Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Rising Trend of macOS Malware

Date of Publication	Admiralty Code	TA Number
March 23, 2023	A1	TA2023156

Summary

Date: March 22, 2023
Attack Region: Worldwide
Affected OS: macOS
Malware: CloudMensis(BadRAT), DazzleSpy, EggShell RAT, KeySteal, Poseidon, Pureland InfoStealer, Xloader & Zuru
Attack: The rising trend of macOS malware targeting valuable data, including session cookies and keychains, is a growing concern, and various Remote Access Trojans (RATs) are being used by hacking groups to gain remote access and control of victims' computers.

Attack Regions

Attack Details

#1

The increasing trend of macOS malware that targets valuable data and exploits it for malicious purposes such as underground forums, espionage campaigns, and supply chain attacks is a cause of concern. The primary targets for such malware are session cookies, keychains, SSH keys, and other data assets. Session cookies are often targeted to allow an unauthorized user to remain logged in to apps and enterprise software across different devices. Keychains, on the other hand, are highly coveted targets that hold passwords, authentication tokens, and encryption keys.

#2

Remote Access Trojans (RATs) are been used by hacking groups to gain remote access and control over victims' computers, including CloudMensis (BadRAT), DazzleSpy, EggShell RAT, KeySteal, Poseidon, Pureland InfoStealer, Xloader, and Zuru. These RATs can steal sensitive information, such as login credentials and personal information, and are often distributed via phishing emails.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1496 Resource Hijacking	T1115 Clipboard Data
T1021 Remote Services	T1134 Access Token Manipulation	T1555 Credentials from Password Stores	T1555.001 Keychain
T1555.003 Credentials from Web Browsers	T1543 Create or Modify System Process	T1543.001 Launch Agent	T1543.004 Launch Daemon
T1553 Subvert Trust Controls	T1553.001 Gatekeeper Bypass	T1560 Archive Collected Data	T1560.002 Archive via Library
T1056 Input Capture	T1056.001 Keylogging	T1056.002 GUI Input Capture	T1113 Screen Capture
T1005 Data from Local System	T1025 Data from Removable Media	T1114 Email Collection	T1114.001 Local Email Collection
T1573 Encrypted Channel	T1573.001 Symmetric Cryptography	T1573.002 Asymmetric Cryptography	T1102 Web Service
T1102.002 Bidirectional Communication	T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage	T1204 User Execution
T1204.002 Malicious File	T1222 File and Directory Permissions Modification	T1222.002 Linux and Mac File and Directory Permissions Modification	T1036 Masquerading
T1036.005 Match Legitimate Name or Location	T1132 Data Encoding	T1132.002 Non-Standard Encoding	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	d7bf702f56ca53140f4f03b590e9afcbc83809db 0aa94d8df1840d734f25426926e529588502bc08 c3e48c2a2d43c752121e55b909fc705fe4fdaef6 ee0678e58868ebd6603cc2e06a134680d2012c1b 556a2174398890e3d628aec0163a42a7b7fb8ffd 26622e050d5ce4d68445b0cdc2cb23f9e27318ba 3951a7bd03e827caf7a0be90fdfc245e6b1e9f8a 5a8a7e665fdd7a422798d5c055c290fa8b7356d9 749ee9eaa0157de200f3316d912b9b8d8bb3a553 79c222b00b91801bb255376c9454d5bc8079c4a9 7f537a0a77fc8d629b335d52ffef40ea376bd673 8446f80f073db57466459bcbfcaefda3c367cd52 b81bf1b65b8ec0a11105d96cc9f95bb25214add5 ca985f4395e47f1bf9274013b36a0901343fc5a5 d2314f1534ecc1ab97f03cdacf9ed05349f5c574 d4e30bce71e025594339dacf4004075fa22962ea d85b6531843d5c29cc3bbb86e59d47249db89b9a d8cd78c16ca865d69f2eb72212b71754f72b4479 cb8be6d2cefe46f3173cb6b9600fb40edb5c5248 c91b0b85a4e1d3409f7bc5195634b88883367cad 0b5153510529e21df075c75ad3dbfe7340ef1f70 1eec28e16be609b5c678c8bb2d4b09b39aa35c05 2480d3f438693cf713ce627b8e67ab39f8ae6bea 308cb5cbc11e0de60953a16a9b8ad8458b5eda67 397d5edae7086bb804f9384396a03c52c2b38daa 398de17ae751f7b4171d6d88c8d29ee42af9efb5 406c7c1f81c3170771afc328ca0d3882ee790e98 411482a5cebe1fc89661cc0527047fa4596ed2d6 49d7c260e89dd5bc288111cbe2bf521e95bbe199 68be8c909a809487d2a3ae418d7ec5adf9d770cb 8baf7c147d3d54b8e2a2e6e26d852028d03ee64b 8e698a7f186b7eda34a56477d5e86e0ad778b53d aa033e9f102bc8d98360e6079da3c8b4d7e2d3c8 acc1139ecfa0a628edf89b70a3e01a1424a00d5b f462fa129de484b0cf09a9b4d975b168e5c69370 7edead477048b47d2ac3abdc4baef12579c3c348 958147ab54ee433ac57809b0e8fd94f811d523ba fb83d869f476e390277aab16b05aa7f3adc0e841 20acde856a043194595ed88ef7ae0b79191394f9

