MANDIANT

THREAT INTELLIGENCE REPORT

APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations

Executive Summary

- APT43 is a prolific cyber operator that supports the interests of the North Korean regime. The group combines moderately-sophisticated technical capabilities with aggressive social engineering tactics, especially against South Korean and U.S.-based government organizations, academics, and think tanks focused on Korean peninsula geopolitical issues.
- In addition to its espionage campaigns, we believe APT43 funds itself through cybercrime operations to support its primary mission of collecting strategic intelligence.
- The group creates numerous spoofed and fraudulent personas for use in social engineering, as well as cover identities for purchasing operational tooling and infrastructure.
- APT43 has collaborated with other North Korean espionage operators on multiple operations, underscoring the major role APT43 plays in the regime's cyber apparatus.

Threat Details

Mandiant assesses with high confidence that APT43 is a moderately-sophisticated cyber operator that supports the interests of the North Korean regime. Campaigns attributed to APT43 include strategic intelligence collection aligned with Pyongyang's geopolitical interests, credential harvesting and social engineering to support espionage activities, and financially-motivated cybercrime to fund operations. Tracked since 2018, APT43 collection priorities align with the mission of the Reconnaissance General Bureau (RGB), North Korea's main foreign intelligence service. The group's focus on foreign policy and nuclear security issues supports North Korea's strategic and nuclear ambitions. However, the group's focus on health-related verticals throughout the majority of 2021, likely in support of pandemic response efforts, highlights its responsiveness to shifting priorities from Pyongyang.

- Publicly reported activities attributed to APT43 are frequently reported as "Kimsuky" or "Thallium" and include credential harvesting and espionage activity most likely intended to inform North Korean leadership on ongoing geopolitical developments.
- Their most frequently observed operations are spear-phishing campaigns supported by spoofed domains and email addresses as part of their social engineering tactics. Domains masquerading as legitimate sites are used in credential harvesting operations.
- We have not observed APT43 exploiting zero-day vulnerabilities.
- APT43 maintains a high tempo of activity, is prolific in its phishing and credential collection campaigns, and has demonstrated coordination with other elements of the North Korean cyber ecosystem.
- Targeting is regionally focused on South Korea and the U.S., as well as Japan and Europe, especially in the following sectors:
  - government
  - education/research/think tanks focused on geopolitical and nuclear policy
  - business services
  - manufacturing

Although the overall targeting reach is broad, the ultimate aim of campaigns is most likely centered around enabling North Korea's weapons program, including: collecting information about international negotiations, sanctions policy, and other country's foreign relations and domestic politics as these may affect North Korea's nuclear ambitions.

Shifts in Targeting

Campaigns attributed to APT43 are closely aligned with state interests and correlate strongly with geopolitical developments that affect Kim Jong-un and the hermit state's ruling elite. Since Mandiant has been tracking APT43, they have consistently conducted espionage activity against South Korean and U.S. organizations with a stake in security issues affecting the Korean peninsula.

- Prior to October 2020, APT43 primarily targeted government offices, diplomatic organizations, and think tank-related entities with a stake in foreign policy and security issues affecting the Korean peninsula in South Korea and the U.S.
- From October 2020 through October 2021, a significant portion of APT43 activity targeted on health-related verticals and pharmaceutical companies, most likely in support of COVID-19 response efforts in North Korea. Although it is unclear how any targeted information benefited the regime, cooperation with and across other North Korean cyber operators provides some indication of significant resourcing and prioritization of this effort during the COVID-19 global pandemic.
- Throughout this period APT43 espionage campaigns targeting South Korea, the U.S., Europe and Japan were ongoing.
- Notably, observed APT43 activity varied slightly according to targeting, including differences in malware deployed. For example, the use of VENOMBITE (a loader), SWEETDROP (a dropper), and BITTERSWEET (a backdoor) was distinct to APT43 activity targeting South Korea during the COVID-19 pandemic.

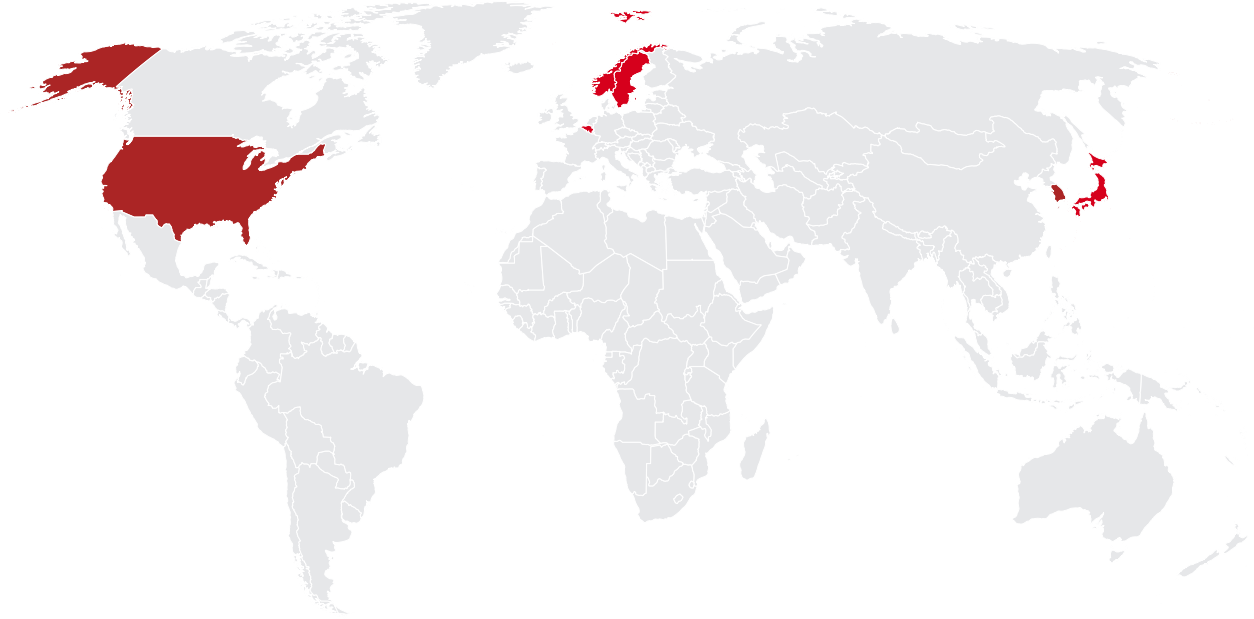

FIGURE 1. Countries targeted by APT43 (dark red indicating more frequently observed activity).

- Civil society and non-profits
- Education
- Governments
- Media and entertainment
- Construction/Materials
- Defense/Aerospace
- Telecoms
- High-tech industry
- Pharmaceuticals
- Consulting/Professional services

FIGURE 2. Industries targeted directly by APT43.

