Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

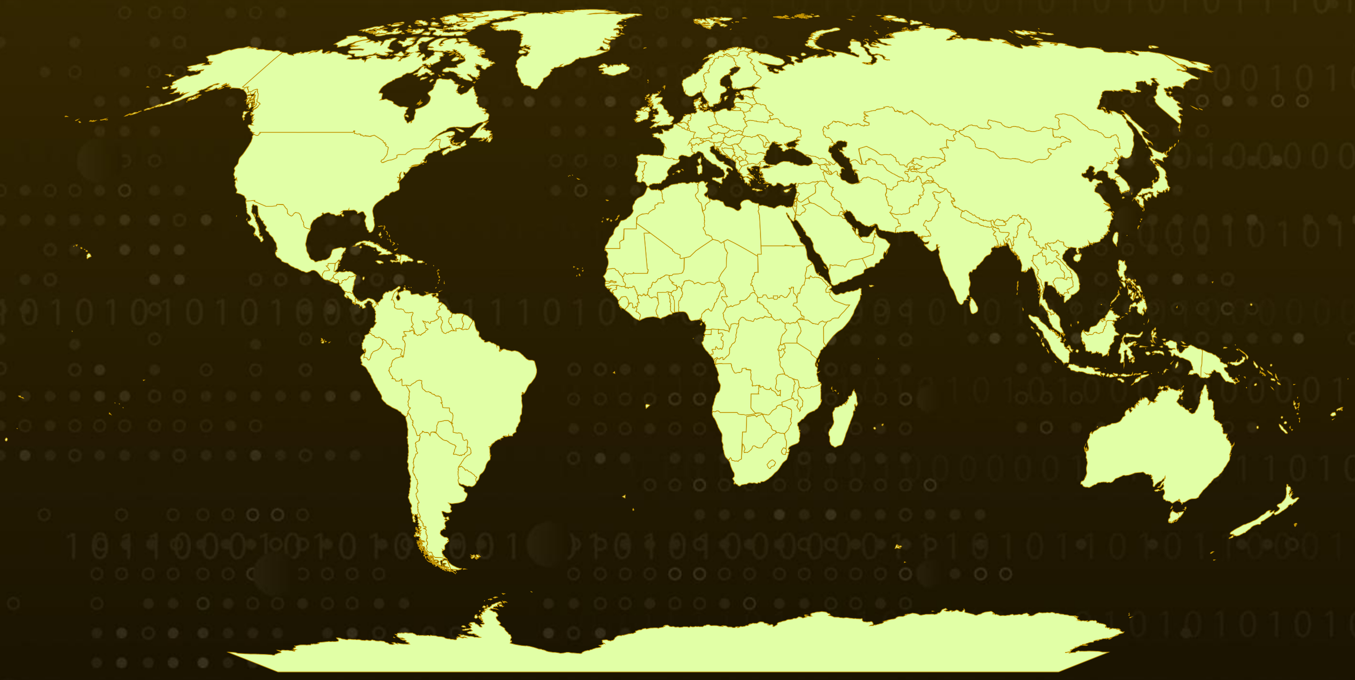
Web3 Under Siege: AI-Powered Scam Deploys Realst Malware to Steal Crypto

Date of Publication	Admiralty Code	TA Number
December 9, 2024	A1	TA2024456

Summary

Attack Discovered: October 2024
Targeted Countries: Worldwide
Affected Platforms: macOS and Windows
Malware: Realst Stealer
Attack: A new scam targeting Web3 workers has been uncovered, involving the crypto stealer Realst, targeting the macOS and Windows systems. The attackers operate under the guise of fake companies, currently known as Meetio, leveraging AI to enhance their credibility. These fraudulent entities frequently rebrand, creating websites with AI generated content and maintaining social media accounts to appear legitimate. Victims are lured into video calls and deceived into downloading the Realst info-stealer, which is designed to steal cryptocurrency.

Attack Regions



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

Attack Details

#1 A sophisticated campaign targeting Web3 professionals has been uncovered, distributing the Realst crypto stealer malware on macOS and Windows. The threat actors frequently change their company name, having used Clusee, Cuesee, Meeten, Meetone, and currently Meetio. They use AI-generated content and fake social media profiles to gain trust. Victims are contacted on Telegram, often impersonating trusted contacts, and urged to download the malware disguised as a meeting app from a compromised website.

#2 Once trust is established, victims are directed to websites laden with malicious JavaScript designed to steal cryptocurrency stored in browsers, even before malware installation. The websites offer downloads for macOS, Windows, and Linux, though most links lead to macOS-specific malware.

#3 The malware, distributed as packages like a 64-bit binary or a DMG file containing multi-architecture binaries, is written in Rust and functions primarily as an information stealer. When executed, it prompts the user for their password via macOS's osascript tool and systematically collects sensitive data, including keychain credentials, banking card details, browser cookies, autofill information, and cryptocurrency wallet credentials. This stolen data is exfiltrated to remote servers, in compressed zip files. The malware also deletes temporary directories after exfiltration to cover its tracks.

#4 A Windows variant of MeetenApp.exe was found distributed as a Nullsoft Scriptable Installer System (NSIS) file with a stolen Brys Software digital signature. It extracts files into a 7zip archive containing malicious resources, including an Electron-based app. The core script, compiled in Bytenode JavaScript, adds obfuscation, making detection harder. This version collects system data (HWID, geo IP, hostname, processes) and sends it to remote servers, along with payloads like UpdateMC.exe.

