Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

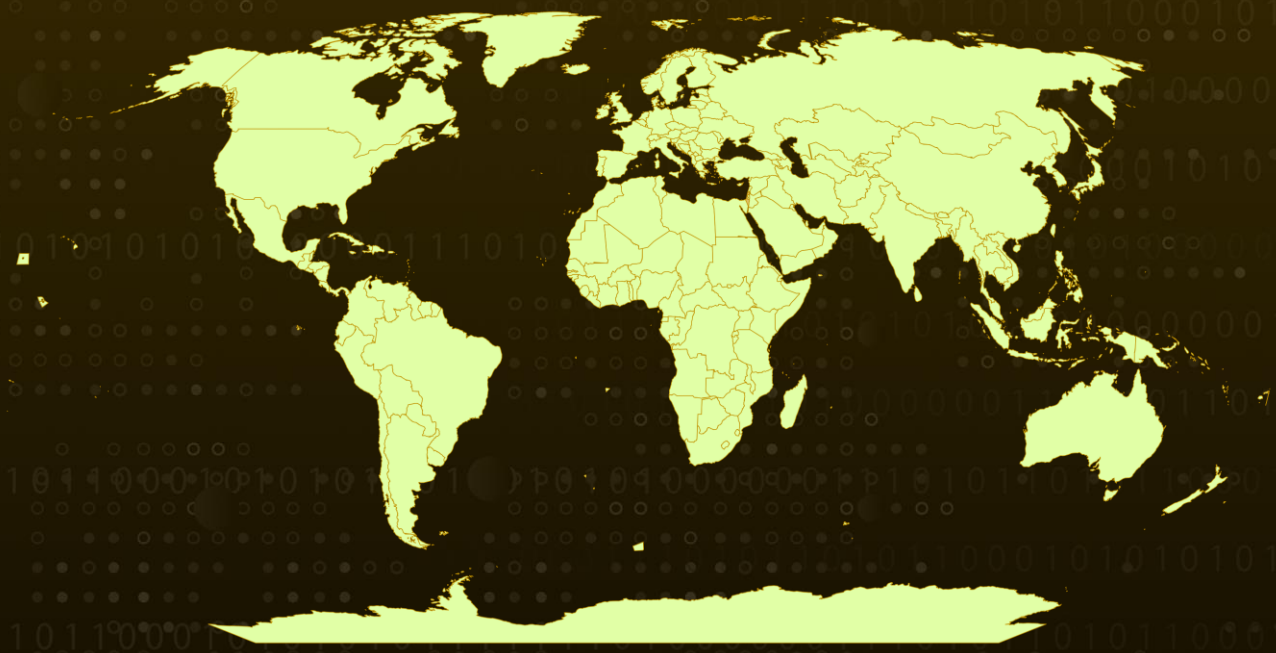
Malicious CPU-Z App Distributed Through Ads on Fake Windows News Site

Date of Publication	Admiralty Code	TA Number
November 10, 2023	A1	TA2023456

Summary

First appeared: November 2023
Attack Region: Worldwide
Malware: FakeBat, Redline stealer
Attack: A threat actor has been using Google Ads as a platform to distribute a tampered version of the CPU-Z tool. CPU-Z is a widely-used utility that provides information about various hardware components in a computer. CPU-Z tool is being utilized to distribute the Redline stealer. The malicious campaign aims to deceive unsuspecting users by displaying malicious ads that redirect them to a fraudulent website.

Attack Regions



Attack Details

#1 A recent malvertising campaign has been discovered using counterfeit websites that pose as authentic Windows news portals, in an attempt to distribute a malicious installer for a widely used system profiling tool known as CPU-Z. CPU-Z is a popular utility among Windows users, providing valuable information about their computer hardware components and assisting with troubleshooting.

#2 Malvertising campaigns often involve the creation of fake websites promoting popular software. However, this latest campaign takes a different approach, with the website mimicking WindowsReport[.]com. Its primary aim is to deceive unwitting users who are searching for CPU-Z on search engines like Google by displaying malicious ads. When users click on these ads, they are redirected to the counterfeit portal. If someone who is not the intended target clicks on the ad, they will see a regular blog with a variety of articles.

#3 Users who have searched for CPU-Z and clicked on the ad are led to a download page for the software. On this page, they may mistakenly believe that they are downloading a legitimate version of the software. However, when they click on the 'Download now' button, they receive a digitally-signed CPU-Z installer (MSI file). This installer contains a malicious PowerShell script, which has been identified as the 'FakeBat' malware loader, acting as a conduit to deploy RedLine Stealer on the compromised host.

#4 Redline is a potent information-stealing malware designed to harvest sensitive data, including passwords, cookies, and cryptocurrency-related information. Employing sophisticated obfuscation techniques at multiple levels, Redline disguises itself as an obfuscated PowerShell script, often masquerading as a legitimate system file. It establishes communication with a C2 server, allowing remote control and discreet data exfiltration.

