Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

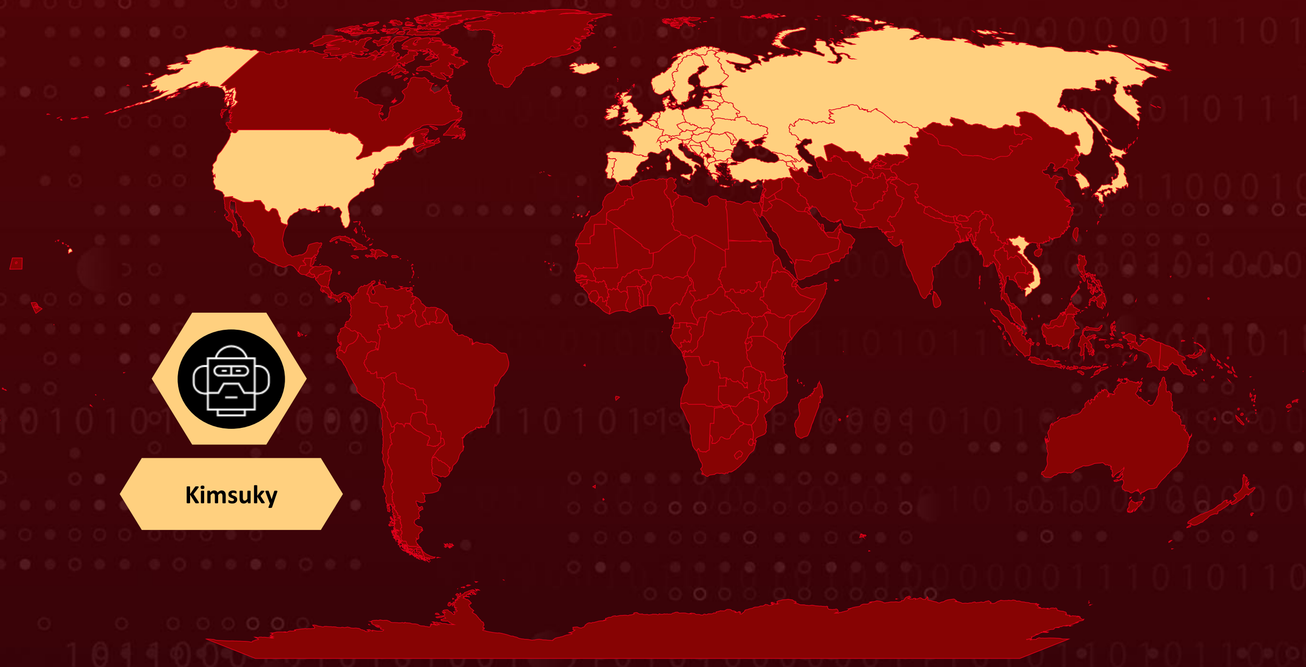
Kimsuky Expands RDP Wrapper & Proxy Malware in Spear-Phishing Attacks

Date of Publication	Admiralty Code	TA Number
February 9, 2025	A1	TA2025035

Summary

Active Since: 2024
Malware: PebbleDash
Targeted Countries: South Korea, United States, Japan, Russia, Vietnam and European nations
Threat Actor: Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394, Sparkling Pisces, Springtail)
Attack: The Kimsuky group continues spear-phishing attacks using malicious LNK files to install PebbleDash and a custom RDP Wrapper for remote control. They also deploy proxy malware, keyloggers, and credential stealers, refining techniques to evade detection. New loaders and injectors enhance stealth, leveraging ReflectiveLoader PowerShell scripts for in-memory execution. Their evolving tactics emphasize remote access over traditional backdoors, targeting South Korean users.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

The Kimsuky group, a North Korean state-sponsored advanced persistent threat (APT) actor, has been active since 2013. Initially, their operations focused on South Korea, targeting entities such as North Korea-related research institutes and energy corporations. Over time, their activities expanded to include countries such as the United States, Japan, Russia, Vietnam, and various European nations.

#2

Recently, the Kimsuky threat group has continued to employ spear-phishing attacks to distribute malware, using malicious shortcut files (.LNK) disguised as documents (PDF, Excel, Word). Once executed, these files launch PowerShell or Mshta commands to download and install PebbleDash (a backdoor) and a custom-built RDP Wrapper for remote system control. While these tools have been used in past attacks, recent modifications suggest efforts to evade detection rather than a significant shift in tactics.

#3

To facilitate remote access, Kimsuky has deployed proxy malware that enables communication between the infected system and external networks. Different variants of these tools have been identified, including ones using mutex names like "MYLPROJECT" and "LPROXYMUTEX", as well as a Go-based revsocks tool found on GitHub. These proxies help the attackers bypass network restrictions and maintain persistence on compromised systems.

#4

Kimsuky also utilizes keyloggers and browser credential theft tools. Their keyloggers, deployed via PowerShell scripts and executables, now store captured keystrokes in different file locations (joeLog.txt, jLog.txt) to avoid detection. Meanwhile, the group has refined its infostealer malware, now extracting encryption keys from Chromium-based browsers rather than stealing stored credentials directly. This method likely helps bypass security defenses and exfiltrate login data more stealthily.

