Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

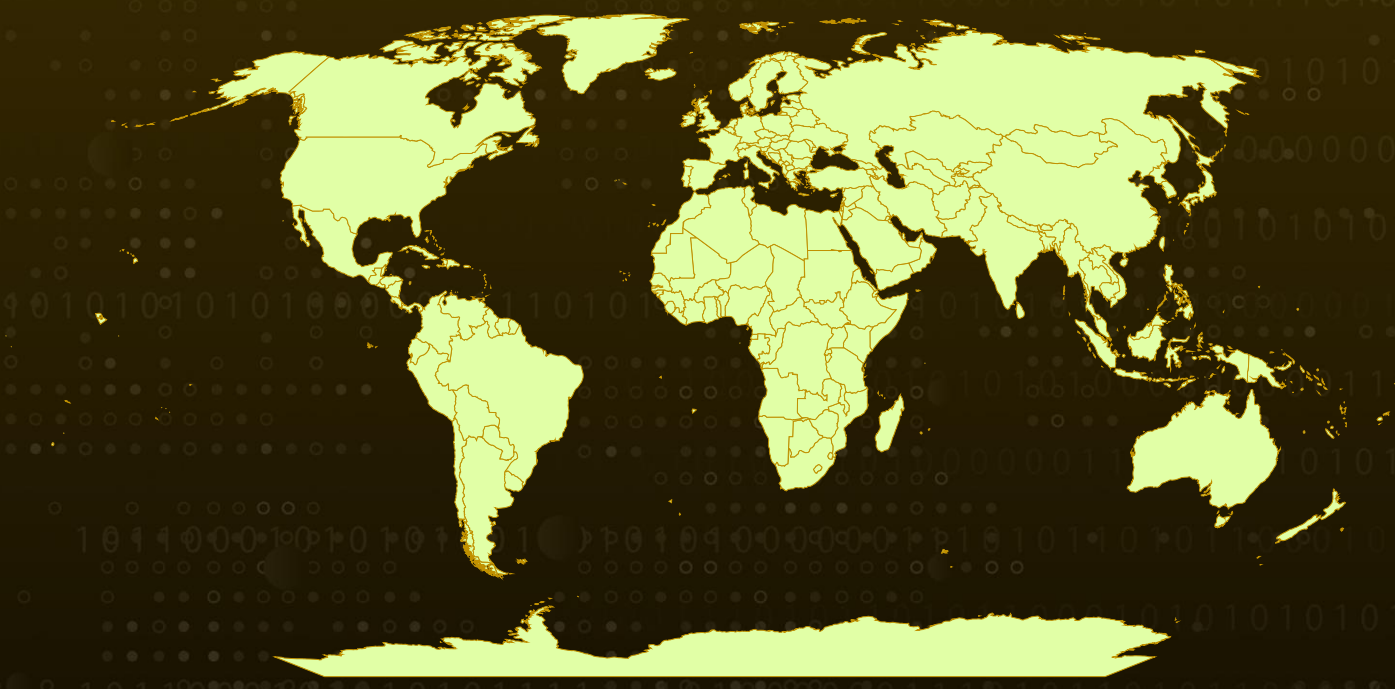
New Banshee Stealer Threatens macOS Systems, Stealing Sensitive Data

Date of Publication	Admiralty Code	TA Number
August 19, 2024	A1	TA2024316

Summary

Attack Discovered: August 2024
Attack Region: Worldwide
Malware: BANSHEE Stealer
Attack: A new macOS malware named "BANSHEE Stealer" has been discovered, specifically targeting Apple macOS systems. This sophisticated malware is being sold on the cybercrime underground for a hefty price of $3,000 per month and is compatible with both x86_64 and ARM64 architectures. BANSHEE Stealer poses a significant threat to macOS users, as it targets crucial system information, browser data, and cryptocurrency wallets.

Attack Regions



Attack Details

#1 In August 2024, a newly identified macOS malware dubbed "BANSHEE Stealer" emerged, likely the handiwork of Russian cybercriminals. This sophisticated malware is designed to siphon a broad spectrum of sensitive information, including system details, browser data, and cryptocurrency wallets. Notably, it was developed within an underground forum and is compatible with both macOS x86_64 and ARM64 architectures. With a steep monthly price tag of $3,000, BANSHEE Stealer highlights the increasing focus of cybercriminals on macOS platforms.

#2 BANSHEE Stealer employs basic evasion techniques to avoid detection. It can detect debugging attempts via the `sysctl` API and recognize virtual machines using the system_profiler command output. Additionally, the malware checks the system's preferred language through the API and avoids infecting machines where Russian is set as the primary language.

#3 One of its deceptive tactics includes presenting a fake Osascript password prompt, which tricks users into entering their password under the guise of a system update. The entered password is then verified using the `dscl` command and stored in a file. These credentials can subsequently be used to decrypt the system’s keychain, granting attackers access to stored passwords.

