Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

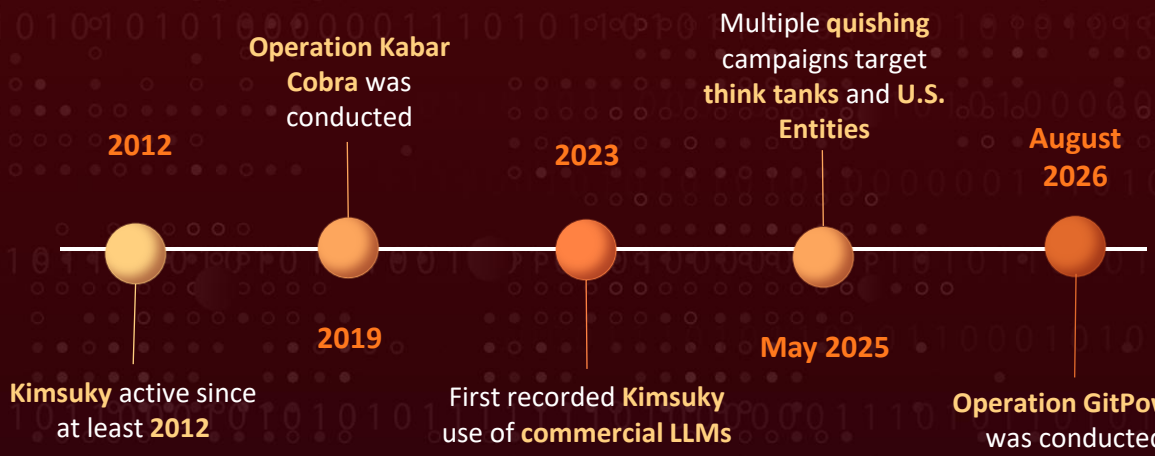
Kimsuky Blends AI-Generated Lures and Quishing into an Expanded Espionage Arsenal