Cyber Operations

APT43 most commonly leverages tailored spear-phishing emails to gain access to victim information. However the group also engages in various other activities to support collecting strategic intelligence, including using spoofed websites for credential harvesting and carrying out cybercrime to fund itself.

- The actors regularly update lure content and tailor it to the specific target audience, particularly around nuclear security and non-proliferation.
- APT43 is adept at creating convincing personas, including masquerading as key individuals within their target area (such as security and defense), as well as leveraging stolen personally identifiable information (PII) to create accounts and register domains.
- APT43 uses highly relevant lure content together with spoofed email addresses.
  - APT43 also leverages contact lists stolen from compromised individuals to identify additional targets for spear-phishing operations.
- APT43 steals and launders enough cryptocurrency to buy operational infrastructure in a manner aligned with North Korea's juche state ideology of self-reliance, reducing fiscal strain on the central government.

Espionage

We consider cyber espionage to be the primary mission for APT43 and available data indicates that the group's other activities are carried out to support collecting strategic intelligence.

- The group is primarily interested in information developed and stored within the U.S. military and government, defense industrial base (DIB), and research and security policies developed by U.S.-based academia and think tanks focused on nuclear security policy and nonproliferation.
- APT43 has displayed interest in similar industries within South Korea, specifically non-profit organizations and universities that focus on global and regional policies, as well as businesses, such as manufacturing, that can provide information around goods whose export to North Korea has been restricted. This includes fuel, machinery, metals, transportation vehicles, and weapons.
- APT43 poses as reporters and think-tank analysts to build rapport with targeted individuals to collect intelligence (Figure 3). Corroborated by public reporting, the group has convinced academics to deliver strategic analysis directly to espionage operators.

Date: Fri, 14 Oct 2022 03:13:48 -0400
Subject: Request for comments
X-Sender: <redacted>@voanews[.]live

Greetings,
I hope you've been well! This is <redacted> with <redacted>.
North Korea Fires Powerful Missile on 4 Oct using Old Playbook in a New Worlds.The last time Pyongyang launched a weapon over Japan was in 2017, when Donald J. Trump was president and Kim Jong-un seemed intent on escalating conflict with Washington.

I have some questions regarding this:
1) Would Pyongyang conduct its next nuclear test soon after China's Communist Party Congress in mid-October?
2) May a quieter approach to North Korean aggression be warranted?
3) Would Japan increase the defense budget and a more proactive defense policy?
I would be very grateful if you could send me your answers within 5 days.
Have a good weekend.

Sincerely,
<redacted>

FIGURE 3. A sample email exchange in which APT43 builds rapport with a potential victim by masquerading as a journalist

- Technical indicators linked to APT43 partially corroborate Korean language reporting that the group targeted South Korean political organizations, especially ahead of South Korea's presidential elections in 2022, most likely to glean insight into possible policy shifts.

We have some indication that APT43 also carries out internal monitoring of other North Korean operations, including non-cyber activities. APT43 has compromised individual espionage actors, including those within its own operations. However it is unclear if this is intentional for self-monitoring purposes or accidental and indicative of poor operational security.

Credential Collection

APT43 operates credential collection campaigns to directly compromise financial data, PII, and client data from entities within the academic, manufacturing, and national security industries—especially in South Korea. In particular, the group registers domains masquerading as popular search engines, web platforms, and cryptocurrency exchanges in relevant target countries of interest. We believe these credentials are used to support operations that further APT43 missions.

- Collected credential data was used to create online personas and set up infrastructure for cyber espionage operations, including sites spoofing legitimate services (Figure 4).

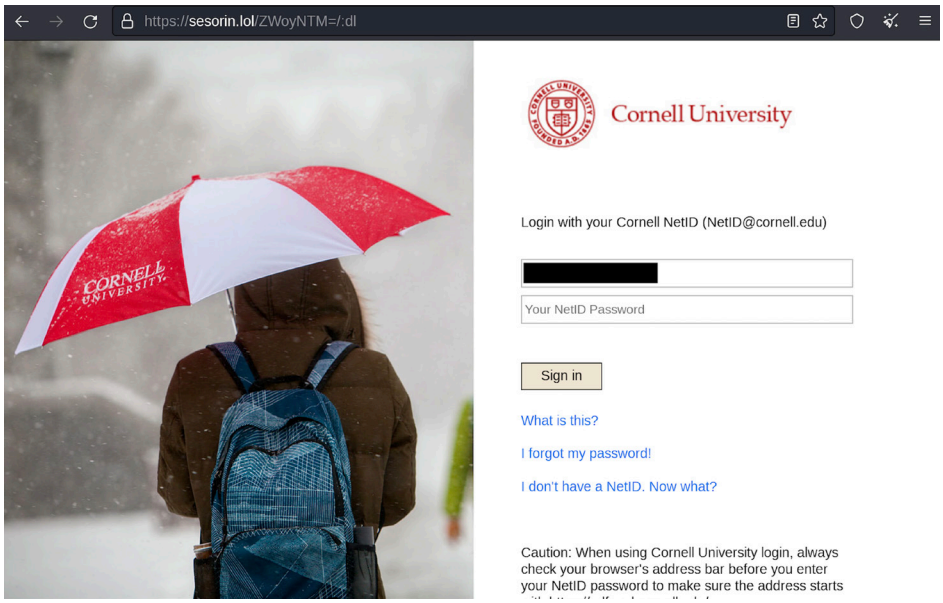

FIGURE 4. A credential collection website at APT43-controlled sesorin.lol, spoofing Cornell University

- The group has leveraged both compromised and actor-owned infrastructure to host and deliver malware to targets and collect credentials.
  - Compromised websites were used as part of network infrastructure to deliver both PASSMARK and LATEOP malware in 2018

Changes in targeting may reflect tactical shifts in collection requirements.

- In late 2021, APT43 resumed credential harvesting campaigns against religious groups, universities, and non-governmental organizations (NGOs), providing some indication that these campaigns were targeting "track two" diplomatic channels between North Korea and counterparts in South Korea and Japan. Notably, the activity represented a return to a primary focus on espionage targeting after a temporary focus on COVID-19 related organizations.
- In early 2022, Mandiant Intelligence observed multiple credential collection campaigns targeting academics, journalists, politicians, bloggers, and other private sector individuals, primarily in South Korea.
- By mid-2022, credential theft campaigns shifted to targeting South Korean bloggers and social media users associated with South Korean affairs, human rights, academia, religion, and cryptocurrency.

Cryptocurrency Targeting

APT43 has targeted cryptocurrency and cryptocurrency-related services. In contrast to other North Korean groups such as APT38, which are likely primarily tasked to bring in funds for the regime, APT43 most likely carries out such operations to sustain its own operations.

