Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

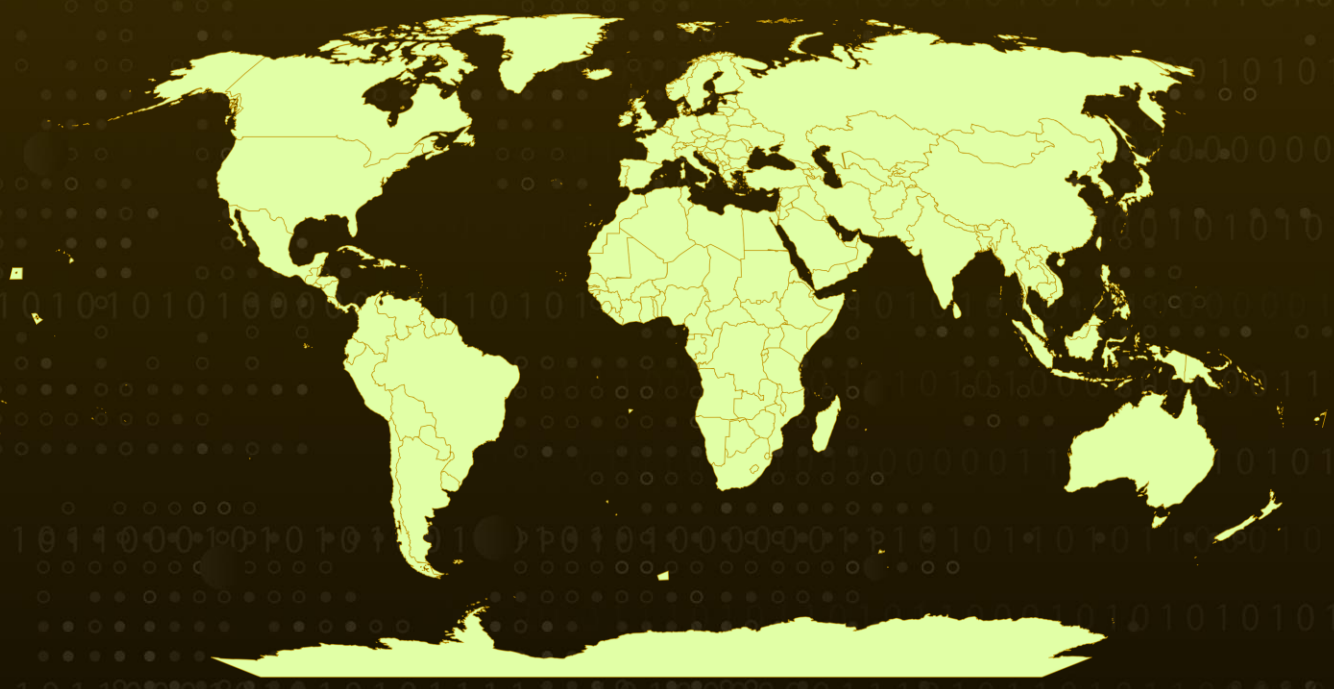
New macOS Backdoor Stealthily Stealing Cryptowallets

Date of Publication	Admiralty Code	TA Number
January 25, 2024	A1	TA2024034

Summary

Attack Discovered: December 2023
Attack Region: Worldwide
Attack: MacOS users have reported infections resulting from the use of cracked software, exposing a previously undisclosed stealer malware that has the capability to collect data from cryptocurrency wallets and system configurations.

Attack Regions



Attack Details

#1 Apple macOS users are experiencing infections from a previously undisclosed stealer malware distributed through cracked software. The malware targets Mac running macOS Ventura 13.6 and later, on both Intel and Apple silicon processor architectures. The compromise involves a program named "Activator" and a cracked application packaged together. Users are instructed to copy the app to /Applications/ and launch it.