Date of Publication	Admiralty Code	TA Number
September 16, 2026	A1	TA2026270

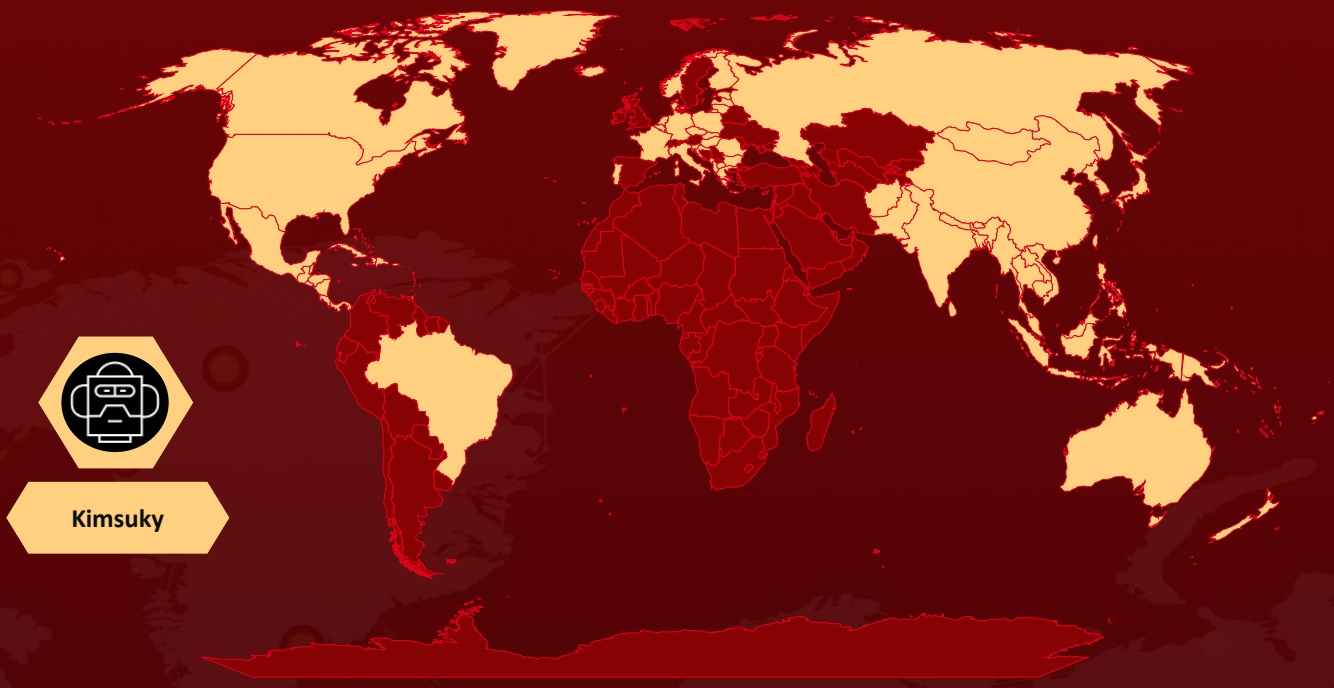
Summary

Active since: 2012
Targeted Regions: South Korea, United States, Japan, Vietnam, Thailand, Brazil, Germany, Russia, Canada, and broader Europe, including Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, and Albania. East Asia, Southeast Asia, Asia-Pacific, and North America are described as regional focus areas.
Targeted Platforms: Windows, Android, Linux, macOS, and cloud or web services and VPN portals
Targeted Products: GitHub, Pastebin, Dropbox, Slack, Cloudflare Quick Tunnels, Visual Studio, Microsoft 365, Okta
Targeted Industries: Government, Public Administration, Defense, Think Tanks, Policy Research Institutes, Academia, Universities, NGOs, Human Rights Organizations, Media, Healthcare, Machinery, Energy, Nuclear Power Operations, Manufacturing, Business Services, Legal Services, Construction, Financial, Insurance, Retail, Cryptocurrency
Threat Actor: Kimsuky (aka APT43, Thallium, THALLIUM, Velvet Chollima, Black Banshee, Emerald Sleet, Ruby Sleet, Sparkling Pisces, Springtail, TA427, TA406, Earth Kumiho, PatheticSlug, ARCHIPELAGO, SharpTongue, ITG16, Greendinosa, RGB-D5, Cerium)
Malware: AppleSeed (KGH_SPY), AlphaSeed, HappyDoor, PebbleDash, HelloDoor, httpMalice, httpTroy, MemLoad, HTTPSpy, AsyncRAT, BabyShark, GoldDragon, KLogEXE, Troll Stealer, Gomir, NavRAT, NikiHTTP, NikiTeaR, ComeBacker, DRATzarus, FastFire, FastSpy, FlowerPower, RandomQuery, Yorekey, Grease, TRANSLATEXT, QuasarRAT, Gh0st RAT, KimJongRAT, CSPY Downloader, BITTERSWEET, VENOMBITE, xRAT, MailFetch.py, Reger Dropper, Pidoc Dropper
Campaign Names: Operation GitPower, quishing (QR code phishing) campaigns, and Operation Kabar Cobra

Timeline



Actor Map



Targeted Non-Targeted

Actor Details

#1

Kimsuky is a Democratic People's Republic of Korea state-sponsored cyber espionage group that has been operating since at least 2012. It is tracked across the vendor landscape as APT43, Thallium, Velvet Chollima, Black Banshee, Emerald Sleet, Ruby Sleet, Sparkling Pisces, Springtail, TA427, TA406, Earth Kumiho, PatheticSlug, ARCHIPELAGO, SharpTongue, and ITG16. Kimsuky's priorities center on foreign policy and national security matters tied to the Korean Peninsula, nuclear policy, and sanctions, and the group supplements espionage with revenue-generating cybercrime that, in the most recent reporting, extends to cryptocurrency exchanges, DeFi platforms, and token fundraising operations.

#2

In 2019, the Kimsuky group mounted a sustained campaign of attacks against South Korea's defense-related organizations and media companies; the attackers were recently found to be targeting several enterprises, including those dealing in cryptocurrencies, for financial gain. A spate of malware was distributed with the file name "Cobra," and a mutex called "KABAR" was identified in several of the attacks.

#3

Initial access is overwhelmingly social: spear-phishing emails carrying compressed archives with LNK, CHM, JSE, PIF, SCR, HTA, HWP, and Office attachments; spoofed security software and Cisco Webex installation pages, in one case built around genuine meeting schedules the operators are assessed to have obtained through prior device or account compromise; counterfeit B2B messaging service installers aimed at administrators; and weaponized QR codes embedded in spearphishing emails that steer victims either to mobile-optimized credential harvesting pages impersonating Microsoft 365, Okta, and VPN portals or to trojanized Android APK downloads. Additionally, attributes exploitation of external remote services and public-facing applications to the group, naming CVE-2017-11882 and CVE-2019-0708, a broader set of exploited vulnerabilities, including CVE-2018-0802, CVE-2019-1405, CVE-2020-0787, CVE-2024-1709, and CVE-2025-48703.

