Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

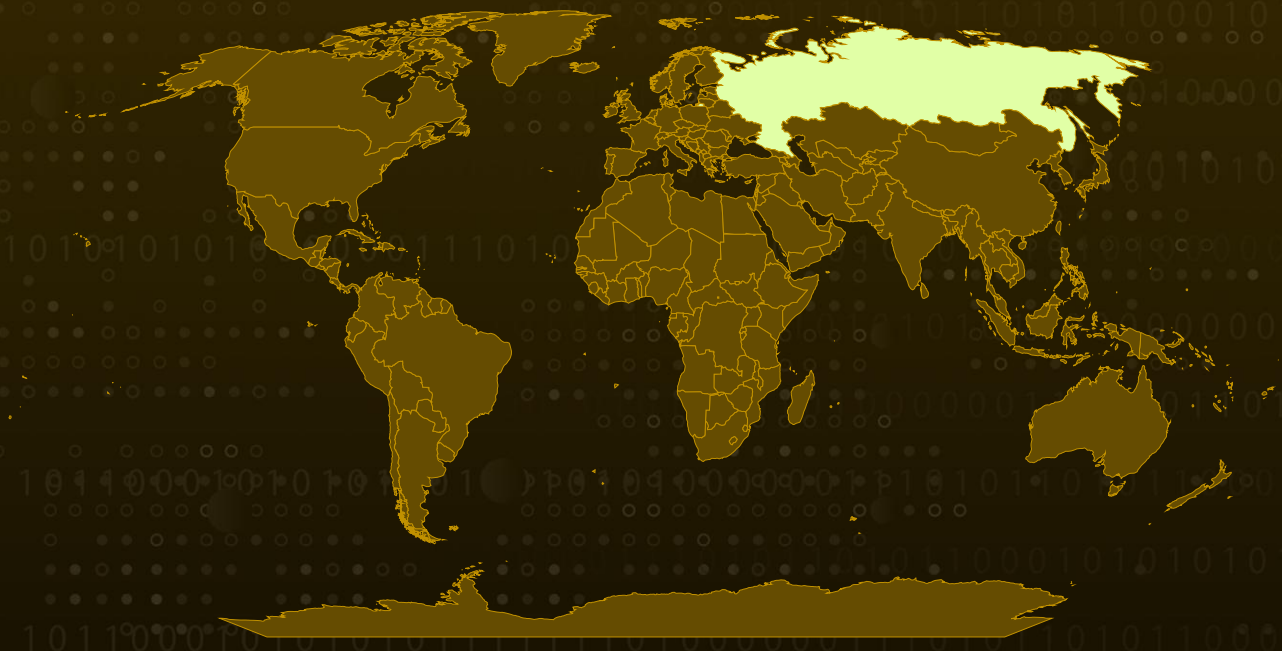
SilentCryptoMiner Spreading via YouTube Blackmail Scams

Date of Publication	Admiralty Code	TA Number
March 11, 2025	A1	TA2025072

Summary

Attack Discovered: August 2024
Targeted Countries: Russia
Malware: SilentCryptoMiner
Attack: The use of Windows Packet Divert drivers to manipulate network traffic has surged, with over 2.4 million detections in the past six months. Cybercriminals have exploited this technique in a large-scale malware campaign, distributing SilentCryptoMiner under the guise of an internet restriction bypass tool. To expand their reach, attackers falsely accused content creators of copyright violations, threatening to shut down their YouTube channels unless they promoted malicious links. While the campaign currently focuses on covert cryptocurrency mining, it has the potential to evolve into a more serious threat, enabling data theft and the deployment of additional malware.

Attack Regions



Attack Details

#1 The use of Windows Packet Divert drivers to intercept and modify network traffic has surged in recent months, with over 2.4 million detections recorded in the past six months. This growing trend has attracted cybercriminals who exploit these drivers by distributing malware disguised as restriction bypass tools or injecting malicious code into legitimate applications. These deceptive programs are often bundled in archive files with simple text-based installation instructions, allowing attackers to establish persistence on unprotected systems while remaining undetected.

