Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Kimsuky's Stealthy RDP Espionage Campaign

Date of Publication

April 22, 2025

Admiralty Code

A1

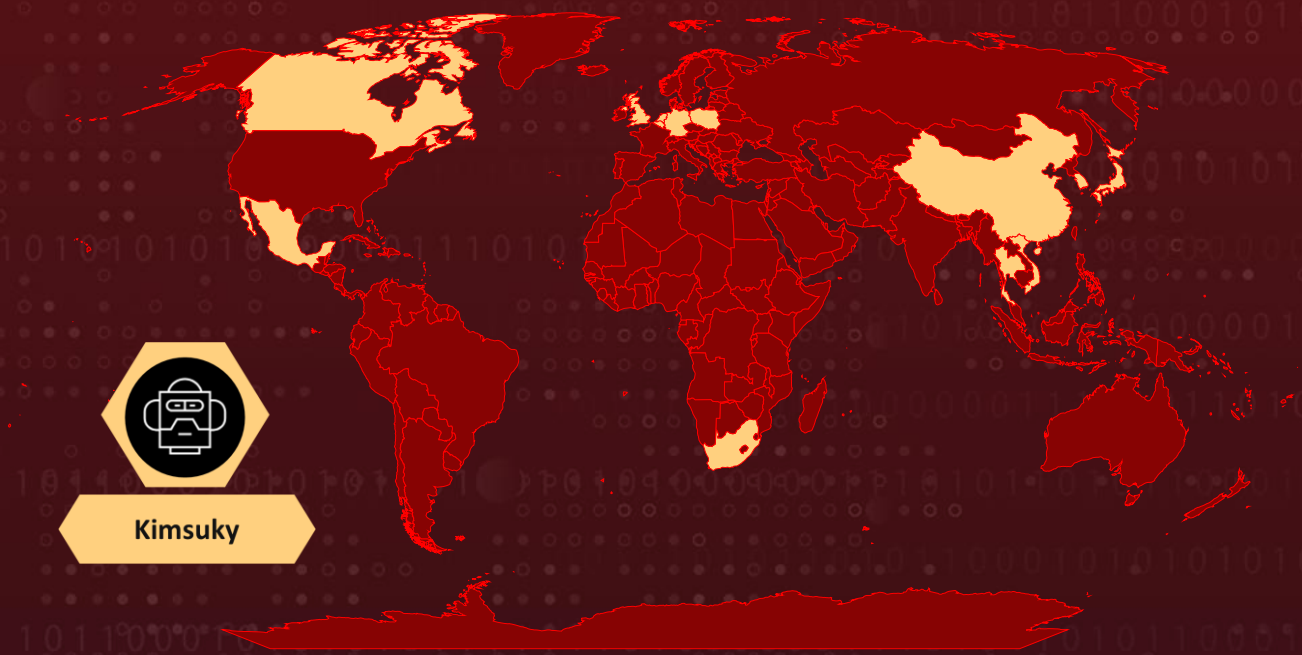
TA Number

TA2025122

Summary

Attack Discovered: September 2023
Targeted Countries: South Korea, Japan, United States, China, Germany, Singapore, South Africa, Netherlands, Mexico, Vietnam, Belgium, United Kingdom, Canada, Thailand, and Poland
Affected Industries: Software Companies, Energy, Finance
Actor: Kimsuky (aka Velvet Chollima, Larva-24005, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394, Sparkling Pisces, Springtail)
Malware: MySpy, RandomQuery, KimaLogger
Attack: A newly uncovered cyber espionage campaign by North Korea-linked Kimsuky (aka Larva-24005) has been active since at least October 2023, targeting South Korea's software, energy, and financial sectors, as well as global organizations. The group used spear-phishing emails and exploited vulnerabilities like CVE-2017-11882 and CVE-2019-0708 (BlueKeep) to gain access, leveraging tools such as RDPWrap for persistent remote control. Once inside, they moved laterally and deployed keyloggers like KimaLogger to steal credentials and exfiltrate sensitive data to attacker-controlled C2 servers.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2019-0708	BlueKeep (Microsoft Remote Desktop Services Remote Code Execution Vulnerability)	Windows: 10 - 11 23H2 Windows Server: 2019 – 2022 23H2	✗	✓	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓

Attack Details

#1 A newly uncovered cyber operation linked to North Korea's Kimsuky group (also tracked as Larva-24005) reveals a methodical and well-resourced espionage campaign that has been active since at least October 2023. This operation primarily targets South Korea's software, energy, and financial sectors but has also reached global entities in countries like Japan, China, Germany, the U.S., and more, using spear-phishing emails as the initial attack vector. These emails often contained malicious attachments or links designed to deliver malware or exploit vulnerability in Microsoft Office (CVE-2017-11882).

#2 In several instances, attackers appear to have attempted exploiting the BlueKeep RDP vulnerability (CVE-2019-0708) to gain initial access. Once inside, they deployed a dropper that installed RDPWrap, a tool that modifies Windows systems to allow multiple RDP sessions and unauthorized remote access.

#3 After establishing remote control, the attackers carried out lateral movement across compromised systems and deployed keyloggers such as KimaLogger and RandomQuery to monitor user activity and steal credentials. These keyloggers silently recorded sensitive input and communicated with command-and-control (C2) servers operated by the attackers.

#4 This attack chain shows how victims in multiple countries were targeted through phishing, followed by potential exploitation of RDP. After gaining a foothold, the attackers installed RDPWrap and used KimaLogger to keep a close watch on infected systems, allowing them to move across the network and quietly steal data over time. The keyloggers connected to Kimsuky's C2 servers to transmit stolen data, ultimately leading to data leaks.