#4

Operation GitPower, run in August 2026, shows how the current Windows attack works. The victim receives a ZIP file containing a Windows shortcut dressed up as a Korean business document, with a Chrome icon and a forged 2023 timestamp. Opening it runs a scrambled PowerShell command that the operators pushed past the visible edge of the shortcut's Properties window using roughly 300 blank spaces, so the file looks harmless on inspection. That command rebuilds a second script inside the user's AppData folder and runs it in a hidden window. Before anything else, the malware checks whether it is being watched, looking for virtual machine services, common analysis tools, and a known sandbox username, and it wipes the PowerShell command history behind it. It then creates a scheduled task that fires every few minutes under a name imitating BitLocker, MATLAB, or a .NET component, each carrying a small spelling error that is easy to miss.

#5

The group targets keystrokes, clipboard contents, screenshots, documents, stored browser credentials, credentials held in memory, and the session tokens that support multi-factor authentication. The keylogger writes captured data to a file named to resemble an Office configuration file and uploads it at intervals of roughly one to two hours, using browser identifiers that differ slightly from the legitimate strings. Within the toolset, AppleSeed is responsible for document theft and for collecting South Korean government GPKI certificates, while the PebbleDash family provides remote control and reconnaissance.

#6

Command and control is routed through services that most organizations already permit. Payloads are retrieved from GitHub and Pastebin, stolen data is sent out through Dropbox and Slack, and part of the infrastructure is hosted on compromised South Korean websites. The remainder uses free Korean dynamic DNS domains registered in volume and rotated frequently across providers in Korea, Hong Kong, Canada, and the United States. Command traffic is encrypted, and the malware executes commands under a Korean code page, which is consistent with the intended victim set.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Kimsuky (aka APT43, Thallium, Velvet Chollima, Black Banshee, Emerald Sleet, Ruby Sleet, Sparkling Pisces, Springtail, TA427, TA406, Earth Kumiho, PatheticSlug, ARCHIPELAGO, SharpTongue, ITG16, G0094)	North Korea (DPRK) **MOTIVE** Espionage, Financial Gains	South Korea, United States, Japan, Vietnam, Thailand, Brazil, Germany, Russia, Canada, and broader Europe including Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, and Albania. East Asia, Southeast Asia, Asia-Pacific, and North America are described as regional focus areas.	Government, Public Administration, Defense, Think Tanks, Policy Research Institutes, Academia, Universities, NGOs, Human Rights Organizations, Media, Healthcare, Machinery, Energy, Nuclear Power Operations, Manufacturing, Business Services, Legal Services, Construction, Financial, Insurance, Retail, Cryptocurrency

Recommendations

Hunt the Scheduled Task Names Directly: Query for tasks named Edge Updater, ChromeUpdate, EdgeUpdate, ChromeCheck, and EdgeCheck, plus any task whose name pairs a real product name with a misspelling or a ten-digit-plus numeric string, such as BitLockor Encrypter All Drives or MATLAB R2022bsdugbvr Startup Accelerator. Hidden tasks running PowerShell or regsvr32 at 5 to 60 minute intervals are the single most consistent persistence artifact across all four 2026 campaign clusters.

Detect Shortcut Files with Oversized Arguments: Build detection for LNK files whose command-line argument field exceeds a few hundred characters or contains long runs of whitespace, and for LNK files delivered inside ZIP archives. Roughly 300 leading spaces and 5,800 to 9,500 character PowerShell arguments are the Operation GitPower fingerprint, and both are visible to endpoint telemetry before any payload executes.

Alert on Headless Console and Hidden Window Execution: Flag conhost.exe launched with the --headless flag, powershell.exe with -windowstyle hidden, and PowerShell child processes spawned by hh.exe, wscript.exe, or explorer.exe following archive extraction. These parent-child chains appear in the CHM, LNK, and JSE clusters alike and rarely occur in normal user activity.