- We have identified APT43 using cryptocurrency services to launder stolen currency. Associated activity included identified payment methods, aliases, and addresses used for purchases (Figure 5), and the likely use of hash rental and cloud mining services to launder stolen cryptocurrency into clean cryptocurrency.

Dear B,

We would like to inform you that your Bitcoin payment for $120.00 has been added into your Namecheap account. You can now use the account balance to purchase or renew products on Namecheap.com.

Username : BRoyal1990
Transaction Id : 82073030
Transaction Ref: GKRwiyWiTTUXreqpvxNv4A
Amount : $120.00

You can find more information about this transaction on our Add Funds History page located at https://manage.www.namecheap.com/myaccount/reports/funds-report.asp.

If you have any questions, please contact our support at http://www.namecheap.com/support

Thank you.

Namecheap.com Support

FIGURE 5. APT43 likely used stolen Bitcoin to pay for Namecheap services

  - For a fee, these hash rental and cloud mining services provide hash power, which is used to mine cryptocurrency to a wallet selected by the buyer without any blockchain-based association to the buyer's original payments.
  - Several payment methods were used for infrastructure and hardware purchases including PayPal, American Express cards, and Bitcoin likely derived from previous operations.
- APT43 used a malicious Android app to most likely target Chinese users looking for cryptocurrency loans. The app and an associated domain probably harvested credentials, as depicted in Figure 6.

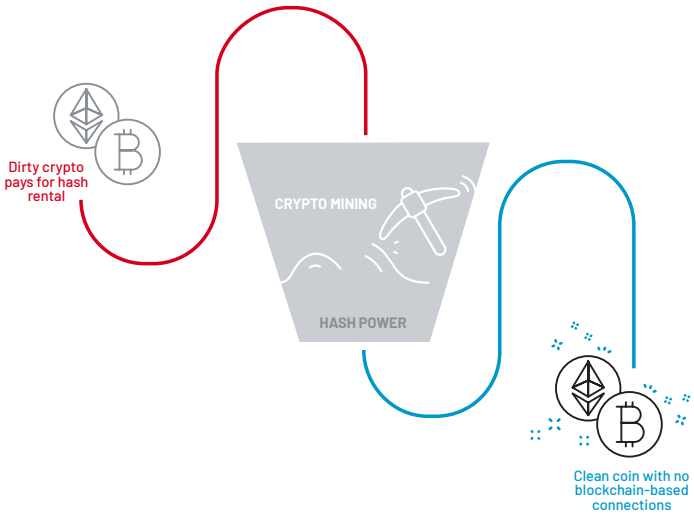

FIGURE 6. The laundering of cryptocurrency via hash rental services as used by APT43

- The prevalence of financially-motivated activity among North Korean groups, even among those which have historically focused on cyber espionage, suggests a widespread mandate to self-fund and an expectation to sustain themselves without additional resourcing.

Attribution

We assess with high confidence that APT43 is a state-sponsored cyber operator that acts in support of the North Korean government's wider geopolitical aims.

- The group's targeting is consistent with North Korea's shifting interests, although its dominant activity is to collect intelligence on the country's primary rival: South Korea.
  - By extension, the United States' support of South Korea also makes it a priority target.
- APT43 has shared infrastructure and tools with known North Korean operators, highlighting its role and mission alignment in a wider state-sponsored cyber apparatus.

More specifically, Mandiant assesses with moderate confidence that APT43 is attributable to the North Korean Reconnaissance General Bureau (RGB), the country's primary foreign intelligence service.

- Elements of APT43 have been identified cooperating with other RGB-linked cyber espionage operators, namely TEMP. Hermit (e.g. UNC1758). This is detailed further in the next section.

Links to Other Espionage Operators

APT43 operations have at times, overlapped with those of other North Korean cyber espionage operators. However, we assess these groups to be distinct and separate and, believe the overlaps are likely the result of ad hoc collaborations or other limited resource sharing. These overlaps principally take the form of malware families that had historically been used by a single North Korean cluster being employed by additional actors.

- APT43 employed malware first associated with suspected TEMP.Hermit clusters (often publicly reported as "Lazarus") during the height of the COVID-19 pandemic. Although this demonstrated some shared resources between APT43 and TEMP.Hermit clusters, we assess that these links were temporary (Figure 7).
  - Specifically, such activities included campaigns targeting global organizations involved in COVID-19 response. In some of these operations, a subset of APT43 almost certainly worked closely with other RGB-linked units, including sharing existing malware tools, developing new tools initially used in the expanded tasking, and carrying out sustained campaigns against healthcare research and related organizations.
    - Distinct tools derived from APT43 malware—such as the downloader PENCILDOWN—for use in these campaigns included PENDOWN, VENOMBITE, and EGGHATCH (also all downloaders, see Figure 7).
    - These tools were used alongside core APT43 tooling such as LOGCABIN and LATEOP.
    - APT43's use of malware variants such as HANGMAN.V2, a derivative of the HANGMAN backdoor usually linked with TEMP.Hermit, suggests some level of cross-pollination occurred during coordinated operations in 2020.
- These apparent cross-group operations were publicly reported as "Bureau 325" and also matched activity reported as "Cerium".
- Additional uncategorized clusters have been identified leveraging some of the same tools as APT43. A cluster using PENCILDOWN, for example, compromised an Android mobile wallet app to steal cryptocurrency.
- Conversely, in a separate instance we observed APT43 deploying LONEJOGGER, a tool strongly associated with UNC1069 cryptocurrency targeting.
  - UNC1069 is a suspected North Korean cybercrime operation with low confidence links to APT38.

Open sources often include additional operations in public reporting on "Kimsuky" activity. However, Mandiant continues to track these separately, especially those that leverage malware families such as KONNI and related tools CABRIDE and PLANEPATCH. Although these clusters of activity have overlaps with APT43, we believe that these links are tenuous and are the work of a separate group.

