Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

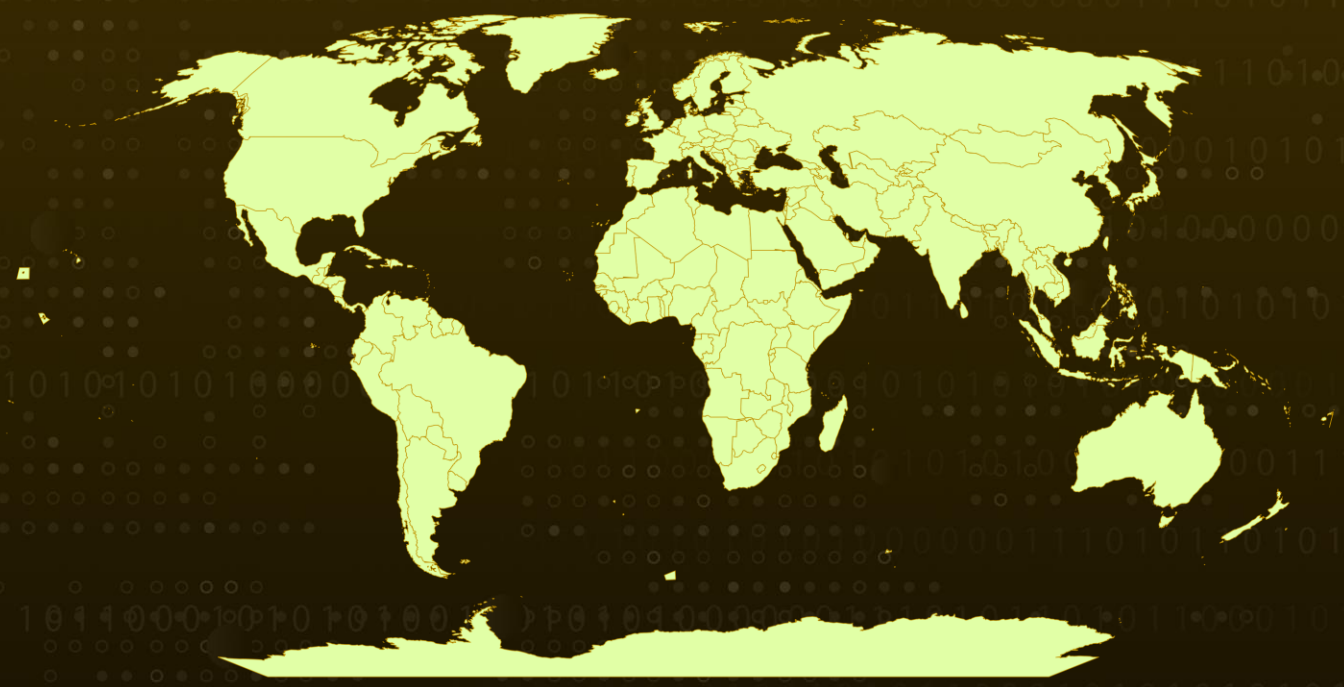
Atomic Stealer Sneaks In via Fake Browser Updates

Date of Publication	Admiralty Code	TA Number
November 23, 2023	A1	TA2023473

Summary

Attack Discovered: November 17, 2023
Attack Region: Worldwide
Affected Platform: Mac OS
Malware: Atomic Stealer
Attack: The macOS information-stealing malware known as Atomic, or AMOS, is currently being delivered to targets through a deceptive web browser update chain known as ClearFake. ClearFake is a recent malware campaign that exploits compromised websites to distribute fake browser updates.

Attack Regions



Attack Details

#1 The macOS information-stealing malware, Atomic Stealer (aka AMOS), is now being distributed to Mac users through a deceptive web browser update chain known as 'ClearFake.' ClearFake is a relatively recent malware campaign that utilizes compromised websites to distribute fraudulent browser updates.

#2 Atomic Stealer, a commercially available malware family, is sold through a subscription model priced at $1,000 per month. This macOS stealer can extract various types of information from the victim's machine, including Keychain passwords, comprehensive system details, files from the desktop and documents folder, as well as the macOS password.

#3 In contrast, ClearFake is an emerging malware distribution operation that utilizes compromised WordPress sites. It delivers deceptive web browser update notifications to deploy stealers and other malware. The ClearFake campaign has extended its targeting to macOS systems, employing a nearly identical infection chain. It relies on compromised websites to distribute Atomic Stealer, delivering it in the form of a DMG file. ClearFake was disseminated to Mac users, accompanied by a corresponding payload.

#4 The Safari template replicates the official Apple website and is available in various languages. Furthermore, recognizing the prevalence of Google Chrome on Macs, a template tailored for it has been created. Victims are guided on how to open the file, triggering immediate commands after entering the administrative password.

