier:	Attacker
Actor:	APT38
File Name:	ORANGE/Sample1/srservice.chm
Malware Family:	WHITEOUT
File Size:	729088
SHA256:	424f6c3cda1ec91a97f74ea7e652fc5f44c13971364f28ae8eeb27c590f9beeb
Type:	fileType
MD5:	9216b29114fb6713ef228370cbfe4045
SHA1:	e57713866a28487098d6b735a55468a1570d00a1
Identifier:	Attacker
Actor:	APT38
File Name:	falcon.zip
File Size:	1748042
SHA256:	4eb2dd5e90bda6da5efbd213c8472775bdd16e67bcf559f58802a8c371848212
Type:	fileType
MD5:	985d627f638bbd89ba48676625ec9073
SHA1:	e41fa3589245d58d359de51255d6b025c617704b
Identifier:	Attacker
Actor:	APT38
File Name:	character.gif
Malware Family:	QUICKRIDE.POWER
File Size:	213945
SHA256:	99523fa81b0a2767236d6a3b11a363ad4f5bfb54e11ff99dd362adfce8d671f4
Type:	fileType
MD5:	04d072b5df97c9b3f9ff9fb0bb829028
SHA1:	d89760df8ce3c1fcd69d533334621132f88e459e
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	18507

SHA256:	699a7d396bc8b49b61a80897726b463d64081adc0f80e21bbdb92064d008cc81
Type:	fileType
MD5:	c3ecaa60f6da846cd856c00bfb0a7281
SHA1:	688183a9b36993c6dcc93d7be7a3e96a364447c9
Identifier:	Attacker
Actor:	APT38
File Name:	bithumb.zip
Malware Family:	QUICKCAFE
File Size:	1051
SHA256:	100c6400331fa1919958bed122b88f1599a61b3bb113d98b218a535443ebc3a7
Type:	fileType
MD5:	9ed66ef9fba9984fe7788eb1ec09d4ba
SHA1:	781386119695d5d38bd533130d724c9abf6f4ff6
Fuzzy Hash:	192:fR2ZAfr9QAWXN0KvSrIx5LC1jk8HRP4oynyNPZjh:6Afr9cNfK0LC9k8H94U9
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	carved_pe
Malware Family:	DYEPACK.FOX
SHA256:	764189cf2707175251df6837da12797420ae4c482ad70f50cc0ec4acd21e4dff
File Size:	20480
File Compilation Date Time:	December 04, 2015 01:04:25 AM
Identifier:	Attacker
Type:	fileType
MD5:	909e1b840909522fe6ba3d4dfd197d93
SHA1:	a543fb81077e261dacf07765d52acd4e2609ab18
Fuzzy Hash:	1536:pZyBY4gHHe5eNarTVvBer0/oedgyurNjU0FnTolfkQpgtbc+cz:/yBYjHHe5eNygI/7kFJtTBfkztvcz
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	hkcmd.exe
Malware Family:	SNAPSHOT
SHA256:	72a874868517f7e5104d18a526e52da71d374e2b733a5d5cafef66072c365f09
File Size:	102400
File Compilation Date Time:	April 13, 2008 05:38:12 PM
Identifier:	Attacker
Type:	fileType
MD5:	79a8b0c70e9a3770c4e6bdb60f57e723
SHA1:	2c6c244b3858ce06a0b646ae386f65e69ae5c046
Fuzzy Hash:	3072:NYLaCnWDXTttz6b1wTSzbrUPDBgFcQCnRB:SLaCnetzPTSzbrUtQCR
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,

Actor:	APT38
File Name:	svchost.tmp
Malware Family:	QUICKRIDE
SHA256:	95c8ffe03547bcb0afd4d025fb14908f5230c6dc6fdd16686609681c7f40aca2
File Size:	128512
File Compilation Date Time:	October 21, 2016 03:07:39 AM
Identifier:	Attacker
Type:	fileType
MD5:	cb52c013f7af0219d45953bae663c9a2
SHA1:	be2e900c64cd985cde9e8515fb4e5b5d70c853f0
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	1869659
SHA256:	6d4415a2cbedc960c7c7055626c61842b3a3ca4718e2ac0e3d2ac0c7ef41b84d
Type:	fileType
MD5:	ddabaa2740f590ac964996fd4b691880
SHA1:	4714d9b776c0eb5ec675a74b8d2b3731ca7c057a
Identifier:	Attacker
Actor:	APT38
File Name:	ORANGE/Sample1/srservice.hlp
Malware Family:	WHITEOUT
File Size:	3696
SHA256:	5a2bcd7edf31e772d10efd6e062778850de428e3fc0a12981a5a38bb4a91c073
Type:	fileType
MD5:	8e32fccd70cec634d13795bcb1da85ff
SHA1:	1999fdf4f32faa9ccc4ff6da91c10298b0402678
Fuzzy Hash:	1536:QqYwjSliowZe42SS6vU8UaHwLFmAnssnRNVEy/qKxZXiSBvG:TVSlibrvDjjI86ssTOy/qKJiuv
Identifier:	Attacker
Actor:	APT38
File Name:	embeded.bin
Malware Family:	RatankbaPOS
File Size:	79872
File Compilation Date Time:	December 05, 2017 01:53:14 PM
SHA256:	79a4b6329e35e23c3974960b2cecc68ee30ce803619158ef3fefcec5d4671c98
Type:	fileType
MD5:	203b1ceff471f8519d9df5a31243ed0d
SHA1:	0fee4153276b477e3b3fc292a6723d34b5bf550c
Identifier:	Attacker
Actor:	APT38
File Name:	payload.bin
Malware Family:	KEYLIME

File Size:	83968
SHA256:	c9717e04da266d036aa52142ccf879dd6c3f9642b7e5681444ee37606d8baf74
Type:	fileType
MD5:	5604d94db60fa406e6f9d3951d0ba7be
SHA1:	66d1b71c307e20dd033feee5590b32a97c3eb23f
Identifier:	Attacker
Actor:	APT38
File Name:	F-321dog_DSKNovBiznes.doc
File Size:	86528
SHA256:	2c703415a502316986b30c816fb434427ceb4f9673f45f84eec6de7e5315a261
Type:	fileType
MD5:	74440c1c517ce94c83ed7acd8a41c35c
SHA1:	4d2d4efcaef7f871c2d3e570200f1d17b4d92093
Fuzzy Hash:	1536:uX7MDHAOdbRHntND4x9/UaFtO5a/ACTYN77bFFpC8Fe8F/RLWc79:uoLl3Hnv4jUa7O5PCuvI+TVWc79
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	C:\MSO10\fltmsg.exe
Malware Family:	DYEPACK
SHA256:	f200d99817777b94e17a82110543ef7034fac184c30d1ef9417cfc7ae3a0737f
File Size:	90112
File Compilation Date Time:	August 18, 2016 09:24:41 PM
Identifier:	Attacker
Type:	fileType
MD5:	0abdaebbdbd5e6507e6db15f628d6fd7
SHA1:	fb17a710aa690d939d74a6687ae04787fb6324ca
Identifier:	Attacker
Actor:	APT38
File Name:	MailSender.chm
File Size:	18401
SHA256:	772b9b873100375c9696d87724f8efa2c8c1484853d40b52c6dc6f7759f5db01
Type:	fileType
MD5:	878ececefc811b91361b69ff25290a6e
SHA1:	ed5105d690b05f74beba93bc4f1be0a0e987a1e6
Fuzzy Hash:	768:H6BTOjFjv9aQn4qhv3ppkZLtX8BPca3Jwmn9FKe:HAKjJ1JZ5ca3H9Ff
Packer:	Microsoft Visual C# / Basic .NET,
Actor:	APT38
File Name:	Shell_siver.dll
SHA256:	2a6f218c6907859a62673116625500b11cd855f28e32968e84e4d1e0558b47fb
File Size:	41472
File Compilation Date Time:	April 27, 2016 02:40:26 PM

