Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

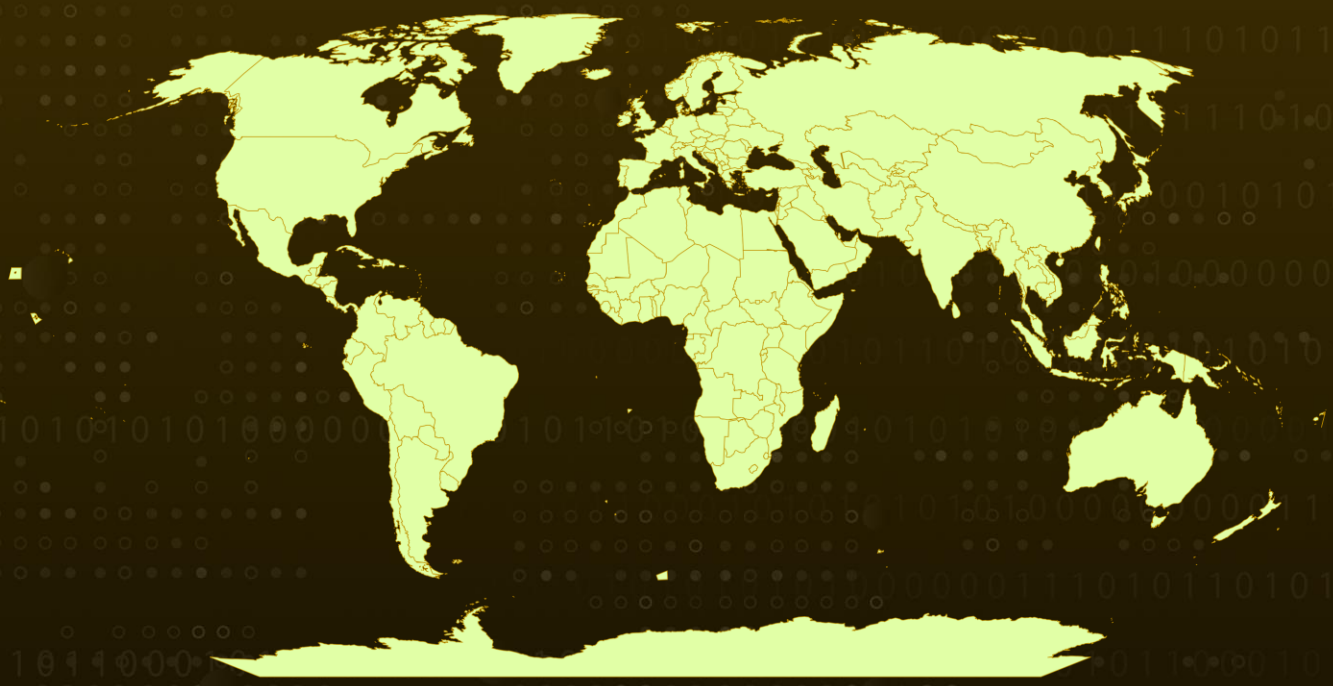
Cuckoo Malware Operates as Both an Infostealer and Spyware

Date of Publication	Admiralty Code	TA Number
May 3, 2024	A1	TA2024171

Summary

Discovered On: April 24th, 2024
Attack Region: Worldwide
Affected Platform: macOS
Malware: Cuckoo
Attack: A newly discovered malware threat for macOS, displaying traits of both an infostealer and spyware, has surfaced. Named "Cuckoo" in reference to the brood parasitic bird, this malicious code infiltrates systems and appropriates resources for its own benefit.

Attack Regions



Attack Details

#1 The discovery of the previously undetected "Cuckoo" malware presents a significant threat to macOS users, as it combines the functionalities of an infostealer and spyware. Initially posing as a legitimate music conversion application called DumpMediaSpotifyMusicConverter, Cuckoo infiltrates macOS systems, hijacks system resources, and exfiltrates sensitive data to a command-and-control server controlled by the malware operators.

#2 Upon execution, Cuckoo employs various evasion techniques to avoid detection and maintain persistence on infected systems. It gathers host information using system_profiler commands and stores hardware UUIDs for future use. Additionally, the malware obfuscates its strings through XOR encoding, decoding them at runtime, and executing them via the popen() function.

#3 To ensure its longevity on compromised systems, Cuckoo establishes persistence by copying itself to hidden directories within the user's home folder and creating LaunchAgent plist files to execute login scripts periodically. It also prompts users for their passwords using osascript and stores them in a file. Furthermore, the malware requests access to critical system resources, such as Finder, microphone, and downloads, and collects information about the host using commands like sw_vers and ps aux.

#4 Cuckoo's primary functionality revolves around stealing sensitive information, including passwords, cryptographic keys, screen captures, and application data. This stolen data is then sent to a remote command-and-control server under the control of the malware operators. To evade detection, Cuckoo encrypts its network traffic and employs sophisticated evasion tactics, ensuring that its malicious components only run under specific conditions.

