Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

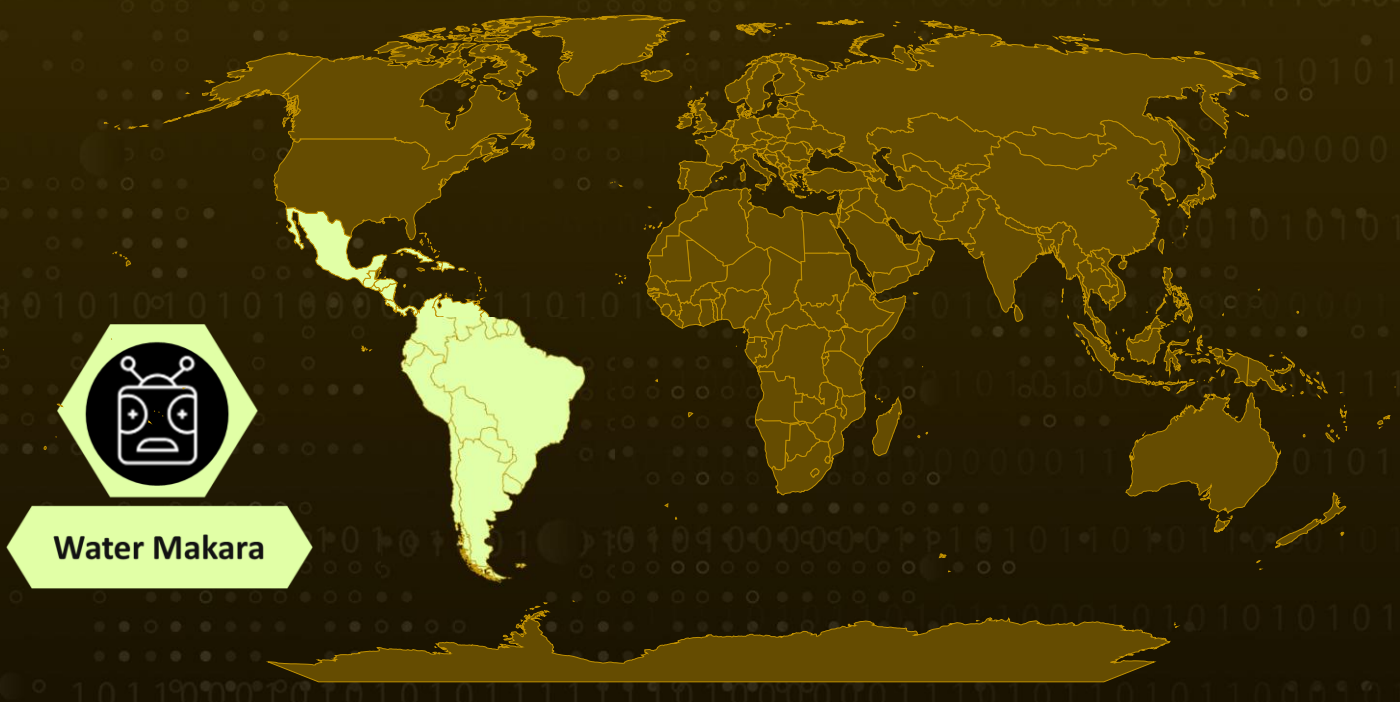
Astaroth Strikes Again: Water Makara's Sophisticated Phishing Attacks Targeting Brazil

Date of Publication	Admiralty Code	TA Number
October 17, 2024	A1	TA2024399

Summary

Attack Discovered: 2024
Targeted Countries: Latin America
Targeted Industries: Manufacturing, Retail, Government, Healthcare, Construction, Automotive, Agriculture, Biotechnology, Technology, Media, Consulting
Malware: Astaroth malware (aka Guildma)
Actor: Water Makara
Attack: A spear-phishing campaign primarily targeting companies across Latin America, with a focus on Brazil, has been uncovered. The group behind this attack, known as Water Makara, employs advanced evasion techniques to bypass detection, posing a significant threat. The campaign delivers the banking malware Astaroth, using heavily obfuscated JavaScript to slip past security defenses and infect victims' systems.

Attack Regions



Attack Details

#1 A recent spear-phishing campaign has emerged, primarily targeting organizations in Brazil, orchestrated by the group Water Makara. These attackers cleverly disguise their emails as urgent tax notifications, often labeled "Personal Income Tax" (IRPF), enticing recipients to download a malicious ZIP attachment. When opened, this file deploys Astaroth, a sophisticated banking malware designed to steal sensitive information. Inside the ZIP file, users find a malicious LNK file or obfuscated JavaScript. By exploiting mshta.exe, the malware can bypass security measures, establishing a connection to a C&C server and granting the attackers remote access to the compromised system.