Identifier:	Attacker
Type:	fileType
MD5:	aceca55c73b3fc3d768d4d2b7314c1f7
SHA1:	a7322764ed01ba9b65ae83c9f4dfd884fe90dd8f
Fuzzy Hash:	768:u4EdIS2BDUshUAZnUh6unT8U7FC0rwG8Xr0ggj3Vvi/nM6R2jzqQFlbHjV:zEySAQspZnU58qM0U0ggj3VynM6R2jz9
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	jusched.exe
Malware Family:	KEYLIME
SHA256:	e8fae9085adbc1cf2acf026b34a81cdae7a35f922096f96528e9b3e4d34a2db8
File Size:	45056
File Compilation Date Time:	October 26, 2015 12:50:43 PM
Identifier:	Attacker
Type:	fileType
MD5:	08fb4c4b5fd8d80dd248e5c2b921dfa4
SHA1:	d367d8de3cfd49110aa7e9b5f8cb5af7f0cf1208
Identifier:	Attacker
Actor:	APT38
File Name:	icoplatform.zip
File Size:	10219
SHA256:	3e91f399d207178a5aa6de3d680b58fc3f239004e541a8bff2cc3e851b76e8bb
Type:	fileType
MD5:	3fcdf6aaa5010a53b50237eb83f8caa9
SHA1:	ff44bc9c1392eb51b2fbbace65dfb6afcb7b2af5
Identifier:	Attacker
Actor:	APT38
File Name:	deobfuscated
File Size:	151842
SHA256:	c94c789e614b69b9670c0461f689f3eaafa48d0a72b63bf3d29551309a1eb8c5
Type:	fileType
MD5:	846ce6d1dffb62f992284253a81c765b
SHA1:	eb1b592461a6efc6b006fd8b2850177b59981110
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
Malware Family:	QUICKRIDE.POWER
File Size:	153692
SHA256:	20f7e342a5f3224cab8f0439e2ba02bb051cd3e1afcd603142a60ac8af9699ba
Type:	fileType
MD5:	eb5d430f919711656c1d22dca36ce320

SHA1:	1a6ce54d005929ce28269c5f4ea7fced6be2c21a
Identifier:	Attacker
Actor:	APT38
File Name:	3.bin.swf
File Size:	18739
SHA256:	5e3c194c0257aa4e952e039ff22ed994bb236c6eec80301746dc1204a0c0eeb6
Type:	fileType
MD5:	2e92f42c3c240fddeef8e497ca632122

SHA1:	8c49715595695f7685dd708f0b0dedebff8c146d
Fuzzy Hash:	6144:MkQRqrtisdV856KiwLBtHZo5eeqB3Fx+w92KFcYX:FX8IKiCBtW5zqB3+6RcYX
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	igfxpers.exe
Malware Family:	NESTEGG
SHA256:	05a7e4edd80ac1c929808622d5287703885cc0d217e308ea05c2babc96b1e5ea
File Size:	253952
File Compilation Date Time:	September 22, 2014 12:12:17 PM
Identifier:	Attacker
Type:	fileType
MD5:	6eec1de7708020a25ee38a0822a59e88

SHA1:	4630a00691e51193a51f3c9a76f85662235e12e4
Identifier:	Attacker
Actor:	APT38
File Name:	alchain.js
Malware Family:	QUICKCAFE
File Size:	3208
SHA256:	8d75a57818dc8cfba0451aaf6f25a4b706b78ebc2a8fa57c0a1396ef077bb948
Type:	fileType
MD5:	b89639507de6236d038f27dec6d8d041

SHA1:	ffed9b25d6ac89d6ce149a2993bd8a58023c232e
Fuzzy Hash:	1536:KPEJKQPKHxeuKO0w31nlwSiUA7UlaPU4NgyNfHPK:FKQP7uKhwVbHAsR4NgyNfS
Identifier:	Attacker
Actor:	APT38
File Name:	C:\MSO10\MXS.dll
Malware Family:	DYEPACK
File Size:	91136
File Compilation Date Time:	August 18, 2016 09:24:31 PM
SHA256:	6d8d14768be117a968beb226403a70e18be210df9b1509aa7c0d9cb70b06198b
Type:	fileType
MD5:	f5e0f57684e9da7ef96dd459b554fded

SHA1:	87d8803f0c399eca0c613bf90c917d66e1e2d57e

Fuzzy Hash:	192:odrH8nT4ErAtkHPH+JmP1oynWsmOWl0W:Y8nT4ErA/Q1xmOWl0W
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	taskeng.exe
Malware Family:	SLIMDOWN
SHA256:	bdcfa3b6ca6b351e76241bca17e8f30cc8f35bed0309cee91966be9bd01cb848
File Size:	24576
File Compilation Date Time:	January 03, 2016 07:37:52 AM
Identifier:	Attacker
Type:	fileType
MD5:	0d7d0f6728bfb5413fe69f897503a0a3

SHA1:	72b92e4da9d1f77ff35f05c22cc46b788d25a7a0
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	18738
SHA256:	47aa24ad42484f1da08db82f823e41e0e148d687df03bdefb10323bb1c64ab91
Type:	fileType
MD5:	27f9c5aada3a3fc468ddb416a9d2e199

SHA1:	be20491fecd8ce7cab33c6371db05a99a9190925
Fuzzy Hash:	768:FC0rK3wCW4Myh6soUDNyVQN1y0EU8lxODtvUUSv9YdN:U0mPWrysq0QXy0yUDBUUSSN
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	igfxpers.exe
Malware Family:	KEYLIME
SHA256:	5c21813c60c4145390779eee23943d6b0dd3e07cd63a56ad3a8c76502bd0dd76
File Size:	36864
File Compilation Date Time:	October 26, 2015 12:50:43 PM
Identifier:	Attacker
Type:	fileType
MD5:	b8c97064d3fb4f2c5a15ff738a8c5b0c

SHA1:	6ab10bd838f9b060f2380caafdea5ff09080f536
Identifier:	Attacker
Actor:	APT38
File Name:	alchain.zip
File Size:	1450227
SHA256:	81617bd4fa5d6c1a703c40157fbe16c55c11260723b7f63de022fd5dd241bdbf
Type:	fileType
MD5:	43f7512685e72de1e8c0201ee4e189a7

SHA1:	424cf0fdf41b711556d0b9ac01a12926f7755580
Identifier:	Attacker
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,Installer VISE Custom,
Actor:	APT38
File Name:	hkcmd.exe
Malware Family:	WORMHOLE
File Size:	49152
SHA256:	0fc1dc03a51f57fa0a24ad32248cb14765a14de9d30d847a3a1add3f678abfc4
Type:	fileType
MD5:	02f75c2b47b1733f1889d6bbc026157c

SHA1:	f891fde8908ae18801d7a0be1eeab07391c00c1b
Fuzzy Hash:	768:KBPgLwzlNyQZMtjrwUn3/T3q5EzBh200SEpunj3fi3kDsRSXTXpxPJBz2dM3PF:WnROtjLTMMBh28EIjfiNCDhwdMf
Identifier:	Attacker
Actor:	APT38
File Name:	filetokenbroker.dll
Malware Family:	BLINDTOAD
File Size:	60416
File Compilation Date Time:	January 05, 2017 12:11:33 AM
SHA256:	1b3c22ad57d48674e3cad45794daa6e08edad45ad7a1d1c2ac871e1ff2043a88
Type:	fileType
MD5:	0edbad9e6041d43f97c7369439a40138