#5 In summary, Cuckoo represents a highly sophisticated and dangerous threat to macOS users, underscoring the importance of robust security measures and user vigilance to prevent malware infections and safeguard sensitive information.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

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. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Download from Trusted Sources: Only download software from trusted sources. Avoid downloading software from third-party websites or torrents, as they may contain malware or modified versions of the software.

Endpoint Protection: Deploy reputable endpoint protection software that includes anti-malware and behavior-based detection capabilities to identify and block suspicious activities on endpoints.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1204 User Execution	T1204.001 Malicious Link
T1569 System Services	T1569.001 Launchctl	T1068 Exploitation for Privilege Escalation	T1555 Credentials from Password Stores
T1555.001 Keychain	T1113 Screen Capture	T1125 Video Capture	T1539 Steal Web Session Cookie

T1041 Exfiltration Over C2 Channel	**T1543** Create or Modify System Process	**T1543.001** Launch Agent	**T1573** Encrypted Channel
T1036 Masquerading	**T1566** Phishing	**T1592** Gather Victim Host Information	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	254663d6f4968b220795e0742284f9a846f995ba66590d97562e8f19049ffd4b, 1827db474aa94870aafdd63bdc25d61799c2f405ef94e88432e8e212dfa51ac7, d8c3c7eedd41b35a9a30a99727b9e0b47e652b8f601b58e2c20e2a7d30ce14a8, 39f1224d7d71100f86651012c87c181a545b0a1606edc49131730f8c5b56bdb7, a709dacc4d741926a7f04cad40a22adfc12dd7406f016dd668dd98725686a2dc
Domain	http://tunesolo[.]com, http://fonedog[.]com, http://tunesfun[.]com, http://dumpmedia[.]com, http://tunefab[.]com
URL	http://146[.]70[.]80[.]123/static[.]php, http://146[.]70[.]80[.]123/index[.]php

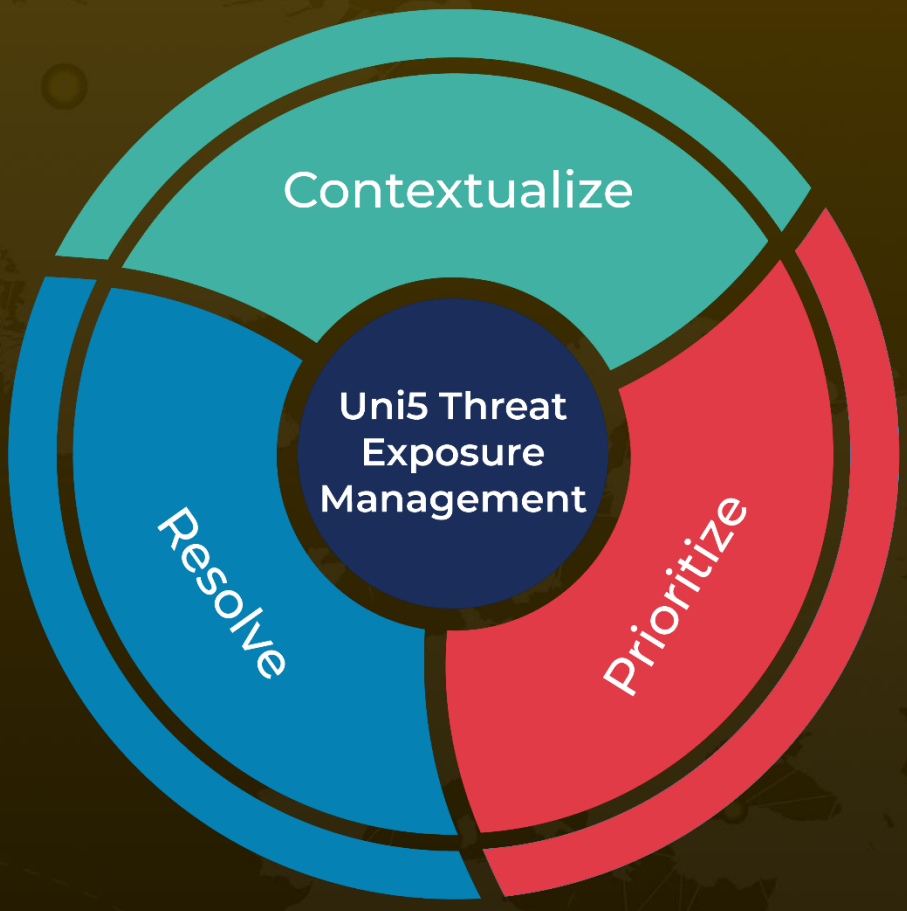
References

https://blog.kandji.io/malware-cuckoo-infostealer-spyware#indicators-of-compromise

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

May 3, 2024 • 5:30 AM

More at www.hivepro.com