Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

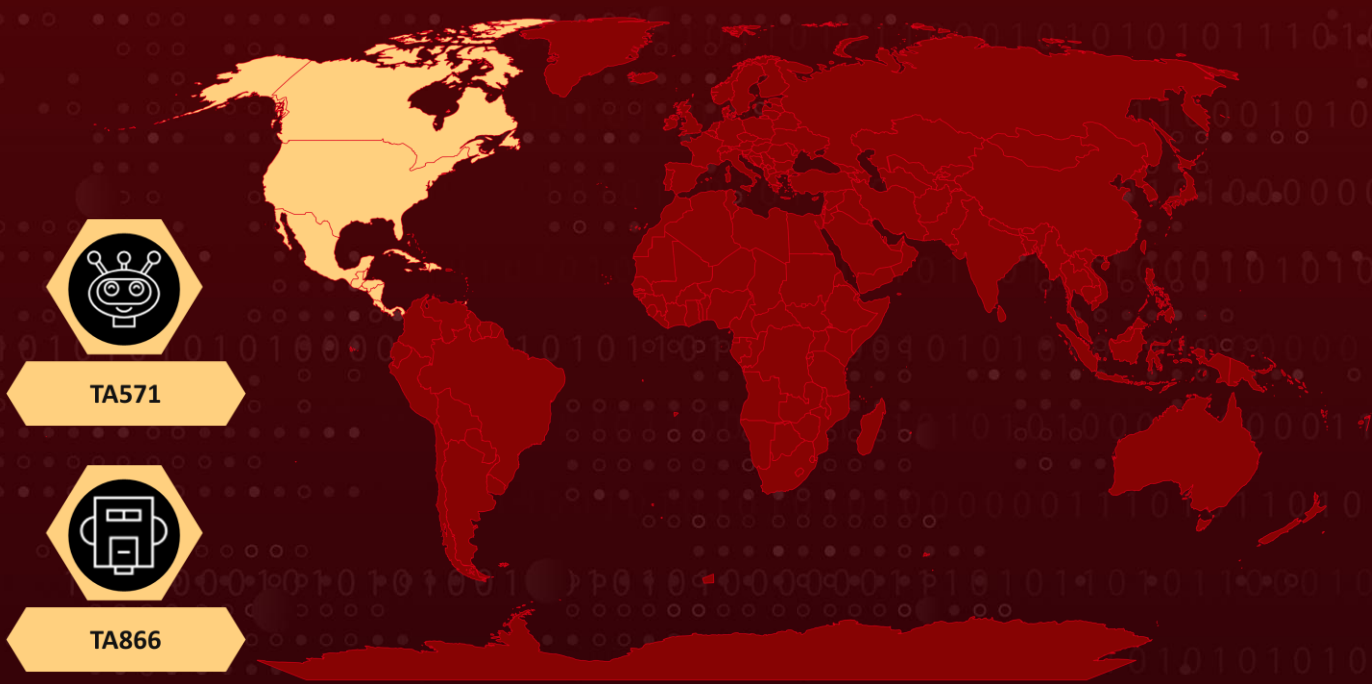
TA866 Makes a Comeback with Extensive Email Campaign

Date of Publication	Admiralty Code	TA Number
January 22, 2024	A1	TA2024025

Summary

Attack Discovered: January 2024
Attack Region: North America
Actor: TA866, TA571
Malware: WasabiSeed and Screenshotter
Attack: The threat actor identified as TA866 has returned after a hiatus of nine months, launching a new extensive phishing campaign aimed at distributing well-known malware families like WasabiSeed and Screenshotter.

Attack Regions



Attack Details

#1 TA866 has made a comeback in the email threat campaign landscape after a nine-month hiatus. In this resurgence, a significant volume of emails, numbering in the thousands, targeted North America. These emails, with an invoice theme, included attached PDFs. The PDFs harbored OneDrive URLs, which, when clicked, set off a multi-step infection chain, ultimately resulting in the deployment of a variant of the WasabiSeed and Screenshotter custom toolset.

#2 Following a user's click on a PDF URL, a JavaScript file hosted on OneDrive was served. The JavaScript proceeded to download and execute an MSI file, within which an embedded WasabiSeed VBS script was executed. Subsequently, the script initiated the download and execution of a second MSI file, which continually polled for additional payloads in a loop. The second MSI file housed components of the Screenshotter screenshot utility, capturing desktop screenshots and transmitting them to the C2 server.

#3 TA866 first came to light in February 2023 during the Screentime campaign. This initiative involved the distribution of WasabiSeed, a Visual Basic script dropper utilized for downloading Screenshotter. Screenshotter has the capability to capture desktop screenshots at predetermined intervals and send the gathered data to a domain controlled by the threat actor.