SHA1:	f2260f801c37118b7f9945628d414d09cd1f7c8d
Fuzzy Hash:	1536:GY/z37Djcph119u7Y9qUxa2RcTPpoT6ON34h0uNQtWzorSC6us8:v/zLDjcXv9u77k6vCtWzcSCG8
Packer:	Microsoft Visual C++ v6.0 DLL,Armadillo v1.xx - v2.xx,Microsoft Visual C++ 6.0,
Actor:	APT38
File Name:	secmgr.dll
Malware Family:	WHITEOUT
SHA256:	ef368e2af3118970a81231db2beec6ad181f513e6db8f8bdfdc205e9739c8421
File Size:	102400
File Compilation Date Time:	January 07, 2016 06:58:24 PM
Identifier:	Attacker
Type:	fileType
MD5:	c7263515a33989ced3cd07731357fe34

SHA1:	e859c90964f59405c53316cf092fa29a3ccfdadd
Fuzzy Hash:	98304:41LJjV9VaSIA3MKF2o4NG4hmZRJNFD4eA8C+nxszkpnWv:41LJjVqA8KF4NG4hmZRrxAhAW
Packer:	Microsoft Visual C++ 8.0 (DLL),
Actor:	APT38
File Name:	e264340f4d7c0179cd2453e9297b3388.unpacked.memory.dmp
Malware Family:	CLEANTOAD

SHA256:	a7b088ed168806eece93396578470dac2bddb1e78f1f9f3c7ab342d3cbdd9eb6
File Size:	5531136
File Compilation Date Time:	January 09, 2018 09:13:41 AM
Identifier:	Attacker
Type:	fileType
MD5:	d95b208aed0d04958888229f1ead54b6
SHA1:	ec0752b7fc651f31efc86e1eb2cd368e741bbab2
Fuzzy Hash:	384:fiVozFHCJWomL6oLzWXCTMHTTBGyA3Humm82XGY4XfJbJdiYG:uhEogf3Omx2XvYJbJs
Packer:	Microsoft Visual C# / Basic .NET,Microsoft Visual Studio .NET,.NET executable,Microsoft Visual C# v7.0 / Basic .NET,
Actor:	APT38
File Name:	binaryreader.dll
SHA256:	e535cf04335e92587f640432d4ec3838b4605cd7e3864cfba2db94baae060415
File Size:	30720
File Compilation Date Time:	March 28, 2016 07:23:49 PM
Identifier:	Attacker
Type:	fileType
MD5:	7b4a8be258ecb191c4c519d7c486ed8a
SHA1:	d08573c5e825b7beeb9629d03e0f8ff3cb7d1716
Fuzzy Hash:	768:qV/3fZLqIWp1NQtGhT9zYaMg0XxS4wVex+1yIU:qVnJqIaf7R0XF2
Identifier:	Attacker
Actor:	APT38
File Name:	$Recycle.Bin/S-1-5-21-4181698017-2819414590-2523785033-1012/RSWB79E.tmp
Malware Family:	HERMES
File Size:	29696
File Compilation Date Time:	October 01, 2017 10:34:07 AM
SHA256:	e08fc761cc22953de7fcc1684b7424755fa52f361dd5c6605b1469a80cb858bb
Type:	fileType
MD5:	b27881f59c8d8cc529fa80a58709db36
SHA1:	2e344cb889843233ff54e95dd0c5956489d07b7d
Identifier:	Attacker
Actor:	APT38
File Name:	falconcoin.zip
Malware Family:	QUICKCAFE
File Size:	1066
SHA256:	e7581e1f112edc7e9fbb0383dd5780c4f2dd9923c4acc09b407f718ab6f7753d
Type:	fileType
MD5:	239aaff9c0c7b0317df0d0c409780d11
SHA1:	5964013dc698a24495c6542bf2c9e90cad6c7b15
Identifier:	Attacker
Actor:	APT38
File Name:	installwizard.py

File Size:	20955
SHA256:	345a6a13f30599911b986eb489624220ea15dc32215a114f9fff953aeea60e9b
Type:	fileType
MD5:	7c2d5f5b30711b0ea28aedc706c579ad
SHA1:	f2b9b4769f8b6b8919b9109c902120f5637108af
Identifier:	Attacker
Actor:	APT38
File Name:	f84849b6-896f-5608-a30b-e6f11bfc321c
Malware Family:	QUICKRIDE.POWER
File Size:	151859
SHA256:	6cac0be2120be7b3592fe4e1f7c86f4abc7b168d058e07dc8975bf1eafd7cb25
Type:	fileType
MD5:	a957767639bcbbfd9cf8b1cdd2dd9db0
SHA1:	b1e42b4269302ad479b4ebb16954d83c11fc53ef
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
Malware Family:	QUICKRIDE.POWER
File Size:	158489
SHA256:	e085e8c428cd08eee58156cf4c3c50ef82d3a385e352b8303914b4a4a85fc72b
Type:	fileType
MD5:	b25d3a4507d11f0acc11377d0219ca47
SHA1:	5a1e36a4078247ccf659be8afa71e693d9a40922
Fuzzy Hash:	98304:6M61Jy3UvhsKDDjjr90EUjOG9wQwn/kL:6M61Jy3Uv6KbZUj/wQwnc
Identifier:	Attacker
Actor:	APT38
File Name:	SvcTimeBroker_unpacked_dump_dll
Malware Family:	CHEESETRAY
File Size:	5297152
File Compilation Date Time:	October 24, 2016 07:32:11 AM
SHA256:	49ba8bff664f13aac53f85af4de206454ca01e602466a3dc725502800ed2d026
Type:	fileType
MD5:	2e8b028583528a3c559e407445c403c0
SHA1:	234600a43a957672b8145ea6566f9613a1906899
Identifier:	Attacker
Actor:	APT38
File Name:	theme.gif
Malware Family:	QUICKRIDE.POWER
File Size:	206329
SHA256:	1768f2e9cea5f8c97007c6f822531c1c9043c151187c54ebfb289980ff63d666
Type:	fileType

MD5:	ec264b9c938355f1a7d1dc97c73fa9a6
SHA1:	1c174732c0421a0d2058931c8d7eecf28ba32499
Identifier:	Attacker
Packer:	Microsoft Visual C++ v6.0 DLL,Armadillo v1.xx - v2.xx,Microsoft Visual C++ 6.0,Microsoft Visual C++ 6.0 DLL,
Actor:	APT38
File Name:	fmapi.dll
Malware Family:	NESTEGG
File Size:	106496
SHA256:	c9e764e7238d10dbc62d1a7e2398bcdb8822602f5abc6d67ad8d01019b2d6f50
Type:	fileType
MD5:	bbd703f0d6b1cad4ff8f3d2ee3cc073c

SHA1:	7badbfa8b836907018f7a6bca203bc3a66c451f3
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	18704
SHA256:	650d7b814922b58b6580041cb0aa9d27dae7e94e6d899bbb3b4aa5f1047fca0f
Type:	fileType
MD5:	cd3dbbc496ac8ab6c3f0f3f9b0f200e6

SHA1:	bc95ba33d7b714f6c9ea52996ba183dc98eeb040
Fuzzy Hash:	1536:Mn7NtWQnb0SAOv1uThi2C86u7cTUHPCiAQoKt:Mn7jb0SJv1uYs6u7nzoK
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	3af4e21bbbeb846ca295143e03ec0054.virus
Malware Family:	SORRYBRUTE
SHA256:	efa57ca7aa5f42578ab83c9d510393fcf4e981a3eb422197973c65b7415863e7
File Size:	77824
File Compilation Date Time:	October 19, 2016 10:24:47 PM
Identifier:	Attacker
Type:	fileType
MD5:	3af4e21bbbeb846ca295143e03ec0054

SHA1:	e56f9bac422efc22e54d489e039b916ce7d98f2b
Identifier:	Attacker
Actor:	APT38
File Name:	top_bar.gif
File Size:	1253
SHA256:	6952b9e7a69aa0b6e593a665c726fb1d9c3b3277808871a256959e12f899472f
Type:	fileType
MD5:	8c3d37ef7357f3d7ed07ff1782f33aba

