Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

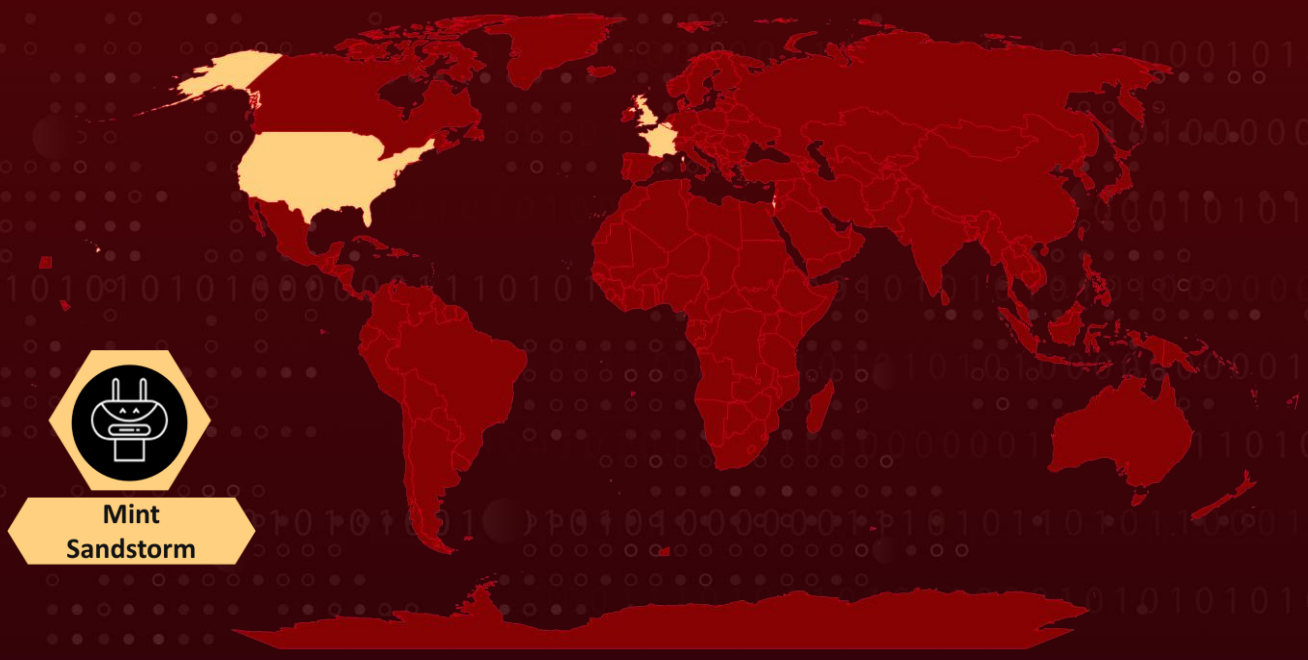
Mint Sandstorm's Campaign Targets Researchers with Novel Backdoor

Date of Publication	Admiralty Code	TA Number
January 18, 2024	A1	TA2024021

Summary

Attack Discovered: November 2023
Attack Region: Belgium, France, Gaza, Israel, the United Kingdom, and the United States
Targeted Industries: High-profile Individuals of research organizations and universities
Actor: Mint Sandstorm (aka Charming Kitten, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Ballistic Bobcat)
Malware: MediaPl backdoor, MischiefTut
Attack: Mint Sandstorm, a threat actor, focuses on high-profile individuals involved in Middle Eastern affairs at universities and research organizations. The group utilizes phishing lures in a campaign to socially engineer targets, enticing them to download malicious files that deploy new backdoor malware.

Attack Regions



Attack Details

#1 Since November 2023, Mint Sandstorm (aka Charming Kitten), has been actively targeting high-profile individuals focused on Middle Eastern affairs at universities and research organizations. This campaign involves the use of tailored phishing lures designed to targets into downloading malicious files. Notably, Mint Sandstorm has introduced new, custom backdoors as part of its tactics.

#2 In the campaign Mint Sandstorm impersonated as high-profile individuals, including journalists, using the pretext of document or article reviews. Upon the targets' expression of interest, Mint Sandstorm extended its campaign by sending subsequent follow-up emails. These emails included malicious links having RAR archive files. Upon download and decompression, a double extension file (.pdf.lnk) was created. Executing this file triggers a curl command, fetching additional payloads from attacker-controlled subdomains.

