Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

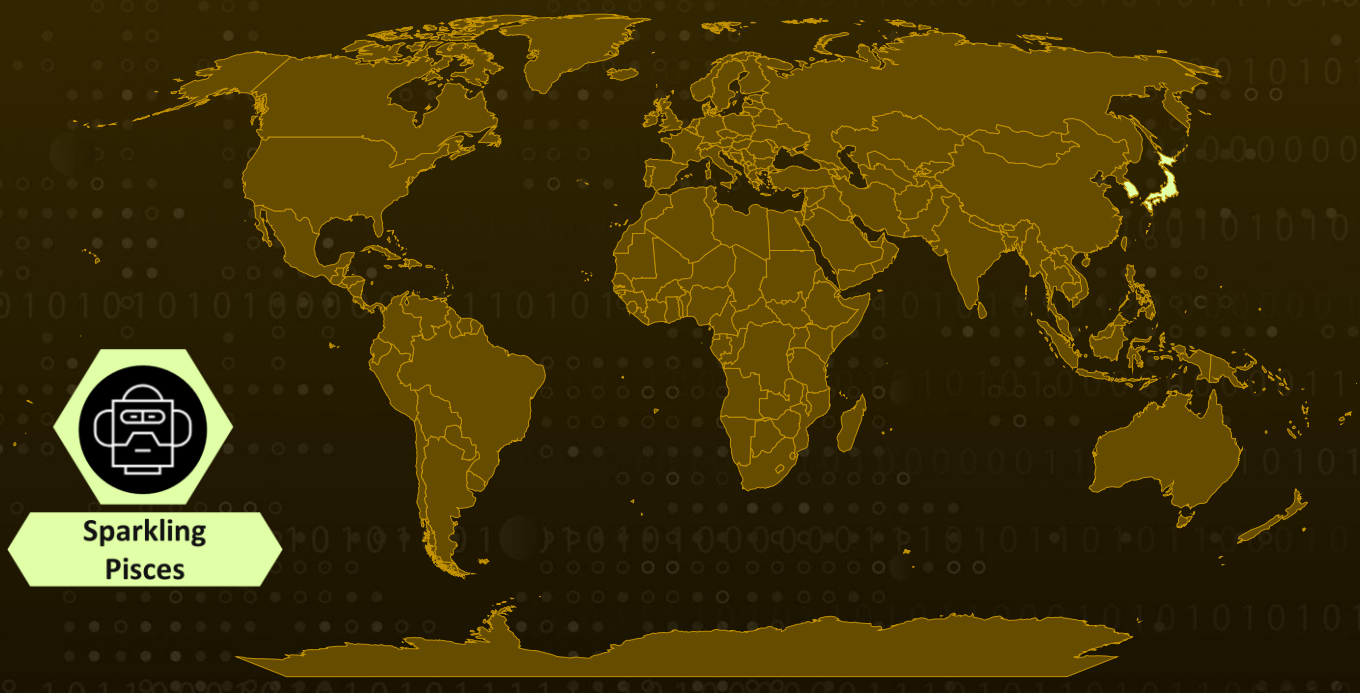
Sparkling Pisces's Latest Tools Unveiled: KLogEXE and FPSpy Enhance Espionage Efforts

Date of Publication	Admiralty Code	TA Number
September 27, 2024	A1	TA2024375

Summary

Attack Discovered: 2024
Targeted Countries: South Korea and Japan
Malware: KLogEXE and FPSpy
Actor: Sparkling Pisces (aka Kimsuky, Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394)
Attack: The North Korean-linked Sparkling Pisces (aka Kimsuky) has been deploying two new malware strains, KLogEXE and FPSpy, as part of their expanding cyber espionage operations. These new tools enhance the group's already extensive arsenal and highlight Sparkling Pisces's evolving tactics and growing technical sophistication. The deployment of KLogEXE and FPSpy demonstrates Sparkling Pisces's relentless focus on intelligence gathering, underscoring their increasing capabilities to target sensitive information and conduct advanced cyber operations.

Attack Regions



Attack Details

#1 The Sparkling Pisces (aka **Kimsuky**), is utilizing newly discovered malware variants, KLogExe and FPSpy, to enhance their sophisticated cyber operations. This group is infamous for conducting targeted spear phishing campaigns designed to trick unsuspecting victims into downloading and executing malicious software. In their previous activities, they have employed a PowerShell keylogger as part of their C2 infrastructure, which communicates with a domain that resolves to a known IP address. Additionally, a Portable Executable (PE) named powershell.exe has been found communicating with another domain tied to the same IP, using an obscure URI pattern. This campaign highlights the interplay between Sparkling Pisces' PowerShell malware and their newly identified PE malware, KLogEXE and FPSpy, which share infrastructure linked by the same registrant email.

#2 The first of these new malware, KLogEXE, is a C++ keylogger that collects data from compromised machines, including running applications, keystrokes, and mouse clicks. It stores this data in a hidden `.ini` file before exfiltrating it to a C2 server when the file reaches a certain size. The second malware, FPSpy is a variant of KGHSpy, an espionage backdoor that has gone largely unnoticed since its discovery in 2020. FPSpy includes more advanced functionalities, such as multithreading, executing arbitrary commands, and downloading additional encrypted modules. It employs stealth techniques like timestomping to hide its true compilation date.