Monitor Signed Binary Proxy Execution: Watch for regsvr32.exe and rundll32.exe loading DLLs from C:\ProgramData, C:\Users\Public, and %TEMP%, and for certutil.exe performing decode operations against files under %USERPROFILE%\Links. Every dropper family in these reports (JSE, Reger, Pidoc) routes execution through one of these three binaries.

Restrict and Inspect Developer Tunnelling Tools: Treat Visual Studio Code Remote Tunnels, Cloudflare Quick Tunnels, and Ngrok as remote access software subject to allowlisting, and alert on the VS Code CLI executing from C:\Users\Public or on 'code tunnel' invocations on hosts with no development role. Kimsuky uses these to obtain interactive access over Microsoft-owned and Cloudflare-owned infrastructure that conventional C2 blocklists will never catch.

Govern Unsanctioned Remote Administration Software: Block or alert on DWAgent installation, the DWService service name, dwagsvc.exe, listener port 7950, and connections to dwservice.net relay nodes. The same control should cover any remote monitoring and management tool not explicitly approved for the environment.

Inspect GitHub, Pastebin, and Cloud Storage Egress: Alert on requests to raw.githubusercontent.com or api.github.com that carry an Authorization: token header from non-developer endpoints, on Pastebin raw path access, and on unexpected Dropbox API or Slack WebHook traffic from workstations. Kimsuky now uses these services as its primary payload delivery and exfiltration path precisely because they are allowlisted almost everywhere.

Protect GPKI Certificate Stores and Code Signing Material: Where South Korean government PKI certificates are used, move them off filesystem paths such as C:\GPKI onto hardware-backed storage, and audit access to that directory. AppleSeed's certificate theft capability is described as a signature behaviour and grants the actor the ability to authenticate as the victim organisation.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1589: Gather Victim Identity Information	T1589.002: Email Addresses
	T1598: Phishing for Information	T1598.003: Spearphishing Link
	T1592: Gather Victim Host Information	
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1585: Establish Accounts	T1585.003: Cloud Accounts
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.007: Artificial Intelligence
	T1682: Query Public AI Services	
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link

Tactic	Technique	Sub-technique
Initial Access	T1660: Phishing (Mobile)	
	T1078: Valid Accounts	T1078.003: Local Accounts
	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.007: JavaScript
	T1106: Native API	
	T1203: Exploitation for Client Execution	
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task

Tactic	Technique	Sub-technique
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1098: Account Manipulation	
Privilege Escalation	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
		T1027.001: Binary Padding
	T1140: Deobfuscate/Decode Files or Information	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1622: Debugger Evasion	
	T1070: Indicator Removal	T1070.003: Clear Command History

Tactic	Technique	Sub-technique
Defense Evasion	T1070: Indicator Removal	T1070.004: File Deletion
		T1070.006: Timestomp
	T1218: System Binary Proxy Execution	T1218.010: Regsvr32
		T1218.011: Rundll32
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1620: Reflective Code Loading	
	T1564: Hide Artifacts	T1564.004: NTFS File Attributes
		T1564.003: Hidden Window
	T1562: Impair Defenses	T1562.004: Disable or Modify System Firewall
Credential Access	T1056: Input Capture	T1056.001: Keylogging
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
	T1557: Adversary-in-the-Middle	

Tactic	Technique	Sub-technique
Credential Access	T1111: Multi-Factor Authentication Interception	
	T1539: Steal Web Session Cookie	
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.004: Cloud Account
Collection	T1005: Data from Local System	
	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1123: Audio Capture	
	T1074: Data Staged	T1074.001: Local Data Staging
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.003: Mail Protocols

Tactic	Technique	Sub-technique
Command and Control	T1102: Web Service	T1102.002: Bidirectional Communication
		T1102.001: Dead Drop Resolver
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1572: Protocol Tunneling	
	T1219: Remote Access Software	
	T1105: Ingress Tool Transfer	
	T1001: Data Obfuscation	T1001.001: Junk Data
	T1584: Compromise Infrastructure	T1584.004: Server
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1030: Data Transfer Size Limits	
	T1020: Automated Exfiltration	
Impact	T1657: Financial Theft	
	T1531: Account Access Removal	

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓
CVE-2018-0802	Microsoft Office Memory Corruption Vulnerability	Microsoft Office, Microsoft Word	✓	✓	✓
CVE-2019-0708	BlueKeep (Microsoft Remote Desktop Services Remote Code Execution Vulnerability)	Windows, Windows Server	✗	✓	✓
CVE-2019-1405	Microsoft Windows Universal Plug and Play (UPnP) Service Privilege Escalation Vulnerability	Windows, Windows Server	✗	✓	✓
CVE-2020-0787	Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓
CVE-2025-48703	CWP Control Web Panel OS Command Injection Vulnerability	CWP (aka Control Web Panel or CentOS Web Panel)	✓	✓	✓

Note: Kimsuky has previously exploited the flaws listed above in various campaigns. The CVEs have patch links hyperlinked to the corresponding tick marks.