#5 The UpdateMC.exe binary is a Rust-based tool capable of extracting credentials and cryptocurrency wallet data, storing it in a folder named after the HWID and ensuring persistence via a registry key. The campaign highlights the increasing sophistication of targeted social engineering attacks using advanced malware.

Recommendations

Verify Sources: Always cross-check the authenticity of unsolicited communications, especially those promoting business opportunities or requesting downloads.

Avoid Suspicious Downloads: Be cautious of unfamiliar websites, especially those offering software downloads.

Enhanced Email Security: Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	TA0040 Impact	T1566 Phishing	T1204 User Execution
T1555 Credentials from Password Stores	T1555.001 Keychain	T1555.003 Credentials from Web Browsers	T1539 Steal Web Session Cookie
T1217 Browser Information Discovery	T1082 System Information Discovery	T1016 System Network Configuration Discovery	T1033 System Owner/User Discovery

T1005 Data from Local System	**T1074** Data Staged	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1041 Exfiltration Over C2 Channel	**T1657** Financial Theft	**T1070** Indicator Removal	**T1070.004** File Deletion
T1553 Subvert Trust Controls	**T1553.001** Gatekeeper Bypass	**T1553.002** Code Signing	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1497** Virtualization/Sandbox Evasion	**T1497.001** System Checks	**T1059** Command and Scripting Interpreter
T1059.001 PowerShell	**T1059.007** JavaScript	**T1007** System Service Discovery	**T1036** Masquerading
T1560 Archive Collected Data	**T1656** Impersonation		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	http[:]//172[.]104[.]133[.]212[:]8880/new_analytics, http[:]//172[.]104[.]133[.]212[:]8880/opened, http[:]//172[.]104[.]133[.]212[:]8880/metrics, http[:]//172[.]104[.]133[.]212[:]8880/sede, deliverynetwork[.]observer/qfast/UpdateMC[.]zip, deliverynetwork[.]observer/qfast/AdditionalFilesForMeet[.]zip, www[.]meeten[.]us, www[.]meetio[.]one, www[.]meetone[.]gg, www[.]clusee[.]com
IPv4:Port	139[.]162[.]179[.]170[:]8080
IPv4	199[.]247[.]4[.]86
MD5	9b2d4837572fb53663fffece9415ec5a, 6a925b71afa41d72e4a7d01034e8501b, 209af36bb119a5e070bad479d73498f7, d74a885545ec5c0143a172047094ed59, 09b7650d8b4a6d8c8fbb855d6626e25d

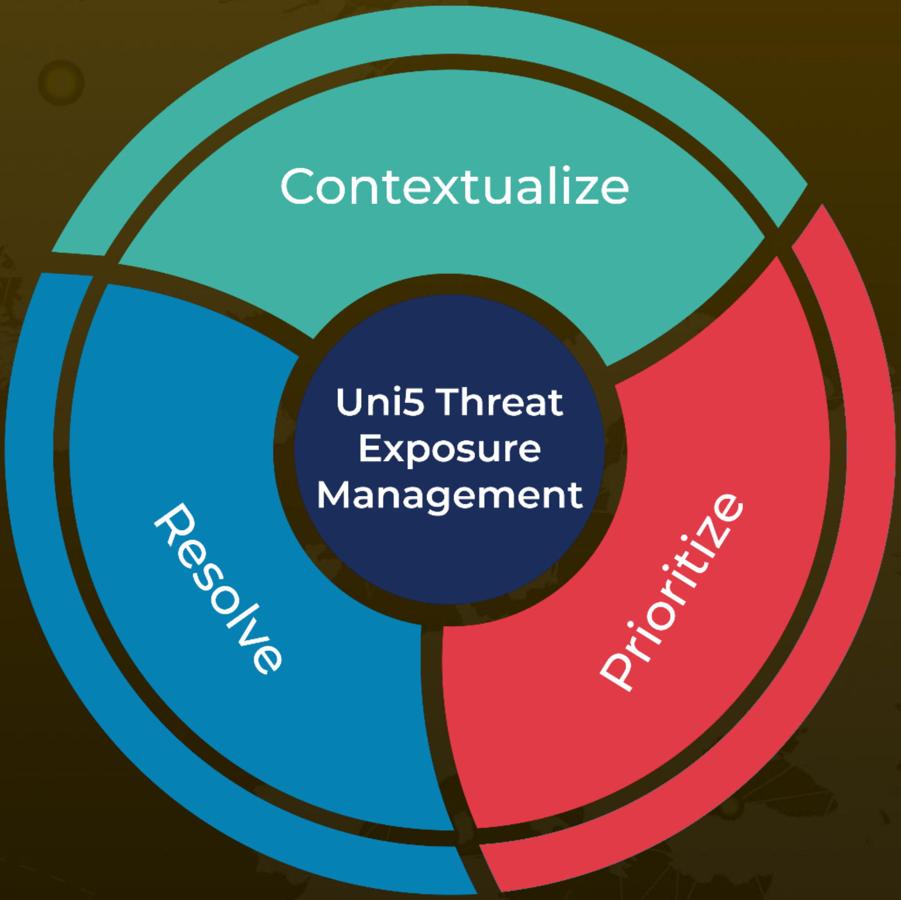
References

https://www.cadosecurity.com/blog/meeten-malware-threat

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

December 9, 2024 • 5:45 AM

More at www.hivepro.com