TLP:WHITE

Alert (AA20-239A)

FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks

Original release date: August 26, 2020

Summary

This joint advisory is the result of analytic efforts among the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury (Treasury), the Federal Bureau of Investigation (FBI) and U.S. Cyber Command (USCYBERCOM). Working with U.S. government partners, CISA, Treasury, FBI, and USCYBERCOM identified malware and indicators of compromise (IOCs) used by the North Korean government in an automated teller machine (ATM) cash-out scheme—referred to by the U.S. Government as "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks."

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

CISA, Treasury, FBI, and USCYBERCOM highlight the cyber threat posed by North Korea—formally known as the Democratic People's Republic of Korea (DPRK)—and provide recommended steps to mitigate the threat.

Refer to the following Malware Analysis Reports for associated IOCs: CROWDEDFLOUNDER, ECCENTRICBANDWAGON, ELECTRICFISH, FASTCash for Windows, HOPLIGHT, and VIVACIOUSGIFT.

Click here for a PDF version of this report.

!!!WARNING!!!
Since February 2020, North Korea has resumed targeting banks in multiple countries to initiate fraudulent international money transfers and ATM cash outs. The recent resurgence follows a lull in bank targeting since late 2019. This advisory provides an overview of North Korea's extensive, global cyber-enabled bank robbery scheme, a short profile of the group responsible for this activity, in-depth technical analysis, and detection and mitigation recommendations to counter this ongoing threat to the Financial Services sector.
!!!WARNING!!!

TLP:WHITE

Technical Details

TLP:WHITE

North Korea's intelligence apparatus controls a hacking team dedicated to robbing banks through remote internet access. To differentiate methods from other North Korean malicious cyber activity, the U.S. Government refers to this team as BeagleBoyz, who represent a subset of HIDDEN COBRA activity. The BeagleBoyz overlap to varying degrees with groups tracked by the cybersecurity industry as Lazarus, Advanced Persistent Threat 38 (APT38), Bluenoroff, and Stardust Chollima and are responsible for the FASTCash ATM cash outs reported in October 2018, fraudulent abuse of compromised bank-operated SWIFT system endpoints since at least 2015, and lucrative cryptocurrency thefts. This illicit behavior has been identified by the United Nations (UN) DPRK Panel of Experts as evasion of UN Security Council resolutions, as it generates substantial revenue for North Korea. North Korea can use these funds for its UN-prohibited nuclear weapons and ballistic missile programs. Additionally, this activity poses significant operational risk to the Financial Services sector and erodes the integrity of the financial system.

The BeagleBoyz's bank robberies pose severe operational risk for individual firms beyond reputational harm and financial loss from theft and recovery costs. The BeagleBoyz have attempted to steal nearly $2 billion since at least 2015, according to public estimates. Equally concerning, these malicious actors have manipulated and, at times, rendered inoperable, critical computer systems at banks and other financial institutions.

- In 2018, a bank in Africa could not resume normal ATM or point of sale services for its customers for almost two months following an attempted FASTCash incident.
- The BeagleBoyz often put destructive anti-forensic tools onto computer networks of victim institutions. Additionally, in 2018, they deployed wiper malware against a bank in Chile that crashed thousands of computers and servers to distract from efforts to send fraudulent messages from the bank's compromised SWIFT terminal.

North Korea's widespread international bank robbery scheme that exploits critical banking systems may erode confidence in those systems and presents risks to financial institutions across the world. Any BeagleBoyz robbery directed at one bank implicates many other financial services firms in both the theft and the flow of illicit funds back to North Korea. BeagleBoyz activity fits a known North Korean pattern of abusing the international financial system for profit.

- Fraudulent ATM cash outs have affected upwards of 30 countries in a single incident. The conspirators have withdrawn cash from ATM machines operated by various unwitting banks in multiple countries, including in the United States.
- The BeagleBoyz also use unwitting banks, including banks in the United States, for their SWIFT fraud scheme. These banks are custodians of accounts belonging to victim banks or unknowingly serve as a pass-through for the fraud. Most infamously, the BeagleBoyz stole $81 million from the Bank of Bangladesh in 2016. The Federal Reserve Bank of New York stopped the remainder of this attempted $1 billion theft after detecting anomalies in the transfer instructions they had received.

TLP:WHITE

FASTCash Update

TLP:WHITE

North Korea's BeagleBoyz are responsible for the sophisticated cyber-enabled ATM cash-out campaigns identified publicly as "FASTCash" in October 2018. Since 2016, the BeagleBoyz have perpetrated the FASTCash scheme, targeting banks' retail payment system infrastructure (i.e., switch application servers processing International Standards Organization [ISO] 8583 messages, which is the standard for financial transaction messaging).

Since the publication of the in October 2018, there have been two particularly significant developments in the campaign: (1) the capability to conduct the FASTCash scheme against banks hosting their switch applications on Windows servers, and (2) an expansion of the FASTCash campaign to target interbank payment processors.

- In October 2018, the U.S. Government identified malware used in the FASTCash scheme that has the capability to manipulate AIX servers running a bank's switch application to intercept financial request messages and reply with fraudulent, but legitimate-looking, affirmative response messages to enable extensive ATM cash outs. The U.S. Government has since identified functionally equivalent malware for the Windows operating system. Please see the Technical Analysis section below for more information about the ISO 8583 malware for Windows.
- The BeagleBoyz initially targeted switch applications at individual banks with FASTCash malware but, more recently, have targeted at least two regional interbank payment processors. This suggests the BeagleBoyz are exploring upstream opportunities in the payments ecosystem.