#2 This campaign uses multiple file formats (.pdf, .jpg, .png, etc.) to disguise the malware and bypass detection, a technique commonly seen in drive-by downloads. Once the malicious payload is executed, encoded JavaScript commands are decoded to reveal URLs that connect to suspicious domains, indicating that the attackers use a domain generation algorithm (DGA) to create and cycle through numerous domains, making it harder to trace or block their activities.

#3 Astaroth continues to evolve, making it a persistent threat. Although it has a notorious history as a banking trojan, its reemergence highlights its adaptability, especially with new techniques for evading security defenses. The consequences of a successful attack could extend beyond stolen credentials, leading to significant business disruptions, financial losses, and regulatory fines.

#4 Organizations should prioritize vigilance, employee training, and strong email security policies to defend against such sophisticated phishing campaigns. The resurgence of Astaroth underscores the need for adaptive security strategies that can keep pace with the constantly evolving threat landscape.

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.

Implement Least Privilege: Limit user privileges to reduce the likelihood of executing malicious code. This includes preventing standard users from executing scripts or binaries that could be used in phishing campaigns.

Monitor for Domain Generation Algorithms (DGA): Implement network security tools that can detect patterns associated with DGA-based attacks to block access to suspicious domains and disrupt communication with C&C servers.

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	TA0011 Command and Control
T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.002 Malicious File
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1218 System Binary Proxy Execution	T1218.005 Mshta
T1036 Masquerading	T1036.008 Masquerade File Type	T1568 Dynamic Resolution	T1568.002 Domain Generation Algorithms
T1027 Obfuscated Files or Information	T1027.010 Command Obfuscation	T1132 Data Encoding	T1132.001 Standard Encoding

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	annotmykim[.]gruposenhordobonfim[.]io/?2/, blogonbel84[.]gruposenhordobonfim[.]org/?1/, blogonben[.]gruposenhordobonfim[.]org/?1/, blogonben8[.]gruposenhordobonfim[.]org/?1/, bruconlincol587[.]luminisconsultoria[.]io/?3/, bruncolinc59[.]lumiscoconsupoltronsia[.]org/?3/, claronqual[.]gruposenhordobonfim[.]org/?2/, clindnor[.]cenithbonfim[.]net/?2/, crafer[.]grupobonfim[.]net/?5/, crecil[.]gruposenhordobonfim[.]org/?2/, crgricill[.]gruposenhordobonfim[.]net/?3/, crigonval[.]gruposenhordobonfim[.]org/?5/, crigoval[.]gruposenhordobonfim[.]org/?5/, crigvalbon[.]gruposenhordobonfim[.]org/?2/, dragounzolonoff[.]ceritbonfim[.]com/?3/, dramainco54[.]groupomonflowsacodonbonsait[.]io/?2/, drapunzol[.]cemiteriobonfim[.]com/?1/, drapunzol[.]cemiteriobonfim[.]com/?5/, drocannanbel[.]veritasinvest[.]io/?1/, florvaz[.]cemisionfinanceinvest[.]com/?3/, flovaz138[.]cemiteriobonfim[.]com/?3/, frulinzol[.]grupobonfim[.]org/?5/, gaminqual[.]soluclaoled[.]world/?2/, gramdinlhar[.]grupobonfim[.]org/?5/, graminqual[.]solucaoled[.]world/?2/, grammidhal[.]gruposenhordobonfim[.]org/?1/, htruriz[.]grupobonfim[.]net/?3/, murankel.limpanzin[.]io/?2/, plaminel516[.]gruposenhordobonfim[.]com/?1/, planhal[.]grupobonfim[.]org/?1/, planhalconnalminsenior[.]io/?3/, plarandiz[.]gruposenhordobonfim[.]org/?3/, plikinvintez371[.]gruposenhordobonfim[.]com/?3/, plikkentin37h[.]gruposenhordobonfim[.]com/?3/, prawinvinbil2[.]clienteasciendig[.]world/?2/, prawinzinbil66[.]clienteasciendig[.]world/?2/, prawinzinbil66[.]clienteascindig[.]world/?2/, pregonfer[.]gruposenhordobonfim[.]com/?5/, prehenninlhar[.]gruposenhordobonfim[.]org/?2/, prenharbisonvirenanal3[.]plurianbonfim[.]net/?2/,