#4 The recent campaign comprises two distinct threat actors: TA571, functioning as a spam distributor, and TA866, a recognized threat actor known for utilizing post-exploitation tools. TA571 focuses on delivering malware through high-volume spam emails, while TA866 engages in activities related to crimeware and cyberespionage. Both actors demonstrate organization and the ability to execute well-planned attacks at scale, facilitated by their deployment of custom tools and connections to procure resources from other actors.

#5 There is evidence to suggest that the actor TA866 may be financially motivated. This is indicated by the use of Screenshotter as a reconnaissance tool to identify high-value targets for post-exploitation. Additionally, the actor deploys an AutoHotKey (AHK)-based bot to ultimately deliver the Rhadamanthys information stealer, further emphasizing potential financial motives.

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.

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

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	**TA0005** Defense Evasion	**TA0009** Collection
TA0010 Exfiltration	**TA0011** Command and Control	**T1105** Ingress Tool Transfer	**T1113** Screen Capture
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1566.002** Spearphishing Link	**T1059** Command and Scripting Interpreter
T1059.007 JavaScript	**T1059.005** Visual Basic	**T1204** User Execution	**T1204.001** Malicious Link
T1218 System Binary Proxy Execution	**T1218.007** Msiexec		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	bdb0b6f52b51d989c489c3605a1534c9603ffb7a373654f62fd6f3e3599341fb, 8277dff37fb068c3590390ca1aa6b96fd8b4f93757d5070f68ee8894e37713b1, c9329007524b3da130c8635a226c8cbe3a4e803b813f5b2237ed976feb9d2c8d, 19938b8918b09852ee8d27a7cc2991ba2eb110f27ce25e70fffde932a74e6a6d, 8b35b21b52780d39ea7832cb918533be7de5b6682cbeffe37797ba92a92aa368, 6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc, aec5bf19e72ed577b0a02cffeb4f5cc713ab4478267ce348cf337b508f2fcade
URLs	hxxps[:]//onedrive.live[.]com/download?resid=720FBFD017217E31%21118&authkey=!ACD7ldpnneZUBtc&a=[4 or more random letters], hxxp[:]//37[.]1.212.198//md.msi, hxxp[:]//193[.]233.133.179/[C: Drive Serial Number], hxxp[:]//193[.]233.133.179:80/screenshot/[C: Drive Serial Number]

References

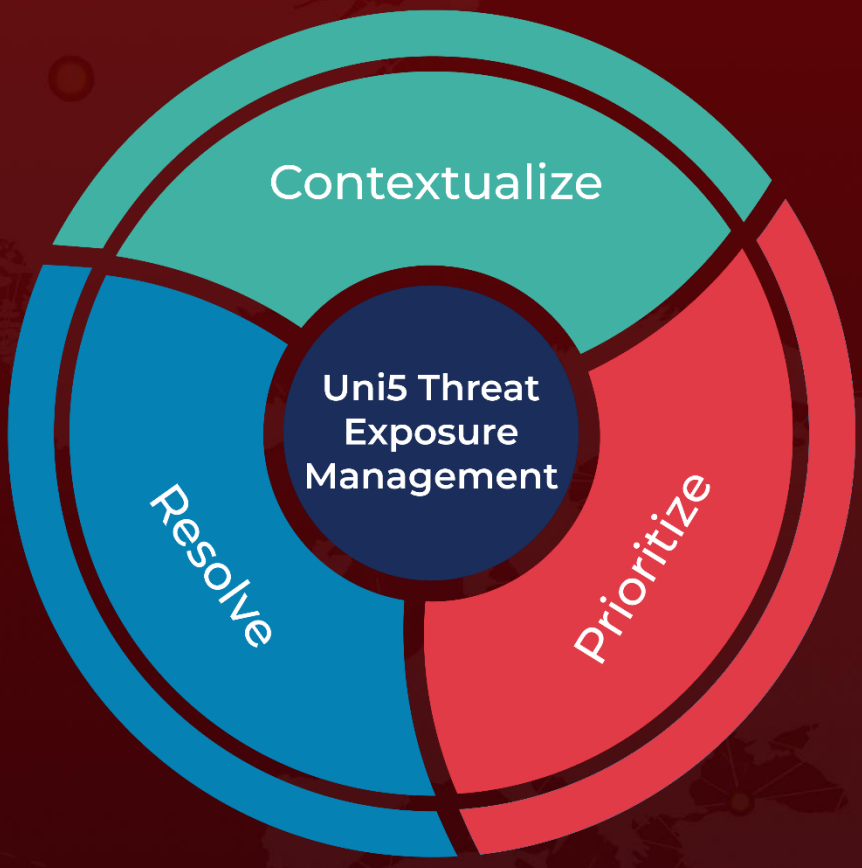
https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta866-returns-large-email-campaign

https://www.hivepro.com/threat-advisory/ta866-new-financially-motivated-threat-actor-targeting-us-and-germany-organizations/

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 22, 2024 . 3:50 AM

More at www.hivepro.com