Kimsuky, Black Banshee, Velvet Chollima, Emerald Sleet, THALLIUM, APT43, TA427, Springtail, Group G0094

Archived: 2026-04-02 10:51:37 UTC

Enterprise T1098 .007 Account Manipulation: Additional Local or Domain Groups

Kimsuky has added accounts to specific groups with `net localgroup` .[15]

Enterprise T1583 Acquire Infrastructure

Kimsuky has used funds from stolen and laundered cryptocurrency to acquire operational infrastructure.[5]

.001 Domains

Kimsuky has registered domains to spoof targeted organizations and trusted third parties including search engines, web platforms, and cryptocurrency exchanges.[12][16][4][2][3][15][5][17]

.004 Server

Kimsuky has purchased hosting servers with virtual currency and prepaid cards.[15]

.006 Web Services

Kimsuky has hosted content used for targeting efforts via web services such as Blogspot.[18] Kimsuky has also leveraged Dropbox for hosting payloads and uploading victim system information. [19]

Enterprise T1557 Adversary-in-the-Middle

Kimsuky has used modified versions of PHProxy to examine web traffic between the victim and the accessed website.[4]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Kimsuky has used HTTP GET and POST requests for C2.[18]

.002 Application Layer Protocol: File Transfer Protocols

Kimsuky has used FTP to download additional malware to the target machine.[20]

.003 Application Layer Protocol: Mail Protocols

Kimsuky has used e-mail to send exfiltrated data to C2 servers.[4]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Kimsuky has used QuickZip to archive stolen files before exfiltration.[18]

.003 Archive Collected Data: Archive via Custom Method

Kimsuky has used RC4 encryption before exfil.[21]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Kimsuky has placed scripts in the startup folder for persistence and modified the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce` Registry key.[21][4][22][18][15]

Enterprise T1185 Browser Session Hijacking

Kimsuky has the ability to use form-grabbing to extract emails and passwords from web data forms.[23]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Kimsuky has executed a variety of PowerShell scripts including Invoke-Mimikatz.[1][4][18][15][5] Kimsuky has also utilized PowerShell scripts for execution, persistence, and defense evasion.[19]

.003 Command and Scripting Interpreter: Windows Command Shell

Kimsuky has executed Windows commands by using `cmd` and running batch scripts.[18][15]

.005 Command and Scripting Interpreter: Visual Basic

Kimsuky has used Visual Basic to download malicious payloads.[12][20][22][18] Kimsuky has also used malicious VBA macros within maldocs disguised as forms that trigger when a victim types any content into the lure.[18]

.006 Command and Scripting Interpreter: Python

Kimsuky has used a macOS Python implant to gather data as well as MailFetcher.py code to automatically collect email data.[4][15]

.007 Command and Scripting Interpreter: JavaScript

Kimsuky has used JScript for logging and downloading additional tools.[20][4] Kimsuky has used TRANSLATEXT, which contained four Javascript files for bypassing defenses, collecting sensitive information and screenshots, and exfiltrating data.[23]

Enterprise T1586 .002 Compromise Accounts: Email Accounts

Kimsuky has compromised email accounts to send spearphishing e-mails.[20][3]

Enterprise T1584 .001 Compromise Infrastructure: Domains

Kimsuky has compromised legitimate sites and used them to distribute malware.[15][5][17]

Enterprise T1136 .001 Create Account: Local Account

Kimsuky has created accounts with `net user`.[15]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Kimsuky has created new services for persistence.[21][4]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Kimsuky has used browser extensions including Google Chrome to steal passwords and cookies from browsers. Kimsuky has also used Nirsoft's WebBrowserPassView tool to dump the passwords obtained from victims.[11][4][7][18]

Enterprise T1005 Data from Local System

Kimsuky has collected Office, PDF, and HWP documents from its victims.[21][18]

Enterprise T1074 .001 Data Staged: Local Data Staging

Kimsuky has staged collected data files under `C:\Program Files\Common Files\System\Ole DB\`.[4][18]

Enterprise T1140 Deobfuscate/Decode Files or Information

Kimsuky has decoded malicious VBScripts using Base64.[18] Kimsuky has also decoded malicious PowerShell scripts using Base64.[19]

Enterprise T1587 Develop Capabilities

Kimsuky created and used a mailing toolkit to use in spearphishing attacks.[20]

.001 Malware

Kimsuky has developed its own unique malware such as MailFetch.py for use in operations.[15][18][5]