For more information about FASTCash, please see https://www.us-cert.gov/ncas/alerts/TA18-275A.

BEAGLEBOYZ Profile

The BeagleBoyz, an element of the North Korean government's Reconnaissance General Bureau, have likely been active since at least 2014. As opposed to typical cybercrime, the group likely conducts well-planned, disciplined, and methodical cyber operations more akin to careful espionage activities. Their malicious cyber operations have netted hundreds of millions of U.S. dollars and are likely a major source of funding for the North Korean regime. The group has always used a calculated approach, which allows them to sharpen their tactics, techniques, and procedures while evading detection. Over time, their operations have become increasingly complex and destructive. The tools and implants employed by this group are consistently complex and demonstrate a strong focus on effectiveness and operational security.

Community Identifiers

The BeagleBoyz overlap to varying degrees with groups tracked by the cybersecurity industry as: APT38 (FireEye), Bluenoroff (Kaspersky), Lazarus Group (ESTSecurity), and Stardust Chollima (CrowdStrike).

TLP:WHITE

Targeted Nations

TLP:WHITE

The BeagleBoyz likely have targeted financial institutions in the following nations from 2015 through 2020: Argentina, Brazil, Bangladesh, Bosnia and Herzegovina, Bulgaria, Chile, Costa Rica, Ecuador, Ghana, India, Indonesia, Japan, Jordan, Kenya, Kuwait, Malaysia, Malta, Mexico, Mozambique, Nepal, Nicaragua, Nigeria, Pakistan, Panama, Peru, Philippines, Singapore, South Africa, South Korea, Spain, Taiwan, Tanzania, Togo, Turkey, Uganda, Uruguay, Vietnam, Zambia (figure 1).

Figure 1: Nations probably targeted by BeagleBoyz since 2015

Anatomy of a BeagleBoyz Bank Heist

Figure 2 provides a graphical depiction of a BeagleBoyz bank heist. The next section describes in detail the end-to-end actions the BeagleBoyz take to rob financial institutions with a malicious cyber operation.