#5 While fake browser updates have been a prevalent concern for Windows users, MacOS users have not encountered consistent threats like AMOS. ClearFake, a notable social engineering campaign, now poses a significant risk to Mac users.

Recommendations

Beware of Deceptive Updates: Exercise caution with web browser updates; be wary of suspicious or unexpected notifications. Avoid clicking on links from unknown sources. Verify updates directly from official sources. This manual verification process ensures authenticity, reducing the risk of falling victim to phishing or malware distribution through deceptive pop-up notifications.

Monitor Network Traffic: Utilize network monitoring tools to scrutinize incoming and outgoing traffic, identifying potential Port Knocking attempts or irregular communication patterns. This can help detect and thwart attackers attempting to establish connections with their command-and-control servers.

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.

Remain vigilant: 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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0011** Command and Control	**T1560** Archive Collected Data	**T1574** Hijack Execution Flow
T1659 Content Injection	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1204** User Execution
T1176 Browser Extensions	**T1543** Create or Modify System Process	**T1211** Exploitation for Defense Evasion	**T1562** Impair Defenses
T1055 Process Injection	**T1555** Credentials from Password Stores	**T1212** Exploitation for Credential Access	**T1105** Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	longlakeweb[.]com, thebestthings1337[.]online, chalomannoakhali[.]com, jaminzaidad[.]com, royaltrustrbc[.]com, wifi-ber[.]com
IPv4	194.169.175[.]117
SHA256	4cb531bd83a1ebf4061c98f799cdc2922059aff1a49939d427054a556e89f464, be634e786d5d01b91f46efd63e8d71f79b423bfb2d23459e5060a9532b4dcc7b, 5b5ffb0d2fb1f2de5147ec270d60a3ac3f02c36153c943fbfe2a3427ce39d13d

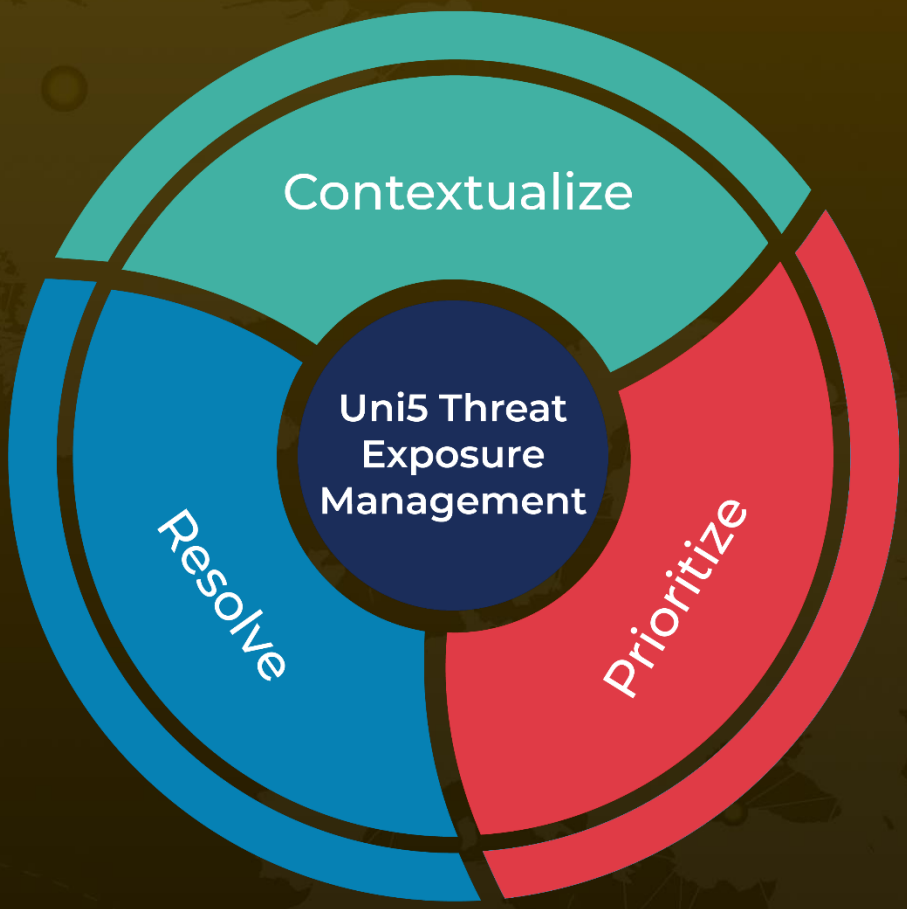
References

https://www.malwarebytes.com/blog/threat-intelligence/2023/11/atomic-stealer-distributed-to-mac-users-via-fake-browser-updates

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

November 23, 2023 . 2:00 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com