Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

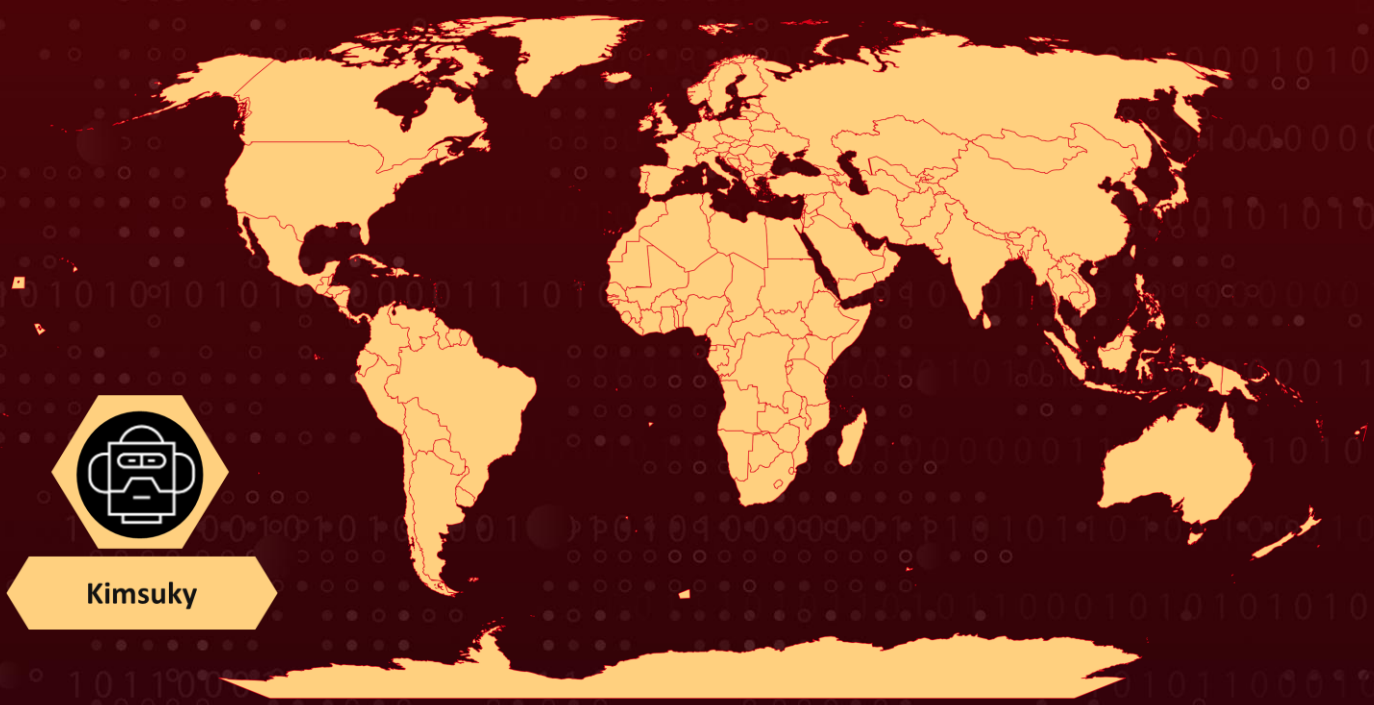
Kimsuky Group's Intriguing Exploits with AppleSeed Malware

Date of Publication	Admiralty Code	TA Number
December 29, 2023	A1	TA2023526

Summary

First Identified: 2021
Attack Region: Worldwide
Actor: Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)
Malware: AppleSeed, AlphaSeed, Meterpreter, TinyNuke, TightVNC
Attack: The Kimsuky group has been actively utilizing weaponized LNK files to deploy the AppleSeed malware. While the group typically relies on spear-phishing attacks for initial access, their recent campaigns have prominently featured the use of shortcut-type malware in LNK file format. AppleSeed variant named AlphaSeed has been identified in their recent activities, showcasing ongoing evolution in their tactics and malware variants.

