Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

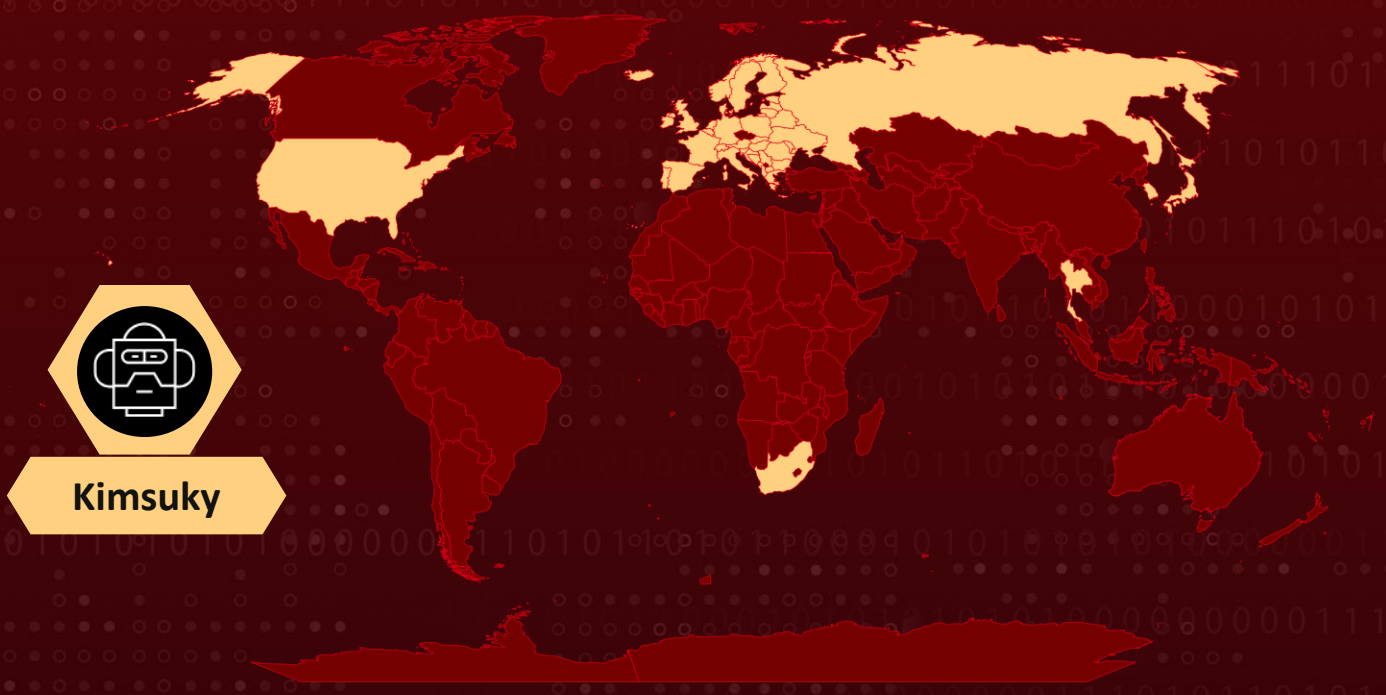
Kimsuky Unveils New Addition to Its Malware Arsenal

Date of Publication	Admiralty code	TA Number
October 18, 2023	A1	TA2023423

Summary

First Appearance: Late 2012
Actor Name: Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)
Target Industries: Defense, Diplomatic, Education, Media industries, Energy, Government, Healthcare, Manufacturing, Think Tanks
Target Region: France, Japan, Russia, South Africa, South Korea, United Kingdom, United States, Thailand, Europe
Malware: xRAT, BabyShark, RevClient, TinyNuke

Actor Map



Actor Details

#1 Kimsuky is a cyber-espionage group believed to be operating out of North Korea. They have been active since late 2012, earlier their targets were the North Korea-related research institutes in South Korea. However, over the years, the group's operations expanded to target other countries and organizations.

#2 Kimsuky typically conducts spear-phishing attacks aimed at various sectors, including national defense, diplomatic, and academic institutions, as well as defense and media industries and national organizations. Their primary objective in these attacks is to exfiltrate internal information, proprietary technology, and sensitive data from their targeted victims.

#3 After gaining initial access to a target system, Kimsuky usually follows a pattern of establishing backdoors and deploying Infostealers to maintain control over the compromised systems and exfiltrate sensitive information. To execute these operations, the group employs various tools and malware, which can include open-source malware such as xRAT (Quasar RAT) or custom-developed malware.

#4 Kimsuky is known for its adaptability in using various types of malware and tools to enable remote control during their campaigns. One of the common methods employed by the group for remote control is the Remote Desktop Protocol (RDP). In some instances, the attackers have utilized other remote desktop solutions and tools/malwares, such as TinyNuke, TightVNC, and Chrome Remote Desktop, to conduct their operations.

