9 September 2025

INTEL471

EMERGING THREATS

AMOS Stealer

AMOS Stealer, also referred to as Atomic Stealer, is a sophisticated macOS-targeting infostealer that has emerged as a persistent threat to individuals and organizations over the past several months. First emerging in 2023, the malware is primarily designed to exfiltrate sensitive information, including browser-stored credentials, system configuration details, cryptocurrency wallet data, and other personal or proprietary files. It was originally observed leveraging phishing campaigns and malicious payloads distributed via compromised applications or social engineering, however it has evolved to adopt a modular architecture, allowing operators to dynamically extend its capabilities based on targeted environments. This evolution demonstrates a shift toward more persistent and evasive operations, including the use of code-signing bypasses and stealth techniques that avoid macOS security controls, increasing the likelihood of prolonged undetected compromise. It is worth noting that several variants derived from AMOS stealer's codebase have also emerged, adding new functionality and features, such as Odyssey Stealer, SHAMOS, Banshee Stealer, and Cthulhu Stealer.

THREAT SUMMARY

AMOS Stealer, also referred to as Atomic Stealer, is a sophisticated macOS-targeting infostealer that has emerged as a persistent threat to individuals and organizations over the past several months. First emerging in 2023, the malware is primarily designed to exfiltrate sensitive information, including browser-stored credentials, system configuration details, cryptocurrency wallet data, and other personal or proprietary files. It was originally observed leveraging phishing campaigns and malicious payloads distributed via compromised applications or social engineering, however it has evolved to adopt a modular architecture, allowing operators to dynamically extend its capabilities based on targeted environments. This evolution demonstrates a shift toward more persistent and evasive operations, including the use of code-signing bypasses and stealth techniques that avoid macOS security controls, increasing the likelihood of prolonged undetected compromise. It is worth noting that several variants derived from AMOS stealer's codebase have also emerged, adding new functionality and features, such as Odyssey Stealer, SHAMOS, Banshee Stealer, and Cthulhu Stealer.

The threat has been observed targeting users across North America, Europe, and parts of Asia, with a specific focus on technology, finance, and enterprise sectors where access to sensitive intellectual property or credentials has high operational value. In addition to exfiltrating data, AMOS Stealer enables malicious actors to gain lateral movement within macOS-centric environments, maintain persistent access via launch agents and hidden directories, and potentially leverage stolen credentials to escalate privileges or compromise associated network resources. The malware’s activity poses significant operational, reputational, and financial impacts, particularly for organizations relying on Apple devices for sensitive communications or operational workflows. As such, AMOS Stealer represents a growing macOS-specific threat, emphasizing the need for proactive endpoint monitoring, application integrity controls, and credential management hygiene.

SYNOPSIS

AMOS Stealer operates by exploiting common macOS persistence and evasion techniques, delivering its payload in a manner designed to evade native security mechanisms. Once executed, the malware installs itself into hidden directories and registers as a launch agent, enabling automatic execution each time it is booted. Researchers have noted that the malware has been observed to use encrypted communication channels to exfiltrate data to remote command-and-control (C2) servers, often employing TLS or HTTP-based protocols to blend with normal network traffic. AMOS Stealer's modular design allows the malware to selectively retrieve targeted information, such as saved passwords, browser history, cookies, and cryptocurrency wallet keys, depending on the configuration pushed from the C2 server.

In addition to data exfiltration, AMOS Stealer can manipulate system settings and monitor user activity to expand the scope of its operations. For instance, the malware can detect the presence of security tools and terminate or bypass them to avoid detection. It also gathers system profiling information, such as macOS version, installed software, and network configurations, which can be leveraged for further exploitation or lateral movement. Notably, researchers observed instances of AMOS Stealer dropping secondary payloads or backdoor components, which allow operators to maintain long-term access and execute arbitrary commands on compromised systems. This combination of credential theft, system reconnaissance, and persistent access establishes AMOS Stealer as a versatile tool for cybercriminals seeking to compromise macOS environments for espionage, financial gain, or the preparation of subsequent attacks.

AMOS STEALER COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('f9a4697f-7528-416d-8095-4744a60c337c'),touched:!t)

RELATED HUNT PACKAGES

INLINE APPLESCRIPT EXECUTION ON MACOS - POTENTIAL UNAUTHORIZED SCRIPT ACTIVITY

https://hunter.cyborgsecurity.io/research/hunt-package/d107f7b0-8c1c-4325-86de-538d68ad5d95

SYSTEM PROFILER USAGE FOR MACOS RECONNAISSANCE - POTENTIAL INFORMATION GATHERING

https://hunter.cyborgsecurity.io/research/hunt-package/e4dda283-e868-49b1-b90e-57a83e40744c

USAGE OF CHMOD TO ENABLE EXECUTION - POTENTIAL PAYLOAD STAGING

https://hunter.cyborgsecurity.io//research/hunt-package/dfbdc565-a37c-472b-a4c7-6c0e5325b255

BASE64 ENCODED COMMAND EXECUTION

https://hunter.cyborgsecurity.io/research/hunt-package/2c6de808-b4c2-4f49-a496-ce4c25e1202d

USE OF DSCL ON ROOT USER - POTENTIAL CREDENTIAL TESTING VIA SHELL

https://hunter.cyborgsecurity.io/research/hunt-package/e3733627-b5ca-47d1-8765-1007511ff19c

PLIST FILE CREATED IN COMMON LAUNCH AT BOOT FOLDERS IN MACOS - POTENTIAL PERSISTENCE

https://hunter.cyborgsecurity.io/research/hunt-package/6345f730-3b8a-4e7a-8a6f-a68aff660ad8

COMMONLY ABUSED MACOS VOLUMES NAMES LOADED IN THE BACKGROUND - POTENTIAL MALICIOUS PACKAGE

https://hunter.cyborgsecurity.io/research/hunt-package/4d4a2bf5-fa4f-4e0c-9f24-564799bfb8a8

MITRE CONTEXT

- Exploits Vulnerabilities:
  - CVE-2021-4436
  - CVE-2025-0282
  - CVE-2024-3400
- MITRE Tactic Names:
  - Discovery
  - Privilege Escalation
  - Defense Evasion
  - Persistence
  - Execution
- MITRE Technique Names:
  - Software Discovery
  - System Information Discovery
  - Local Accounts
  - Hidden File System
  - Startup Items
  - Linux and Mac File and Directory Permissions Modification
  - Obfuscated Files or Information
  - Masquerading
  - Peripheral Device Discovery
  - System Checks
  - AppleScript
  - Plist File Modification
  - PowerShell
  - Local Account
- MITRE Technique IDs:
  - T1036
  - T1120
  - T1082
  - T1222.002
  - T1518
  - T1027
  - T1087.001
  - T1059.002

  - T1647
  - T1497.001
  - T1564.005
  - T1059.001
  - T1037.005
  - T1078.003
- Threat Names:
  - AMOS Stealer

REFERENCES

1. https://moonlock.com/amos-backdoor-persistent-access
2. https://unit42.paloaltonetworks.com/macos-stealers-growing/
3. https://www.jamf.com/blog/signed-and-stealing-uncovering-new-insights-on-odyssey-infostealer/
4. https://thehackernews.com/2025/06/new-atomic-macos-stealer-campaign.html
5. https://www.infosecurity-magazine.com/news/macos-infostealer-amos-backdoor/
6. https://titan.intel471.com/report/inforep/08481597e3f6b6444f6997d6d0133eca
7. https://titan.intel471.com/report/fintel/afd5c4b81c7b8f41603d94f5456b8d5c