SHA1:	63781411bc176f10c970222d21b0cecdc324efc6
Fuzzy Hash:	24576:uKJczq2vEwkTghhLtMkpI+Ens50z9OKg:N2vEwk0rtMj+es58k
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	1f991a86df304cab9ea6fe9a650ded5a_unp.exe
Malware Family:	SCRUBBRUSH
SHA256:	b3b98014fdd1d76a51215471b440e35e3d26b0f1b1916a4da89671a2f170a665
File Size:	1601535
File Compilation Date Time:	June 30, 2016 03:05:43 AM
Identifier:	Attacker
Type:	fileType
MD5:	3f70b0f9836747f5aee28f27aa5fdeae

SHA1:	fa4f2e3f7c56210d1e380ec6d74a0b6dd776994b
Fuzzy Hash:	768:NazIufvSYwDT+ln68lnZZTIgHh3KQaO0zDcEYIXoB5reG466cEmwYQUP5hX+kD+T:PQl6gZZTx3KzYE5VFPYQi9Y4g
Packer:	Microsoft Visual C++ 8.0 (DLL),
Actor:	APT38
File Name:	ORANGE/Sample2/fdsvc.exe
Malware Family:	NACHOCHEESE
SHA256:	cd10ffb7a88f0d2ec69326e7a13f00b9ed211a3a719f89a755a29494ff1142e6
File Size:	60928
File Compilation Date Time:	August 26, 2016 02:19:00 AM
Identifier:	Attacker
Type:	fileType
MD5:	9914075cc687bdc352ee136ac6579707

SHA1:	587fd0d9c15ee93539d629df715c344cba3594ea
Fuzzy Hash:	24576:IlhCO4K6s/w7pb7BDwBfYlxOQptT/Fun2:3O4K6p7wSlMQbTt
Packer:	Microsoft Visual C++ 8.0 (DLL),
Actor:	APT38
File Name:	5dc8080d-58d4-579a-9c54-e42ffe5aba9c
Malware Family:	WHITEOUT
SHA256:	a146cc1d94098644203d5f416ee0a08c6e67d991f944045d7de3eaad93cfc613
File Size:	799744
File Compilation Date Time:	October 05, 2016 05:17:10 PM
Identifier:	Attacker
Type:	fileType
MD5:	c83a707a39fe4b2cb8a2a96bd37a48ba

SHA1:	c71273dd6dbbd0f3d519e9964708e2e18bcf4daa
Fuzzy Hash:	1536:GJcF2Xo4r05+/L35PU/W3MOXTj61AdvhfzFoKtq3SeFnToIf6myt:GS4XoE335PUT2v9xpQ3SetTBf6myt
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38

File Name:	igfxpers.exe
Malware Family:	SNAPSHOT
SHA256:	17af47fb34e683e111b785dc51f10696e6316403e2cf45bf0687056fd72f6e26
File Size:	98304
File Compilation Date Time:	August 27, 2015 07:19:10 AM
Identifier:	Attacker
Type:	fileType
MD5:	660339ec42c12e31582f333cf948ccbc
SHA1:	77c7a17ccd4775b2173a24cd358ad3f2676c3452
Fuzzy Hash:	6144:ee3Vr64hIBQUQsWxfIp/dUloZcNePMi46NsVIC07m7Jch5RUfI:en2IBsp9xWX66NsV/am7JK5f
Identifier:	Attacker
Actor:	APT38
File Name:	IMEKLMG.exe.dmp
Malware Family:	WHITEOUT
File Size:	376832
File Compilation Date Time:	June 14, 2016 10:56:42 AM
SHA256:	642c019f880b38467aadf50a4420a5b0ff6a903613ea4ed81cace46cdba6b348
Type:	fileType
MD5:	06cd99f0f9f152655469156059a8ea25
SHA1:	6a8e5b5b499f82e0bb8e5f89574be3747705d09a
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
Malware Family:	QUICKRIDE.POWER
File Size:	329
SHA256:	d3142f2bf581153afa0a6d5831993fdd77a312bef26f67dde033da083b86830b
Type:	fileType
MD5:	c30aec699e0a8f526e3cc3cc991702cf
SHA1:	11568dffd6325ade217fbe49ce56a3ee5001cbcc
Identifier:	Attacker
Actor:	APT38
File Name:	ORANGE/Sample2/fdsvc.dll
Malware Family:	NACHOCHEESE
File Size:	480768
SHA256:	752b8e93a8f6803b265dd3a7cd39df86997cf99900426635b1b97dd665bd7f9f
Type:	fileType
MD5:	9cc6854bc5e217104734043c89dc4ff8
SHA1:	76bab478dcc70f979ce62cd306e9ba50ee84e37e
Identifier:	Attacker
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	evtsys.exe

Malware Family:	CLOSESHAVE
File Size:	16384
SHA256:	ae08635023938 0f56470c19d6a200f7d251c7422c7bc5ce74730ee8bab8e6283
Type:	fileType
MD5:	5d0ffbc8389f27b0649696f0ef5b3cfe
SHA1:	97319b2d974cfae60bcb1441090a3a6d33e4c01d
Identifier:	Attacker
Actor:	APT38
File Name:	1.bin.swf
File Size:	18508
SHA256:	75f8087cb2ef39df44907909b751e0b2914fc559397c178e9869b8833852fc04
Type:	fileType
MD5:	a2692f8acb3c3e1fdb3030d68b843496
SHA1:	32e180ec765cdb9e25c19b636cfa5b3501827872
Identifier:	Attacker
Actor:	APT38
File Name:	power_ratankba
Malware Family:	QUICKRIDE.POWER
File Size:	153479
SHA256:	5928e54383e61e6df56adf092fc4e50caf12a2af1ce26b34c2aec49bb1fde6fe
Type:	fileType
MD5:	054941d2b8679dff65003d1c224cdda2
SHA1:	178994ab2d4fc0a32a328e97d7d220c8bbb9150c
Fuzzy Hash:	3072:xlhvr5rWIAx8YebVMTKz5biwUV/pNf3Qp3zRW:/hvrc8Y/TKz5biXDYpN
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	unknown
Malware Family:	QUICKRIDE
SHA256:	99017270f0af0e499cfeb19409020bfa0c2de741e5b32b9f6a01c34fe13fda7d
File Size:	129024
File Compilation Date Time:	October 27, 2016 02:55:43 AM
Identifier:	Attacker
Type:	fileType
MD5:	1f7897b041a812f96f1925138ea38c46
SHA1:	27e61e1bb31fe21c00e469afeb0b9f56476461ff
Identifier:	Attacker
Actor:	APT38
File Name:	deobfuscated
File Size:	152251
SHA256:	890c3c81706d00f1e654fd2b41c6100a34477e402269377b99bfc2e8eb8777a8
Type:	fileType

MD5:	d453ad11b6a8bfa2eca3896e44aa2c0d
SHA1:	50420970d17af649affaee6be801968aa4c01e46
Identifier:	Attacker
Actor:	APT38
File Name:	bithumb.js
Malware Family:	QUICKCAFE
File Size:	3412
SHA256:	8ff100ca86cb62117f1290e71d5f9c0519661d6c955d9fcfb71f0bbdf75b51b3
Type:	fileType
MD5:	23cbc415d94b1841a8a737295dc651ce
SHA1:	c5aa78a11cbf8e22fd1b1afb7797d08ac706c391
Identifier:	Attacker
Actor:	APT38
File Name:	installwizard.pyc
File Size:	23091
SHA256:	caf4858a2fa87bf506b9337deadd4a75fdf8d652a8d20d691086fdaf72833f84
Type:	fileType
MD5:	cf58b6b6c72eb24cd27924d56600030f
SHA1:	1f7f9a41505865870a9600f6915aa5a3d4ce3014
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
Malware Family:	CLEANTOAD
File Size:	5104
SHA256:	3c958f7d9db4fed59377442b0ad7880713a2ad9c851bc249aeae3e05e3e5883e
Type:	fileType
MD5:	98952934205a6249edc47b99adf99de5
SHA1:	6ea7ee1d2f83c0dad39eda83ae35db77951eb60f
Identifier:	Attacker
Actor:	APT38
File Name:	2.bin.swf
File Size:	15200
SHA256:	10e8cbaa49990bc1c88bc746d15d47a1641c8ba7c473c6129a4d13a3401d264f
Type:	fileType
MD5:	fcaba866e58e4eabcad81c140b8ebc40
SHA1:	537cf4311fb66b3740c0a1dc9ba073132d9e0d04
Fuzzy Hash:	786432:jQWIx7QxrMk/xMRISdLNBXHYz+xOuw/zuKBV99TIr:jQWIx7QFMOqDy+2/qK/9lK
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	ElectronGold-1.1.exe