Enterprise T1114 .002 Email Collection: Remote Email Collection

Kimsuky has used tools such as the MailFetch mail crawler to collect victim emails (excluding spam) from online services via IMAP.[15]

.003 Email Collection: Email Forwarding Rule

Kimsuky has set auto-forward rules on victim's e-mail accounts.[4]

Enterprise T1585 Establish Accounts

Kimsuky has leveraged stolen PII to create accounts.[17]

.001 Social Media Accounts

Kimsuky has created social media accounts to monitor news and security trends as well as potential targets.[15]

.002 Email Accounts

Kimsuky has created email accounts for phishing operations.[15][5][6]

Enterprise T1546 .001 Event Triggered Execution: Change Default File Association

Kimsuky has a HWP document stealer module which changes the default program association in the registry to open HWP documents.[21]

Enterprise T1041 Exfiltration Over C2 Channel

Kimsuky has exfiltrated data over its C2 channel.[21][18]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Kimsuky has exfiltrated stolen files and data to actor-controlled Blogspot accounts.[18] Kimsuky has also leveraged Dropbox for uploading victim system information.[19]

Enterprise T1190 Exploit Public-Facing Application

Kimsuky has exploited various vulnerabilities for initial access, including Microsoft Exchange vulnerability CVE-2020-0688.[15]

Enterprise T1133 External Remote Services

Kimsuky has used RDP to establish persistence.[4]

Enterprise T1083 File and Directory Discovery

Kimsuky has the ability to enumerate all files and directories on an infected system.[21][18][15]

Enterprise T1657 Financial Theft

Kimsuky has stolen and laundered cryptocurrency to self-fund operations including the acquisition of infrastructure.[5][17]

Enterprise T1589 .002 Gather Victim Identity Information: Email Addresses

Kimsuky has collected valid email addresses including personal accounts that were subsequently used for spearphishing and other forms of social engineering.[3][6][17]

.003 Gather Victim Identity Information: Employee Names

Kimsuky has collected victim employee name information.[15]

Enterprise T1591 Gather Victim Org Information

Kimsuky has collected victim organization information including but not limited to organization hierarchy, functions, press releases, and others.[15] Kimsuky has also used large language models (LLMs) to gather information about potential targets of interest.[10]

Enterprise T1564 .002 Hide Artifacts: Hidden Users

Kimsuky has run `reg add 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList' /v` to hide a newly created user.[15]

.003 Hide Artifacts: Hidden Window

Kimsuky has used an information gathering module that will hide an AV software window from the victim.[18] Kimsuky has also been known to use `-WindowStyle Hidden` to conceal PowerShell windows.[19]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Kimsuky has been observed turning off Windows Security Center and can hide the AV software window from the view of the infected user.[21][18]

.004 Impair Defenses: Disable or Modify System Firewall

Kimsuky has been observed disabling the system firewall.[21]

Enterprise T1656 Impersonation

Kimsuky has impersonated academic institutions and NGOs in order to gain information related to North Korea.[10]

Enterprise T1070 .004 Indicator Removal: File Deletion

Kimsuky has deleted the exfiltrated data on disk after transmission. Kimsuky has also used an instrumentor script to terminate browser processes running on an infected system and then delete the cookie files on disk.[21][18][15] Kimsuky has deleted files using the `Remove-Item` PowerShell commandlet to remove traces of executed payloads.[19]

.006 Indicator Removal: Timestomp

Kimsuky has manipulated timestamps for creation or compilation dates to defeat anti-forensics.[2]

Enterprise T1105 Ingress Tool Transfer

Kimsuky has downloaded additional scripts, tools, and malware onto victim systems.[18][22][19]

Enterprise T1056 .001 Input Capture: Keylogging

Kimsuky has used a PowerShell-based keylogger as well as a tool called MECHANICAL to log keystrokes.[1][21][4][7][18][15]

Enterprise T1534 Internal Spearphishing

Kimsuky has sent internal spearphishing emails for lateral movement after stealing victim information.[15]

Enterprise T1680 Local Storage Discovery

Kimsuky has enumerated drives.[21][18]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Kimsuky has disguised services to appear as benign software or related to operating system functions.[4][19]

.005 Masquerading: Match Legitimate Resource Name or Location

Kimsuky has renamed malware to legitimate names such as `ESTCommon.dll` or `patch.dll`.[24] Kimsuky has also disguised payloads using legitimate file names including a PowerShell payload named chrome.ps1. [19]