TLP:WHITE

TLP:WHITE

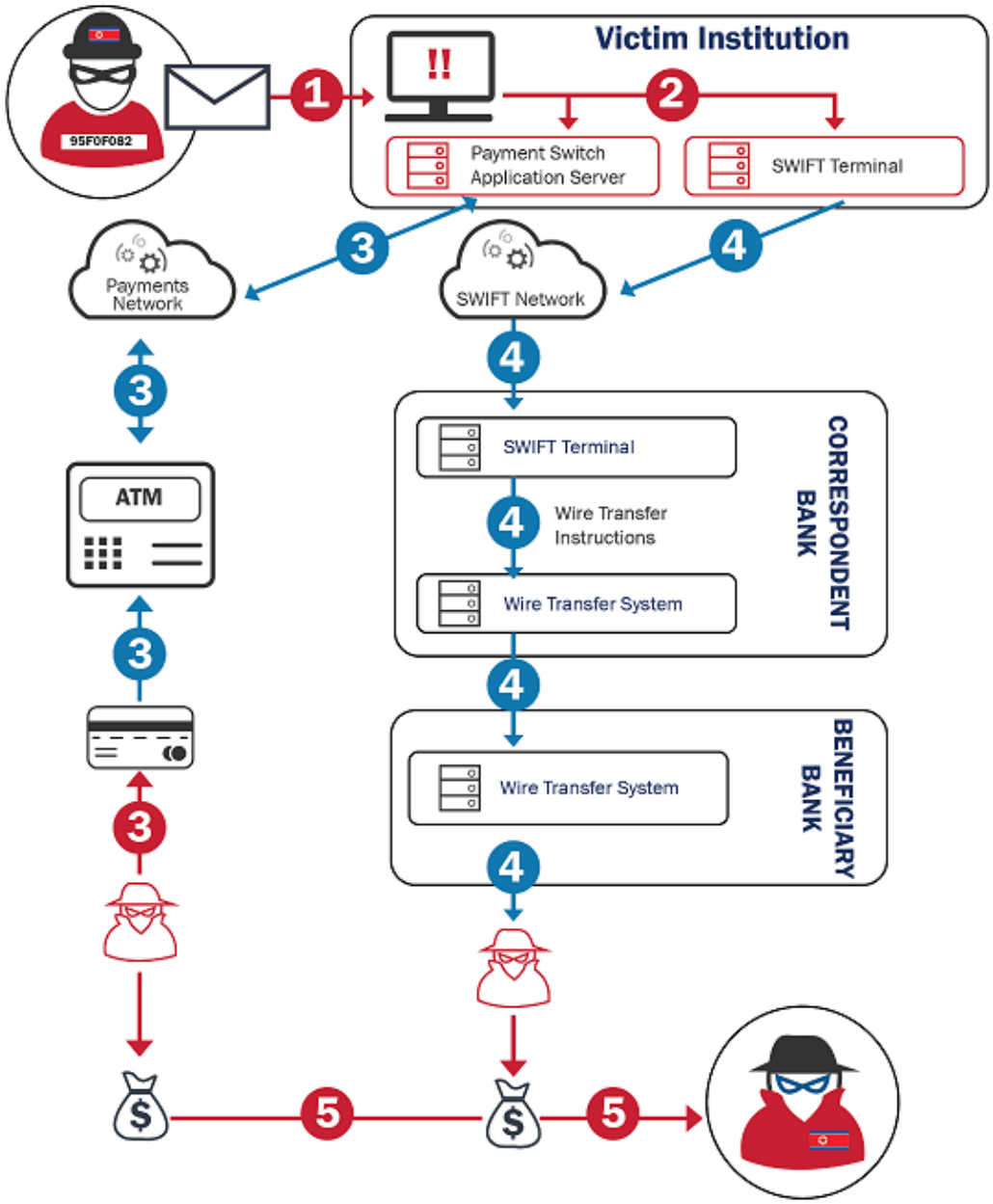

Figure 2: BeagleBoyz Bank Heist overview

Technical Analysis

The BeagleBoyz use a variety of tools and techniques to gain access to a financial institution's network, learn the topology to discover key systems, and monetize their access. The technical analysis below represents an amalgamation of multiple known incidents, rather than details of a single operation. These findings are presented to highlight the group's ability to tailor their techniques to different targets and to adapt their methods over time. Consequently, there is a need for layered mitigations to effectively defend against this activity, as relying solely on network signature detection will not sufficiently protect against North Korea's BeagleBoyz.

Initial Access

TLP:WHITE

TLP:WHITE

The BeagleBoyz have used a variety of techniques, such as spearphishing and watering holes, to enable initial access into targeted financial institutions. Towards the end of 2018 through 2019 and in early 2020, the BeagleBoyz demonstrated the use of social engineering tactics by carrying out job-application themed phishing attacks using the following publicly available malicious files.

MD5: b484b0dff093f358897486b58266d069
MD5: f34b72471a205c4eee5221ab9a349c55
MD5: 4c26b2d0e5cd3bfe0a3d07c4b85909a4
MD5: 52ec074d8cb8243976963674dd40ffe7
MD5: d1d779314250fab284fd348888c2f955
MD5: 41fd85ff44107e4604db2f00e911a766
MD5: cf733e719e9677ebfbc84a3ab08dd0dc
MD5: 01d397df2a1cf1d4c8e3615b7064856c

The BeagleBoyz may also be working with or contracting out to criminal hacking groups, like TA505, for initial access development. The third party typically uses commodity malware to establish initial access on a victim's network and then turns over the access to the BeagleBoyz for follow-on exploitation, which may not occur until months later.

The BeagleBoyz have also used the following techniques to gain an initial foothold on a targeted computer network (*Initial Access* [TA0001]).

- Email an attachment with malware to a specific individual, company, or industry (*Phishing: Spearphishing Attachment* [T1566.001])
- Compromise a website visited by users in specific communities, industries, or regions (*Drive-by Compromise* [T1189])
- Exploit a weakness (a bug, glitch, or design vulnerability) in an internet-facing computer system (such as a database or web server) (*Exploit Public Facing Application* [T1190])
- Steal the credentials of a specific user or service account to bypass access controls and gain increased privileges (*Valid Accounts* [T1078])
- Breach organizations that have access to the intended victim's organization and exploit their trusted relationship (*Trusted Relationship* [T1199])
- Use remote services to initially access and persist within a victim's network (*External Remote Services* [T1133])

Execution

TLP:WHITE

The BeagleBoyz selectively exploit victim computer systems after initially compromising a

computer connected to a financial institution's corporate network. After gaining initial access to a financial institution's corporate network, the BeagleBoyz are selective in which victim systems they further exploit. The BeagleBoyz use a variety of techniques to run their code on local and remote victim systems [*Execution* [TA0002]).

- Use command-line interfaces to interact with systems and execute other software (*Command and Scripting Interpreter* [T1059])
- Use scripts (e.g., VBScript and PowerShell) to speed up operational tasks, reduce the time required to gain access to critical resources, and bypass process monitoring mechanisms by directly interacting with the operating system (OS) at an Application Programming Interface (API) level instead of calling other programs (*Command and Scripting Interpreter: PowerShell* [T1059.001], *Command and Scripting Interpreter: Visual Basic* [T1059.005])
- Rely upon specific user actions, such as opening a malicious email attachment (*User Execution* [T1204])
- Exploit software vulnerabilities to execute code on a system (*Exploitation for Client Execution* [T1203])
- Create new services or modify existing services to execute executables, commands, or scripts (*System Services: Service Execution* [T1569.002])
- Employ the Windows module loader to load Dynamic Link Libraries (DLLs) from arbitrary local paths or arbitrary Universal Naming Convention (UNC) network paths and execute arbitrary code on a system (Shared Modules [T1129])
- Use the Windows API to execute arbitrary code on the victim's system (*Native API* [T1106])
- Use a system's graphical user interface (GUI) to search for information and execute files (*Remote Services* [T1021])
- Use the Task Scheduler to run programs at system startup or on a scheduled basis for persistence, conduct remote execution for lateral movement, gain SYSTEM privileges for privilege escalation, or run a process under the context of a specified account (*Scheduled Task/Job* [T1053])
- Abuse compiled Hypertext Markup Language (HTML) files (.chm), commonly distributed as part of the Microsoft HTML Help system, to conceal malicious code (*Signed Binary Proxy Execution: Compiled HTML File* [T1218.001])
- Abuse Windows rundll32.exe to execute binaries, scripts, and Control Panel Item files (.CPL) and execute code via proxy to avoid triggering security tools (*Signed Binary Proxy Execution: Rundl32* [T1218.001])
- Exploit cron in Linux and launchd in macOS systems to create pre-scheduled and periodic background jobs (*Scheduled Task/Job: Cron* [T1053.003], *Scheduled Task/Job: Launchd* [T1053.004])

Persistence

The BeagleBoyz use many techniques to maintain access on compromised networks through system restarts, changed credentials, and other interruptions that could affect their access (*Persistence* [TA0003]).