TYPE	VALUE
URLs	prenherninal6v[.]gruposenhordobonfim[.]com/?2/, prepor854[.]grupobonfim[.]net/?1/, prerherningbron38[.]grupatibonfim[.]net/?2/, prisonfinfel[.]grupobonfim[.]org/?3/, pritonggopatrimoniosoberano[.]world/?5/, pritongongor[.]patrimoniosoberano[.]world/?5/, rawinzinbil66[.]clienteascindig[.]world/?2/, rigonval[.]gruposenhordobonfim[.]org/?5/, sasanal[.]gruposenhordobonfim[.]org/?2/, scropenpaz[.]subindometa[.]world/?1/, sp[.]runal[.]pad[.]rimonios[.]oberano[.]world/?5/, sprunal[.]patrimoniosoberano[.]world/?5/, spunalu[.]patrimoniosoberano[.]world/?5/, stragir[.]nexuspatrimonial[.]city/?3/, stragiran48xpatrimonianal[.]city/?3/, stredenpintal7[.]sistemapreparatorio[.]io/?5/, stredential7[.]sistemaaproparatorio[.]io/?5/, stredential7[.]sistemapreparatorio[.]io/?5/, strehen78zinal[.]islandofinvolomartyreasurgical[.]io/?5/, strehensinvel[.]jlldobrasil[.]world/?1/, stresanal[.]gruposenhordobonfim[.]com/?2/, tibilaniznale7[.]intyoberbonfim[.]net/?2/, titblansuperioniank3[.]cenithbonfim[.]net/?3/, tribenpantrimonianal[.]cfdauctions[.]org/?2/, tripanroncol68[.]aberturaazulvision[.]xyz/?5/, tritanpinvaz[.]nexuspatrimonial[.]city/?5/, tritum[.]gruposenhordobonfim[.]org/?5/, trubenpal[.]paineira[.]cfd/?2/, trugomen[.]copinasultanbolimansire[.]io/?2/, trugonmennil[.]luminisconsultoria[.]io/?3/, trujanel[.]gruposenhordobonfim[.]net/?5/, urnasinvest[.]yunusgroup[.]net/?2/, valcredonlin59[.]unicicomonsultanlonko[.]org/?1/, valentinvest37[.]patrickbonfim[.]net/?5/, vaval[.]gruposenhordobonfim[.]net/?5/, velvinet6[.]unovetsnahels[.]org/?3/, veritasinvestio[.]io/?1/, veritasinvestio[.]io/?3/, vinherena[.]sonyofbonfim[.]net/?3/

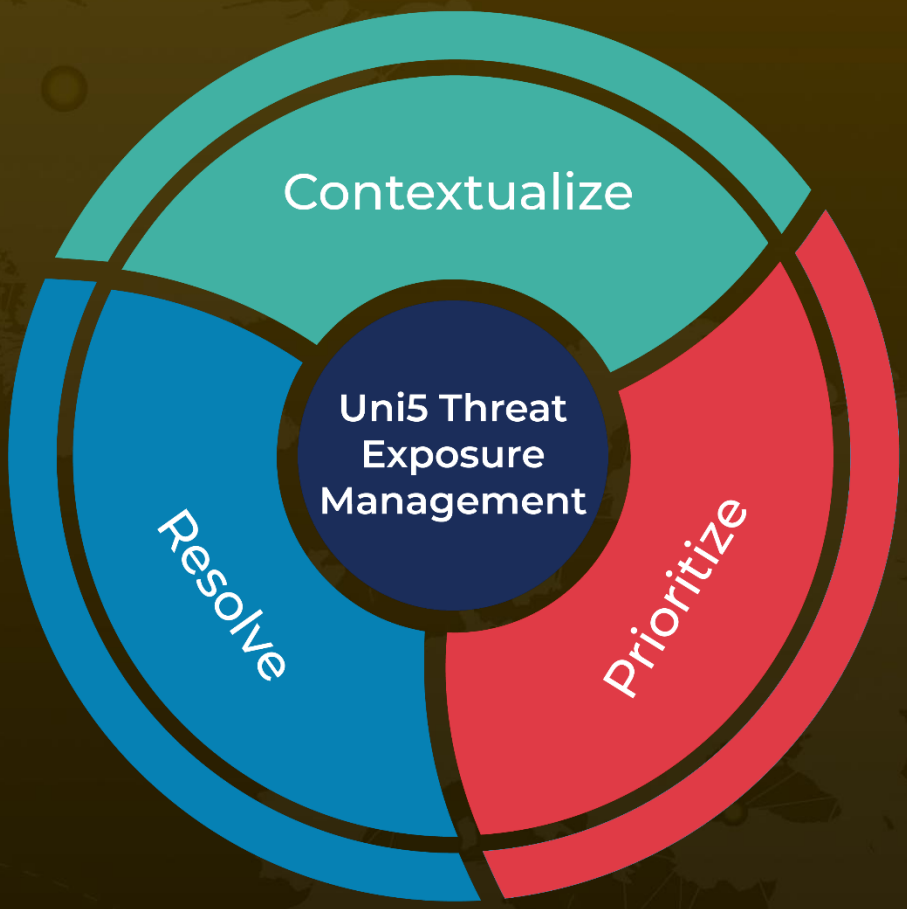
References

https://www.trendmicro.com/en_us/research/24/j/water-makara-uses-obfuscated-javascript-in-spear-phishing-campai.html

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

October 17, 2024 . 7:00 AM

More at www.hivepro.com