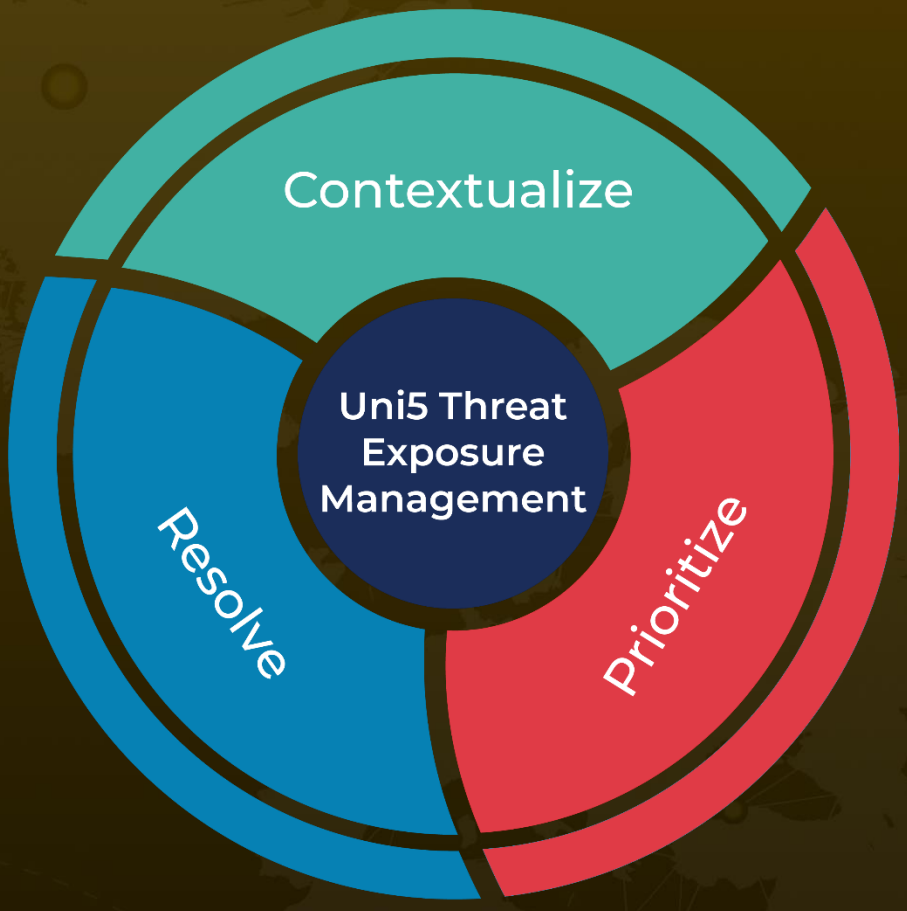
References

https://www.sentinelone.com/blog/session-cookies-keychains-ssh-keys-and-more-7-kinds-of-data-malware-steals-from-macos-users/

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 23, 2023 • 4:00 AM

More at www.hivepro.com