- Add an entry to the "run keys" in the Registry or an executable to the startup folder to execute malware as the user logs in under the context of the user's associated permissions levels (*Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder* [T1547.001])
- Install a new service that can be configured to execute at startup using utilities to interact with services or by directly modifying the Registry (*Create or Modify System Process: Windows Service* [T1543.003])
- Compromise an openly accessible web server with a web script (known as web shell) to use the web server as a gateway into a network and to serve as redundant access or persistence mechanism (*Server Software Component: Web Shell* [T1505.003])
- Manipulate accounts (e.g., modifying permissions, modifying credentials, adding or changing permission groups, modifying account settings, or modifying how authentication is performed) to maintain access to credentials and certain permission levels within an environment (*Account Manipulation* [T1098])
- Steal the credentials of a specific user or service account to bypass access controls and retain access to remote systems and externally available services (*Valid Accounts* [T1078])
- Use the Task Scheduler to run programs at system startup or on a scheduled basis for persistence, conduct remote execution for lateral movement, gain SYSTEM privileges for privilege escalation, or run a process under the context of a specified account (*Scheduled Task/Job* [T1053])
- Abuse the Windows DLLs search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence (*Hijack Execution Flow: DLL Search Order Hijacking* [T1056.004])
- Exploit hooking to load and execute malicious code within the context of another process to mask the execution, allow access to the process's memory, and, possibly, gain elevated privileges (*Input Capture: Credential API Hooking* [T1574.001])
- Use remote services to persist within a victim's network (External Remote Services [T1133])

Privilege Escalation

The BeagleBoyz often seek access to financial institutions' systems that have tiered user and system accounts with customized privileges. The BeagleBoyz must overcome these restrictions to access necessary systems, monitor normal user behavior, and install and execute additional malicious tools. To do so, the BeagleBoyz have used the following techniques to gain higher-level permissions on a system or network (*Privilege Escalation* [TA0004]).

- Inject code into processes to evade process-based defenses and elevate privileges (*Process Injection* [T1055])
- Install a new service that can be configured to execute at startup using utilities to interact with services or by directly modifying the Registry (*Create or Modify System Process: Windows Service* [T1543.003])
- Compromise an openly accessible web server with web shell to use the web server as a

gateway into a network (*Server Software Component: Web Shell* [T1505.003])
- Use the Task Scheduler to run programs at system startup or on a scheduled basis for persistence, conduct remote execution as part of lateral movement, gain SYSTEM privileges for privilege escalation, or run a process under the context of a specified account (*Scheduled Task/Job* [T1053])
- Steal the credentials of a specific user or service account to bypass access controls and grant increased privileges (*Valid Accounts* [T1078])
- Exploit hooking to load and execute malicious code within the context of another process to mask the execution, allow access to the process's memory, and, possibly, gain elevated privileges (*Input Capture: Credential API Hooking* [T1574.001])
- Perform Sudo (sometimes referred to as "super user do") caching or use the Soudoers file to elevate privileges in Linux and macOS systems (*Abuse Elevation Control Mechanism: Sudo and Sudo Caching* [T1548.003])
- Execute malicious payloads by hijacking the search order used to load DLLs (*Hijack Execution Flow: DLL Search Order Hijacking* [T1574.001])

Defense Evasion

Throughout their exploitation of a financial institution's computer network, the BeagleBoyz have used different techniques to avoid detection by OS security features, system and network security software, and system audits (*Defense Evasion* [TA0005]).

- Exploit code signing certificates to masquerade malware and tools as legitimate binaries and bypass security policies that allow only signed binaries to execute on a system (*Subvert Trust Controls Signing* [T1553.002])
- Remove malware, tools, or other non-native files dropped or created throughout an intrusion to reduce their footprint or as part of the post-intrusion cleanup process (*Indicator Removal on Host: File Deletion* [T1070.004])
- Inject code into processes to evade process-based defenses (*Process Injection* [T1055])
- Use scripts (such as VBScript and PowerShell) to bypass process monitoring mechanisms by directly interacting with the OS at an API level instead of calling other programs (*Command and Scripting Interpreter: PowerShell* [T1059.001], *Command and Scripting Interpreter: Visual Basic* [T1059.005])
- Attempt to make an executable or file challenging to discover or analyze by encrypting, encoding, or obfuscating its contents on the system or in transit (*Obfuscated Files or Information* [T1027])
- Use external previously compromised web services to relay commands to a victim system (*Web Service* [T1102])
- Use software packing to change the file signature, bypass signature-based detection, and decompress the executable code in memory (*Unsecured Credentials: Private Keys* [T1552.004])
- Use obfuscated files or information to hide intrusion artifacts (*Deobfuscate/Decode Files or Information* [T1140])
- Modify the data timestamps (the modify, access, create, and change times fields) to mimic files that are in the same folder, making them appear inconspicuous to forensic