SHA256:	b530de08530d1ba19a94bc075e74e2236c106466dedc92be3abdee9908e8cf7e
File Size:	30014566
File Compilation Date Time:	July 31, 2017 02:20:53 PM
Identifier:	Attacker
Type:	fileType
MD5:	f3dd79ffb45d226dd029da7c61192e26
SHA1:	d05b54ec58d116e7913e2034c1e556e40acf7d5e
Fuzzy Hash:	6144:pnkwsc7Dc+eFvnERQXegKyHDCkFuwPO2NZcXzOii00cCqs/RrV1WTBrJhBV:pY+AvnERQOgrD7FubAibi9/NbWThDBV
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	mso.exe
Malware Family:	WHITEOUT
SHA256:	e5bc4c5794483273dd610ae69913d473440d5533d4f8b2abb77cd64f5af47374
File Size:	487424
File Compilation Date Time:	June 14, 2016 10:56:42 AM
Identifier:	Attacker
Type:	fileType
MD5:	2ef2703cfc9f6858ad9527588198b1b6
SHA1:	f5fc9d893ae99f97e43adcef49801782daced2d7
Fuzzy Hash:	6144:sdqAqUok+00rm9TOi9Vc7/VtXvWLnJlh+efvoRKmjbL/xY4fTKKWSFle3IDgDi2C:xABogwttXuLnJlkkiKU/xtKYydF9iIU
Identifier:	Attacker
Actor:	APT38
File Name:	decrypted-fdsvc.dll
Malware Family:	NACHOCHEESE
File Size:	480768
File Compilation Date Time:	August 26, 2016 03:11:49 AM
SHA256:	8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1
Type:	fileType
MD5:	889e320cf66520485e1a0475107d7419
SHA1:	e0d5117ed5035658e9d5e67bc4b695958260eeaf
Fuzzy Hash:	6144:sdqAqUok+00rm9TOi9Vc7/VtXvWLnJlh+efvoRKmjbL/xY4fTKKWSFle3IDgDi2C:xABogwttXuLnJlkkiKU/xtKYydF9iIU
Identifier:	Attacker
Actor:	APT38
File Name:	fdsvc_decrypted.dll
Malware Family:	NACHOCHEESE
File Size:	480776
File Compilation Date Time:	August 26, 2016 03:11:49 AM
SHA256:	aff19e65f87b672f7e89a4f07ae551a679bd2ceb2bb04814a79983ce77655457
Type:	fileType
MD5:	5994a8fd8c68dd1cc51ce7ca0d9c2749
SHA1:	74a3a013dca36c31bc240f63332637dc1d7fb0c5

Fuzzy Hash:	768:FKwRDVVGhgvTnTyo4zEhXizz3k4dq4PPkPVUgAno:FKzgvLToOXizztM43AVmo
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	msdtc.exe
Malware Family:	MAPMAKER
SHA256:	fc5885b56995b0f7a3e0f8a49aebc9f76c945f545f224c3e670593302cf688ab
File Size:	49152
File Compilation Date Time:	February 05, 2016 01:55:37 AM
Identifier:	Attacker
Type:	fileType
MD5:	2d759966b88efe4b193db78e05b0130b
SHA1:	5b730432a01fbd4a4cb346ffe690f671699cd21e
Fuzzy Hash:	1536:PfMN0EvInxfd/gXck1YaBiJB6wUoSDXmyROIjKUHC:8N0L9d/Ic7d6NoSDXmyROWHC
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	bpi_old.scr
Malware Family:	WHITEOUT
SHA256:	ac2dc644e767a78e5739e327aa671e4f4f731b880464a5c0389bb51477ae5d4a
File Size:	73728
File Compilation Date Time:	January 03, 2016 02:58:10 PM
Identifier:	Attacker
Type:	fileType
MD5:	55aa499da876e339528df71cd028617f
SHA1:	a1bc507b1c5c7a82e713554afe0f4cece900b6a2
Fuzzy Hash:	12288:wg9R9uzvkdQYRt6o1hgvS+Oe6Mx57ZiagQYLn4yFuZ:wg9Kzvkt6o1aZTYLn4yFuZ
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	foxit_reader.exe
Malware Family:	DYEPACK.FOX
SHA256:	ab9031e553b439290b9852ad39651c03bde00c300ea54bd61279fb9ae9f9434d
File Size:	1327104
File Compilation Date Time:	December 04, 2015 01:04:23 AM
Identifier:	Attacker
Type:	fileType
MD5:	0b9bf941e2539eaa34756a9e2c0d5343
SHA1:	2cf5412955d509c43cf915fd42ad0c952f68c920
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	15199

SHA256:	e47117c57a38dd2e16459d5a559579d2be44f48bcb8e62db56f9261cf87273fa
Type:	fileType
MD5:	549afa09ed3d26935381977349294573
SHA1:	fbc9e003690727f3bff6957beabad58b018c00b7
Fuzzy Hash:	3072:b4N6zXn2iTGCoYrIvhOaR8X3dfE8VQKMVZJlq:b4N6zXmCoZOaR8X3ZoKM7Jlq
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	53da95da2842fb3a84aba16a4d2b346b2308e832d69dd4034f9b98880f7c51c2.exe
Malware Family:	QUICKRIDE
SHA256:	53da95da2842fb3a84aba16a4d2b346b2308e832d69dd4034f9b98880f7c51c2
File Size:	128515
File Compilation Date Time:	October 20, 2016 05:30:05 AM
Identifier:	Attacker
Type:	fileType
MD5:	bf377a0225615e6cc90d57654bd3b45e

SHA1:	69031f915b89da98c82d43742909efaf7fe36137
Identifier:	Attacker
Actor:	APT38
File Name:	shellcode.bin
Malware Family:	RAWHIDE
File Size:	2328
SHA256:	7ebf07ccf9862584b63208ed16b06bf9ffc7139f0088abfd3671022c1db2a16f
Type:	fileType
MD5:	9bddb2c678605297a7f519afcd179edb

SHA1:	9cc396887f57d1d266644cbefed48f33880fb218
Identifier:	Attacker
Actor:	APT38
File Name:	1.ps1
Malware Family:	QUICKRIDE.POWER
File Size:	158494
SHA256:	db8163d054a35522d0dec35743cfd2c9872e0eb446467b573a79f84d61761471
Type:	fileType
MD5:	ed2cace34381b6bbeb98af31e73e7904

SHA1:	8fd089df71a5f48098dc41886631ea6604f108e9
Identifier:	Attacker
Actor:	APT38
File Name:	ICOPlatform.chm
File Size:	17768
SHA256:	9d10911a7bbf26f58b5e39342540761885422b878617f864bfdb16195b7cd0f5
Type:	fileType