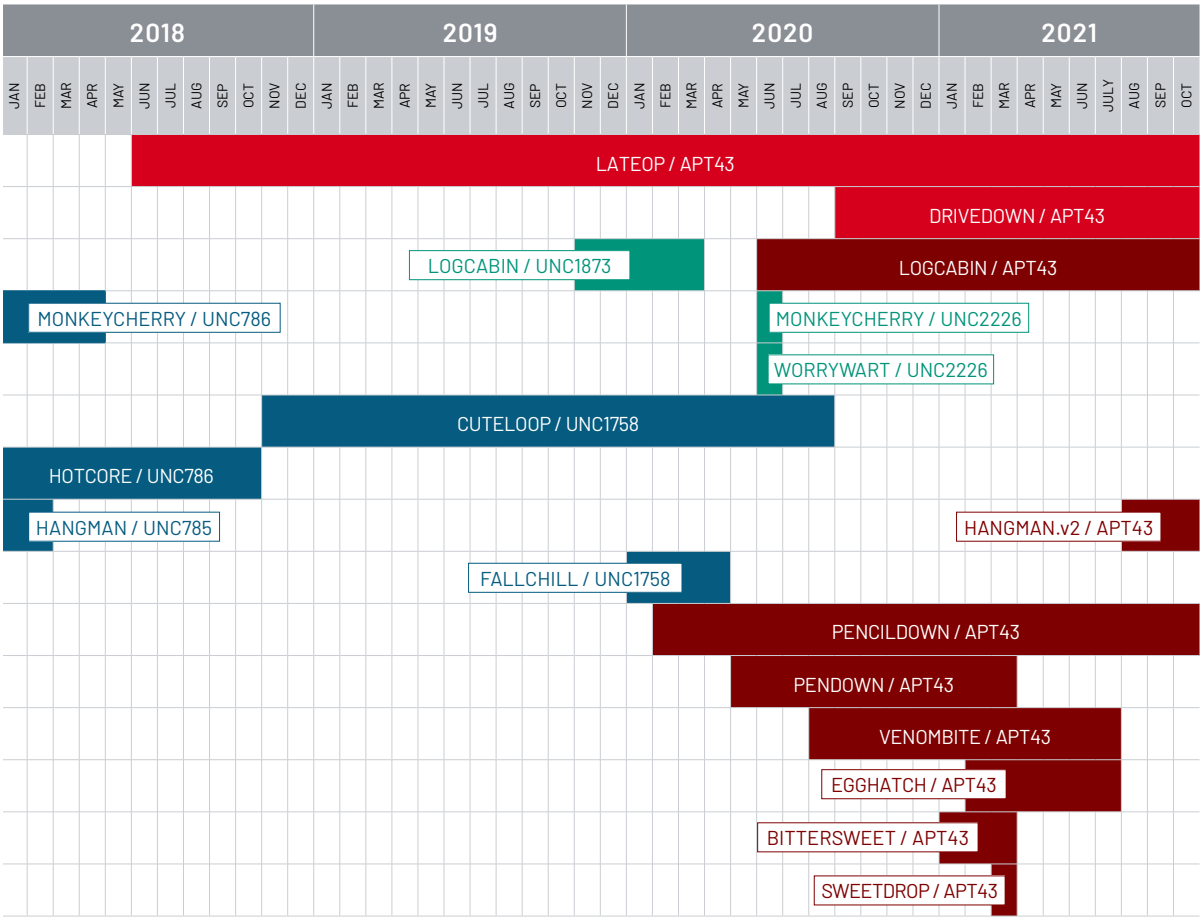

FIGURE 7. Convergence between APT43, TEMP.Hermit, and other tracked North Korean clusters based on malware deployment

Malware

APT43 relies on a relatively large toolkit composed of both non-public malware and widely available tools. Most open source reporting on APT43 tracks the group using LATEOP (known publicly as "BabyShark"), but we have observed a steady evolution and expansion of the operation's malware library over time. Some of the tools borrow code heavily from preceding tools (Figure 8), implementing improvements and adding features.

- The group has deployed publicly available malware including gh0st RAT, QUASARRAT, and AMADEY, but its activities are much better known for being associated with LATEOP, a backdoor based on VisualBasic scripts.
- APT43 has developed different variants of some of their tools, enabling multi-platform targeting. For example, we have identified an Android variant of PENCILDOWN, a Windows-based downloader.

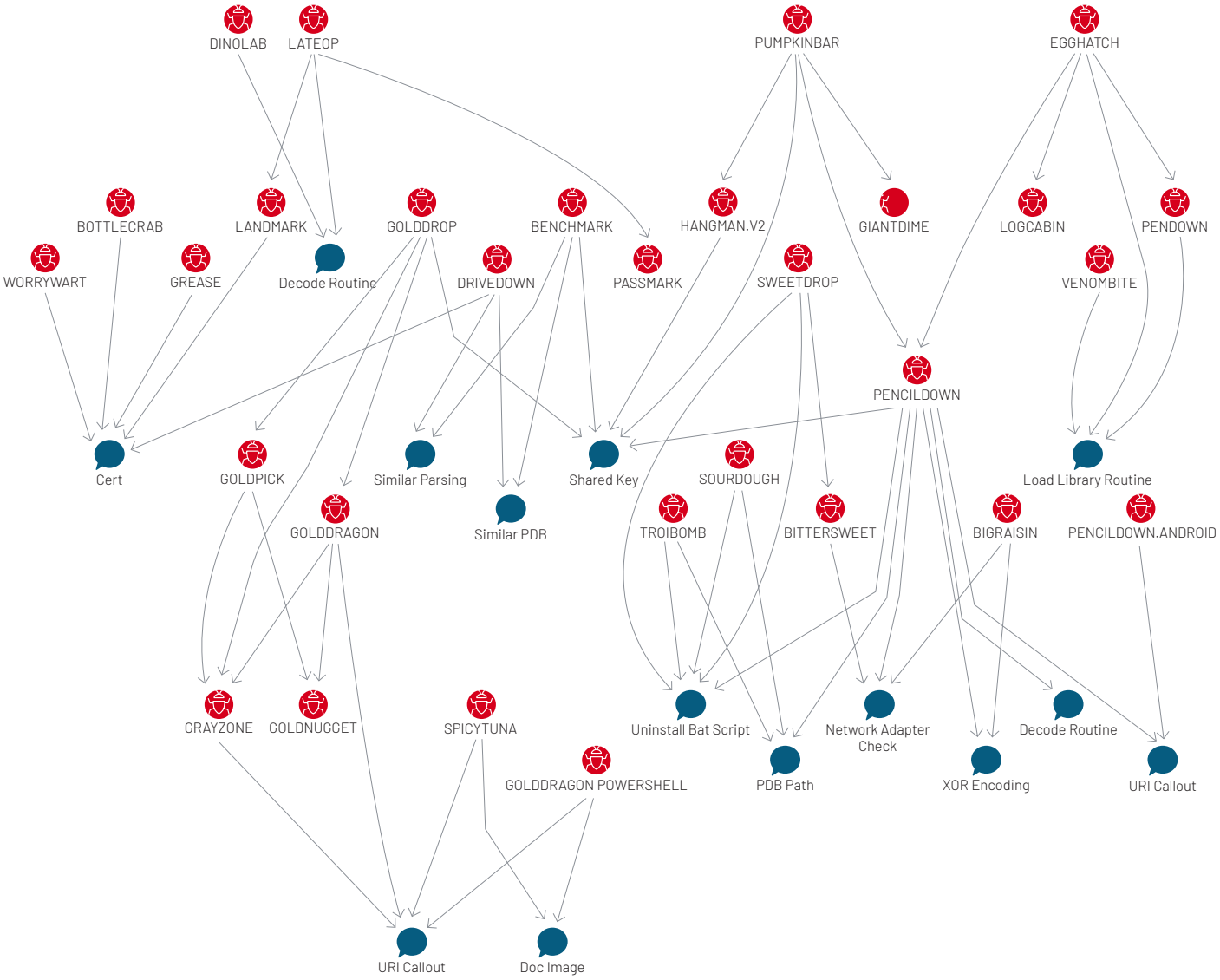

FIGURE 8. Code family overlap across tools used by APT43.