analysts or file analysis tools (*Indicator Removal on Host: Remove Timestamp* [T1070.006])
- Abuse Windows utilities to implement arbitrary execution commands and subvert detection and mitigation controls (such as Group Policy) that limit or prevent the usage of cmd.exe or file extensions commonly associated with malicious payloads (*Indirect Command Execution* [T1202])
- Use various methods to prevent their commands from appearing in logs and clear command history to remove activity traces (*Indicator Removal on Host: Clear Command History* [T1070.003])
- Disable security tools to avoid possible detection of tools and events (*Impair Defenses: Disable or Modify Tools* [T1562.001])
- Steal the credentials of a specific user or service account to bypass access controls and grant increased privileges (*Valid Accounts* [T1078])
- Delete or alter generated artifacts on a host system, including logs and potentially captured files, to remove traces of activity (*Indicator Removal on Host: File Deletion* [T1070.004])
- Abuse compiled HTML files (.chm), commonly distributed as part of the Microsoft HTML Help system, to conceal malicious code (*Signed Binary Proxy Execution: Compiled HTML File* [T1218.001])
- Prepend a space to all their terminal commands to operate without leaving traces in the HISTCONTROL environment, which is configured to ignore commands that start with a space (*Impair Defenses: HISTCONTROL* [T1562.003])
- Modify malware so it has a different signature and re-use it in cases when the group determines it was quarantined (*Obfuscated Files or Information: Indicator Removal from Tools* [T1027.005])
- Attempt to block indicators or events typically captured by sensors from being gathered and analyzed (*Impair Defenses: Indicator Blocking* [T1562.006])
- Use the Windows DLLs search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence (*Hijack Execution Flow: DLL Search Order Hijacking* [T1574.001])
- Manipulate or abuse the attributes or location of an executable (masquerading) to better blend in with the environment and increase the chances of deceiving a security analyst or product (*Masquerading* [T1036])
- Exploit rootkits to hide programs, files, network connections, services, drivers, and other system components (*Rootkit* [T1014])
- Abuse the Windows rundll32.exe to execute binaries, scripts, and .CPL files, and execute code via proxy to avoid triggering security tools (*Signed Binary Proxy Execution: Rundl32* [T1218.001])

Credential Access

The BeagleBoyz may use malware like ECCENTRICBANDWAGON to log key strokes and take screen captures. The U.S. Government has identified some ECCENTRICBANDWAGON samples that have the ability to RC4 encrypt logged data, but the tool has no network

TLP:WHITE

functionality. The implant uses specific formatting for logged data and saves the file locally; another tool obtains the logged data. The implant also contains no mechanism for persistence or self-loading and expects a specific configuration file to be present on the system. A full technical report for ECCENTRICBANDWAGON is available at https://us-cert.cisa.gov/northkorea.

The BeagleBoyz may not always need to use custom keyloggers like ECCENTRICBANDWAGON or other tools to obtain credentials from a compromised system. Depending on the victim's environment, the BeagleBoyz have used the following techniques to steal credentials (*Credential Access* [TA0006]).

- Capture user input, such as keylogging (the most prevalent type of input capture), to obtain credentials for valid accounts and information collection (*Input Capture* [T1056])
- Obtain account login and password information, generally in the form of a hash or a clear text password, from the operating system and software (*OS Credential Dumping* [T1056])
- Gather private keys from compromised systems to authenticate to remote services or decrypt other collected files (*Unsecured Credentials: Private Keys* [T1552.004])
- Manipulate default, domain, local, and cloud accounts to maintain access to credentials and certain permission levels within an environment (*Account Manipulation* [T1098])
- Abuse hooking to load and execute malicious code within the context of another process to mask the execution, allow access to the process's memory, and, possibly, gain elevated privileges (*Input Capture: Credential API Hooking* [T1056.004])
- Use brute force techniques to attempt account access when passwords are unknown or when password hashes are unavailable (*Brute Force* [T1110])

Discovery

Once inside a financial institution's network, the BeagleBoyz appear to seek two specific systems—the SWIFT terminal and the server hosting the institution's payment switch application. As they progress through a network, they learn about the systems they have accessed in order to map the network and gain access to the two goal systems. To do so, the BeagleBoyz have used the following techniques to gain knowledge about the systems and internal network (*Discovery* [TA0007]).

- Attempt to get detailed information about the operating system and hardware, such as version, patches, hotfixes, service packs, and architecture (*System Information Discovery* [T1082])
- Enumerate files and directories or search in specific locations of a host or network share for particular information within a file system (*File and Directory Discovery* [T1083])
- Get a list of security software, configurations, defensive tools, and sensors installed on the system (*Software Discovery: Security Software Discovery* [T1518.001])
- Procure information about running processes on a system to understand standard software running on network systems (*Process Discovery* [T1057])
- Identify primary users, currently logged in users, sets of users that commonly use a system, or active or inactive users (*System Owner/User Discovery* [T1033])

