Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

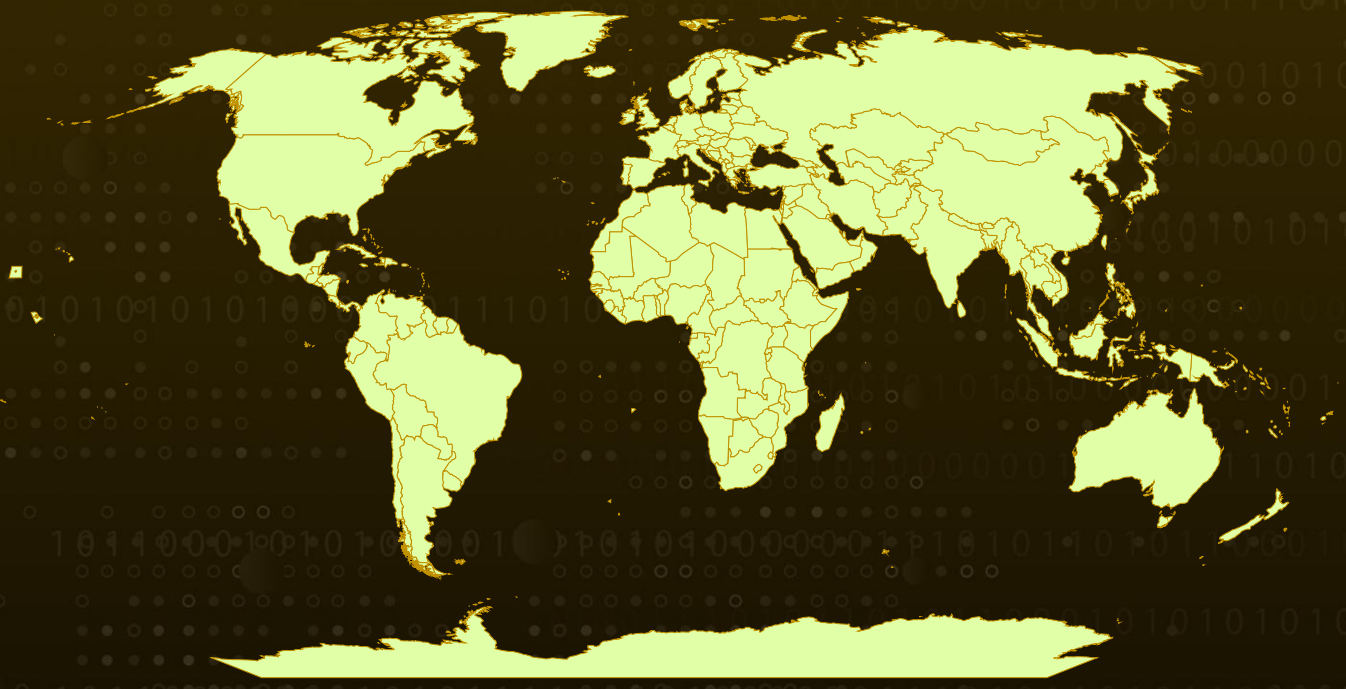
New Malware Alert: StilachiRAT Can Steal Your Credentials & Crypto!

Date of Publication	Admiralty Code	TA Number
March 18, 2025	A1	TA2025083

Summary

First Seen: November 2024
Targeted Region: Worldwide
Malware: StilachiRAT
Affected Platform: Windows
Targted Industry: Cryptocurrency
Attack: StilachiRAT is a newly identified remote access trojan (RAT) that poses a significant threat, particularly to cryptocurrency users. It targets 20 cryptocurrency wallets in Google Chrome, including MetaMask and Coinbase Wallet, to steal financial data. The malware evades detection through delayed execution, API obfuscation, and sandbox detection. It also enables lateral movement, credential theft, and remote command execution, making it a major cybersecurity risk.

Attack Regions



Attack Details

#1

StilachiRAT is a newly identified remote access trojan (RAT) with advanced evasion, persistence, and data theft capabilities. This malware specifically targets 20 cryptocurrency wallets within the Google Chrome browser, including popular extensions like MetaMask, Coinbase Wallet, and Trust Wallet, aiming to extract sensitive financial data. The malware delays its connection to command-and-control (C2) servers and evades detection by checking for monitoring tools. Its sophisticated design makes it difficult to analyze and mitigate.

#2

One of its key functions is system reconnaissance, collecting OS details, BIOS serial numbers, camera presence, and RDP sessions. It retrieves information using Windows Management Instrumentation (WMI) queries to map out the target environment. Additionally, it gathers data on installed software and active GUI applications. This allows attackers to profile infected systems for further exploitation.

#3

StilachiRAT also specializes in credential theft, extracting passwords stored in Google Chrome and targeting cryptocurrency wallets. It can decrypt stored credentials and monitor clipboard data to capture sensitive information like crypto keys. By focusing on popular wallet extensions, the malware poses a severe risk to cryptocurrency users. Its ability to steal financial data makes it particularly dangerous.

#4

The RAT enables lateral movement by monitoring RDP sessions and duplicating security tokens for user impersonation. This feature allows attackers to gain administrative access and spread within a network. It also executes remote commands, modifies Windows registry values, and clears security logs. These capabilities make it a serious threat to enterprise environments.