.007 Masquerading: Double File Extension

Kimsuky has used an additional filename extension to hide the true file type. Kimsuky has also masqueraded malicious LNK files as PDF objects using the double extension .pdf.lnk.[19]

Enterprise T1112 Modify Registry

Kimsuky has modified Registry settings for default file associations to enable all macros and for persistence.[4][22][18][15]

Enterprise T1111 Multi-Factor Authentication Interception

Kimsuky has used a proprietary tool to intercept one time passwords required for two-factor authentication.[15]

Enterprise T1040 Network Sniffing

Kimsuky has used the Nirsoft SniffPass network sniffer to obtain passwords sent over non-secure protocols.[4][7]

Enterprise T1027 Obfuscated Files or Information

Kimsuky has obfuscated binary strings including the use of XOR encryption and Base64 encoding.[12][20] Kimsuky has also modified the first byte of DLL implants targeting victims to prevent recognition of the executable file format.[18]

.001 Binary Padding

Kimsuky has performed padding of PowerShell command line code with over 100 spaces.[19]

.002 Software Packing

Kimsuky has packed malware with UPX.[3]

.010 Command Obfuscation

Kimsuky has encoded malicious PowerShell scripts using Base64.[19]

.012 LNK Icon Smuggling

Kimsuky has used the LNK icon location to execute malicious scripts. Kimsuky has also padded the LNK target field properties with extra spaces to obscure the script.[19]

.016 Junk Code Insertion

Kimsuky has obfuscated code by filling scripts with junk code and concatenating strings to hamper analysis and detection.[19]

Enterprise T1588 .002 Obtain Capabilities: Tool

Kimsuky has obtained and used tools such as Nirsoft WebBrowserPassVIew, Mimikatz, and PsExec.[7][18][5]

.003 Obtain Capabilities: Code Signing Certificates

Kimsuky has stolen a valid certificate that is used to sign the malware and the dropper.[25]

.005 Obtain Capabilities: Exploits

Kimsuky has obtained exploit code for various CVEs.[15]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Kimsuky has gathered credentials using Mimikatz and ProcDump.[4][7][15]

Enterprise T1566 Phishing

Kimsuky has used spearphishing to gain initial access and intelligence.[10][17]

.001 Spearphishing Attachment

Kimsuky has used emails containing Word, Excel and/or HWP (Hangul Word Processor) documents in their spearphishing campaigns.[11][21][12][20][2][3][18][15] Kimsuky has also distributed emails with attached compressed zip files that contained malicious .LNK files masquerading as legitimate files.[19]

.002 Spearphishing Link

Kimsuky has sent spearphishing emails containing a link to a document that contained malicious macros or took the victim to an actor-controlled domain.[1][7][15]

Enterprise T1598 Phishing for Information

Kimsuky has used tailored spearphishing emails to gather victim information including contat lists to identify additional targets.[5]

.003 Spearphishing Link

Kimsuky has used links in e-mail to steal account information including web beacons for target profiling.[20][3][15][6]

Enterprise T1057 Process Discovery

Kimsuky can gather a list of all processes running on a victim's machine.[18] Kimsuky has also obtained running processes on the victim device utilizing PowerShell cmdlet `Get-Process`.[19]

Enterprise T1055 Process Injection

Kimsuky has used Win7Elevate to inject malicious code into explorer.exe.[21]

.012 Process Hollowing

Kimsuky has used a file injector DLL to spawn a benign process on the victim's system and inject the malicious payload into it via process hollowing.[18]

Enterprise T1012 Query Registry

Kimsuky has obtained specific Registry keys and values on a compromised host.[18]

Enterprise T1620 Reflective Code Loading

Kimsuky has used the Invoke-Mimikatz PowerShell script to reflectively load a Mimikatz credential stealing DLL into memory.[5] Kimsuky has also used reflective loading through .NET assembly using `[System.Reflection.Assembly]::Load`.[19]

Enterprise T1219 .002 Remote Access Tools: Remote Desktop Software

Kimsuky has used a modified TeamViewer client as a command and control channel.[21][22]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Kimsuky has used RDP for direct remote point-and-click access.[7]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Kimsuky has downloaded additional malware with scheduled tasks.[15] Kimsuky has established persistence by creating a scheduled task named "ChromeUpdateTaskMachine" through the PowerShell cmdlet `Register-ScheduleTask` which was set to execute another PowerShell script once, then five minutes after its creation and periodically repeat every 30 minutes.[19]

