Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

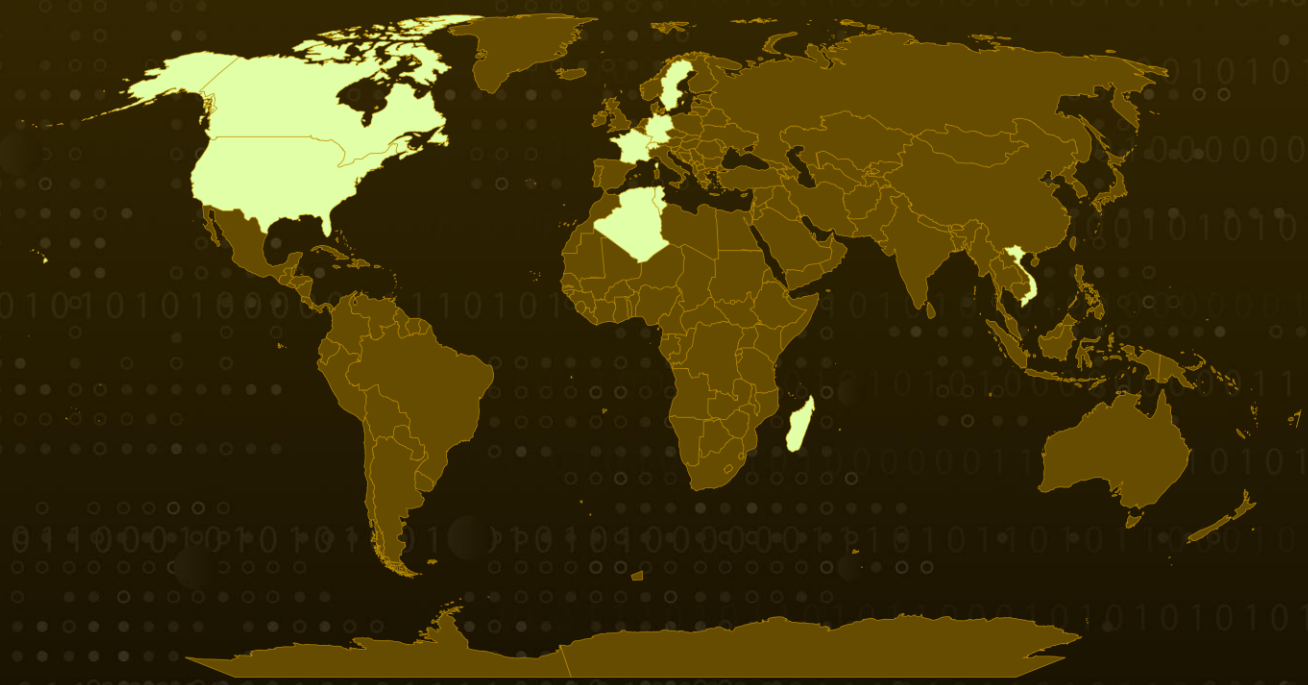
Cybercriminals Target Graphic Designers with Cryptojacking Malware

Date of Publication	Admiralty Code	TA Number
September 12, 2023	A1	TA2023366

Summary

Attack Began: November 2021
Malware: PhoenixMiner, lolMiner, M3_Mini_Rat
Attack Region: France, Switzerland, U.S., Canada, Algeria, Sweden, Germany, Tunisia, Madagascar, Singapore and Vietnam
Targeted Industry: Architecture, Engineering, Construction, Manufacturing and Entertainment
Attack: Cybercriminals are taking advantage of a legitimate Windows tool known as Advanced Installer to compromise the computers of graphic designers with cryptocurrency mining malware. These scripts are designed to infect individuals who download them with a combination of remote access trojans (RATs) and cryptomining payloads.

Attack Regions



Attack Details

#1 Cybercriminals exploit Advanced Installer, a legitimate utility for creating installation packages, to distribute and deploy cryptocurrency-mining malware on compromised computers. The attacker uses this program to insert malicious PowerShell and Windows batch scripts into legitimate product installations, disseminating adverse payloads as part of their cryptocurrency mining campaign.

#2 The campaign employs two distinct attack methods. In the first method, a batch script (core.bat) launches a PowerShell script (M3_Mini_Rat) responsible for decrypting and deploying the final payload. In the second method, two malicious scripts, core.bat and win.bat, are employed. These scripts create scheduled tasks that execute PowerShell scripts during the infection process.

#3 M3_Mini_Rat client stub, a PowerShell script created by M3_Mini_Rat is found to be one of the primary payload. This script establishes a backdoor on the victim's computer, allowing unauthorized access and control for the attacker.

#4 The campaign primarily deploys cryptominers including PhoenixMiner, Ethereum cryptocurrency-mining malware, and lolMiner, a multi-coin mining threat. Both are open-source mining programs that leverage the GPUs on the targeted machines for cryptocurrency mining.

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.

Monitor Network Traffic: Utilize network monitoring tools to scrutinize incoming and outgoing traffic, identifying potential Port Knocking attempts or irregular communication patterns. This can help detect and thwart attackers attempting to establish connections with their command-and-control servers.

