ClickLock macOS Malware Steals Credentials and Installs Persistent Backdoor

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

ClickLock is a new information-stealing malware that targets Apple Mac computers. It steals credentials and installs a backdoor that gives attackers continued remote access to the device.

Overview

ClickLock is a new information-stealing malware that targets macOS, the operating system used by Apple Mac computers. Group-IB identified at least 100 victims across 33 countries, with most located in Europe and North America.

The attack likely begins with a fake Cloudflare verification page that tells the user to paste a command into Terminal. This method is known as the ClickFix technique. Running the command downloads additional malware components in the background.

A fake macOS password prompt then appears with the victim's real username. If the user cancels it, the malware creates LaunchAgents that restart its credential-stealing components at the next login. It can also repeatedly close applications and continue displaying the password prompt.

The stolen information may include macOS login passwords, browser credentials, session cookies, Keychain data, password-manager information, and cryptocurrency wallets. Collected data is sent through Telegram, while a modified GSocket backdoor gives the attacker continued remote access to the device.

This attack does not exploit a macOS vulnerability or initially require administrator privileges. There is no security update for ClickLock because the user must run the malicious command for the infection to begin.

Affected Systems

- Devices on which a user runs the malicious Terminal command

***Note**: No specific macOS version has been associated with the campaign.*

Aspire Protects

- Instruct users never to paste Terminal commands provided by a website. Legitimate Cloudflare verification takes place within the browser.
- Alert on repeated pkill or killall activity targeting Finder, Dock, Terminal, Activity Monitor, and web browsers.
- Monitor for osascript password prompts and shell processes requesting Chrome Safe Storage data.
- Search for the listed LaunchAgents, hidden directories, hashes, and network indicators.
- If compromise is suspected, isolate the Mac and revoke active browser sessions. Reset exposed credentials from a clean device after the malware has been removed.
- If the GSocket backdoor is present, follow incident-response procedures to rebuild the affected device.

TTPs to Watch

Execution

- User Execution: Malicious Copy and Paste [T1204.004] – An attacker may use a fake verification page to convince a user to paste a malicious command into Terminal.
- Command and Scripting Interpreter: Unix Shell [T1059.004] – An attacker may use shell scripts to execute ClickLock and download its components.

Persistence

- Create or Modify System Process: Launch Agent [T1543.001] – An attacker may create LaunchAgents that restart the credential-stealing components when the user logs in.

Credential Access

- Input Capture: GUI Input Capture [T1056.002] – An attacker may display a fake macOS password prompt to capture the user's login password.
- Credentials from Password Stores: Keychain [T1555.001] – An attacker may obtain the Chrome Safe Storage encryption key from macOS Keychain.
- Credentials from Password Stores: Credentials from Web Browsers [T1555.003] – An attacker may collect saved passwords, cookies, and other authentication data from browser profile files.

Exfiltration

- Exfiltration Over Web Service: Exfiltration to Cloud Storage [T1567.002] – An attacker may upload credentials and archived data through the Telegram Bot API.

IoCs

Domains and Network Infrastructure

- panalobet[.]ph
- store[.]grafsynergy[.]com
- cottonbox[.]co[.]il
- gsnc[.]eu:67

Files and Directories

- ~/.cacheb/
- ~/Library/LaunchAgents/com.authirity.plist
- ~/Library/LaunchAgents/com.chromer.plist
- ~/Library/Application Support/iCloudsync

SHA-1 Hashes

- d9617710d4ed8e9b87f6fee0b7014c4101effba0
- b67aa4f598c0ea625a7409ea7884e10a7bc9c3ff
- 8dda05168ea8610a2449419a47517bc32823d6ec
- 0a1fb016bd10bac5455175c79aa4511e5ff1a330
- 2fc970e25570532f9cbe33b7ebfe1f0383a7341a

Targeted Industries

Cryptocurrency users appear to be the primary targets, but any organization with employees who use Mac computers could be impacted.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

ClickLock Stealer: Paste Once, Lose Everything | Group-IB Blog

ClickLock Stealer malware