Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

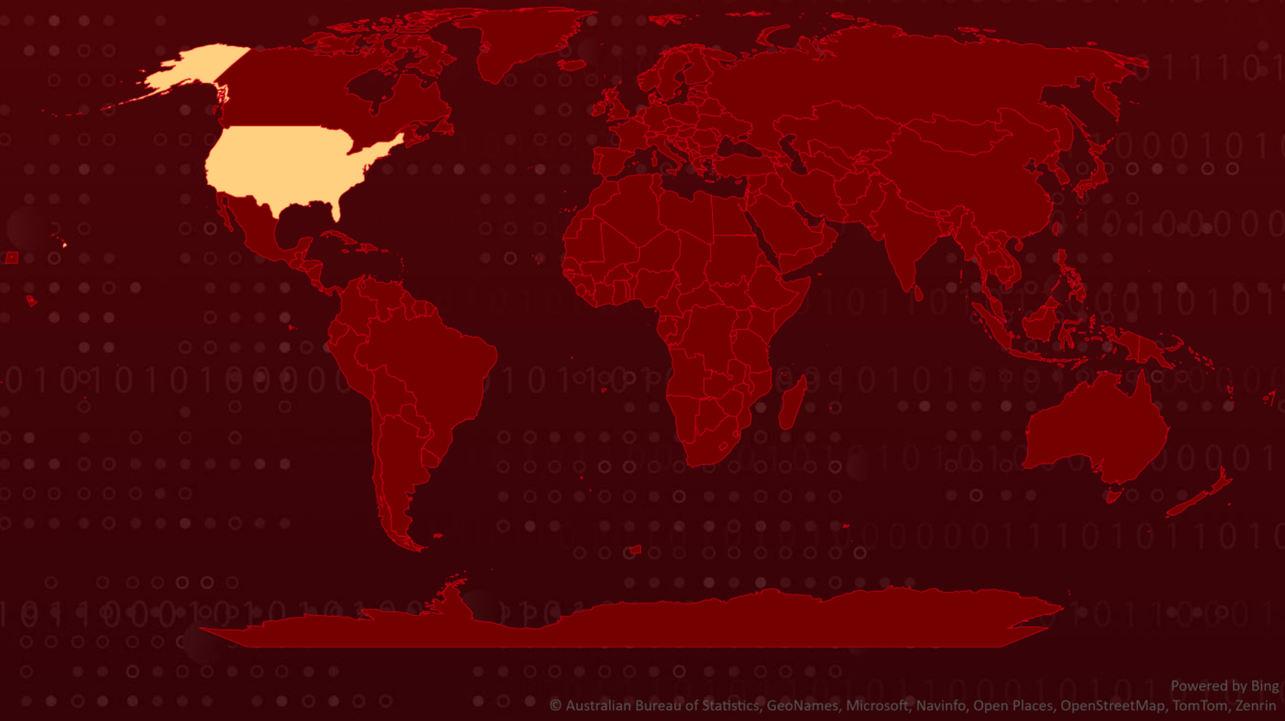
Operation PhantomBlu Deploys NetSupport RAT via OLE Template

Date of Publication	Admiralty Code	TA Number
March 20, 2024	A1	TA2024109

Summary

Attack Discovered: March 2024
Attack Region: US
Malware: NetSupport RAT
Attack: Under the guise of Operation PhantomBlu, a new phishing campaign is aimed at American companies with the goal of deploying the remote access trojan NetSupport RAT. By utilising OLE template manipulation, the PhantomBlu operation presents a sophisticated exploitation technique. This technique uses Microsoft Office document templates to run malicious code covertly and avoid detection.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 The PhantomBlu campaign, targeting organizations in the United States, particularly in the distribution of the NetSupport RAT. Unlike typical delivery methods, PhantomBlu campaign employs an innovative technique known as OLE template modification, leveraging Microsoft Office document templates to execute malicious code discreetly. This approach hides the harmful payload outside the document, activating it only upon user interaction, which helps evade detection.

#2 The phishing campaign begins with emails sent to US-based employees, supposedly from an accounting service, offering a monthly salary report in a password-protected Office Word file (.doc). Recipients are instructed to enable editing and interact with an embedded printer image within the document to view their salary graph. By using legitimate email delivery platforms like "SendInBlue" or Brevo, the attackers aim to disguise their malicious intent.

#3 Once the user clicks the printer icon in the document, an LNK file included in a zip package opens up. LNK file is a PowerShell dropper that had been designed to obtain and run a script from a given URL. This script, further downloads the payload including a RAT executable and registry settings to achieves persistence. To hide its true purpose, the PowerShell script is obfuscated. It creates a secondary ZIP file, unpacks it, and launches the NetSupport RAT. By creating a new registry key, this procedure guarantees the malware's persistence and AutoStart.

