Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

CloudMensis Spyware Actively Targets Apple macOS Users

Date of Publication	Admiralty Code	TA Number
July 21, 2022	A1	TA2022152

Summary

Previously unidentified macOS backdoor malware, CloudMensis, leverages cloud storage as its command and control channel to exfiltrate documents, keystrokes, and screenshots from affected Macs.

CVE Table

CVE	NAME	PATCH
CVE-2017-2533	Time-Of-Check/Time-Of-Use Privilege Escalation	✓
CVE-2017-2535	Sandbox Escape Privilege Escalation	✓
CVE-2017-2534	Library Loading Privilege Escalation	✓
CVE-2017-6977	Memory Corruption	✓
CVE-2020-9934	Leak sensitive user information	✓

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0005 Defense Evasion	TA0009 Collection	TA0010 Exfiltration	TA0037 Command and Control
T1543.004 Create or Modify System Process	T1553 Subvert Trust Controls	T1560.001 Input Capture: Keylogging	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1573.002 Encrypted Channel: Asymmetric Cryptography
T1114.001 Email Collection: Local Email Collection	T1560.002 Archive Collected Data: Archive via Library	T1113 Screen Capture	T1025 Data from removable media	T1573.001 Encrypted Channel: Symmetric Cryptography
T1005 Data from local system	T1102.002 Web Service: Bidirectional Communication			

Technical Details

#1

CloudMensis leverages open-source cloud storage platforms like pCloud, Yandex Disk, and Dropbox to receive commands and exfiltrate files. It uses an access token to download the MyExecute file from the cloud storage drive instead of using publicly accessible link. The attack chain follows the execution of arbitrary code and gaining admin privileges to launch a first-stage payload that is then used to fetch and run a second-stage malware housed on cloud, which in turn exfiltrates data including screenshots, email attachments, and documents.

#2

The first-stage downloader erases the traces of Safari sandbox escape and privilege escalation exploits that use four security flaws CVE-2017-2533, CVE-2017-2534, CVE-2017-2535 and CVE-2017-6977 reported during Pwn2Own 2017 event. It also exploits another security vulnerability tracked as CVE-2020-9934 by bypassing the Transparency, Consent, and Control (TCC) security framework that forces the TCC daemon (tccd) to load a database that CloudMensis can write to and occurs when System Integrity Protection (SIP) is disabled or enabled but running any version of macOS Catalina prior to 10.15.6.

#3

Other functions supported by the backdoor includes getting the list of running processes, capturing screenshots, listing files from removable storage devices, and running shell commands and other arbitrary payloads. Another intriguing aspect of CloudMensis is its ability to steal files with the '.hwp' and '.hwpx' extensions, which are files used by the Hancom Office software in South Korea. The malware's computer code also demonstrates that it has the ability to infect Intel-based systems.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2017-2533	macOS versions 10.11.x through 10.11.6 and 10.12.x through 10.12.4 prior to 10.12.5	cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:* versions up to 10.12.4 (inclusive)	CWE- 362
CVE-2017-2535	macOS versions prior to 10.12.5		CWE-20
CVE-2017-2534	macOS versions 10.10.x through 10.10.5, 10.11.x through 10.11.6 and 10.12.x through 10.12.4 prior to 10.12.5		CWE-20
CVE-2017-6977	macOS versions prior to 10.12.5		CWE-119
CVE-2020-9934	macOS versions prior to 10.15.6	cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:* versions up to 10.5.15 (inclusive)	CWE-285

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-1	D7BF702F56CA53140F4F03B590E9AFCBC83809DB 0AA94D8DF1840D734F25426926E529588502BC08 C3E48C2A2D43C752121E55B909FC705FE4FDAEF6
Public key	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsGRY SEVvwmfBFNBjOz+Q pax5rzWf/LT/yFUQA1zrA1njjyIHrzphgc9tgGHs/7tsWp8e5dLk AYsVGhWAPsjy 1gx0drbdMjlTbBYTyEg5Pgy/5MsENDdnsCRWr23ZaOELvHHV V8CMC8Fu4Wbaz80L Ghg8isVPEHC8H/yGtjHPYFVe6lwVr/MXoKcpx13S1K8nmDQN AhMpT1aLaG/6Qijh W4P/RFQq+Fdia3fFehPg5DtYD90rS3sdFKmj9N6MO0/WAVdZ zGuEXD53LHz9eZwR 9Y8786nVDrlma5YCKpqUZ5c46wW3gYWi3sY+VS3b2FdAKCJh TfCy82AUGqPSVfLa mQIDAQAB
File Path	/Library/WebServer/share/httpd/manual/WindowServer /Library/LaunchDaemons/.com.apple.WindowServer.plist ~/Library/Containers/com.apple.FaceTime/Data/Library/windowserver ~/Library/Containers/com.apple.Notes/Data/Library/.CFUserTextDecoding ~/Library/Containers/com.apple.languageassetd/loginwindow ~/Library/Application Support/com.apple.spotlight/Resources_V3/.CrashRep

Patch Links

https://support.apple.com/en-us/HT211289
https://support.apple.com/en-us/HT207797

References

https://phoenhex.re/2017-07-06/pwn2own-sandbox-escape

https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 21, 2022 • 10:14 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com