Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

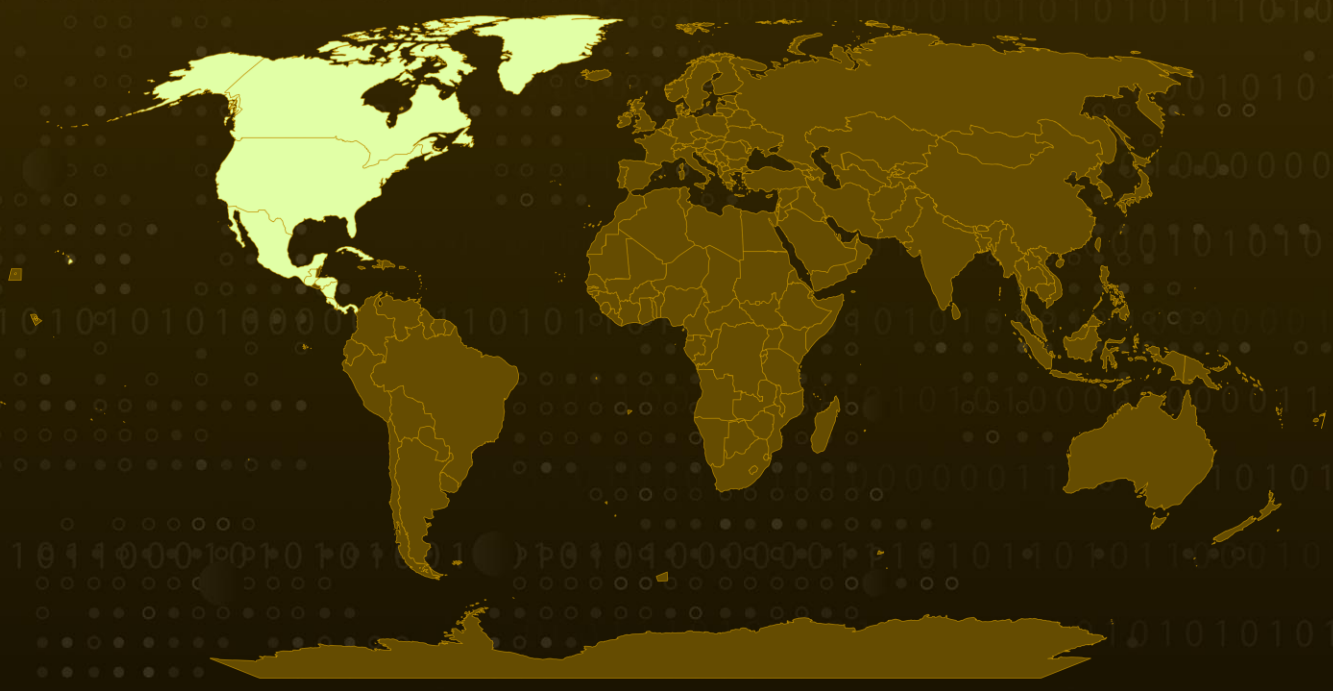
Malvertising Campaign Unleashes Nitrogen Malware Via Fake Installers

Date of Publication	Admiralty Code	TA Number
April 11, 2024	A1	TA2024139

Summary

Attack Discovered: April 2024
Attack Region: North America
Malware: Nitrogen
Attack: System administrators in North America are being targeted by a sophisticated malvertising operation. Attackers are distributing the dangerous Nitrogen malware strain through fake advertisements posing as installations for well-known system tools like FileZilla or PuTTY.

Attack Regions



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

Attack Details

#1 A persistent campaign is underway, utilizing fake advertisements for popular system utilities to target system administrators. These malicious ads, localized to North America, appear as sponsored results on Google search pages. By masquerading as a PuTTY or FileZilla installer, the Nitrogen malware lures victims into downloading and executing it.

#2 The initial infiltration often originates from a malicious advertisement discovered via a Google search. The perpetrators exploit the familiarity of common IT administrator tools like PuTTY and FileZilla to lure victims into their trap.

#3 The Nitrogen threat actors employ a cloaking page within their malvertising infrastructure, which may redirect users to the infamous or a spoof website. In cases where the campaign is not yet armed or detects invalid traffic, such as bots or crawlers, it may redirect users to a decoy website instead. These lookalike pages aim to entice potential victims, presenting themselves as attractive impersonations that could deceive almost anyone.

#4 The distribution of the Nitrogen malware through fake installers marks the final phase of this harmful cycle. Using a technique called DLL sideloading, the malware executes a malicious DLL file by launching a legitimate program. In this scenario, a seemingly harmless setup.exe file sideloads a potentially malicious file named python311.dll, associated with Nitrogen.