#2 This widespread campaign involves a cryptominer masquerading as a tool for bypassing deep packet inspection (DPI) restrictions. The original version of this tool, hosted on GitHub, gained significant popularity, accumulating over 10,000 stars. However, attackers modified the tool to distribute malware, infecting more than 2,000 victims in Russia. The campaign was further amplified when a YouTuber unknowingly shared a tutorial on using the tool, drawing over 400,000 views. At a later stage, the attackers edited the video description, replacing the legitimate download link with a message claiming the program was no longer functional.

#3 To expand their reach, the attackers also engaged in coercion tactics, falsely accusing content creators of copyright violations and threatening to have their YouTube channels shut down unless they promoted malicious links. A Telegram channel was identified actively distributing the infected software, while a YouTube channel with 340,000 subscribers hosted a tutorial guiding users through the installation process.

#4 The infection process followed a multi-stage approach. It began with a Python-based loader, packaged as an executable using PyInstaller. When executed, the loader retrieved the next-stage payload from one of two hardcoded domains, saving it as “t.py” in a temporary directory before execution. The next stage involved a custom Python script designed to evade detection by scanning for signs of virtual machines and sandbox environments. It also modified system settings by adding the AppData directory to Microsoft Defender’s exclusion list before attempting to download the final payload. If the download failed, the malware extracted the payload from a hardcoded Base64-encoded data block.

#5 To bypass security measures, the malware artificially inflated the size of its executable to appending random data, making it harder for antivirus solutions to analyze. It also created a fake Windows service disguising it as the legitimate WIA service. The final payload, “di.exe,” was identified as a SilentCryptoMiner variant based on the open-source XMRig miner. Configured to mine multiple cryptocurrencies, the malware used encrypted configurations stored on Pastebin, leveraging multiple accounts to sustain the campaign.

Recommendations

Strengthen System Security: Keep Windows systems and security software up to date to protect against known vulnerabilities and exploits. To reduce the risk of malicious Packet, Divert drivers, limit the installation of unsigned drivers and only allow trusted software from verified sources.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Monitor Network Activity: Implement network monitoring solutions to identify suspicious traffic modifications or unauthorized tunneling attempts. Strengthen defenses by blocking known malicious domains and IP addresses linked to SilentCryptoMiner and similar threats.

Be Cautious with Downloads: Avoid installing software from unknown or unverified sources. Stick to official platforms, but remain vigilant, as malware can sometimes infiltrate legitimate sites as well. Be aware that even reputable bloggers and content creators may unknowingly distribute malicious software, including cryptocurrency miners and information stealers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**T1033** System Owner/User Discovery	**T1082** System Information Discovery
T1140 Deobfuscate/Decode Files or Information	**T1036** Masquerading	**T1055** Process Injection	**T1055.012** Process Hollowing
T1016 System Network Configuration Discovery	**T1083** File and Directory Discovery	**T1497** Virtualization/Sandbox Evasion	**T1057** Process Discovery
T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information	**T1059** Command and Scripting Interpreter

T1059.006 Python	T1059.001 PowerShell	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1105 Ingress Tool Transfer	T1566 Phishing		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	574ed9859fcdcc060e912cb2a8d1142c, 91b7cfd1f9f08c24e17d730233b80d5f, 9808b8430667f896bcc0cb132057a683, 0c380d648c0c4b65ff66269e331a0f00, 1f52ec40d3120014bb9c6858e3ba907f, a14794984c8f8ab03b21890ecd7b89cb, a2a9eeb3113a3e6958836e8226a8f78f, 5c5c617b53f388176173768ae19952e8, ac5cb1c0be04e68c7aee9a4348b37195
SHA256	DE7C1BBC731E0BDCEF5CDDCB9C853CAFCB171342965A85D973CDA72F99C56259, 40486D71829F4A487A8D72DCD0C8D41E8215C0866552ED92E148328AF074E5B6, 0779622BAD51F6F11DED8331A76A7624FE0FBDA03A5FC905AC11AD243ABBAA19, 455269197313E79AAFE79364C3495477D928D1E148CCFD2357F1AAD31BFE7BD3, 5B013DAD41AB67FA8EB7CD527F4F59CA1290749626FB7A34B37409D68B70D624, 44B212683CDEF95C55DD2E645B414B5179B589C64F1DBD6F5B4252BD4CA59790, 9D93E3AB8D0D9BD84F9F0F9FA2F997DF187CCCE49F9A2BDE7B49AD17E3A3CE08, F5232578BF310696F4E1D89F2A51369EFC32819DAF83A3BE38C3C11962F3A8BE
IPv4	193[.]233[.]203[.]138, 150[.]241[.]93[.]90