MD5:	dc688e6ddd3a1298dd372ec7d0ccb1fb
SHA1:	09c1756064f15fcdd29ff8f239b3d5dcc22ac492
Identifier:	Attacker
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	Svchost.exe
Malware Family:	QUICKRIDE
File Size:	129024
SHA256:	825624d8a93c88a811262bd32cc51e19538c5d65f6f9137e30e72c5de4f044cc
Type:	fileType
MD5:	911de8d67af652a87415f8c0a30688b2
SHA1:	a771ceecbd4cc5f5196d6cede489e1d29752241c
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	2024
SHA256:	e0d7b8d962666e98bfd8380597fd5c13e7928fb42995ea25eb35d97b7cfaaa57
Type:	fileType
MD5:	490f5282f42a2bc9525ba650adc03cb7
SHA1:	70bf16597e375ad691f2c1efa194dbe7f60e4eeb
Identifier:	Attacker
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	nroff_b.exe
Malware Family:	DYEPACK
File Size:	24576
SHA256:	5b7c970fee7ebe08d50665f278d47d0e34c04acc19a91838de6a3fc63a8e5630
Type:	fileType
MD5:	1d0e79feb6d7ed23eb1bf7f257ce4fee
SHA1:	5117cf04030ad67c09c70f3d0772815e4f9ae08a
Fuzzy Hash:	3072:Kgd8z0pasUC6O4tuiSTeBm6Fh1W0bt9TBf5ZX:KgezODUC6O/iSTeBm6j7bt9TB
Packer:	Microsoft Visual C++ 8.0 (DLL),
Actor:	APT38
File Name:	sllaunch.exe
Malware Family:	SNAPSHOT
SHA256:	2c41854a6adf4d3f8b37048ec12ff087b4014a8ae5538e667e6933a37f3d7df3
File Size:	117248
File Compilation Date Time:	August 27, 2015 07:22:01 AM
Identifier:	Attacker
Type:	fileType

MD5:	b73479d4ce3f5e72f270145a756d1088
SHA1:	9be1d789b7b795036f11f38da6d81d7722ab3204
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	55708
SHA256:	10b2b3957d8f33bf14481a4e9676fa82476549a7a66aa9134be2d77f47603f82
Type:	fileType
MD5:	36365cef4169d92b678718c2d6e5ca99
SHA1:	a07dc261645c7b3ff5f37f5ae7ee0b629ab8f109
Identifier:	Attacker
Actor:	APT38
File Name:	falconcoin.js
Malware Family:	QUICKCAFE
File Size:	3232
SHA256:	7975c09dd436fededd38acee9769ad367bfe07c769770bd152f33a10ed36529e
Type:	fileType
MD5:	01118e4cd8adec69c84e0311ec677971
SHA1:	de9ab0f1eefbaa7256dc33eeaf6eb6c519b9fb2c
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
Malware Family:	BLINDTOAD
File Size:	4019200
SHA256:	c7b275788950eec3d76c048ef2c6ca60fab60fc173beef0d36c941a5e4d496e5
Type:	fileType
MD5:	e31b8d0cdf695605075edfd371f8c721
SHA1:	99342e6325cdf5c26bfbedbd88d5ff8987b5a76a
Fuzzy Hash:	12288:/hy8Rx5jApZ9+DB2b++lB1Y7wTEWOTghhLtMkpOOCjWq70QJnTynGUkHzpbQ+GKg:s+czq2vEwkTghhLtMkpI+Ens50z9OKg
Identifier:	Attacker
Actor:	APT38
File Name:	Windows/System32/MpShell.exe
Malware Family:	SCRUBBRUSH
File Size:	799232
File Compilation Date Time:	June 30, 2016 03:05:43 AM
SHA256:	6528731168b5c759af75d2728d93536ef91d27e18334b45adf026db9b609c3dc
Type:	fileType
MD5:	1f991a86df304cab9ea6fe9a650ded5a
SHA1:	76c7877910182d0eee9424bcd18048a724045c0f

Fuzzy Hash:	3072:nR1lEuvwbJEJQtaEGE2dt4ehJTHgvSdsVXoEZG9rG6dtzPMnhEe:nJHo21r4eTHg8BrdtQnhE
Packer:	Microsoft Visual C++ v6.0 DLL,Armadillo v1.xx - v2.xx,Microsoft Visual C++ 6.0,
Actor:	APT38
File Name:	waindex.dll
SHA256:	290fb8184958c628b93a2f787b0ba0b1466f0e1bcf6ffa17fb4e36ee9659e663
File Size:	196608
File Compilation Date Time:	December 28, 2014 07:27:50 PM
Identifier:	Attacker
Type:	fileType
MD5:	00cd1418f8b808fd9f2aca81c31804d7
SHA1:	aa115e6587a535146b7493d6c02896a7d322879e
Fuzzy Hash:	24576:5uP41Xvb//dCfl+Qfk7BEJc+XlRO7KRCrFTWB43TZ7rtvx33:5uP41z/ID/c2OFyBYTRrJxn
Identifier:	Attacker
Actor:	APT38
File Name:	srservice.dll
Malware Family:	HOTWAX
File Size:	1515008
File Compilation Date Time:	December 07, 2016 11:53:43 PM
SHA256:	8578a73ca08c708b8242d58cdb4579c0e7ceff0a0f9a9dddad448d2a3e3842ef
Type:	fileType
MD5:	16a278d0ec24458c8e47672529835117

SHA1:	ba5a2230ff2068b7fb22de3b83031457d18c3298
Identifier:	Attacker
Actor:	APT38
File Name:	cambio.swf
Malware Family:	SMOOTHRIDE
File Size:	57035
SHA256:	c1b29afcfddb79cfd57545b8600922150843ae2b170fff9aeacdeaa17adbf792
Type:	fileType
MD5:	6dffcfa68433f886b2e88fd984b4995a

SHA1:	8f404c9a75e881f8ca05ce6c5934a369c1c7ac1d
Identifier:	Attacker
Actor:	APT38
File Name:	accordian-src[1].js
File Size:	4382
SHA256:	d41823606d781e07f58df2f132d9fb9dfa5b92a5bd7cbebe858207f22bfed317
Type:	fileType
MD5:	5129694968b4cce04c38ebb21f5bab03

SHA1:	5c2ef418a36799541cec673dd7d9f87371a9e3bd
Fuzzy Hash:	1536:8f0XnibgFacx2jecu0FRf6Ut3JhH0Y4LZ2FkRg:fEecVNvhUYqS

Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	dimens.exe
Malware Family:	BOOTWRECK
SHA256:	8a81a1d0fae933862b51f63064069aa5af3854763f5edc29c997964de5e284e5
File Size:	61440
File Compilation Date Time:	December 26, 2017 01:47:19 AM
Identifier:	Attacker
Type:	fileType
MD5:	571de903333a6951b8875a73f6cf99c5
SHA1:	7a6bb34dcd0acf33cd8b3dceb6321db03a11d01e
Fuzzy Hash:	3072:+tHzTmKNTDEJ0t4anwbVSlibrvDjjI86ssTOy/qKJiuv:czT/NT/tLnsVlvDjjCsKOyyVuv
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	b66624ab8591c2b10730b7138cbf44703abec62bfc7774d626191468869bf21c
Malware Family:	RatankbaPOS
SHA256:	e5208e1ad4f31c20f500774963ab1a19c96016040528deac6311163056580e13
File Size:	136671
File Compilation Date Time:	December 07, 2017 03:54:12 AM
Identifier:	Attacker
Type:	fileType
MD5:	5803efcd5dd2f20ac56eb7e333be0996
SHA1:	041c2a1a5810aa91788fc8b1604078c8133de1c3
Fuzzy Hash:	6144:sdqAqUok+00rm9TOi9Vc7/VtXvWLnJlh+efvoRKmjbL/xY4fTKKWSFle3IDgDi2j:xABogwttXuLnJlkkiKU/xtKYydF9iIUa
Identifier:	Attacker
Actor:	APT38
File Name:	041c2a1a5810aa91788fc8b1604078c8133de1c3
Malware Family:	NACHOCHEESE
File Size:	522160
File Compilation Date Time:	August 26, 2016 03:11:49 AM
SHA256:	9c62a70397370d5de689c66c667266ed4ebaa899d159a472c977fd94efcc1ef3
Type:	fileType
MD5:	284c1d29e54201447180dd174d9397e3
SHA1:	1bf7913b1d266cedcea8ed70f0cbdc7609df1c71
Fuzzy Hash:	12288:wg9R9uzvkdQYRt6o1hgvS+Oe6Mx57ZiagQYLT:wg9Kzvkt6o1aZTYLT
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	2cf958232095d71507512eca49dacbf3d4e77864
Malware Family:	DYEPACK.FOX