Attack Regions



Attack Details

#1

The **Kimsuky** threat group, reportedly supported by North Korea, has been active since 2013. Traditionally employing spear-phishing attacks for initial access, the group focuses on stealing internal information and technology from targeted organizations. Notably, their recent attacks have predominantly featured the use of shortcut-type malware in LNK file format, showcasing a shift in tactics and tools over time.

#2

AppleSeed is a backdoor designed to execute commands from a C&C server, providing the threat actor with control over the compromised system. It comes equipped with various features, including a downloader for additional malware, keylogging capabilities, the ability to capture screenshots, and data theft by collecting files from the user system. AppleSeed is commonly distributed through a JavaScript dropper, which installs it while opening document files like HWP and PDF. Notably, the AppleSeed DLL is designed to avoid performing malicious behaviors when running in a sandbox environment.

#3

AlphaSeed is a malware developed in Golang and bears resemblances to AppleSeed in terms of functionalities such as command execution and information theft. It employs ChromeDP for communication with the C&C server and utilizes cookie values for login purposes. AlphaSeed has been often distributed using a JavaScript dropper. The installation process mirrors that of AppleSeed, utilizing a binary in DLL format and executing via the Regsvr32 process. Notably, the threat actor may deploy both AlphaSeed and AppleSeed on the same targeted system.

#4

Metasploit is a widely utilized penetration testing framework by Kimsuky designed for assessing security vulnerabilities in networks and systems. It offers a range of tools, and one notable component is Meterpreter, a versatile backdoor that allows threat actors to take control of compromised systems. In AppleSeed attacks conducted by the Kimsuky group, Meterpreter is frequently employed.

#5

Kimsuky has also designed VNC malware to manipulate the compromised systems. TightVNC, an open-source utility, facilitates the independent use of the Reverse VNC feature. TinyNuke, a banking malware, incorporates functionalities like HVNC, reverse SOCKS4 proxy, and form grabbing. When distributing the malware, the group activates only the HVNC feature, employing "AVE_MARIA" for verification purposes. Notably, users should check email senders, avoid unknown files, and update software.

Recommendations

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.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
T1547 Boot or Logon Autostart Execution	T1056 Input Capture	T1036 Masquerading	T1543 Create or Modify System Process
T1071 Application Layer Protocol	T1102 Web Service	T1113 Screen Capture	T1059 Command and Scripting Interpreter
T1059.007 JavaScript	T1021 Remote Services	T1566 Phishing	T1566.002 Spearphishing Link

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	db5fc5cf50f8c1e19141eb238e57658c, 6a968fd1608bca7255c329a0701dbf58, cafc26b215550521a12b38de38fa802b, 76831271eb117b77a57869c80bfd6ba6, b5d3e0c3c470d2d41967229e17259c87, 4511e57ae1eacdf1c2922bf1a94bfb8d, 02843206001cd952472abf5ae2b981b2, 8aeacd58d371f57774e63d217b6b6f98, cacf04cd560b70eaaf0e75f3da9a5e8f, 7a7937f8d4dcb335e96db05b2fb64a1b, f3a55d49562e41c7d339fb52457513ba, 5d3ab2baacf2ad986ed7542eeabf3dab, d4ad31f316dc4ca0e7170109174827cf, 1f7d2cbfc75d6eb2c4f2b8b7a3eec1bf, ae9593c0c80e55ff49c28e28bf8bc887, b6f17d59f38aba69d6da55ce36406729, 153383634ee35b7db6ab59cde68bf526, c560d3371a16ef17dd79412f6ea99d3a, 0cce02d2d835a996ad5dfc0406b44b01, d94c6323c3f77965451c0b7ebeb32e13, 52ff761212eeaadcd3a95a1f8cce4030, 4cb843f2a5b6ed7e806c69e6c25a1025, b6ab96dc4778c6704b6def5db448a020, 232046aff635f1a5d81e415ef64649b7, 58fafabd6ae8360c9d604cd314a27159, e582bd909800e87952eb1f206a279e47, ac99b5c1d66b5f0ddb4423c627ca8333, e34669d56a13d607da1f76618eb4b27e, ee76638004c68cfc34ff1fea2a7565a7
URLs	hxxp://bitburny.kro[.]kr/aha/, hxxp://bitthum.kro[.]kr/hu/, hxxp://doma2.o-r[.]kr//, hxxp://my.topton.r-e[.]kr/address/, hxxp://nobtwoseb1.n-e[.]kr//, hxxp://octseven1.p-e[.]kr//, hxxp://tehyeran1.r-e[.]kr//, hxxp://update.ahnlaib.kro[.]kr/aha/, hxxp://update.doumi.kro[.]kr/aha/, hxxp://update.onedrive.p-e[.]kr/aha/, hxxp://yes24.r-e[.]kr/aha/