TLP:WHITE

- Enumerate browser bookmarks to learn more about compromised hosts, reveal personal information about users, and expose details about internal network resources (*Browser Bookmark Discovery* [T1217])
- Look for information on network configuration and system settings on compromised systems, or perform remote system discovery (*System Network Configuration Discovery* [T1016])
- Interact with the Windows Registry to gather information about the system, configuration, and installed software (*Query Registry* [T1012])
- Get a list of open application windows to learn how the system is used or give context to data collected (*Application Window Discovery* [T1010])
- Attempt to get a listing of local system or domain accounts in the compromised system (*Account Discovery* [T1087])
- Obtain a list of network connections to and from the compromised system or remote system by querying for information over the network (*System Network Connections Discovery* [T1049])

Lateral Movement

To access a compromised financial institution's SWIFT terminal and the server hosting the institution's payment switch application, the BeagleBoyz leverage harvested credentials and take advantage of the accessibility of these critical systems from other systems in the institution's corporate network. Specifically, the BeagleBoyz have been known to create firewall exemptions on specific ports, including ports 443, 6443, 8443, and 9443. Depending on the configuration of compromised systems and the security environment of the victim's computer network, the BeagleBoyz have used the following techniques to enter and control remote systems on a compromised network (*Lateral Movement* [TA0008]).

- Copy files from one system to another to stage adversary tools or other files throughout an operation (*Ingress Tool Transfer* [T1105])
- Use Remote Desktop Protocol (RDP) to log into an interactive session with a system desktop GUI on a remote system (*Remote Services: Remote Desktop Protocol* [T1021.001])
- Employ hidden network shares, in conjunction with administrator-level valid accounts, to remotely access a networked system over Server Message Block (SMB) in order to interact with systems using remote procedure calls (RPCs), transfer files, and run transferred binaries through remote execution (*Remote Services: SMB/Windows Admin Shares* [T1021.002])
- Exploit valid accounts to log into a service specifically designed to accept remote connections and perform actions as the logged-on user (*Remote Services* [T1021])

Collection

Depending on various environmental attributes the BeagleBoyz encounter during their exploitation, they may deploy a variety of reconnaissance tools or use commonly available administrative tools for malicious purposes.

TLP:WHITE

The BeagleBoyz, like other sophisticated cyber actors, also appear to use resident, legitimate administrative tools for reconnaissance purposes when they are available; this is commonly known as “living off the land.” PowerShell appears to be a popular otherwise-legitimate tool the BeagleBoyz favor for reconnaissance activities. For example, the BeagleBoyz often use publicly available code from PowerShell Empire for malicious purposes.

The BeagleBoyz have used the following techniques to gather information from exploited systems (*Collection* [TA0009]).

- Use automated methods, such as scripts, for collecting data (*Automated Collection* [T1119])
- Capture user input to obtain credentials and collect information (*Input Capture* [T1056])
- Collect local systems data from a compromised system (*Data from Local System* [T1005])
- Take screen captures of the desktop (*Screen Capture* [T1113])
- Collect data stored in the Windows clipboard from users (*Clipboard Data* [T1115])

Command and Control

The BeagleBoyz likely change tools—such as CROWDEDFLOUNDER and HOPLIGHT—over time to maintain remote access to financial institution networks and to interact with those systems.

Analysis of the following CROWDEDFLOUNDER samples was first released in October 2018 as part of the FASTCash campaign.

```
MD5 hash: 5cfa1c2cb430bec721063e3e2d144feb
MD5 hash: 4f67f3e4a7509af1b2b1c6180a03b3e4
```

The BeagleBoyz have used CROWDEDFLOUNDER as a remote access trojan (RAT) since at least 2018. The implant is designed to operate on Microsoft Windows hosts and can upload and download files, launch a remote command shell, inject into victim processes, obtain user and host information, and securely delete files. The implant may be packed with Themida to degrade or prevent effective reverse engineering or evade detection on a Windows host. It can be set to act in beacon or listening modes, depending on command line arguments or configuration specifications. The implant obfuscates network communications using a simple encoding algorithm. The listening mode of CROWDEDFLOUNDER facilitates proxies like ELECTRICFISH (discussed below) with tunneling traffic in a victim’s network.

More recently, the U.S. Government has found HOPLIGHT malware on victim systems, suggesting the BeagleBoyz are using HOPLIGHT for similar purposes. HOPLIGHT has the same basic RAT functionality as the CROWDEDFLOUNDER implant. In addition, HOPLIGHT has the capability to create fraudulent Transport Layer Security (TLS) sessions to obfuscate command and control (C2) connections, making detection and tracking of the malware’s communications difficult.

Full technical reports for CROWDEDFLOUNDER and HOPLIGHT are available at https://us-

TLP:WHITE

cert.cisa.gov/northkorea.

TLP:WHITE

The BeagleBoyz use network proxy tunneling tools—including VIVACIOUSGIFT and ELECTRICFISH—to tunnel communications from non-internet facing systems like an ATM switch application server or a SWIFT terminal to internet-facing systems. The BeagleBoyz use these network proxy tunneling tools, likely placed at or near a victim's network boundary, to tunnel other protocols such as RDP and Secure Shell or other implant traffic out from the internal network.

It appears that as the BeagleBoyz change proxy tools, there is some overlap between their use of older and newer malware. For example, the BeagleBoyz appear to have begun using ELECTRICFISH as they wound down use of VIVACIOUSGIFT. There has been a noticeable decline in ELECTRICFISH use following the U.S. Government's disclosure of it in May 2019.

Full technical reports for VIVACIOUSGIFT and ELECTRICFISH are available at https://us-cert.cisa.gov/northkorea.