SHA256:	47ea0abdb35b66df6498630e39fa1ded9aed02f8bb77db9842267b7a01035c5d
File Size:	472500
File Compilation Date Time:	December 04, 2015 01:04:23 AM
Identifier:	Attacker
Type:	fileType
MD5:	422e4a929934c0b7011db49b16074aec
SHA1:	06d941556831c3413591b078a70c8484e0b5d30b
Identifier:	Attacker
Actor:	APT38
File Name:	hide.gif
File Size:	1980
SHA256:	4722138dda262a2dca5cbf9acd40f150759c006f56b7637769282dba54de0cab
Type:	fileType
MD5:	6258f16dfc57e6b98e8ed5a748fde904
SHA1:	ee6464c4a360e8a87303ccb293ae2f563258519c
Fuzzy Hash:	1536:PfMN0EvInxfd/gXck1YaBiJB6wUoSDXmyROIjKUnC:8N0L9d/Ic7d6NoSDXmyROWnC
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	SCLGNTFY.DLL
Malware Family:	WHITEOUT
SHA256:	ddebee8fe97252203e6c943fb4f9b37ade3d5fefe90edba7a37e4856056f8cd6
File Size:	73728
File Compilation Date Time:	January 03, 2016 02:58:10 PM
Identifier:	Attacker
Type:	fileType
MD5:	7f549a71dddac3de68015ad489da4cca
SHA1:	1eff40761643f310a5cd7449230d5cfe9bc2e15f
Fuzzy Hash:	12288:g1wIwj2hnFVA0Ge79ess0OdYwmQ6VnsQyztjyDY9mlZ7GhZo4o:FIwj2hnz9HstdYwmDVnsQyN/E0f
Identifier:	Attacker
Actor:	APT38
File Name:	srservice_chm_to_dll_decrypted.dll
Malware Family:	WHITEOUT
File Size:	729088
File Compilation Date Time:	October 22, 2016 06:09:50 AM
SHA256:	21c83fe249400991acb83820261e8d252c4d24689bf9ecd4595c47dd630d7b9f
Type:	fileType
MD5:	fde55de117cc611826db0983bc054624
SHA1:	6058c906bc82326256a793b8494c0a84b2303f12
Fuzzy Hash:	3072:hLIlsDbXt4x0I/o9WsSEMkYvcimbkxA2fgRlCwK:SIYax3FiYvcnHlC
Packer:	Microsoft Visual C++ v6.0 DLL,Armadillo v1.xx - v2.xx,Microsoft Visual C++ 6.0,

Actor:	APT38
File Name:	c_windows_system32_diagmgs.dll
Malware Family:	NESTEGG
SHA256:	cc3829bd9c1c580dc8ae070e447789f2557d6e8b200c9f01c896b413b93a1d79
File Size:	192512
File Compilation Date Time:	October 15, 2014 01:17:14 AM
Identifier:	Attacker
Type:	fileType
MD5:	03a3a4dca00d218c5a8817c2c224143c
SHA1:	d9476b3018be277da1aa2b03543166a1a8d1ff03
Fuzzy Hash:	786432:tQWIx7QxrMk/xMRISdLNBXHYz+xOuw/zuKBV99TIra:tQWIx7QFMOqDy+2/qK/9lKa
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	ElectronGold-1.1.1.exe
SHA256:	eab612e333baaec0709f3f213f73388607e495d8af9a2851f352481e996283f1
File Size:	30020312
File Compilation Date Time:	July 31, 2017 02:20:53 PM
Identifier:	Attacker
Type:	fileType
MD5:	2dfebcb60dfa706e2a9c6e73709ebff5
SHA1:	b5290f23d5346cf02c075845543f00093f2e79b1
Fuzzy Hash:	192:odrH8nT4ErAtkHPH+JmP1oynWsmOWl0W:Y8nT4ErA/Q1xmOWl0W
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	taskeng.exe
Malware Family:	SLIMDOWN
SHA256:	138464214c78a73e3714d784697745acbf692ef40419d31418e4018e752cb92b
File Size:	24576
File Compilation Date Time:	January 03, 2016 07:37:52 AM
Identifier:	Attacker
Type:	fileType
MD5:	c157acf215bba49b893649fd59804265
SHA1:	46b6f05be5436098f5ed9012063fb9292a640224
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
Malware Family:	QUICKRIDE.POWER
File Size:	103310
SHA256:	0abde79e9de5f7b18f328e70d86e941634a0a75ce7696b522a90742011a6dd77
Type:	fileType

MD5:	ac62603ff2862a219e3a885fe8a65c92
SHA1:	46a1d019c1069a8da16224ba6e964d929f42f204
Identifier:	Attacker
Actor:	APT38
File Name:	Bitcoin Trading Platform.chm
File Size:	20435
SHA256:	6cb1e9850dd853880bbaf68ea23243bac9c430df576fa1e679d7f26d56785984
Type:	fileType
MD5:	e3fc2fbc512b90c54d81989cf42bb885
SHA1:	63088b27de67ca726a01cd4e2a233c48af974993
Fuzzy Hash:	12288:XNiGkKwVC4AAQUy+msfd73XmyDNSh1TcdjYhflbLSbCGtJB3t+izi3hu:dPkVwUy+mimDoUpMCG3t+i1
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,Safeguard 1.03 -> Simonzh,
Actor:	APT38
File Name:	45959307
Malware Family:	WORMHOLE
SHA256:	9c7063a03a6628549d826ae754f0ceaec1725273bf3c75d14bf08c2bf82833d2
File Size:	729088
File Compilation Date Time:	September 17, 2014 03:59:33 PM
Identifier:	Attacker
Type:	fileType
MD5:	459593079763f4ae74986070f47452cf
SHA1:	be4267725a51440fe7a31a63ea19b9d3afa7adfa
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	3079
SHA256:	2065e6aec2622ecb6980ceaab73af81d80cd4f8844eb3832f61b72747e7b714e
Type:	fileType
MD5:	e62c30df1f9739573950bccc909cc3eb
SHA1:	d2e455cf20d9200a33d31eaaba19452e24a977b8
Fuzzy Hash:	3072:UY/5SbJz+luvaq+4IrCMZ+mZmqEQShWTBfgHdoc2N1:UY/cbJ5vaq+4IuMZ+mUqUWTB6v2
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,Microsoft Visual C++ v6.0,
Actor:	APT38
File Name:	compact.exe
Malware Family:	NESTEGG
SHA256:	c05329f101979fa75ca297c4f77c8cd69fe8eb499d4f693550b734beb9f564b9
File Size:	102400
File Compilation Date Time:	January 08, 2016 03:41:18 PM
Identifier:	Attacker
Type:	fileType