#5

Additionally, Loader and Injector malware have been identified, responsible for loading payloads into memory and injecting malicious code into legitimate processes. Notably, Kimsuky has leveraged an obfuscated ReflectiveLoader script (Invoke-ReflectivePEInjection.ps1) to execute payloads in memory, further complicating detection. These techniques highlight the group’s ongoing refinement of stealth and persistence mechanisms.

Recommendations

Strengthen Email Security: Implement email filtering solutions to detect and block spear-phishing emails containing malicious LNK attachments. Educate employees and users on how to identify phishing attempts, particularly emails impersonating trusted contacts or organizations. Enforce policies requiring email authentication standards such as DMARC, DKIM, and SPF to prevent email spoofing.

Restrict Execution of Malicious Scripts & Files: Disable execution of LNK files from external sources by adjusting Group Policy settings. Block execution of PowerShell, Mshta, and other scripting languages unless explicitly required. Implement application whitelisting to prevent unauthorized executables and scripts from running.

Enhance Endpoint & Network Security: Deploy endpoint detection and response (EDR) solutions to detect PebbleDash, RDP Wrapper, and other malware used in Kimsuky's campaigns. Regularly monitor network traffic for unusual outbound connections, particularly those related to proxy malware and revsocks. Use behavioral-based threat detection to identify unauthorized RDP access attempts.

Secure Remote Access: Disable Remote Desktop Protocol (RDP) unless explicitly necessary. If required, enforce Multi-factor authentication (MFA) for all remote access. Network segmentation to isolate critical systems from internet-exposed RDP instances. Strict firewall rules to allow RDP connections only from trusted IP addresses. Regularly audit RDP Wrapper and other remote access tools to ensure they are not installed without authorization.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0004 Privilege Escalation	TA0001 Initial Access	TA0002 Execution
TA0005 Defense Evasion	TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link
T1218.005 Mshta	T1059.001 PowerShell	T1021 Remote Services	T1090 Proxy

T1056.001 Keylogging	T1056 Input Capture	T1217 Browser Information Discovery	T1548.002 Bypass User Account Control
T1548 Abuse Elevation Control Mechanism	T1055 Process Injection		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	04e5f813da28b5975d0b6445f687bc48, 26d96d40e4c8aed03d80740e1d5a4559, 2ea71ff410088bbe79f28e7588a6fb47, 3211ef223177310021e174c928f96bab, 5565b337bfba78970b73ae65b95f2c4f
IPv4	216[.]219[.]87[.]41, 74[.]50[.]94[.]175

References

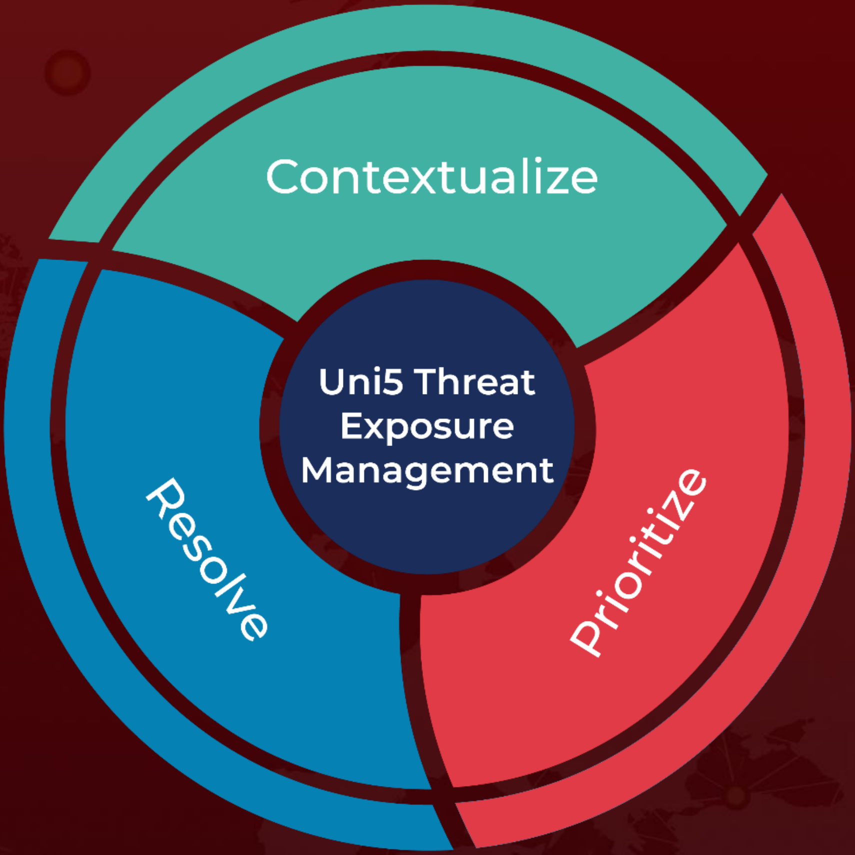
https://asec.ahnlab.com/en/86098/

http://hivepro.com/threat-advisory/kimsukys-evolving-phishing-playbook-url-tactics-and-global-deception/

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 9, 2025 • 9:30 PM

More at www.hivepro.com