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1eff237dee95172363bfc0342d0389f809f753a6ec5e6848e57b3fd5482e9793, 85f8f8a3f28d2956776fbbd0365cdb78ac8dc1e6ed12818ef18caed0bb2f74c8, af50f35701916d3909f2727cdcbde1a7af47f46eb8db3996905b1c0725aa133f, d7c09e7bf79aa9b786dcd9f870427f4a1110f702646fba9d3835215ad3649d0b, a36576a096db24a1c91327eb547dedf52e5bd4b0d4593b88d9593d377585b922, 981dadc1a7ab50d6ff600a69c904a350fcc2d2050ac94589321f51ac5527c78d, 18fa10ff013cf82974f00875e23dae48d4d2dc0993a348f8069dd32845de39a1, a4f72ce8b5736fe3ca2083cfe21bd51697f12e900e307c357cb8523b8f86e3ec, c62677543eeb50e0def44fc75009a7748cdbedd0a3ccf62f50d7f219f6a5aa05, e8000ddfddbe120b5f2fb3677abbad901615d1abd01a0de204fade5d2dd5ad0d, da79eea1198a1a10e2ffd50fd949521632d8f252fb1aadb57a45218482b9fd89
SHA1	b5224224fdbabdea53a91a96e9f816c6f9a8708c, 5c7b2705155023e6e438399d895d30bf924e0547, d4fa57f9c9e35222a8cacddc79055c1d76907fb9
TLS Certificate SHA256	9de541b039cfdb96c7810df49efd958b28cc2df73e314f67c1a91469a2b19796
IPv4	130[.]94[.]29[.]111, 27[.]102[.]137[.]38, 118[.]194[.]249[.]109, 27[.]102[.]137[.]150, 51[.]79[.]185[.]184, 162[.]255[.]119[.]150, 38[.]60[.]220[.]135, 163[.]245[.]221[.]218, 163[.]245[.]215[.]46, 27[.]102[.]113[.]106, 157[.]250[.]202[.]123

TYPE	VALUE
MD5	10780939962b54addc9d31f57d80edfc, 1523a2fcc901965ab4568d9fe829e4af, 500e0bc0d7579fb338912770964076fe, 685bfc6b2c29fbc16cfad908894add55, 7a53089053b1381742856a5cf2b95f8b, 8db2f20b719dcb7029d6296505622093, 900e832c10d851bbdef3fb191a15db0e, a2015665a3e18bf0ef86e3931245c7e6, bb88940e915b11f6330b7446f6037f5b, ce5932b88f879f26006df81f2fa7667e, d0894d4626aae0f96d6b84ca3bb71a36, e50f2ae7fb03675a1ef58b1cf9cda6d1, f648bdd3c2cd902e239149de86d43e8f, 4a476abcf741323b367eda0ec49f8c38, 00f957b7dafd8d210e717041add02eab, cc837d2b2af4bd9c1c3faf61cefeb848, 97b4c2e67e5e18b70949690a69820c2a, bea602695d58cbf25fff058834e36c1d, ea5f32e1273ec93d43ee09a337fb60e1, 0d07fb6d1a3736ea543ab8364115e435, 6d2dfd7ca77530afec000a197d6b8677, b4dd4c76d7deef4cf532e240b7f84c9d, be31a38bab026f229afd5e3174c363f7, c61a6efe1a169c6c1d8595af3ff0dd74, c6de1be41dcfbad9cae76c58eae7f5a3, 50f619aaba1d28882022ced135b13a07, a581fdea0970f8a5b6cfec4853c802d7, 9df5ca76ac085b89c1ddcb3963e9fe97, be978477fe7c179cb9607a6e08a05dff, 8833a270ddef0f464d5916958b6778e6, d09c0744273355b6da719fdb62923bed, fcaf03060e34a73fe499b906492d9f13, dd47c97b44408e0a5ecd8f482fcd0dbc, f57a9e973e1cecd6b361467041e464f4, 3369b911cf3706a2660d2af9b3c35f9a, 39e091e981d9daab56e680927508bd1f, 00fd7272f9a3044b5f62680d9e576e55, bd8e948a6e61436532cd2ed2b62db3f3, 3315229011b2fa2b05bd4c7b4fbb58e3, a87cd5fd8fe223816005e81e0da70b21, c05f074c70a6cacb0e6f05578aab3c9d, 1efaf988fded55cd3b974c66f4ca8f7e,