MD5:	b9be8d53542f5b4abad4687a891b1c03
SHA1:	7260340b7d7b08b7a9c7e27d9226e17b7170a436
Fuzzy Hash:	1536:VbqYu6Hr3HAzWtXdRITCAAGaG8qrCeofYHxcy4QiinN+l5:9qYuayWhfITC9ZdQO4cXQBN0
Identifier:	Attacker
Actor:	APT38
File Name:	ORANGE/Sample1/srservice.dll
Malware Family:	WHITEOUT
File Size:	79360
File Compilation Date Time:	October 22, 2016 06:08:16 AM
SHA256:	6c1d8c4afbc7f85f05fb2e4d17e5553255b0195a0b56ba5309e362e2156debfc
Type:	fileType
MD5:	e29fe3c181ac9ddbb242688b151f3310
SHA1:	47d2c4b0fba7b9cb5093ad31b5269349bf2ebcaa
Fuzzy Hash:	1536:+GOjFQP+VOunBSeWNT+xXrPSCTjFN1o6pXd4Demt8wm4Cw4:+VjFQqOuBRMKxXbvNoamtvvCw4
Packer:	Microsoft Visual C++ v6.0 DLL,Armadillo v1.xx - v2.xx,Microsoft Visual C++ 6.0,
Actor:	APT38
File Name:	rassapi32.dll
Malware Family:	WHITEOUT
SHA256:	ce893ef34eaa94cb63fb6efe129f43d511fb2685745aae494cbd81486ad71fb7
File Size:	98304
File Compilation Date Time:	January 08, 2016 05:56:46 PM
Identifier:	Attacker
Type:	fileType
MD5:	d0411922ee3a0427591371efb39829f2
SHA1:	6422f7a9e123c21038e614b08936b036ce8dfe28
Fuzzy Hash:	3072:mAt2RZOGK3Hugi2n5T8HlN+GDu2JAuTdByY6WgC:mAg+GK+gi2n5T8HlNFaINTeYZ
Identifier:	Attacker
Actor:	APT38
File Name:	qwinsta.dll
Malware Family:	WHITEOUT
File Size:	132096
File Compilation Date Time:	January 07, 2016 07:22:14 PM
SHA256:	4f9e05bc30291f39e0f682954fecd168a6fe2e95ec4007f9aa25d4f142de84d8
Type:	fileType
MD5:	4798e1942b4902b7a8709e8ae1ff4619
SHA1:	6207b92842b28a438330a2bf0ee8dcab7ef0a163
Identifier:	Attacker
Actor:	APT38
File Name:	gpca.dat
Malware Family:	DYEPACK
File Size:	33848

SHA256:	b07b37f0246bd436addbe5d702b12485d7bc8a9ef1475b54bff513a18e68fef7
Type:	fileType
MD5:	f7272bb1374bf3af193ea1d1845b27fd
SHA1:	2abfd795397a343596c9f95ecb721250f80eda61
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
File Size:	3444
SHA256:	25f13dca780bafb0001d521ea6e76a3bd4dd74ce137596b948d41794ece59a66
Type:	fileType
MD5:	980272269926a187ec4fe17ec9505a5f
SHA1:	1592ba6fcacee9e12ca09373f2264838139dafbb
Fuzzy Hash:	6144:sdqAqUok+00rm9TOi9Vc7/VtXvWLnJlh+efvoRKmjbL/xY4fTKKWSFle3IDgDi2C:xABogwttXuLnJlkkiKU/xtKYydF9iIU
Identifier:	Attacker
Actor:	APT38
File Name:	25200d3fe30785f3c90a91faf8ebf1b5.dll
Malware Family:	NACHOCHEESE
File Size:	519392
File Compilation Date Time:	August 26, 2016 03:11:49 AM
SHA256:	7d0ffd9fa1b21581fe9a1e1d852e348c83d4c3bbbd6751eb7f232e1bb27cc1ac
Type:	fileType
MD5:	25200d3fe30785f3c90a91faf8ebf1b5
SHA1:	39ed922d998ba650e166b28be86a193959a1b69b
Fuzzy Hash:	12288:wg9R9uzvkdQYRt6o1hgvS+Oe6Mx57ZiagQYLn4yFp:wg9Kzvkt6o1aZTYLn4yFp
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	f50fbed4582e44062897d1a388eea207df454005
Malware Family:	DYEPACK.FOX
SHA256:	9448ab6006a6fb5c347e43c2c61f51d54d7afb27f4d2f96905ae893f1624d16e
File Size:	639100
File Compilation Date Time:	December 04, 2015 01:04:23 AM
Identifier:	Attacker
Type:	fileType
MD5:	f5ad21678c5336cc67084201cb2578e2
SHA1:	e352bc25b88ea7e1179fc79db5a08674fdf29b81
Identifier:	Attacker
Actor:	APT38
File Name:	lsultana.cer__dec.txt
Malware Family:	KEYLIME
File Size:	36836
SHA256:	143c0c8e449975a9587bd43ce948d358aaa098ee7af7f0ebf8b3158fe72f5d0f

Type:	fileType
MD5:	8c2f4ce230bdd2b36c409cb4bdea65f0
SHA1:	1983b60d923b01fcb14ba813532b2f41f2d6c2fe
Identifier:	Attacker
Actor:	APT38
File Name:	Bithumb/bithumb.xls
File Size:	537088
SHA256:	972b598d709b66b35900dc21c5225e5f0d474f241fefa890b381089afd7d44ee
Type:	fileType
MD5:	d253d65adf4285fa5004cd96e647a11f
SHA1:	525a8e3ae4e3df8c9c61f2a49e38541d196e9228
Fuzzy Hash:	768:P+rhB2lc1zNHru6hLQwAzrtNcbnVo/K/103QI1k2jh/skyFMbMhnqw/0OiKgBUKa:qB2WpPhjw3cmw01k2jh/shyggRlkR
Packer:	Microsoft Visual C++ v6.0,Microsoft Visual C++ 5.0,Microsoft Visual C++,
Actor:	APT38
File Name:	evtdiag.exe
Malware Family:	DYEPACK
SHA256:	4659dadbf5b07c8c3c36ae941f71b631737631bc3fded2fe2af250ceba98959a
File Size:	65536
File Compilation Date Time:	February 05, 2016 10:46:20 AM
Identifier:	Attacker
Type:	fileType
MD5:	24d76abbc0a10e4c977a28b33c879248
SHA1:	d7fbef81c5d6b9293766b2ac1b4913b9184ba42d
Identifier:	Attacker
Actor:	APT38
File Name:	unknown
Malware Family:	QUICKRIDE.POWER
File Size:	153686
SHA256:	99ad06cca4910c62e8d6b68801c6122137cf8458083bb58cbc767eebc220180d
Type:	fileType
MD5:	3ddb0e4b5fda8c76919ba4d9b01145a2
SHA1:	c7e7dd96fefca77bb1097aeeefef126d597126bd
Fuzzy Hash:	3072:6U5r72JE+FYWR0jZLShk4cPT/QzSaQ0sCFneZTznIhZJJcrJ1GHeV9:6U5uJpYnZL05STQNddFnAnGZIrV
Packer:	Microsoft Visual C++ 8,VC8 -> Microsoft Corporation,Microsoft Visual C++ 8,
Actor:	APT38
File Name:	splwow32.exe
Malware Family:	NACHOCHEESE
SHA256:	9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852
File Size:	232960
File Compilation Date Time:	February 20, 2017 10:09:30 AM

Identifier:	Attacker
Type:	fileType
MD5:	97aaf130cfa251e5207ea74b2558293d
SHA1:	de201a51f96af1405f58ec02b7802088ecae6a2d
Identifier:	Attacker
Actor:	APT38
File Name:	5_6283065828631904327.chm
File Size:	1850147
SHA256:	030b4525558f2c411f972d91b144870b388380b59372e1798926cc2958242863
Type:	fileType
MD5:	a3487b13cbda458bf91c7e802a1ea4f5

Common Vulnerabilities and Exposures

CVE ID:	CVE-2016-4119(NVD Description)External Link CVE-2015-8651(NVD Description)External Link CVE-2016-1019(NVD Description)External Link

Version Information

Version:1.0, September 27, 2018 11:52:00 AM
APT38: Unusual Suspects

Version:2.0, September 28, 2018 01:15:00 PM
APT38: Unusual Suspects

Version:3.0, October 05, 2018 08:15:00 PM
APT38: Unusual Suspects

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/18-00016353