#3 Both KLogEXE and FPSpy share a codebase, utilizing HackingTeam's leaked code for dynamic API calls, and both rely on `.ini` files for storing exfiltrated data. These overlaps indicate a deep connection between the malware, further highlighting Sparkling Pisces' sophisticated and evolving arsenal. The group's tactics and infrastructure showcase their growing capabilities, with most of their operations targeting South Korea and Japan, consistent with past campaigns attributed to Sparkling Pisces.

#4 This discovery sheds light on Sparkling Pisces' evolving toolkit, with KLogEXE focusing on keylogging and data exfiltration, while FPSpy offers a broader range of espionage functionalities. Their infrastructure and malware show continuous refinement, further solidifying Sparkling Pisces's reputation as a highly adaptable and persistent cyberespionage group.

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.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1070 Indicator Removal	T1070.006 Timestomp
T1041 Exfiltration Over C2 Channel	T1056 Input Capture	T1056.001 Keylogging	T1105 Ingress Tool Transfer
T1048 Exfiltration Over Alternative Protocol	T1082 System Information Discovery	T1083 File and Directory Discovery	T1074 Data Staged
T1057 Process Discovery	T1027 Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	990b7eec4e0d9a22ec0b5c82df535cf1666d9021f2e417b49dc5110a67228e27, a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb22162895641dda0dc2, faf666019333f4515f241c1d3fcfc25c67532463245e358b90f9e498fe4f6801, c69cd6a9a09405ae5a60acba2f9770c722afde952bd5a227a72393501b4f5343, 2e768cee1c89ad5fc89be9df5061110d2a4953b336309014e0593eb65c75e715
Domains	mail[.]apollo-page[.]r-e[.]kr, nidlogin[.]apollo[.]r-e[.]kr, bitjoker2024[.]000webhostapp[.]com, www[.]vic[.]apollo-star7[.]kro[.]kr
IPv4	152[.]32[.]138[.]167
URLs	hxxp[:]//mail[.]apollo-page[.]r-e[.]kr/wp-content/include[.]php?_sys_=7, hxxp[:]//mail[.]apollo-page[.]r-e[.]kr/plugin/include[.]php?_sys_=7, hxxps[:]//nidlogin[.]apollo[.]r-e[.]kr/cmd/index[.]php?_idx_=7

References

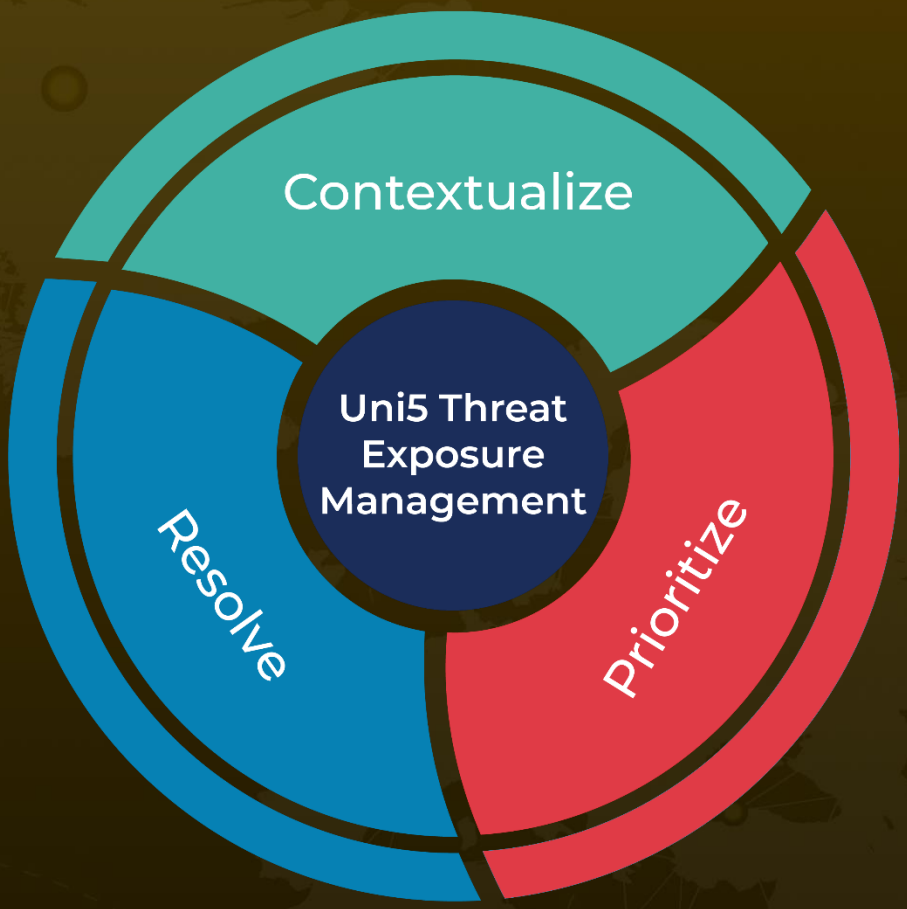
https://unit42.paloaltonetworks.com/kimsuky-new-keylogger-backdoor-variant/

https://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

September 27, 2024 • 7:30 AM

More at www.hivepro.com