Outlook and Implications

Barring a drastic change in North Korea's national priorities, we expect that APT43 will remain highly prolific in carrying out espionage campaigns and financially-motivated activities supporting these interests. We believe North Korea has become increasingly dependent on its cyber capabilities and, APT43's persistent and continuously-developing operations reflect the country's sustained investment and reliance on groups like APT43.

As demonstrated by the group's sudden but temporary shift towards healthcare and pharmaceutical-related targeting, APT43 is highly responsive to the demands of Pyongyang's leadership. Although spear-phishing and credential collection against government, military, and diplomatic organizations have been core taskings for the group, APT43 ultimately modifies its targeting and tactics, techniques and procedures to suit its sponsors, including carrying out financially-motivated cybercrime as needed to support the regime.

Technical Annex: Attack Lifecycle

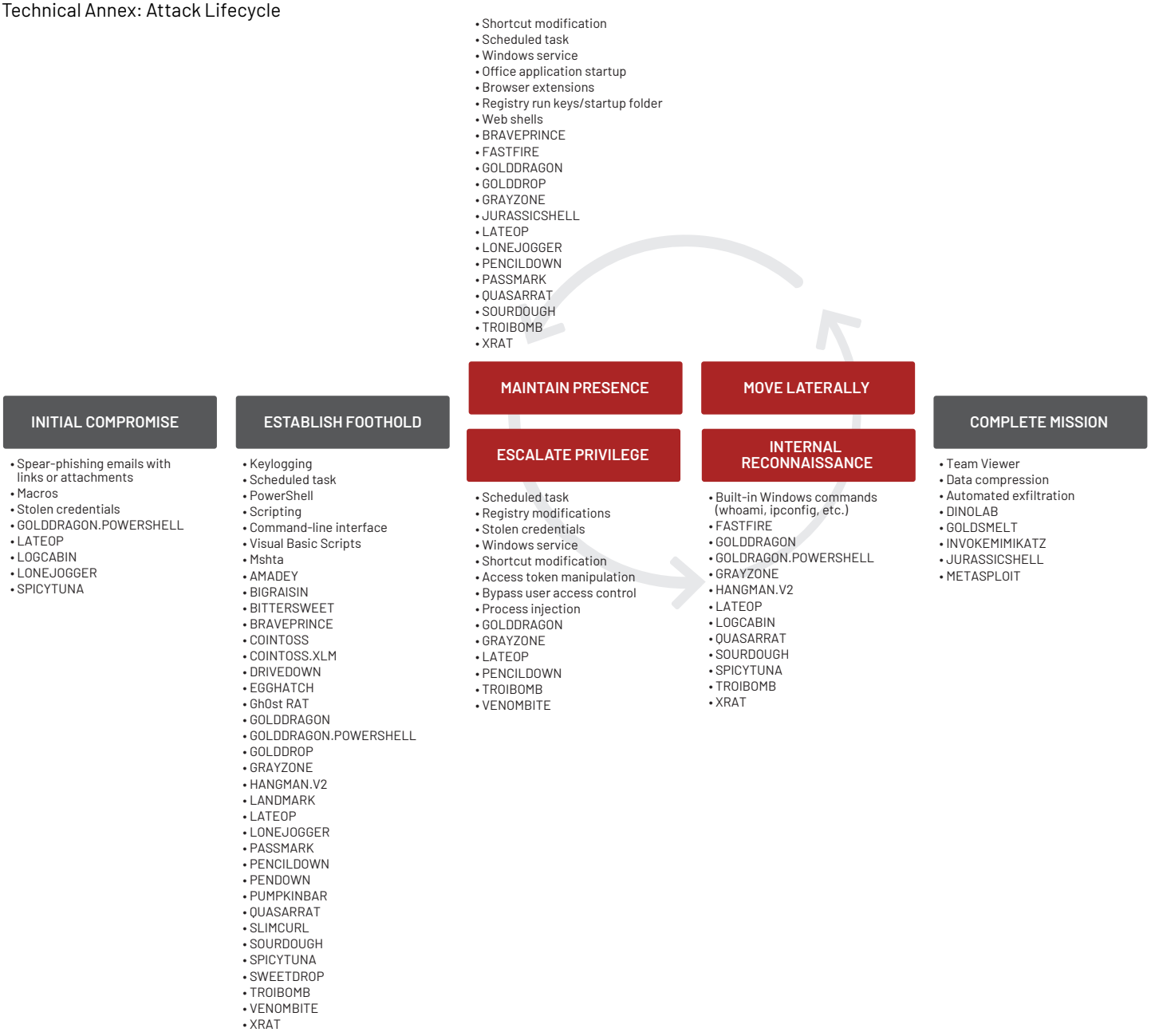

FIGURE 9. APT43 attack lifecycle

Technical Annex: MITRE ATT&CK

Initial Access	
T1566	Phishing
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link

Resource Development	
T1583.003	Virtual Private Server
T1584	Compromise Infrastructure
T1588.003	Code Signing Certificates
T1588.004	Digital Certificates
T1608.003	Install Digital Certificate
T1608.005	Link Target

Execution	
T1047	Windows Management Instrumentation
T1053.005	Scheduled Task
T1059	Command and Scripting Interpreter
T1059.00:	PowerShell
T1059.003	Windows Command Shell
T1059.005	Visual Basic
T1059.007	JavaScript
T1129	Shared Modules
T1203	Exploitation for Client Execution
T1204.001	Malicious Link
T1204.002	Malicious File
T1569.002	Service Execution

Command and Control	
T1071.001	Web Protocols
T1071.004	DNS
T1090.003	Multi-hop Proxy
T1095	Non-Application Layer Protocol
T1102	Web Service
T1102.002	Bidirectional Communication
T1105	Ingress Tool Transfer
T1132.001	Standard Encoding
T1573.002	Asymmetric Cryptography