#2 The application also includes a Python 3.9.6 installer and a Mach-O file called "tool" which are executed on launch of "Activator". The attackers trick user to launch Activator which invokes tool running pre-packaged cracked application. It further contacts a command-and-control server to retrieve an encrypted script, constructed using words from hardcoded lists and a random sequence as a third-level domain name.

#3 The DNS request retrieves three DNS TXT records, each holding a Base64-encoded ciphertext fragment. Decoding and assembling these fragments create a Python script that establishes persistence and serves as a downloader. It reaches out to "apple-health[.]org" to download and execute the primary payload at 30-second intervals.

#4 The script transmits system details to the server, including the operating system version, directories, installed applications, CPU type, external IP address, and payload version. The C2 server provides a new version of the script, automatically updating metadata, including changes in the C2 server IP address, domain name, program GUID, and version every 10-20 minutes.

#5 The attackers employed a script capable of identifying relevant cryptowallet applications on the device, replacing them with a version downloaded from apple-analyser[.]com. This Mach-O executable targeted Exodus, stealing critical information such as the wallet unlock password, wallet details, name, and balance, causing significant damage to affected users.

#6 A backdoor with administrator rights, allowing the execution of any script, served as the final payload. The compromised machine had its installed Exodus and Bitcoin cryptowallet applications replaced with malicious versions that immediately stole secret recovery phrases upon the wallet's activation.

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.

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.

Avoid cracked software: It is strongly advised to refrain from using cracked or free software obtained from unofficial sources, as these versions often come with hidden malware. Opt for legitimate and licensed software from official vendors to ensure the integrity and security of your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0010** Exfiltration	**TA0011** Command and Control
T1204 User Execution	**T1090** Proxy	**T1036** Masquerading	**T1041** Exfiltration Over C2 Channel
T1059 Command and Scripting Interpreter	**T1059.006** Python	**T1132** Data Encoding	**T1132.001** Standard Encoding
T1082 System Information Discovery	**T1518** Software Discovery	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1033 System Owner/User Discovery	**T1140** Deobfuscate/Decode Files or Information	**T1078** Valid Accounts	**T1566** Phishing
T1528 Steal Application Access Token	**T1547** Boot or Logon Autostart Execution	**T1547.013** XDG Autostart Entries	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c88c28149387ccf52ca3869442533fd9, a5924fff42d60a732853da167a743182, 9c0e8d45cbf5cae428bef90b5824e5b1, a9231044dd45a85a0bf45e01584bf213, 2ed32d3df8b4a2ef891b44a6397cf6ea, 7fd9a401fd0d7901cf4494333d1896cb, e12566cd9d72a9b56d5e53f00b7d2d53, 4c2ec35d13c5f44000caf658e40e444c, 4886a687ada61fc7f53b41f6020e76cc, c7178d08c13f3e49a6ebefe23d1fedff, cad3081fc6174ca4a4c18b8f73b3fe59, 3a89719527d51e7c60854704e9f49a32, 5bab5ba8c509a9baa5db246d932a099f, 948c1bdc9edf3e57758b677a0a449f34, e64773b03ad1eae52180c2b58907f1f6, 3f89644dfc394e888a741f6c09638d98, 29a35e0e65bba727a97747acdf921c09, 3b357b8d65537d40e87599c5329d2a3d, adede572ad9599e331592103f9eea2a2, a386380e03097055c24b0f35263d5492, 67e1f194c37968bb2edaf469bf40b837, 005fb6dee90eeefa89d6400f7a06d058, ba41c9f6d89671b729eafbe6d5f1c85e, 95c86de53ad9ca116f8c6eb2e6a152f5, be7e6e625d15d30ff47e34ebb1ee4511, 2ebfe93a39ce3fcecca883b5f182029e, e5f12e92b1fa956d02d35d6224abdbc8, 3af3d6ba3c80b7bf5d67deddb2971c61, 29b1ba90407a93400e062fb65dc9b667, a33b6c5905cefced329fa89f5eebb481, 71eefe83f836ebceadc9f68ff0e37d3b, d1177ed07dddb09415c175a205143eb6, b2d519d13125c29832b132e927fd141b, 609596d15e684f4a8ea80b7ee4b8c6a8, bbe4c19f3b675705073ba3e8a560b768, 9124843fdbf27e7b31d2f883042021a9, ff608ab027db4d1e076c1d8098e8dc8a, f4282d7e32c7e8ab4e075c572ac43803, 09ab22fcf21385cc5702ec52ac4eca02, 352f0d288e612e4f66c50aaf9214a81d, 948a90b43ade9dbc559fd27be404f9f0, 18c564a5cc4b7414df8345a8bdce7418,