TYPE	VALUE
IPv4:PORT	104.168.145[.]83:993, 159.100.6[.]137:993, 38.110.1[.]69:993, 107.148.71[.]88:993, 45.114.129[.]138:33890, 45.114.129[.]138:5500

References

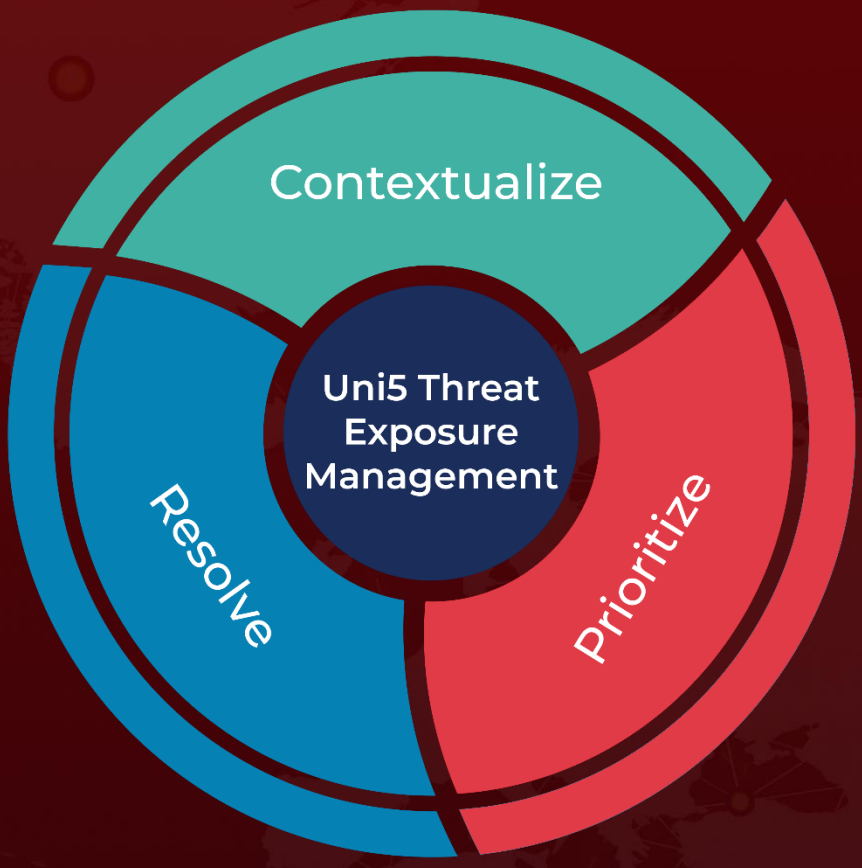
https://asec.ahnlab.com/en/60054/

https://www.hivepro.com/threat-advisory/kimsuky-unveils-new-addition-to-its-malware-arsenal/

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

December 29, 2023 . 3:50 AM

More at www.hivepro.com