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

TA0002 Execution	TA0005 Defense Evasion	TA0001 Initial Access	TA0011 Command and Control
TA0040 Impact	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1036 Masquerading
T1036.008 Masquerade File Type	T1059.003 Windows Command Shell	T1140 Deobfuscate/Decode Files or Information	T1102 Web Service
T1566 Phishing	T1496 Resource Hijacking		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3ceb959554450c4ed97bc7c7fbe1d84815a8a3d5be07da9e8d9bb2e705caf9eb, 9113b447722ccfcc7b6d6811c3a4f9434c6537697d0bc1cb16966bf8bfbb47c1, b133e715a391d653d2c736c95ac8a58cfd37362a77bec4bcce363e61398ffd2b, b8d323a348aac4e101a3dd0639b2b03d17c2d14f2eba15a70ea0b3e5fb4811a9, c785a3da9a7acca0bc8bcc1de92dfd6647d0bc2f897a1a747b595f89650378e8, dfa96bee7ba6bf98a9594b568bc8c02012081c8822a5f52d62dd7fac0b0c6974, 024b6e2e1d8cabb07215686e005e302c5e16e442902225daffe8f1e3382d02d1, 29740ff47e77833032744bbbef669755d864da0e1c2a834b903adcb914d6e8a6, 92463ea41e384f462226e473c40f6011d9f9463a05b441782596a2e6d760fe42, 2db2fe6e7b7482f14d5d44446353a277f80afb4905493443a93cc48c1ef120ef, c0fb29c35a026be5839f10f5a1d889b70107cc836fa894091bf721135f3c6e13,

TYPE	VALUE
SHA256	b297496f7723c21162e2598f6d914f148c55409197f26a1fe6936f86d566d50d, e1a272780aa760870a793bde01697ed5f425bbe7f862e85dc06091317f573394, 1075c837d0d6b3195c8a2aa2d70419c22ff98e96ebb17ec6e1d1251a5c415db1, 99ca71460b7cb4aabde41fed37e647042cfc53bc8dff91aa0a2a28b96c5d2089, e6220dcfa3ebaa19c2ef65ca79ac48a9b2a212e142f37e465adac34c112a8a52, e559e603702ed249b5c6d057d71be08a1bdba90a19aceaee15d410985c704dde, 7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08, 3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3, 2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73
Domains	Sysnod[.]duckdns[.]org, educu[.]xyz[:]9999
IPv4	51[.]178[.]39[.]184
URLs	hxxp[://]51[.]178[.]39[.]184[/]?smd_process_download=1&download_id=90, hxxp[://]51[.]178[.]39[.]184[/]kit[.]bin, hxxp[://]51[.]178[.]39[.]184

References

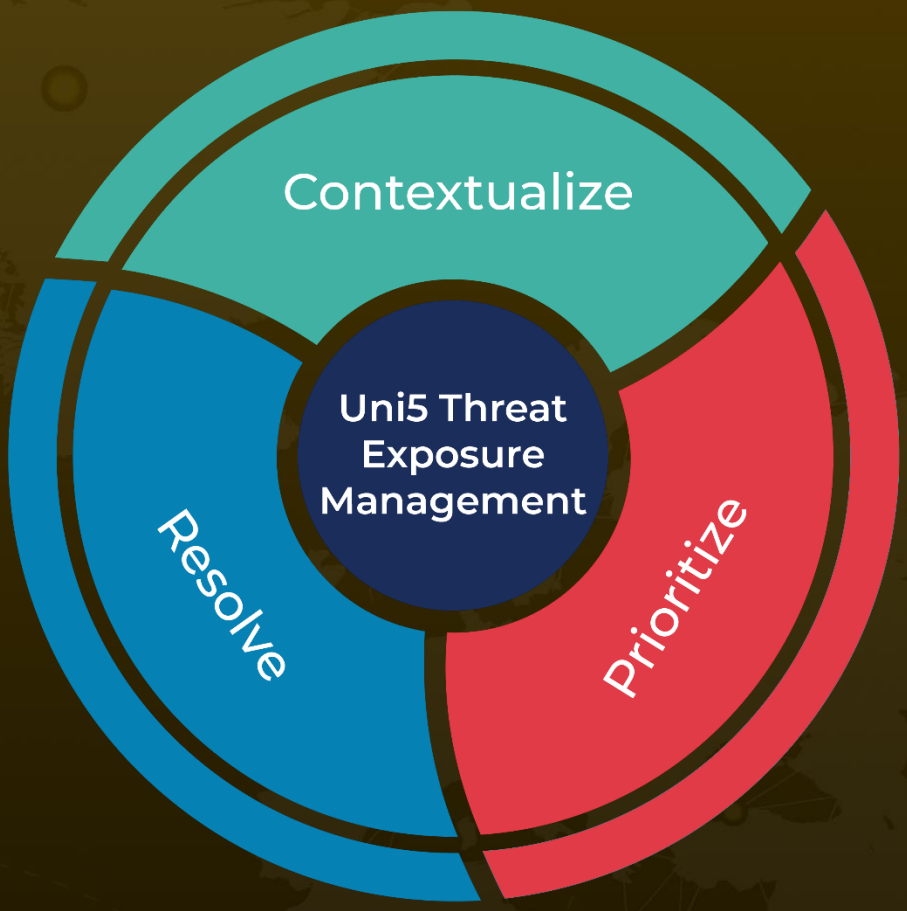
https://blog.talosintelligence.com/cybercriminals-target-graphic-designers-with-gpu-miners/

https://github.com/Cisco-Talos/IOCs/blob/main/2023/09/cybercriminals-target-graphic-designers-with-gpu-miners.txt

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

September 12, 2023 . 8:15 AM

More at www.hivepro.com