TYPE	VALUE
MD5	3422f0cefa0c4612d18643bbf07a4a98, fb050f4c29a166480ff2f5a1fa8b9800, 5abe156cb33b18a46c7279d9c52b1c64, 38e4ef0d9221b25510cc50bcc8f4b4e8
Domains	imohub[.]net, 22[.]imohub[.]workers[.]dev, apple-analyser[.]com, apple-health[.]org

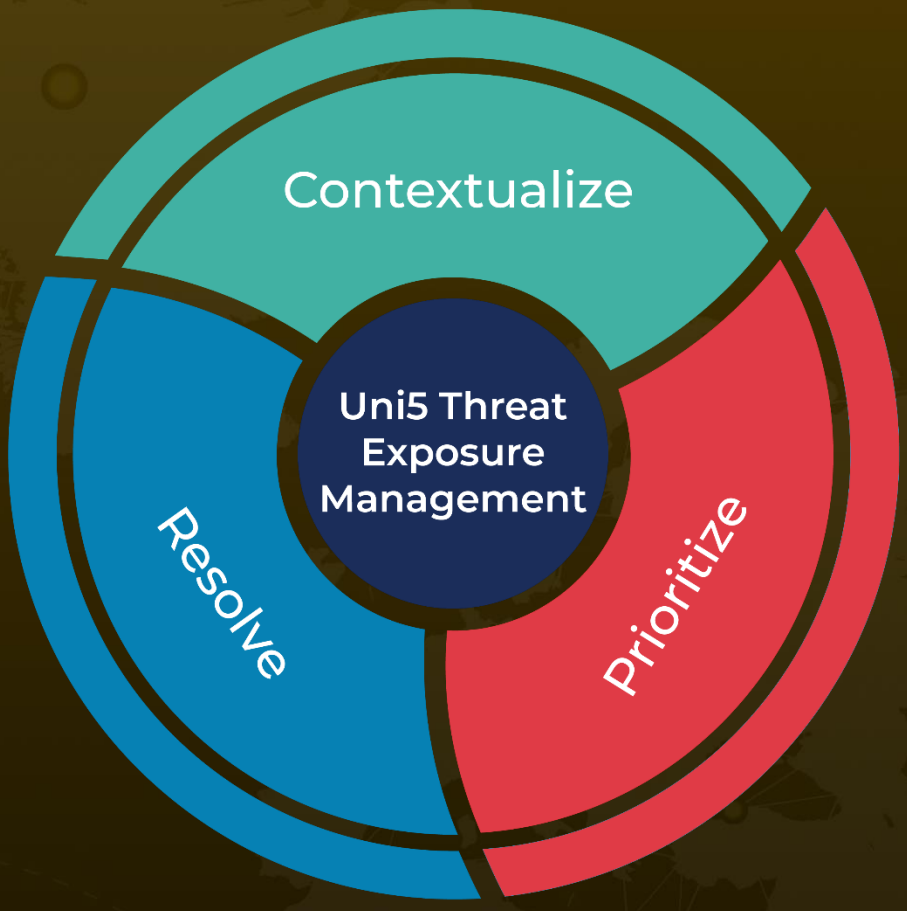
References

https://securelist.com/new-macos-backdoor-crypto-stealer/111778/

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

January 25, 2024 • 4:30 AM

More at www.hivepro.com