TYPE	VALUE
MD5	50e89a4e50392e4235822e9e92df4c32, 7b9484d719f39faa71abd90f57525cc8, 91d1a7153606dedef92502553962cf67, 02897faac6e41781152f480565e5d572, 995a0a49ae4b244928b3f67e2bfd7a6e, 52f1ff082e981cbdfd1f045c6021c63f, 9fe43e08c8f446554340f972dac8a68c, 8e15c4d4f71bdd9dbc48cd2cabc87806, 65fc9f06de5603e2c1af9b4f288bb22c, c19aeaedbbfc4e029f7e9bdface495b9, 8983ffa6da23e0b99ccc58c17b9788c7, a7f0a18ac87e982d6f32f7a715e12532, f4465403f9693939fe9c439f0ab33610, 5c373c2116ab4a615e622f577e22e9be, d1ec20144c83bba921243e72c517da5e, 58ac2f65e335922be3f60e57099dc8a3, f73ba062116ea9f37d072aa41c7f5108, 7e0825019d0de0c1c4a1673f94043ddb, 08160acf08fccecde7b34090db18b321, 94faed9af49c98a89c8acc55e97276c9, c42ae004badddd3017adadbdd1421e00, 9ca5f93a732f404bbb2cee848f5bbda0, 678fb1a87af525c33ba2492552d5c0e2, 4599ac1bbe483c73064df1353feafd01, 364d4fdf430477222fe854b3cd5b6d40, 71db2ae9c36403cec1fd38864d64f239, f35b05779e9538cec363ca37ab38e287
Domains	www[.]ibizplus[.]n-e[.]kr, load[.]serverpit[.]com, conference[.]birdriver[.]org, download[.]birdriver[.]org, hdrgdrfes[.]chickenkiller[.]com, pipeline[.]embeddedonline[.]org, appview[.]imagetemplate[.]com, bigfile[.]jaycloudlab[.]com, bigfile[.]crabdance[.]com, 00701111[.]000webhostapp[.]com, gosiweb[.]gosiclass[.]com, niscarea[.]com, www[.]yespp[.]co[.]kr, www[.]pyrotech[.]co[.]kr, newjo-imd[.]com

TYPE	VALUE
Domains	nid-log[.]com, check[.]nid-log[.]com, nid-tax[.]dns[.]army, tax-invoice[.]dns[.]army, pay-tax[.]dns[.]navy, ntax-doc[.]v6[.]rocks, miss-tax[.]dns[.]navy, k-invoice[.]v6[.]navy, nid-log[.]electric-support[.]v6[.]rocks, nid-htl[.]duckdns[.]org, verify[.]efine-log[.]kro[.]kr, deliver-doc[.]v6[.]navy, nid-navertca[.]servehalflife[.]com, nid-naverfxc[.]servecounterstrike[.]com, nid-naverpep[.]servequake[.]com, nid-navercwu[.]servecounterstrike[.]com, noreplymail[.]space, opedromos1[.]r-e[.]kr, morames[.]r-e[.]kr, load[.]ssangyongcne[.]o-r[.]kr, load[.]yju[.]o-r[.]kr, attach[.]docucloud[.]o-r[.]kr, load[.]supershop[.]o-r[.]kr, load[.]erasecloud[.]n-e[.]kr, cms[.]spaceyou[.]o-r[.]kr, erp[.]spaceme[.]p-e[.]kr, file[.]bigcloud[.]n-e[.]kr, load[.]auraria[.]org, female-disorder-beta-metropolitan[.]trycloudflare[.]com, node896147[.]dwservice[.]net, node828765[.]dwservice[.]net, node484265[.]dwservice[.]net, www[.]dwservice[.]net
URLs	hxxps[:]//www[.]ibizplus[.]n-e[.]kr/install[.]html, hxxps[:]//load[.]serverpit[.]com/fwrite[.]php, hxxps[:]//load[.]erasecloud[.]n-e[.]kr/login[.]php, hxxps[:]//conference[.]birdriver[.]org/, hxxps[:]//download[.]birdriver[.]org/download[.]php?id=425623, hxxps[:]//download[.]birdriver[.]org/download[.]php?id=393156, hxxp[:]//hdrgdrfes[.]chickenkiller[.]com/index[.]php, hxxps[:]//pipeline[.]embeddedonline[.]org/check[.]php?x-csrf-token=gateless,