Discovery	
T1007	System Service Discovery
T1010	Application Window Discovery
T1012	Query Registry
T1016	System Network Configuration Discovery
T1033	System Owner/User Discovery
T1057	Process Discovery
T1082	System Information Discovery
T1083	File and Directory Discovery
T1087	Account Discovery
T1518	Software Discovery
T1614.001	System Language Discovery

Collection	
T1056.001	Keylogging
T1113	Screen Capture
T1115	Clipboard Data
T1213	Data from Information Repositories
T1560	Archive Collected Data
T1560.001	Archive via Utility

Persistence	
T1137	Office Application Startup
T1505.00	Web Shell
T1543.003	Windows Service
T1547.001:	Registry Run Keys / Startup Folder
T1547.004	Winlogon Helper DLL
T1547.009	Shortcut Modification

Defense Evasion	
T1027	Obfuscated Files or Information
T1027.001	Binary Padding
T1027.002	Software Packing
T1027.005	Indicator Removal from Tools
T1027.009	Embedded Payloads
T1036	Masquerading
T1036.001	Invalid Code Signature
T1036.007	Double File Extension
T1055	Process Injection
T1055.001	Dynamic-link Library Injection
T1055.003	Thread Execution Hijacking
T1070.004	File Deletion
T1070.006	Timestomp
T1112	Modify Registry
T1134	Access Token Manipulation
T1140	Deobfuscate/Decode Files or Information
T1218.005	Mshta
T1497	Virtualization/Sandbox Evasion
T1497.001	System Checks
T1548.002:	Bypass User Account Control
T1553.002	Code Signing
T1564.003	Hidden Window
T1564.007	VBA Stomping
T1620:	Reflective Code Loading
T1622	Debugger Evasion

Impact	
T1489	Service Stop
T1529	System Shutdown/Reboot

Exfiltration	
T1020	Automated Exfiltration

Credential Access:	
T1110	Brute Force
T1555.003	Credentials from Web Browsers

Technical Annex: Malware Used by APT43

Malware Family	Role	Availability	Description
AMADEY	Downloader	Public	AMADEY is a downloader written in C that retrieves payloads via HTTP. Downloaded payloads are written to disk and executed.
BENCHMARK	Dropper	Non-public	BENCHMARK is a dropper written in C/C++ that reads a filename and extracts a Base64 encoded payload from a hard-coded path, decodes the payload and drops it to disk.
BIGRAISIN	Backdoor	Non-public	BIGRAISIN is a C\C++ Windows based backdoor. It is capable of executing downloaded commands, executing downloaded files, and deleting files.
BITTERSWEET	Downloader	Non-public	BITTERSWEET is a C/C++ Windows downloader. It collects basic system information before downloading the next stage to disk and executing.
BRAVEPRINCE	Downloader	Public	BRAVEPRINCE is a C/C++ downloader. It uses the Daum email service to upload collected system information and download files.
COINTOSS **COINTOSS.XLM**	Downloader	Non-public	COINTOSS is a C/C++ downloader. It uses the Windows Management Instrumentation command-line (WMIC) utility to download the payload over FTP. COINTOSS then creates and runs a batch script to uninstall itself.
DINOLAB	Builder	Non-public	DINOLAB is a C/C++ builder. It is used to encrypt and decrypt files, obfuscate VBS scripts, and infect files.
DRIVEDOWN	Downloader	Non-public	DRIVEDOWN is a C/C++ Windows downloader capable of executing embedded scripts and downloading stages from OneDrive.
EGGHATCH	Downloader	Non-public	EGGHATCH is a C/C++ Windows downloader. It uses mshta.exe to download and execute a script.
FASTFIRE	Backdoor	Non-public	FASTFIRE is a malicious APK that connects to a server and sends details of the compromised device back to command and control (C2).
GhOst RAT	Backdoor	Public	GHOST is a backdoor written in C++ that communicates via a custom binary protocol over TCP or UDP. It typically features a packet signature at the start of each message that varies between samples.
GOLDDRAGON **GOLDDRAGON.POWERSHELL**	Downloader	Non-public	GOLDDRAGON is a downloader written in C that retrieves a payload from a remote server via HTTP. The downloaded payload is written to disk and executed. GOLDDRAGON also extracts a payload from a Hangul Word Processor document and writes it to a startup directory. As a result, the new file is executed when the current user logs in.
GOLDDROP	Dropper	Non-public	GOLDDROP is a C/C++ Windows dropper. It decrypts a resource file, saves it to the file system, and injects it into another process.
GOLDSMELT	Utility	Non-public	GOLDSMELT is a C/C++ utility used to close the rundll32.exe process and delete a file likely used for logs.
GRAYZONE	Backdoor	Non-public	GRAYZONE is a C/C++ Windows backdoor capable of collecting system information, logging keystrokes, and downloading additional stages from the C2 server.
HANGMAN.V2	Backdoor	Non-public	HANGMAN.V2 is a variant of the backdoor HANGMAN. HANGMAN.V2 is very similar to HANGMAN, but uses HTTP for the network communications and formats data passed to the C2 server differently.
Invoke-Mimikatz	Credential theft	Public	Invoke-Mimikatz is PowerShell script that reflectively loads a Mimikatz credential-stealing DLL into memory.
JURASSICSHELL	Utility	Non-public	JURASSICSHELL is a PHP file management web shell that allows the actor to download and upload files.