#5

To evade detection, StilachiRAT clears security logs and detects analysis tools or sandbox environments. It delays execution to avoid immediate detection and obfuscates Windows API calls to hinder analysis. Network monitoring tools can help detect its unusual outbound connections. Organizations should employ endpoint security measures to mitigate the risk of infection.

Recommendations

- **Maintain Up-to-Date Software:** Regularly update operating systems, applications, and security software to patch vulnerabilities that StilachiRAT could exploit.
- **Enhance Browser Security:** Be cautious when installing browser extensions, especially cryptocurrency wallet extensions. Ensure they are downloaded from official sources and keep them updated to reduce potential attack vectors.
- **Implement Robust Endpoint Protection:** Use advanced security solutions with real-time monitoring and behavioral analysis to detect StilachiRAT. Deploy EDR tools to track unusual outbound connections, especially on ports 53, 443, and 16000, to block malicious activity.
- **Monitor Network Traffic:** Regularly analyze network traffic for unusual patterns or connections to unknown command-and-control (C2) servers. This can aid in early detection of malware communications.
- **Restrict Administrative Privileges:** Limit administrative rights to essential personnel only. This minimizes the potential impact of malware attempting to perform unauthorized actions or lateral movement within the network.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	T1106 Native API	T1497 Virtualization/Sandbox Evasion	T1518.001 Security Software Discovery

T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1082 System Information Discovery	T1176 Browser Extensions
T1115 Clipboard Data	T1041 Exfiltration Over C2 Channel	T1543.003 Windows Service	T1543 Create or Modify System Process
T1134 Access Token Manipulation	T1656 Impersonation	T1021.001 Remote Desktop Protocol	T1071.001 Web Protocols
T1071.004 DNS	T1071 Application Layer Protocol	T1027 Obfuscated Files or Information	T1070.001 Clear Windows Event Logs
T1070 Indicator Removal	T1592 Gather Victim Host Information	T1046 Network Service Discovery	T1518 Software Discovery
T1529 System Shutdown/Reboot	T1497.003 Time Based Evasion		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	394743dd67eb018b02e069e915f64417bc1cd8b33e139b92240a8cf45ce10fcb
IPv4	194[.]195[.]89[.]47
Domain	App[.]95560[.]cc

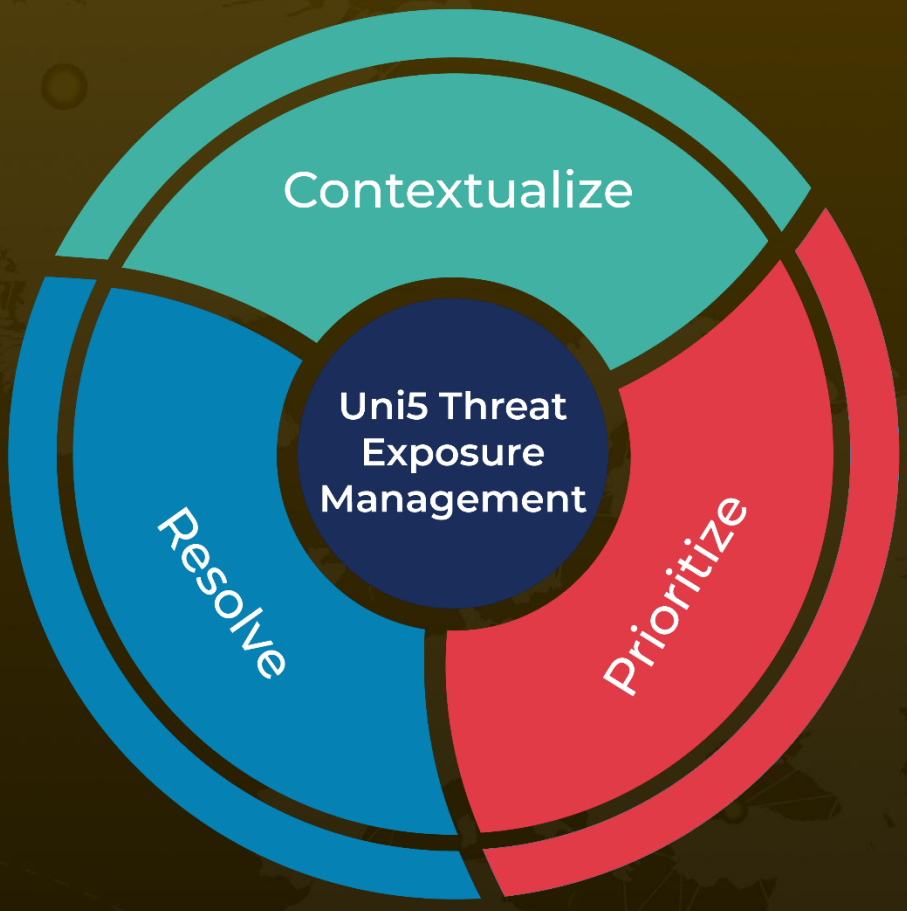
References

https://www.microsoft.com/en-us/security/blog/2025/03/17/stilachirat-analysis-from-system-reconnaissance-to-cryptocurrency-theft/

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 18, 2025 • 11:30 PM

More at www.hivepro.com