TYPE	VALUE
URLs	hxxps[:]//pipeline[.]embeddedonline[.]org/download3[.]php?sessid=54126&user-token=gateless, hxxps[:]//appview[.]imagetemplate[.]com/gateless_icon<Counter>[.]png, hxxps[:]//bigfile[.]jaycloudlab[.]com/download[.]php?id=745896, hxxps[:]//bigfile[.]crabdance[.]com/recaptcha[.]html, hxxp[:]//female-disorder-beta-metropolitan[.]trycloudflare[.]com/index[.]php, hxxps[:]//file[.]bigcloud[.]n-e[.]kr/index[.]php, hxxps[:]//www[.]yespp[.]co[.]kr/common/include/code/out[.]php, hxxps[:]//www[.]pyrotech[.]co[.]kr/common/include/tech/default[.]php, hxxp[:]//newjo-imd[.]com/common/include/library/default[.]php, hxxps[:]//www[.]dwservice[.]net/, pastebin[.]com/raw/gybpx38s, 00701111[.]000webhostapp[.]com/wp-extra, gosiweb[.]gosiclass[.]com/m/gnu/convert/html/com/list[.]php?query=6, niscarea[.]com/in[.]php?cn=[base64]&fn=[DateTime], noreplymail[.]space/BitJoker/bootservice[.]php, hxxps[:]//github[.]com/sven5500, hxxps[:]//github[.]com/montry111, hxxps[:]//github[.]com/jamjack2026, hxxps[:]//github[.]com/urusa4400, hxxps[:]//github[.]com/jamestony88, hxxps[:]//github[.]com/baras6600P, hxxps[:]//github[.]com/choemiyang, hxxps[:]//github[.]com/jeni534
Email	baras6600[@]proton[.]me, choemiyang[@]hotmail[.]com, dustinharrise91[@]outlook[.]com, jackal3300[@]proton[.]me, jametony8[@]outlook[.]com, jamjack2026[@]proton[.]me, montry111[@]proton[.]me, sven5500[@]proton[.]me, taini7700[@]outlook[.]com, urusa4400[@]proton[.]m

TYPE	VALUE
Filenames	20260811_자금집행.lnk, Security_20260811.lnk, Visa5499.lnk, 보험료 납부 안내_202608.lnk, 인증서 갱긴 안내.lnk, fgkpxjbgthy.ps1, kvnourgr.ps1, mlxchjvose.ps1, qpmvixibrg.ps1, p5234fop.ps1, xnciuegwpo.pdf, NWfie.xlsx, Visa_5499.png, api_reference.chm, SecurityMaker.chm, Link.dat, Link.ini, Office_Config.xml, Info.txt, nos-setup.exe, astx-setup.exe, fix-camera.jse, mTSTCv8.mdxm, engine.dat, cacheMon.dat, spyInster.dll, spyLoader.dll, httpSpy.dll, MemLoader.dll, loadDll.dll, meeting.html, 420109_최종본_수정요청2차_반영.hwp.jse, 2026-0146-에스큐아이소프트-망연계시스템 유지보수 발주 .pdf.jse, [별지 제8호서식] 개인정보(열람 정정삭제 처리정지) 요구서(개인정보 보호법 시행규칙).hwp.jse, 2026년 상반기 국내대학원 석사야간과정 위탁교육생 선발관련 서류.hwpx.jse, 2026년 상반기 국내대학원 석사야간과정 위탁교육생 선발관련 서류 (1).hwpx.jse, 노현정님.pdf.jse, security_20260126.scr,