#5 Over the past year, malware has been installed on computers through a range of deceptive tactics used by cybercriminals who have made software downloads a major target. Users should be cautious when clicking on advertised results in Google Search and make sure the loaded site and the domain match to reduce the likelihood of malware infections when searching for specific software products.

Recommendations

Download Packages from Official Websites: Always download software packages from the official website of the vendor or developer. Verify the website's URL to make sure it's the correct and official domain.

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.

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

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0005** Defense Evasion
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1608** Stage Capabilities
T1608.001 Upload Malware	**T1189** Drive-by Compromise	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1204 User Execution	**T1204.001** Malicious Link	**T1036** Masquerading	**T1105** Ingress Tool Transfer
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	argenferia[.]com, realvnc[.]pro, corporatecomf[.]online, cilrix-corp[.]pro, thecoopmodel[.]com, winscp-apps[.]online, wireshark-app[.]online, cilrix-corporate[.]online, workspace-app[.]online, 11234jkhfkujhs[.]site, 11234jkhfkujhs[.]top
IP	94.131.111[.]240, 81.177.136[.]179
URLs	thecoopmodel[.]com/CPU-Z-x86.msix, kaotickontracting[.]info/account/hdr.jpg, ivcgroup[.]in/temp/Citrix-x64.msix, robo-claim[.]site/order/team.tar.gpg, argenferia[.]com/RealVNC-x64.msix
SHA256	55d3ed51c3d8f56ab305a40936b446f761021abfc55e5cc8234c98a2c93e99e1, 9acbf1a5cd040c6dcecbe4e8e65044b380b7432f46c5fbf2ecdc97549487ca88, 419e06194c01ca930ed5d7484222e6827fd24520e72bfe6892cfde95573ffa16, cf9589665615375d1ad22d3b84e97bb686616157f2092e2047adb1a7b378cc95

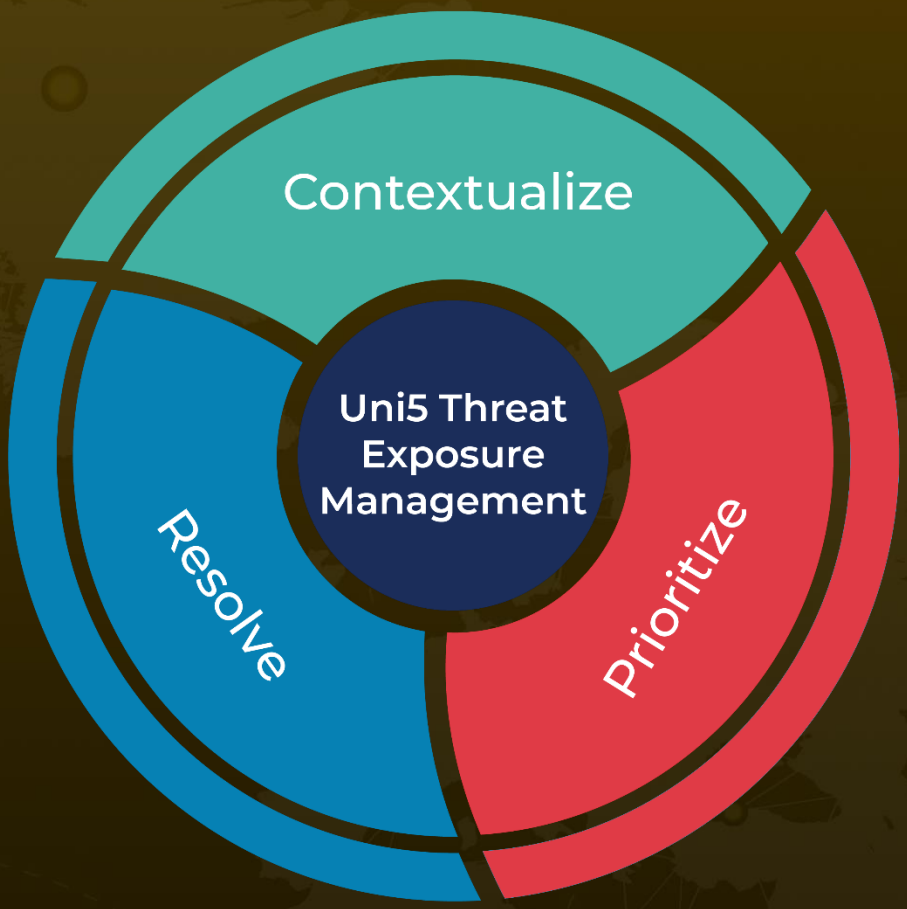
References

https://www.malwarebytes.com/blog/threat-intelligence/2023/11/malvertiser-copies-pc-news-site-to-deliver-infostealer

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

November 10, 2023 . 3:30 AM

More at www.hivepro.com