#5 The recent activities of the Kimsuky group have revealed deployment of BabyShark malware through presumed spear phishing attacks, followed using various malware strains related to the RDP. One of the newly identified malware components used in these attacks is "RevClient," which appears to have been created or modified specifically for these campaigns. RevClient functions by receiving commands from the threat actor via a Command and Control (C&C) server. Depending on the commands it receives, RevClient can execute various actions, such as creating user accounts or enabling port forwarding.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Kimsuky	North Korea **MOTIVE** Information theft and espionage	France, Japan, Russia, South Africa, South Korea, United Kingdom, United States, Thailand, Europe	Defense, Diplomatic, Education, Media industries, Energy, Government, Healthcare, Manufacturing, Think Tanks

Recommendations

- **Limit Access:** Restrict RDP access to only those users who need it. This minimizes the attack surface. Consider using a VPN to allow remote access to your network first, and then use RDP.
- **Monitor and Log RDP Access:** Set up comprehensive logging for RDP access and regularly review logs for suspicious activity.
- **Email Security:** Implement robust email filtering to counteract spam, phishing, and malicious attachments, and exercise caution with unverified links and email attachments by validating their authenticity before opening.
- **Remain vigilant:** It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.
- **Robust Endpoint Security:** Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0011** Command and Control	**TA0010** Exfiltration
TA0005 Defense Evasion	**TA0008** Lateral Movement	**TA0007** Discovery	**TA0009** Collection
T1047 Windows Management Instrumentation	**T1055** Process Injection	**T1087** Account Discovery	**T1140** Deobfuscate/Decode Files or Information
T1016 System Network Configuration Discovery	**T1497** Virtualization/Sandbox Evasion	**T1566** Phishing	**T1566.001** Spearphishing Attachment
T1021 Remote Services	**T1056** Input Capture	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1059.003 Windows Command Shell	**T1059.005** Visual Basic	**T1204** User Execution	**T1204.002** Malicious File
T1204.001 Malicious Link	**T1105** Ingress Tool Transfer	**T1104** Multi-Stage Channels	**T1041** Exfiltration Over C2 Channel

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	Ad9a3e893abdac7549a7d66ca32142e8, 116a71365b83cc38211ccfc8059b363e, C8d589ac5c872b12e502ec1fc2fee0c7, 0d6717c3fa713c5f5f5cb0539b94b84f, 0d691673af913dc0942e55548f6e2e4e, 2dbe8e89310b42e295bfdf3aad955ba9, 7313dc4d9d6228e442fc6ef9ba5a1b9a, Be2f73a637258aa872bdf548daf55336, 02804d632675b2a3711e19ef217a2877

TYPE	VALUE
URLs	hxxps://onessearth[.]online/up/upload_dotm.php, hxxps://powsecme[.]co/up/upload_dotm.php
IP	5.61.59[.]53:2086

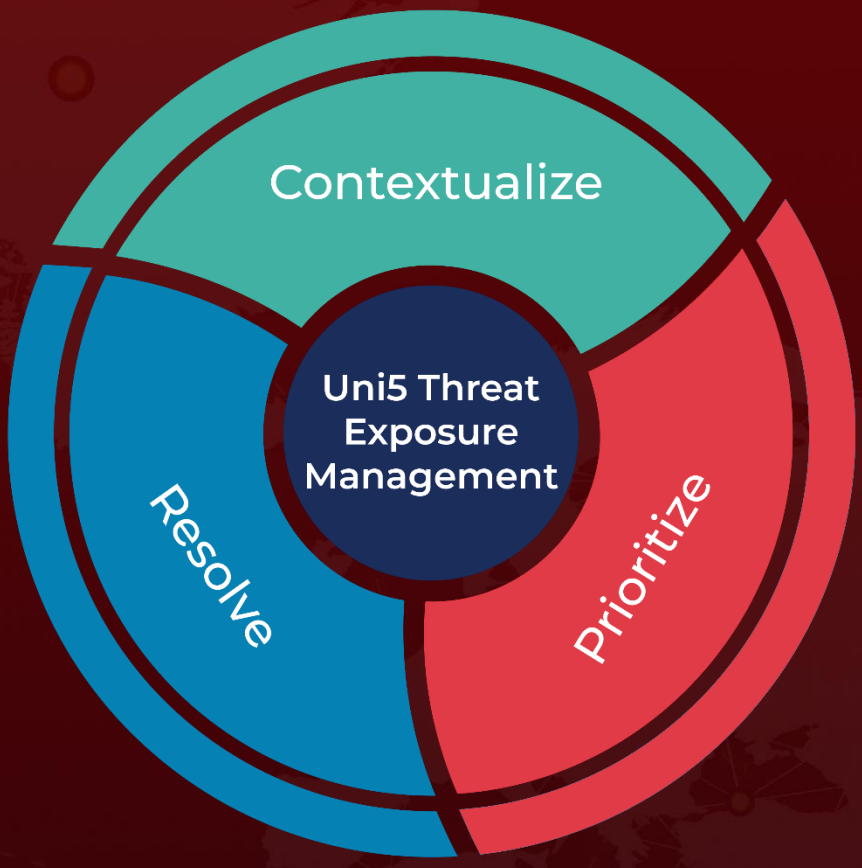
References

https://asec.ahnlab.com/en/57873/

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

October 18, 2023 . 9:10 AM

More at www.hivepro.com