TYPE	VALUE
Filenames	secu.scr, 대국민서비스관리운영체계_현장점검_증적(초안).pif, jhsakqvv.dat, xipbkmaw.exe, out.txt, user.txt, 1.zip, unrar.exe, dwagsvc.exe, config.json, config.db, 2034923.bat, 9583423.bat, 1295049.bat
File Path	%USERPROFILE%\Links\Link.dat, %USERPROFILE%\Links\Link.ini, %WINDIR%\System32\OfficeUpdater_*_*_*.ini, %APPDATA%\Microsoft\Windows\Templates\Office_Config.xml, %AppData%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt, %TEMP%\자금집행첨부자료.pdf, %TEMP%\영수증.xlsx, C:\Programdata\[a-z]{8}.dat, C:\programdata\calc.exe, C:\Users\Public\cacheMon.dat, C:\ProgramData\mTSTCv8.mdxm, C:\ProgramData\meeting.html, %Temp%\msbuil.bat, %Temp%\msbuild.bat, %TEMP%\NK[0-9a-fA-F]+\.tmp, %TEMP%\JG[0-9a-fA-F]{4}\.tmp, C:\ProgramData\1.zip, C:\programdata\unrar.exe, C:\programdata\dwagent\native\dwagsvc.exe, c:\programdata\config.db, C:\GPKI, %USERPROFILE%\Links\MXFhejJ3c3gzZWRjA.dat, %USERPROFILE%\Links\MXFhejJ3c3gzZWRjA.vbs, C:\Users\Public\Libraries\
Mutex	Global\AlreadyRunning19122345

TYPE	VALUE
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MSEdgeUpdateInstaller, HKCU\Software\Microsoft\Windows\CurrentVersion\Run (value: tdll), HKCU\Software\Microsoft\Windows\CurrentVersion\Run (value: Everything 1.9a-[filesize]), HKCU\Software\Microsoft\Windows\CurrentVersion\Run (value: Everything 1.8a-[filesize]), HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (value: Document)
Scheduled Task	Edge Updater, ChromeUpdate, EdgeUpdate, ChromeCheck, EdgeCheck, BitLockor Encrypter All Drives_102974298364124_skillerty, MATLAB R2022bsdugbvr Startup Acceleratorsdpvishdgreg, .NET Framework NGEN v4.0.3031923879465346234523
PDB Path	C:\Users\jira\Documents\My_Received_Files\loadDll\x64\Release\loadDll.pdb
HTTP Request	/api/bootservice.php?tag=<ID>&query=1, /api/bootservice.php?tag=<ID>&query=6, /api/checkservice.php?idx=5&tag=<ID>, /api/finalservice.php, /pc/index.php, /loggerservice.php
User Agent	Chremo/87.0.4280.141, Edgo/87.0.664.75, HeadlessChrome/151.0.0.0
Encryption Key	#RsfsetraW#@EsfesgsgAJOPj4eml;, %^fseRW#r3qwrwfsddREfGEgse)(14);, RGdcsedfd@#%dg9ser3$#$^@34sdfxl, fwr3errsettwererfs, kDRNGmWGTMpjQmREgQzU, N*32h^G, KK*3bU(), N&*2hn, k*5jhc#, *bebhj&U7, 27%&G3j, J83&^3, VNi^k, V&63bJ&, OPu&6vh

References

https://www.genians.co.kr/en/blog/threat_intelligence/ai-agent-opencode?hsCtaAttrib=392306999998

https://intel.breakglass.tech/post/kimsuky-chm-nidlog-c2-dump-full-payload-recovery

https://www.cyfirma.com/research/apt-profile-kimsuki/

https://zimperium.com/blog/kimsuky-expands-mobile-attacks-with-weaponized-qr-codes

https://www.enki.co.kr/en/media-center/blog/kimsuky-s-advanced-attack-techniques-jsonping-webex-spoofing-and-a-new-httpspy-variant

https://securelist.com/kimsuky-appleseed-pebbledash-campaigns/119785/

https://www.fbi.gov/file-repository/cyber-alerts/north-korean-kimsuky-actors-leverage-malicious-qr.pdf/view

https://www.rapid7.com/blog/post/2024/03/20/the-updated-apt-playbook-tales-from-the-kimsuky-threat-actor-group/

https://www.huntress.com/threat-library/threat-actors/kimsuky

https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a

https://attack.mitre.org/groups/G0094/

https://fortiguard.fortinet.com/threat-actor/5536/kimsuky

https://www.hivepro.com/threat-advisory/kimsukys-stealthy-rdp-espionage-campaign

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 16, 2026 • 7:00 AM

More at www.hivepro.com