LastPass Warns of macOS Atomic Stealer Campaign

TL;DR

Threat actors are using fraudulent GitHub repositories optimized with SEO to impersonate well-known apps (LastPass, 1Password, Dropbox, Adobe, SentinelOne, etc.) and trick macOS users into installing the Atomic Stealer (AMOS).

The campaign relies on "ClickFix" tactics (instructing victims to paste malicious commands into Terminal) and is actively delivering malware. AMOS now includes a backdoor for persistent access.

Overview

LastPass has issued a warning about a widespread campaign using fraudulent GitHub repositories to impersonate popular software, including LastPass, 1Password, Dropbox, Fidelity, Notion, SentinelOne, Adobe, and others. The fraudulent repositories are SEO-optimized to appear at the top of Google and Bing search results. This is known as SEO poisoning.

The campaign leverages ClickFix attack, which is when users are instructed to paste a command into Terminal, which executes a curl request to a base64-encoded URL. This delivers the Atomic macOS Stealer (AMOS) malware (install.sh > /tmp), followed by an "Update" payload. AMOS, offered as malware-as-a-service, is capable of stealing credentials, browser data, crypto wallets, and system files. Recent versions also add a backdoor component for persistence.

.

The threat is less about a new exploit and more about user behavior. Attackers are hoping that someone will trust a search result or GitHub repository without checking if it's official.

Aspire Protects

- Add known malicious domains and GitHub repositories to web filters and blocklists.
- Search endpoints for /tmp/install.sh, /tmp/update, suspicious curl | bash commands, and the AMOS SHA256 hash.
- Configure EDR detections for Terminal spawning curl/base64 commands and persistence agents.
- Warn macOS users not to download software from unverified GitHub repos or paste Terminal commands from search results.

- Rotate credentials used on potentially compromised systems.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may use SEO-boosted GitHub repositories to impersonate trusted vendors.

Execution

- User Execution [T1204] – The attacker may rely on victims pasting malicious Terminal commands (ClickFix).

- Command and Scripting Interpreter [T1059] – The attacker may run arbitrary commands after exploitation.

Persistence

- Boot or Logon Autostart Execution [T1547] – The attacker may establish long-term persistence through AMOS's backdoor.

Credential Access

- Credentials from Password Stores [T1555] – The attacker may target password managers and browser-stored secrets.

IoCs

Domains / URLs

- github[.]com/lastpass-on-macbook
- github[.]com/LastPass-on-MacBook/lastpass-premium-mac-download
- ahoastock825[.]github[.]io/.github/lastpass
- macprograms-pro[.]com/mac-git-2-download.html
- bonoud[.]com/get3/install.sh
- bonoud[.]com/get3/update

File Hash

- e52dd70113d1c6eb9a09eafa0a7e7bcf1da816849f47ebcdc66ec9671eb9b350

Targeted Industries

The LastPass Atomic Stealer campaign threatens any organization with macOS endpoints and employees who may download software from unverified sources.

- Education
- Energy
- Financial
- Healthcare
- 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

Brewing Trouble — Dissecting a macOS Malware Campaign | by Dhiraj | Deriv Tech | Medium

Large-Scale Attack Targeting Macs via GitHub Pages Impersonating Companies to Attempt to Deliver Stealer Malware