#5 This campaign highlights Kimsuky's persistent efforts and evolving toolkit, combining both custom and off-the-shelf malware with known exploits and legitimate tools to achieve stealthy, long-term espionage.

Recommendations

Keep Systems Up-to-Date: Make sure to promptly apply patches for vulnerabilities like CVE-2017-11882 in Microsoft Office to prevent exploitation through malicious attachments. Likewise, address CVE-2019-0708 (BlueKeep) by patching RDP vulnerabilities as soon as updates are available. If RDP isn't essential for your operations, disable it altogether, or restrict access to trusted IP addresses to minimize exposure.

Detect and Secure RDP Access: To prevent unauthorized use of tools like RDPWrap, implement monitoring tools that can detect unusual changes to the Windows registry or abnormal RDP-related network traffic. It's also essential to tighten RDP configurations disable it where it's not needed, and if remote access is required, enforce strong multifactor authentication (MFA) for added security. For essential RDP access, ensure that it is only accessible through a secure VPN or trusted devices to further minimize exposure.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Ensure Network Segmentation: To prevent attackers from moving freely within your network, segment critical systems and isolate them from others. Ensure users can only access the resources necessary for their roles. In parallel, apply the principle of least privilege (PoLP) to limit user permissions, especially for administrative accounts.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0010 Exfiltration	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1059 Command and Scripting Interpreter	T1566 Phishing	T1566.001 Spearphishing Attachment	T1021 Remote Services
T1021.001 Remote Desktop Protocol	T1082 System Information Discovery	T1056 Input Capture	T1056.001 Keylogging
T1133 External Remote Services	T1190 Exploit Public-Facing Application	T1204 User Execution	T1560 Archive Collected Data
T1567 Exfiltration Over Web Service	T1595 Active Scanning	T1595.002 Vulnerability Scanning	T1039 Data from Network Shared Drive

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1177fecd07e3ad608c745c81225e4544, 14caab369a364f4dd5f58a7bbca34da6, 184a4f3f00ca40d10790270a20019bb4, 30bcac6815ba2375bef3daf22ff28698, 46cd19c3dac997bfa1a90028a28b5045, 279c86f3796d14d2a4d89049c2b3fa2d, 5bfeef520eb1e62ea2ef313bb979aeae, D404ab9c8722fc97cceb95f258a2e70d

TYPE	VALUE
URLs	hxxp[:]//star7[.]kro[.]kr/login/help/show[.]php?_Dom=991, hxxp[:]//star7[.]kro[.]kr/login/img/show[.]php?uDt=177, hxxp[:]//www[.]sign[.]in[.]mogovernts[.]kro[.]kr/rebin/include[.]php?_sys=7
Domains	access-apollo-page[.]r-e[.]kr, access-apollo-star7[.]kro[.]kr, access-mogovernts[.]kro[.]kr, apollo-page[.]r-e[.]kr, apollo-star7[.]kro[.]kr

Patch Links

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

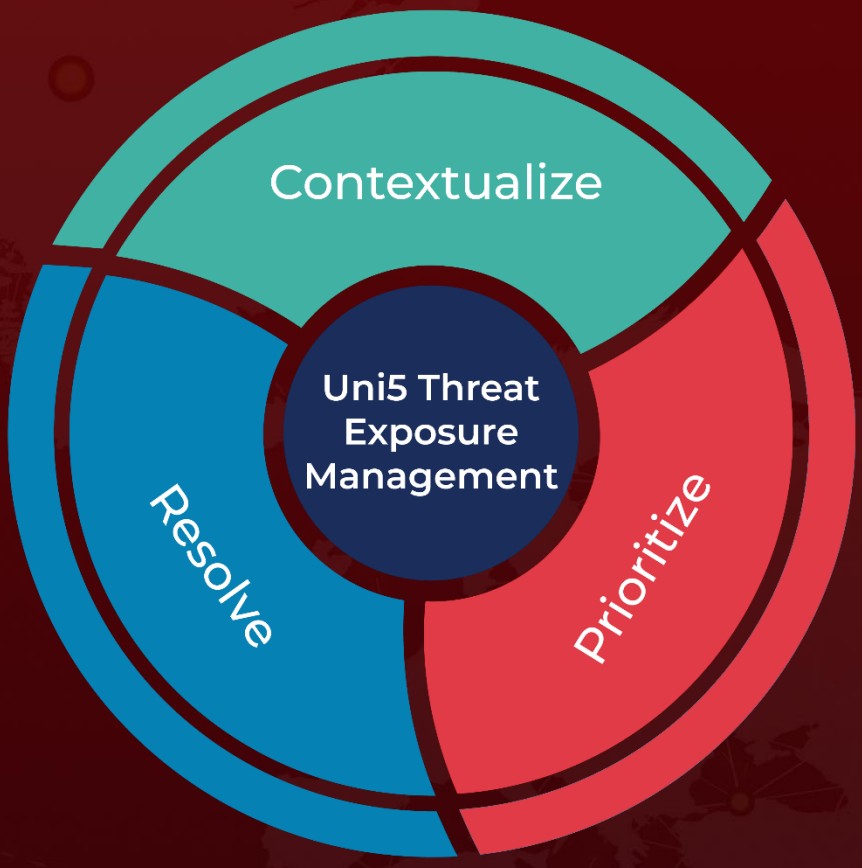
References

https://asec.ahnlab.com/en/87554/

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

April 22, 2025 • 5:20 AM

More at www.hivepro.com