#4 The PhantomBlu campaign deviates from standard approaches by distributing the RAT via OLE template and Template Injection, using encrypted .doc files. This fusion of social engineering techniques and sophisticated evasion methods underscores the complexity of phishing schemes, highlighting how they can circumvent traditional security measures that focus on executable files.

Recommendations

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.

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.

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.

Awareness: Conduct regular cybersecurity awareness training sessions to educate employees about the risks associated with spear-phishing and social engineering tactics. Emphasize the importance of carefully scrutinizing email attachments, especially those received from unfamiliar or suspicious sources.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1219 Remote Access Software	T1047 Windows Management Instrumentation
T1564 Hide Artifacts	T1564.003 Hidden Window	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1112 Modify Registry	T1406 Obfuscated Files or Information	T1406.002 Software Packing	T1049 System Network Connections Discovery

T1221 Template Injection	T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	16e6dfd67d5049ffedb8c55bee6ad80fc0283757bc60d4f12c56675b1da5bf61, 1abf56bc5fbf84805ed0fbf28e7f986c7bb2833972793252f3e358b13b638bb1, 95898c9abce738ca53e44290f4d4aa4e8486398de3163e3482f510633d50ee6c, d07323226c7be1a38ffd8716bc7d77bdb226b81fd6ccd493c55b2711014c0188, 94499196a62341b4f1cd10f3e1ba6003d0c4db66c1eb0d1b7e66b7eb4f2b67b6, 89f0c8f170fe9ea28b1056517160e92e2d7d4e8aa81f4ed696932230413a6ce1
Domains	yourownmart[.]com/solar[.]txt, firstieragency[.]com/depbrndksokkkdkxoqnazneifidmyyjdpji[.]txt, yourownmart[.]com, firstieragency[.]com, parabmasale[.]com, tapouttv28[.]com, Sendinblue[.]com, sender-sib[.]com
IP	192[.]236[.]192[.]48, 173[.]252[.]167[.]50, 199[.]188[.]205[.]15, 46[.]105[.]141[.]54

References

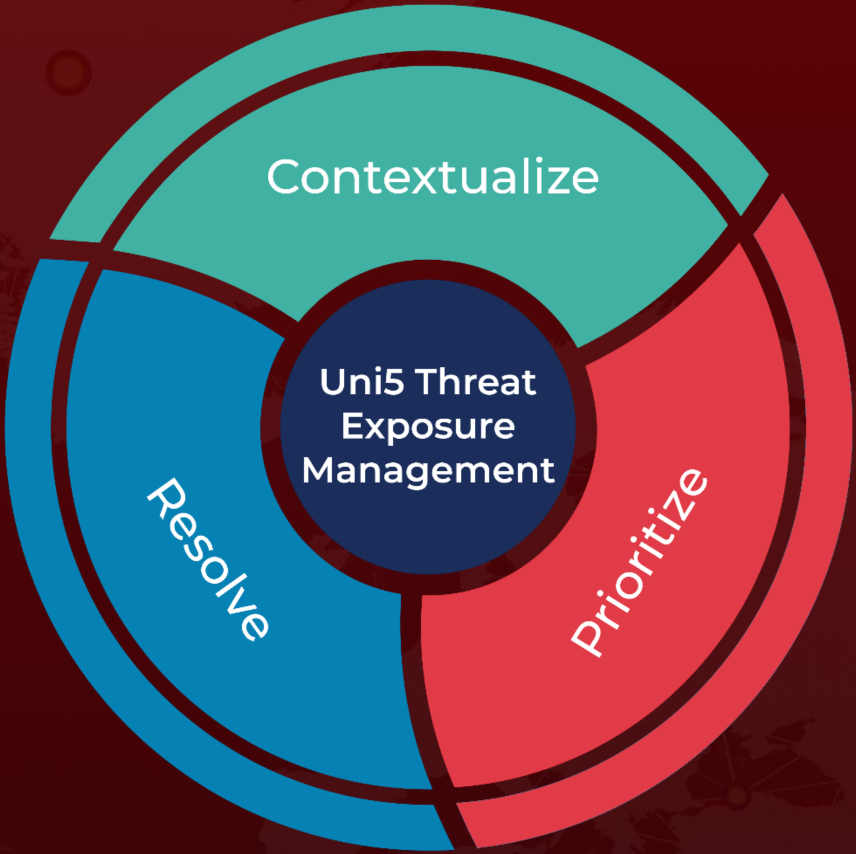
https://perception-point.io/blog/operation-phantomblu-new-and-evasive-method-delivers-netsupport-rat/

https://www.hivepro.com/threat-advisory/the-rise-of-netsupport-rat-recent-infections-and-sector-impact/

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

March 20, 2024 • 6:50 AM

More at www.hivepro.com