#4 BANSHEE Stealer meticulously gathers system information and converts it into a JSON object. Further it copies the keychain file to a directory named `/Passwords`. The malware also executes AppleScripts, which are written to a file in `/tmp/tempAppleScript`. One of the initial scripts mutes the system sound before beginning the collection of files, including Safari cookies, the Notes database, and files with specific extensions from the Desktop and Documents folders.

#5 It targets multiple web browsers and cryptocurrency wallets, including Safari, Google Chrome, Mozilla Firefox, Brave, Microsoft Edge, Vivaldi, Yandex, Opera, OperaGX, Exodus, Electrum, Coinomi, Guarda, Wasabi Wallet, Atomic, and Ledger. The collected data is then compiled, compressed, encoded with XOR, and transmitted via a POST request using the built-in cURL command.

#6 Despite its potential for harm, BANSHEE Stealer lacks advanced obfuscation techniques, and the inclusion of debugging information makes it easier for analysts to dissect its functions. Nonetheless, its specific targeting of macOS systems and extensive data collection capabilities render it a serious threat to users on this platform.

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. 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.

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

TA0043 Reconnaissance	TA0002 Execution	TA0006 Credential Access	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	T1046 Network Service Discovery	T1560 Archive Collected Data
T1560.001 Archive via Utility	T1518 Software Discovery	T1059 Command and Scripting Interpreter	T1059.002 AppleScript
T1119 Automated Collection	T1082 System Information Discovery	T1217 Browser Information Discovery	T1567 Exfiltration Over Web Service
T1592 Gather Victim Host Information	T1592.001 Hardware	T1592.002 Software	T1497 Virtualization/Sandbox Evasion
T1083 File and Directory Discovery	T1056 Input Capture	T1056.002 GUI Input Capture	T1555 Credentials from Password Stores

T1555.001 Keychain	**T1555.003** Credentials from Web Browsers	**T1614** System Location Discovery	**T1614.001** System Language Discovery
T1539 Steal Web Session Cookie	**T1135** Network Share Discovery	**T1005** Data from Local System	**T1074** Data Staged
T1074.001 Local Data Staging			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	45[.]142[.]122[.]92
SHA256	11aa6eeca2547fcf807129787bec0d576de1a29b56945c5a8fb16ed8bf68f782

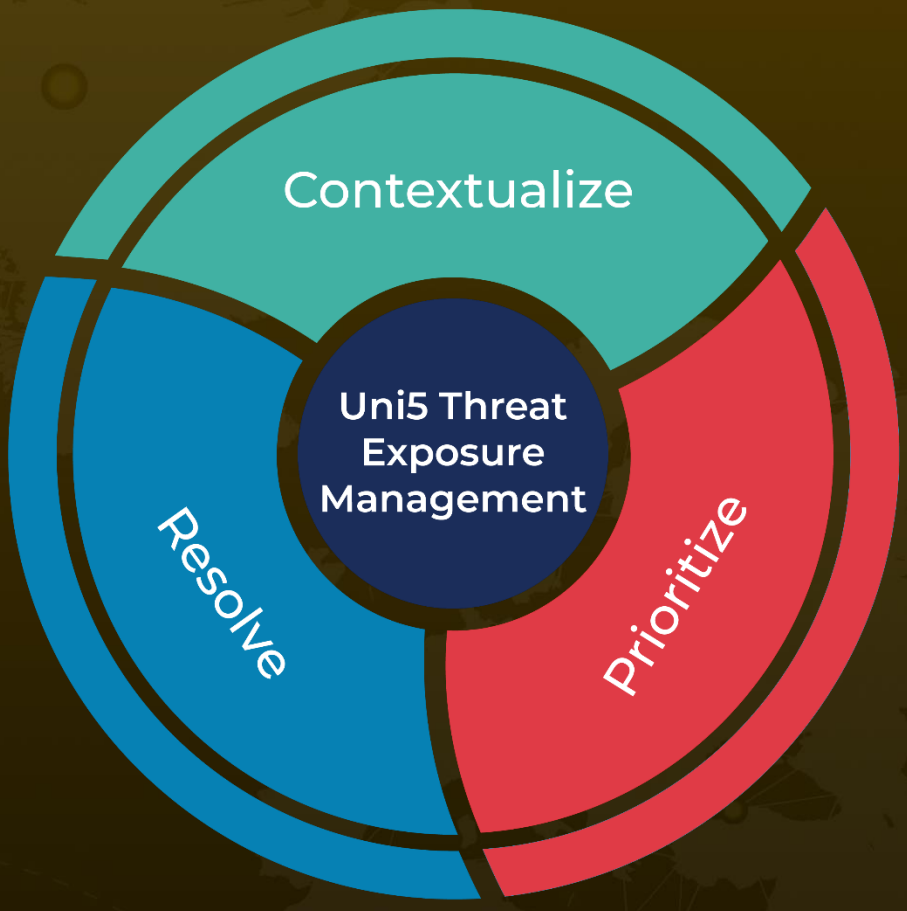
References

https://www.elastic.co/security-labs/beyond-the-wail

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

August 19, 2024 • 6:00 AM

More at www.hivepro.com