#5 Nitrogen, in particular, serves as an initial access malware, allowing threat actors to gain a foothold in private networks. From there, they can proceed to exfiltrate sensitive data and deploy ransomware, such as BlackCat/ALPHV. Given the increasing prevalence of malvertising as a vector for malware distribution, it's crucial to provide user education and training on identifying and mitigating these threats.

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.

Download from Trusted Sources: Only download software from trusted sources. Avoid downloading software from third-party websites or torrents, as they may contain malware or modified versions of the software.

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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0010 Exfiltration	T1583 Acquire Infrastructure	T1583.008 Malvertising
T1566 Phishing	T1036 Masquerading	T1608 Stage Capabilities	T1574 Hijack Execution Flow
T1574.002 DLL Side-Loading	T1204 User Execution	T1204.001 Malicious Link	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	kunalicon[.]com, inzerille[.]com, recovernj[.]com
Lookalike sites	file-zilla-projectt[.]org, puuty[.]org, pputy[.]com, puttyy[.]ca
URLs	amplex-amplification[.]com/wp-includes/FileZilla_3.66.1_win64.zip, newarticles23[.]com/wp-includes/putty-64bit-0.80-installer.zip, support[.]hosting-hero[.]com/wp-includes/putty-64bit-0.80-installer.zip, mkt.geostrategy-ec[.]com/installer.zip
SHA256	ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281, 2037ec95c91731f387d3c0c908db95184c93c3b8412b6b3ca3219f9f8ff60945, 033a286218baca97da19810446f9ebbaf33be6549a5c260889d359e2062778cf
IP	94.156.65[.]98, 94.156.65[.]115

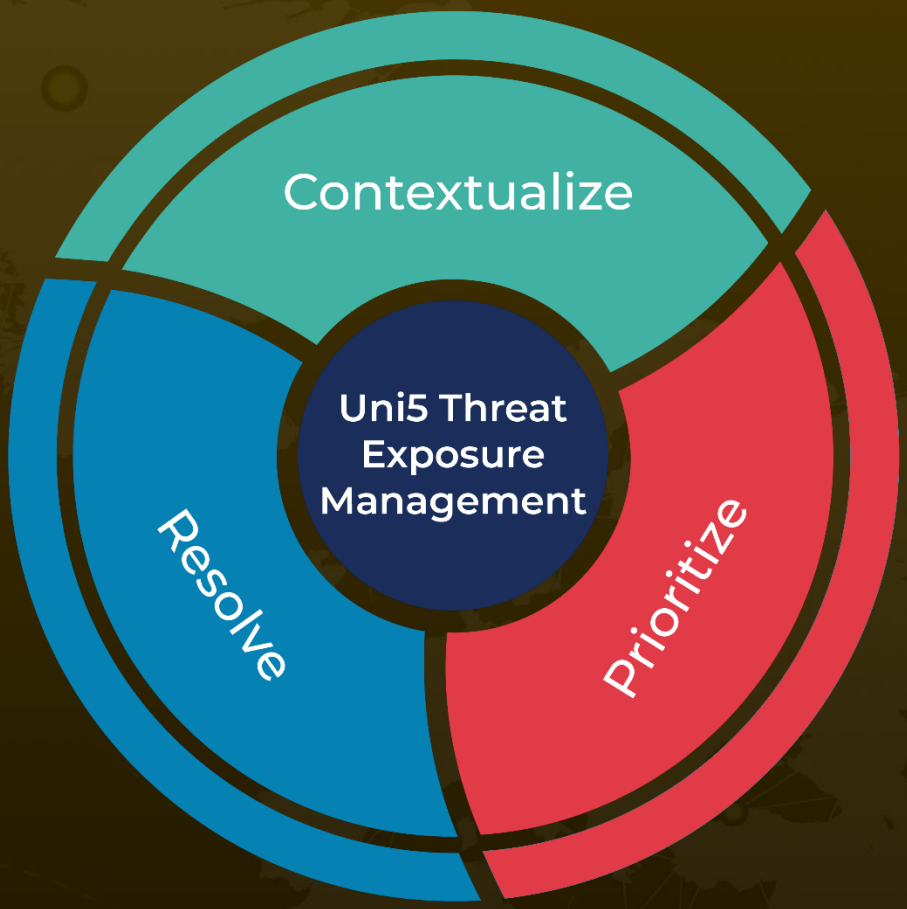
References

https://www.malwarebytes.com/blog/threat-intelligence/2024/04/active-nitrogen-campaign-delivered-via-malicious-ads-for-putty-filezilla

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

April 9, 2024 • 5:45 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com