#3 After the execution of the files, various components, such as .vbs scripts and a renamed version of NirCmd, were downloaded to the targeted devices. To establish persistence in the targeted environments, the threat actor employed a malicious file named "Persistence.vbs" and added a registry entry. Additionally, in certain instances, they created a task to download a .txt file, logging the activity of the target device.

#4 Mint Sandstorm, in certain instances, deployed custom backdoors such as MischiefTut or MediaPl. MediaPl utilizes encrypted communication channels to exchange information with its C2 server and is designed to camouflage itself as Windows Media Player, aiming to evade detection. It employs AES CBC encryption and Base64 encoding in its communication. The variant found on compromised devices comes with features like auto-termination, temporary halting, retrying C2 communications, and executing C2 commands using the _popen function.

#5 A second PowerShell-based backdoor malware known as MischiefTut. This backdoor facilitates the delivery of additional malicious tools and offers reconnaissance capabilities. It enables threat actors to execute commands on compromised systems and send the results to servers controlled by the attackers. Mint Sandstorm's ability to gain remote access to a target's system raises security concerns and can lead to legal issues.

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	TA0005 Defense Evasion
TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.005 Visual Basic	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1036 Masquerading	T1573 Encrypted Channel	T1053 Scheduled Task/Job	T1204 User Execution
T1204.002 Malicious File	T1132 Data Encoding	T1132.001 Standard Encoding	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	east-healthy-dress[.]glitch[.]me, coral-polydactyl-dragonfruit[.]glitch[.]me, kwhfibejjyxregxmnpcs[.]supabase[.]co, epibvgvoszemkwjnplyc[.]supabase[.]co, ndrrftqrlblfecpupppp[.]supabase[.]co, cloud-document-edit[.]onrender[.]com
SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f

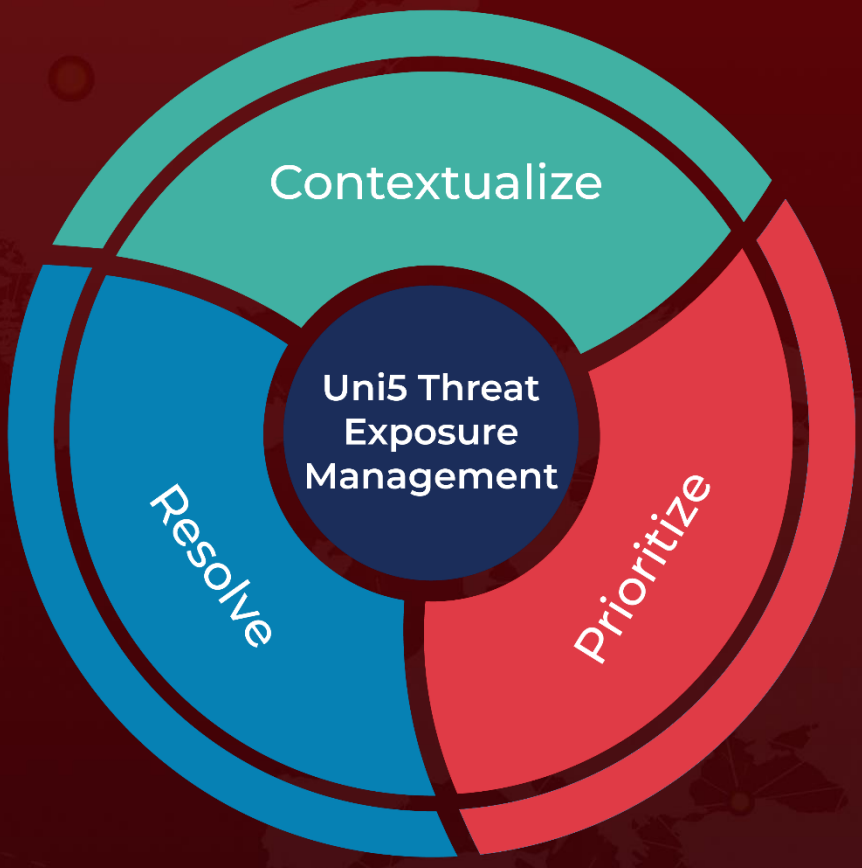
References

https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/

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

January 18, 2024 . 4:30 AM

More at www.hivepro.com