Malware Family	Role	Availability	Description
LANDMARK **LANDMARK.NET**	Launcher	Non-public	LANDMARK is a C/C++ Windows launcher that loads and executes a file on disk stored as desktop.r5u.
LATEOP **LATEOP.V2**	Data miner	Non-public	LATEOP is a datamine VisualBasic script that can enumerate a variety of characteristics of a target system as well as execute additional arbitrary VisualBasic content. Some deployments of LATEOP have led to the download and execution of the PASSMARK credential theft payload. In contrast, some deployments of LATEOP.v2 have originated from BENCHMARK sourced infections.
LOGCABIN	Backdoor	Non-public	LOGCABIN is a file-less and modular backdoor with multiple stages. The stages consist of several VisualBasic and PowerShell scripts that are downloaded and executed. LOGCABIN collects detailed system information and sends it to the C2 before performing additional commands.
LONEJOGGER	Downloader	Non-public	LONEJOGGER is a downloader/dropper which has been observed targeting cryptocurrency services (including exchanges and investment companies), and uses a .lnk shortcut to download guardrailed HTML Application payloads.
METASPLOIT	Framework	Public	METASPLOIT is a penetration testing framework whose features include vulnerability testing, network enumeration, payload generation and execution, and defense evasion.
PASSMARK	Framework	Public	METASPLOIT is a penetration testing framework whose features include vulnerability testing, network enumeration, payload generation and execution, and defense evasion.
PENCILDOWN **PENCILDOWN.ANDROID**	Downloader	Non-public	PENCILDOWN is a C/C++ Windows based downloader. PENCILDOWN collects basic system information and sends it to the C2 server before receiving the next stage. The next stage is then loaded in memory or executed directly based off a flag in the response.
PENDOWN	Downloader	Non-public	PENDOWN is a downloader written in C++ that retrieves a payload via HTTP. The downloaded file is saved to disk and executed.
PUMPKINBAR	Dropper	Non-public	PUMPKINBAR is a C/C++ dropper. PUMPKINBAR can contain multiple payloads encoded and embedded within itself. The key to decode each payload is appended at the end of the PUMPKINBAR executable. The payloads are dropped to disk and executed.
QUASARRAT	Backdoor	Public	QUASARRAT is a publicly available Windows backdoor. It may visit a website, download, upload, and execute files. QUASARRAT may acquire system information, act as a remote desktop or shell, or remotely activate the webcam. The backdoor may also log keystrokes and steal passwords from commonly used browsers and FTP clients. QUASARRAT was originally named xRAT before it was renamed by the developers in August 2015.
SLIMCURL	Downloader	Non-public	SLIMCURL is a C/C++ downloader. It contains the next stage as a Base64 encoded Google Drive link. The next stage is downloaded using cURL.
SOURDOUGH	Backdoor	Non-public	SOURDOUGH is a backdoor written in C that communicates via HTTP. Its capabilities include keylogging, screenshot capture, file transfer, file execution, and directory enumeration.
SPICYTUNA	Downloader	Non-public	SPICYTUNA is a VBA downloader. It collects basic system information and is capable of downloading and executing additional stages.
SWEETDROP	Dropper	Non-public	SWEETDROP is a C/C++ Windows dropper. It drops an embedded binary resource to the file system and executes it.

Malware Family	Role	Availability	Description
TROIBOMB	Backdoor	Non-public	TROIBOMB is a C/C++ Windows backdoor that is capable of collecting system information and performing commands from the C2 server.
VENOMBITE	Downloader	Non-public	VENOMBITE is a C/C++ Windows downloader that has evolved from PENDOWN. It uses the same custom encoding routine, but the network functionality has been moved to an embedded executable. The downloaded file is loaded and executed in memory.

Technical Annex: Sample APT43 IOCs

Malware Family	Sample MD5	SHA1	SHA256
AMADEY	982fc9ded34c854 69269eacb1cb4ef26	e205ed81ccb99641dcc 6c2799d32ef0584fa2175	557ff6c87c81a2d2348bd8d667ea8412a1a 0a055f5e1ae91701c2954ca8a3fdb
BENCHMARK	de9a8c26049699d bbd5d334a8566d38d	47a32bc992e5d4613b3 658b025ab913b0679232c	43c2d5122af50363c29879501776d907ea a568fa142d935f6c80e823d18223f5
BIGRAISIN	144bd7fd423edc3 965cb0161a8b82ab2	1087efbd004f65d226bf 20a52f1dc0b3e756ff9e	2b78d5228737a38fa940e9ab19601747c68 ed28e488696694648e3d70e53eb5a
BITTERSWEET	cd83a51bec0396f 4a0fd563ca9c929d7	f3b047e6eb3964deb04 7767fad52851c5601483f	fb7fb6dbaf568b568cd5e60ab537a42d59 82949a5e577db53cc707012c7f20e3
BRAVEPRINCE	33df74cbb60920d 63fe677c6f90b63f9	539acd9145befd7e670f e826c248766f46f0d041	94aa827a514d7aa70c404ec326edaaad4b 2b738ffaea5a66c0c9f246738df579
	ebaf83302dc78d9 6d5993830430bd169	bc6cb78e20cb2028514 9d55563f6fdcf4aaafa58	5cbc07895d099ce39a3142025c557b7fac 41d79914535ab7ffc2094809f12a4b
COINTOS	b846fa8bc3a55fa 0490a807186a8ece9	c0c6b99796d732fa534 02ff49fd241612a340229	855656bfecc359a1816437223c4a133359e 73ecf45acda667610fbe7875ab3c8
COINTOSS.XLM	f92a75b98249fa61 cf62e8b63cb68fae	e5b312155289cdc6a80 a041821fc82d2cca80bcd	d0971d098b0f8cf2187feeed3ce049930f 19ec3379b141ec6a2f2871b1e90ff7
DRIVEDOWN	1dcd5afeccfe204 0895686eefa0a9629	40826e2064b59b8b7b3 e514b9ef2c1479ac3b038	07aed9fa864556753de0a664d22854167a 3d898820bc92be46b1977c68b12b34
	5fe4da6a1d82561a1 9711e564adc7589	e79527f7307c1dda62c4 2487163616b3e58d5028	8d0bafca8a8e8f3e4544f1822bc4bb08ce aa3c7192c9a92006b1eb500771ab53
EGGHATCH	e8da7fcdf0ca67b 76f9a7967e240d223	b0c2312852d750c4bce b552def6985b8b800d3f3	9dac6553b89645ac8d9e0a3dc877d1264 1e6d05fb52e8de6ae5533b2bdf0abc9
FASTFIRE	2bf26702c6ecbd4 6f68138cdcd45c034	1b9a4c0a5615a4f96a04 1d771646c1a407b17577	38d1d8c3c4ec5ea17c3719af285247cb1d8 879c7cf967e1be1197e60d42c01c5
Gh0st RAT	2d330c354c14b39 368876392d56fb18c	a1f72c890d0b920f4f4c b2d59df6fa40734de90d	f86d05c1d7853c06fc5561f8df19b53506b 724a83bb29c69b39f004a0f7f82d8
GOLDDRAGON	15ec5c7125e6c74f 740d6fc3376c130d	fb09b89803da071b7b7e b23244771c54d979a873	4a1c43258fe0e3b75afc4e020b904910c9 4d9ba08fc1e3f3a99d188b56675211
GOLDDRAGON. POWERSHELL	2a5562de1d3e734 d9328a1c78b43c2e5	4b0d0ebb0c676efe855 bed796221dd475a39ba40	203ea478fa4d2d5ef513cad8b51617e0c9f 7571bf3a3becf9c267a0d590c6d72
GOLDDROP	0cc0aa5877cec91 09b7a5a0e3a250c72	1d49d462a11a00d8ac96 08e49f055961bf79980d	1324acd1f720055e7941b39949116dfe72ce 2e7792e70128f69e228eb48b0821
	2c530adb84111436 6ce6177ce964a5e6	5b69e3e5f4f49cf8b635 a57a8c92e17a4f130d50	873b8fb97b4b0c6d7992f6af1565329578 8526def41f337c651dc64e8e4aeebd
GOLDSMELT	c066b81c4b8b070 3f81f8bc6fb432992	2508f5ff0c28356c0c3f 8e6cae7b750d53495bca	63b4bd01f80d43576c279adf69a5582129 e81cc4adbd036759095816437 65ea8
GRAYZONE	1d30dfa5d8f21d14 65409b207115ded6	942fd7b4ef1ccf7032a4 0acad975c7b5905c3c77	ed0161f2a3337af5e27a84bea85fb4abe35 654f5de22bcb8a503d537952b1e8a
HANGMAN.V2	21cffaa7f9bf224ce 75e264bfb16dd0d	862abce03f7f5de0c466 fdbd24ad796578eaa110	a605570555620cea6d6be211520525fc95 a30961661780da4cc4bafe9864f394