In addition to these tools, the BeagleBoyz have used the following techniques to communicate with financial institution victim systems under their control (*Command and Control* [TA0011]).

- Employ known encryption algorithms to conceal C2 traffic (*Encrypted Channel* [T1573])
- Communicate over commonly used standard application layer protocols and ports to avoid detection or detailed inspection and to blend with existing traffic (*Application Layer Protocol* [T1071])
- Encode C2 information using standard data encoding systems such as the American Standard Code for Information Interchange (ASCII), Unicode, Base64, Multipurpose Internet Mail Extensions, and 8-bit Unicode Transformation Format systems or other binary-to-text and character encoding systems (*Data Encoding: Standard Encoding* [T1132.001])
- Copy files between systems to stage adversary tools or other files (*Ingress Transfer Tool* [T1105])
- Use external previously compromised web services to relay commands to victim systems (*Web Service* [T1102])
- Employ a custom C2 protocol that mimics well-known protocols, or develop custom protocols (including raw sockets) to supplement protocols provided by another standard network stack (*Non-Application Layer Protocol* [T1095])
- Obfuscate C2 communications (but not necessarily encrypt them) to hide commands and make the content less conspicuous and more challenging to discover or decipher (*Data Obfuscation* [T1101])
- Employ connection proxies to direct network traffic between systems, act as an intermediary for network communications to a C2 server, or avoid direct connections to its infrastructure (*Proxy* [T1090])
- Exploit legitimate desktop support and remote access software to establish an interactive C2 channel to target systems within networks (*Remote Access Software* [T1219])

TLP:WHITE

Cryptocurrency Exchange Heists

TLP:WHITE

In addition to robbing traditional financial institutions, the BeagleBoyz target cryptocurrency exchanges to steal large amounts of cryptocurrency, sometimes valued at hundreds of millions of dollars per incident. Cryptocurrency offers the BeagleBoyz an irreversible method of theft that can be converted into fiat currency because the permanent nature of cryptocurrency transfers do not allow for claw-back mechanisms. Working with U.S. Government partners, CISA, Treasury, FBI, and USCYBERCOM identified COPPERHEDGE as the tool of choice for the BeagleBoyz to exploit cryptocurrency exchanges. COPPERHEDGE is a full-featured remote access tool capable of running arbitrary commands, performing system reconnaissance, and exfiltrating data. Full technical analysis of COPPERHEDGE is available at https://us-cert.cisa.gov/northkorea.

Exfiltration

During a cyber operation, the BeagleBoyz need to exfiltrate a variety of data from compromised systems. In addition to the C2 tools noted that have built-in exfiltration features, such as CROWDEDFLOUNDER and HOPLIGHT, the BeagleBoyz use the following techniques to steal data from a network (*Exfiltration* [TA0010]).

- Compress and encrypt collected data before exfiltration to minimize the amount of data sent over the web and make it portable, less conspicuous, and less detectable (*Archive Collected Data* [T1560])
- Steal collected data via scripts (although this may require other exfiltration techniques) (*Automated Exfiltration* [T1020])
- Encode data using the same protocol as the C2 channel and exfiltrate it over the C2 channel (*Exfiltration Over C2 Channel* [T1041])

Impact

The U.S. Government has observed the BeagleBoyz successfully monetize illicit access to financial institutions' SWIFT terminals to enable wire fraud and gain access to the institutions' payment switch application servers, which allowed fraudulent ATM cash outs. After gaining access to either one or both of these operationally critical systems, the BeagleBoyz monitor the systems to learn about their configurations and legitimate use patterns, and then they deploy bespoke tools to facilitate illicit monetization.

The cybersecurity community and Financial Services sector have released substantial information on the BeagleBoyz manipulation of compromised SWIFT terminals, describing their ability to monitor these systems, send fraudulent messages, and attempt to hide the fraudulent activity from detection. The discussion below focuses on the custom tools used to manipulate payment switch applications for ATM cash outs.

The BeagleBoyz use FASTCash malware to intercept financial request messages and reply with fraudulent but legitimate-looking affirmative response messages in the ISO 8583 format. The BeagleBoyz have functionally equivalent FASTCash malware for both UNIX and Windows that they deploy depending on the operating system running on the server hosting

TLP:WHITE

the bank's payment switch application.

FASTCash for UNIX is composed of AIX executable files designed to inject code and libraries into a currently running process. One AIX executable provides export functions, which allows an application to manipulate transactions on financial systems using the ISO 8583 international standard for financial transaction card-originated interchange messaging. The injected executables interpret financial request messages and construct fraudulent financial response messages. For more details on FASTCash for UNIX malware, please see the FASTCash report at https://www.us-cert.gov/ncas/alerts/TA18-275A.

The BeagleBoyz use FASTCash for Windows to manipulate transactions processed by a switch application running on a Windows box. FASTCash for Windows is also specific to the ISO 8583 message format. The BeagleBoyz appear to have modified publicly available source code to write parts of the tool, likely to speed development. The malware contains code probably taken from open-source repositories on the internet to create hashmaps and hook functions and to parse ISO 8583 messages.