TYPE	VALUE
Domains	hxxp[:]//gitrok[.]com, hxxp[:]//swapme[.]fun, hxxp[:]//canvas[.]pet, hxxp[:]//9x9o[.]com

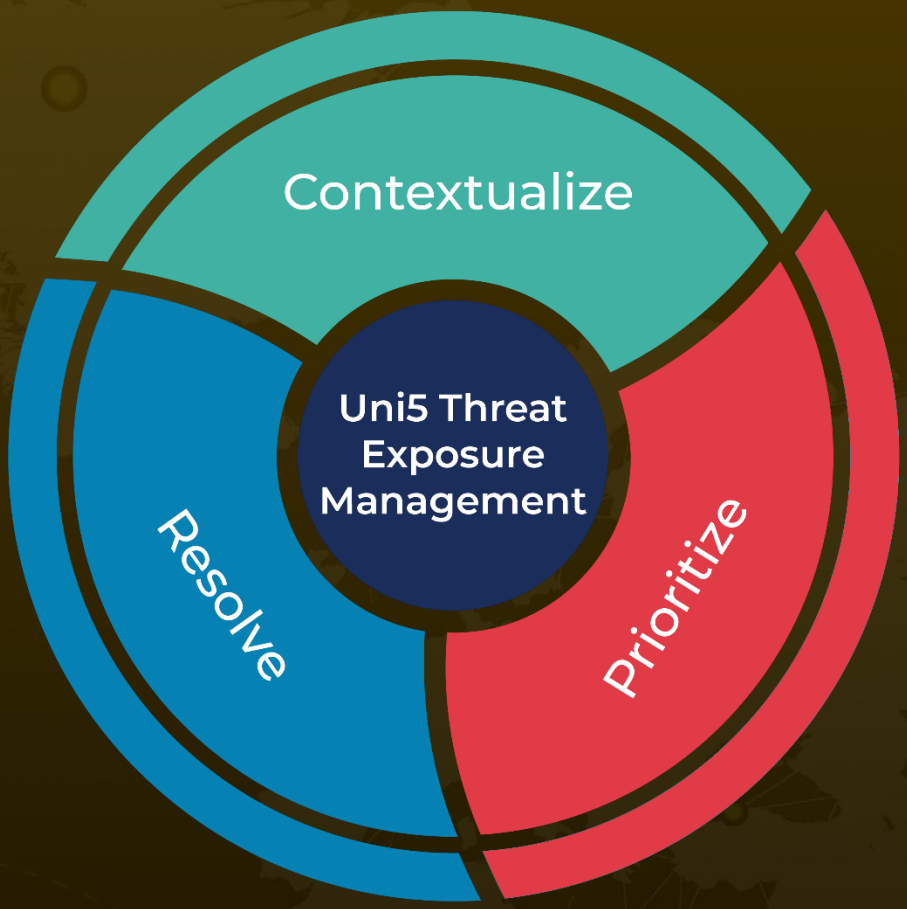
References

https://securelist.com/silentcryptominer-spreads-through-blackmail-on-youtube/115788/

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 11, 2025 • 7:50 AM

More at www.hivepro.com