Enterprise T1113 Screen Capture

Kimsuky has captured browser screenshots using TRANSLATEXT.[23]

Enterprise T1596 Search Open Technical Databases

Kimsuky has used LLMs to better understand publicly reported vulnerabilities.[10][26]

Enterprise T1593 Search Open Websites/Domains

Kimsuky has used LLMs to identify think tanks, government organizations, etc. that have information.[10]

.001 Social Media

Kimsuky has used Twitter to monitor potential victims and to prepare targeted phishing e-mails.[3]

.002 Search Engines

Kimsuky has searched for vulnerabilities, tools, and geopolitical trends on Google to target victims.[15]

Enterprise T1594 Search Victim-Owned Websites

Kimsuky has searched for information on the target company's website.[15]

Enterprise T1505 .003 Server Software Component: Web Shell

Kimsuky has used modified versions of open source PHP web shells to maintain access, often adding "Dinosaur" references within the code.[4]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Kimsuky has checked for the presence of antivirus software with `powershell Get-CimInstance -Namespace root/securityCenter2 - classname antivirusproduct`.[15] Kimsuky has also obtained details on antivirus software through WMI queries using `Win32_OperatingSystem` and `SecurityCenter2.AntiVirusProduct`.[19]

Enterprise T1176 .001 Software Extensions: Browser Extensions

Kimsuky has used Google Chrome browser extensions to infect victims and to steal passwords and cookies.[11][7]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

Kimsuky has used compromised and acquired infrastructure to host and deliver malware including Blogspot to host beacons, file exfiltrators, and implants.[18][5][17] Kimsuky has also hosted malicious payloads on Dropbox.[19]

Enterprise T1539 Steal Web Session Cookie

Kimsuky has used malware, such as TRANSLATEXT, to steal and exfiltrate browser cookies.[23][25]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Kimsuky has signed files with the name EGIS CO,. Ltd. and has stolen a valid certificate that is used to sign the malware and the dropper.[12][25]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

Kimsuky has used mshta.exe to run malicious scripts on the system.[1][4][22][15]

.010 System Binary Proxy Execution: Regsvr32

Kimsuky has executed malware with `regsvr32s`.[15]

.011 System Binary Proxy Execution: Rundll32

Kimsuky has used `rundll32.exe` to execute malicious scripts and malware on a victim's network.[18]

Enterprise T1082 System Information Discovery

Kimsuky has enumerated OS type, OS version, and other information using a script or the "systeminfo" command.[21][18] Kimsuky has also obtained system information such as OS type, OS version, and system type through querying various Windows Management Instrumentation (WMI) classes including `Win32_OperatingSystem`.[19]

Enterprise T1016 System Network Configuration Discovery

Kimsuky has used `ipconfig/all` and web beacons sent via email to gather network configuration information.[18][6] Kimsuky has also identified Host IP addresses leveraging the WMI class `Win32_NetworkAdapterConfiguration`.[19]

Enterprise T1007 System Service Discovery

Kimsuky has used an instrumentor script to gather the names of all services running on a victim's system.[18]

Enterprise T1205 Traffic Signaling

Kimsuky has used TRANSLATEXT to redirect clients to legitimate Gmail, Naver or Kakao pages if the clients connect with no parameters.[23]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Kimsuky has used tools that are capable of obtaining credentials from saved mail.[7]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

Kimsuky has used pass the hash for authentication to remote access software used in C2.[4]

Enterprise T1204 .001 User Execution: Malicious Link

Kimsuky has lured victims into clicking malicious links.[15]

.002 User Execution: Malicious File

Kimsuky has attempted to lure victims into opening malicious e-mail attachments.[12][20][4][2][3][18] Kimsuky has also lured victims with tailored filenames and fake extensions that entice victims to open LNK files.[19]

Enterprise T1078 .003 Valid Accounts: Local Accounts

Kimsuky has used a tool called GREASE to add a Windows admin account in order to allow them continued access via RDP.[7]

Enterprise T1102 .001 Web Service: Dead Drop Resolver

Kimsuky has used TRANSLATEXT and a dead drop resolver to retrieve configurations and commands from a public blog site.[23]

.002 Web Service: Bidirectional Communication

Kimsuky has used Blogspot pages and a Github repository for C2.[18][23] Kimsuky has also leveraged Dropbox for downloading payloads and uploading victim system information.[19]