FASTCash for Windows injects itself into software running on a Windows platform. The malware then takes control of the software's network send and receive functions, allowing it to manipulate ISO 8583 messages. The U.S. Government has identified two variants of FASTCash for Windows. One variant supports ASCII encoding. The BeagleBoyz appear to have modified the second variant's message parsing code to support Extended Binary Coded Decimal Interchange Code (EBCIDC) encoding. Both ASCII and EBCDIC are character encoding formats.

FASTCash for Windows malware uses code from github.com/petewarden/c_hashmap for hashmaps, code from Microsoft's Detours Library at github.com/Microsoft/Detours for hooking, and code from to parse ISO 8583 messages.

The malware hooks onto the send and receive function of the switch application so that it can process inbound request messages as they are received. FASTCash for Windows inspects the inbound message, probably looking for specific account numbers. If the account number matches an expected number, the malware constructs a fraudulent response message. If the account number does not match an expected number, the malware allows the request to pass through normally. If the malware constructs a fraudulent response message, it then sends it back to the acquirer without any further processing by the switch application, leaving the issuer without any awareness of the fraudulent transaction.

Full technical reports for FASTCash and FASTCash for Windows malware are available at https://us-cert.cisa.gov/northkorea.

The BeagleBoyz have used the following techniques to manipulate business and operational processes for monetary or destructive purposes (*Impact* [TA0040]).

- Corrupt or wipe data storage, data structures, and Master Boot Records (MBR) to interrupt network availability, services, and resources (*Disk Wipe: Disk Structure Wipe* [T1561.002], *Data Destruction* [T1485])
- Encrypt data on target systems and withhold access to the decryption key until a ransom

is paid, or render data permanently inaccessible if the ransom is not paid (*Data Encrypted for Impact* [T1486])
- Stop, disable, or render services unavailable on a system to damage the environment or inhibit incident response (*Service Stop* [T1489])
- Insert, delete, or modify data at rest, in transit, or in use to manipulate outcomes, hide activity, and affect the business process, organizational understanding, and decision-making (*Data Manipulation: Stored Data Manipulation* [T1565.001], *Data Manipulation: Transmitted Data Manipulation* [T1565.002], *Data Manipulation: Runtime Data Manipulation* [T1565.003])

Mitigations

- Contact law enforcement, CISA, or Treasury immediately regarding any identified activity related to BeagleBoyz. (Refer to the Contact Information section.)
- Incorporate IOCs identified in CISA's Malware Analysis Reports on https://us-cert.cisa.gov/northkorea into intrusion detection systems and security alert systems to enable active blocking or reporting of suspected malicious activity.

Recommendations for all Financial Institutions

- Verify compliance with Federal Financial Institutions Examination Council (FFIEC) handbooks, especially those related to Information Security and Payment Systems.
  - https://ithandbook.ffiec.gov/
- Verify compliance with industry security standards for critical systems, such as those available at:
  - https://www.pcisecuritystandards.org
  - https://www.swift.com/myswift/customer-security-programme-csp/swift-customer-security-controls-framework

Recommendations for Institutions with Retail Payment Systems

Require chip and personal identification number (PIN) cryptogram validation.

- Implement chip and PIN requirements for debit cards.
- Validate card-generated authorization request cryptograms.
- Use issuer-generated authorization response cryptograms for response messages.
- Require card-generated authorization response cryptogram validation to verify legitimate response messages.

Isolate payment system infrastructure.

- Require multi-factor authentication for any user to access the switch application server.
- Confirm perimeter security controls prevent internet hosts from accessing the private network infrastructure servicing your payment switch application server.
- Confirm perimeter security controls prevent all hosts outside of authorized endpoints from accessing your system, especially if your payment switch application server is

internet accessible.

Logically segregate your operating environment.

- Use firewalls to divide your operating environment into enclaves.
- Use access control lists to permit/deny specific traffic from flowing between those enclaves.
- Give special considerations to segregating enclaves holding sensitive information (e.g., card management systems) from enclaves requiring internet connectivity (e.g., email).

Encrypt data in transit.

- Secure all links to payment system engines with a certificate-based mechanism, such as Mutual Transport Layer Security, for all external and internal traffic external.
- Limit the number of certificates that can be used on the production server and restrict access to those certificates.

Monitor for anomalous behavior as part of layered security.

- Configure the switch application server to log transactions and routinely audit transaction and system logs.
- Develop a baseline of expected software, users, and logons and monitor switch application servers for unusual software installations, updates, account changes, or other activities outside of expected behavior.
- Develop a baseline of expected transaction participants, amounts, frequency, and timing. Monitor and flag anomalous transactions for suspected fraudulent activity.

Recommendations for Organizations with ATM or Point of Sale Devices

Validate issuer responses to financial request messages.

- Implement chip and PIN requirements for debit cards.
- Require and verify message authentication codes on issuer financial request response messages.
- Perform authorization response cryptogram validation for chip and PIN transactions.

Recommendations for All Organizations

Users and administrators should use the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up to date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators' group unless required.
- Enforce a strong password policy and require regular password changes.

- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations and configure it to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its “true file type” (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet before executing.
- Maintain situational awareness of the latest threats.
- Implement appropriate access control lists.

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- CISA (888-282-0870 or Central@cisa.dhs.gov),
- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office, or
- Treasury Office of Cybersecurity and Critical Infrastructure Protection (Treasury OCCIP) (202-622-3000 or OCCIP-Coord@treasury.gov).

Revisions

TLP:WHITE

August 26, 2020: Initial Version

TLP:WHITE