Malware Family	Sample MD5	SHA1	SHA256
Invoke-Mimikatz	20bc53deb7b12145 80e9d9efeaa5e9d7	e74b816f1c6d6347cb40 121e0b50dadd0d8f1f	908777e581616156576636568 61c212ac2569
		97	6741ef69411021474158fa2b4cf
JURASSICSHELL	9cdda333432f403 b408b9fe717163861	d80be054a569df5f20 1191dcc4fea0dde9622da5	d2f4bf0caed5a442198fcdc43c83c7b27ae 04f341a72b270c9ed40778aa77afe
	ddae18c65d583b4 1a2157d496a4bde61	63e113f0a906af82903 dbfac3e78bdd2d146e738	a4ba1e6ab678a1bdf8bc05bea8310d74392 8a4e2c05bad104e61afdd9cccf9a1
LANDMARK	1ffccf6cb3b74d68 df2b899fd33127a5	a61f009e73ae81a18751e 9aee39f8121a3902280	da22d327124a0ee6a93cd07e85f9804fbc 98eda87824ddcf7c8a63d349e87034
LANDMARK.NET	60efecf4e1b5b2c5 80329e9afa05db15	12c508ace6e8aa42be0 2750d759e720b800bf796	034d29fb89a8f68ba714f1868b2181c4cd5 9d4a2604630ef1554a6ccf3fe6d75
LATEOP **LATEOP.V2**	0f77143ce98d0b9 f69c802789e3b1713	7da4e8b743478370fa41 fe39a45e3ff2ca2194b3	54a8b8c933633c089f03d07cfbd5cafbf7 6a6d7095f2706d6604e739bb9c950f
LOGCABIN	0b558ee89a7bb32 968ef78104f6b9a28	b7fdb5e5b31adfc5ada0 de1e05b0c069968e5bce	79c0fe1467dada33e0b097dd772c362296 18b7091baa5f10da083f894192a237
LONEJOGGER	139d2561f5c72fab b099a12c16b8960c	2dd269608dd7f4da171d 1a220fe97347162008c7	2c338055e8245057169f1733846e0490bc 4ae117d1dadefe0a3f07a63dc87520
	14a00f517012279a f53118a491253e5c	98040f42103ce3b840d d54bf3490587f141a0bc3	26a98b752fd8e700776f11bad4169a06708 24d5b5b9337f3c8f46fac33bc03e8
METASPLOIT	37e7d679cd4aa78 8ec63f27cb02962ea	7d66c1f36b4b48d99046 1ec44d626793ade6a8d1	b55e9d65a3130f543360a9c488d35475d4 789ee7a32a4e94d02f33c21a172bcb
PASSMARK	b077ba5af1dfbd4a c523923eab56bcd4	4e93797dd3b383050cf 0ee585aa5b5525efb2380	4a08b78d410bc3d9b78dd63b146767f293 dc3f3f6f8092352d2aa2f589e9c772
PENCILDOWN	04d0856afb1aa916 8377d6aa579c5403	f3b774e921eaad9335b9 c057dd49b918c5dae4a6	e637c86ae20a7f36a0ad43618b00c48f47 b5591a03af3fb689a16c45afa43733
PENCILDOWN.ANDROID	4626ed60dfc8dea f75477bc06bd39be7	a9ff1ebb548f5bba600d 38e709ff331749fa9971	2365a48f7d6cf6dcc83195f06ea11b93c95 5c3a491c60b50ba42788917ba22e2
PENDOWN	768c84100d6e318 1a26fa50261129287	6f4b6938ac8fd9591fc3 99219dbaf4347d8b444b	780e7edbfad5f68051c2039036b00b304d 3f828fdbee85d2d09edbcc6d07ea34
PUMPKINBAR	946f787c129bf469 298aa881fb0843f4	d3b233d6d8b11235929e 4a0cbdb12eefdd47d927	32beeda8cffc2ecc689ea2529194cf80695 5879a334ec68176864d1e6c09800c
	c9d70bf37017260 9da848fa785989939	851ba2182b37bc738042 0a986840e16f73947413	ba3c79dbeca0234fa838ae4c95640911555 6f437372aeeb0737206d71caf4a38
QUASARRAT	0085bc8ce16ef176 43909c4799ead02b	25d94c9ab7635ff330da be96780f330f7f2ba775	a9c404e100bfd2716a8f6bfafc07b0bd617 5bedb047d10b94390c79249258272
SLIMCURL	68ce092f1a3d1985 2ea32db8388de5c7	700acc4e48eae84f80f 4dbaf74bf60b79efd49bd	25c2f4703cbaa1ff4dbcfcc16a10b29ef35c cc174b71b21de360d89854089f8
SOURDOUGH	7e609404cc258bb e283bea6ddd7af293	6618e25dd49b68f7b2 b266eb2d787e6f05c964bc	502136707a70b768800640224e48c6340 57dc651892113b62522f0dd2fcf1e87
SPICYTUNA	0821884168a644f3 c27176a52763acc9	1f6c7c9219f6b6ea30c d481968ae1a038789be67	e7fae41c0bd8d3d95253bd75dce9901559 9ecc404bd8d737cec305fc3e4dd018

Malware Family	Sample MD5	SHA1	SHA256
	8ca84c206fe8436 dcc92bf6c1f7cf168	636f2c20183b45691b 742949d49b3d6c218c9cce	7943bf9cc7b2adf50f7f92dd37347381e6d 0aef23b34a3cd0a3afcda1d72e16d
SWEETDROP	N/A	N/A	N/A
TROIBOMB	18df13900f118158c33	11f646095495d625e7d	98d4471fe549bb3067a
	df904c662e875	71038578cc838a6d5e111	c2f2d9afd50ed1baaddab41ec427083498 9e7f1ade14d
VENOMBITE	107f917a5ddb4d3947 233fbc9d47ddc8	75c516dde8415494c2 88e349d440ce778dede8e3	2d41b04f5d86047dc2353a10595418b0d5 239c22112f36eb9d253b2e8b6eb0d0

Learn more at **www.mandiant.com**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud