FRIGIDSTEALER – NEW MACOS MALWARE DELIVERED VIA FAKE BROWSER UPDATES

Vairav Cyber Security News Report

Date: February 19, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

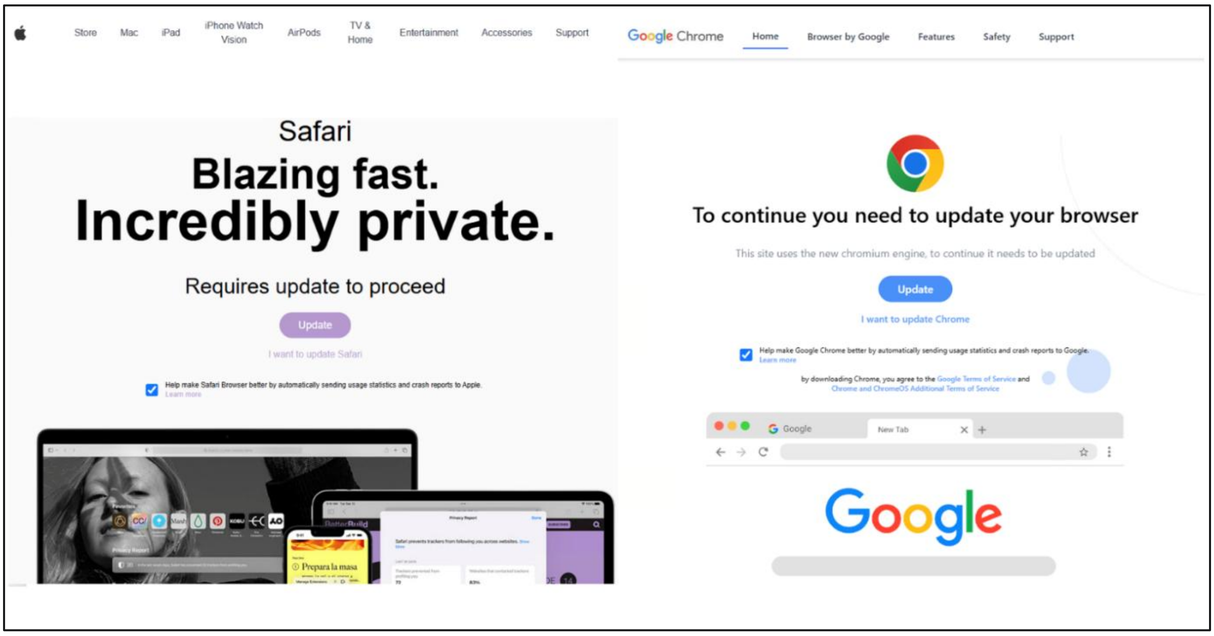
Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

The landscape of malicious website injects has become more complex, with multiple threat actors leveraging JavaScript injects, Traffic Distribution Systems (TDS), and malware payloads to target victims. These attack chains typically involve malicious scripts embedded in compromised websites, which then redirect users to malware downloads based on filtering criteria. **TA2727** was recently observed delivering **FrigidStealer**, a new macOS information stealer, alongside Lumma Stealer for Windows and the Marcher banking trojan for Android. Meanwhile, TA2726 has been identified as a TDS operator, facilitating malware distribution for both TA569 and TA2727. The interconnected nature of these threat actors underscores the growing complexity of web-based malware delivery campaigns.



Safari

Blazing fast.
Incredibly private.

Requires update to proceed

☑ Help make Safari Browser better by automatically sending usage statistics and crash reports to Apple.

To continue you need to update your browser

This site uses the new chromium engine, to continue it needs to be updated

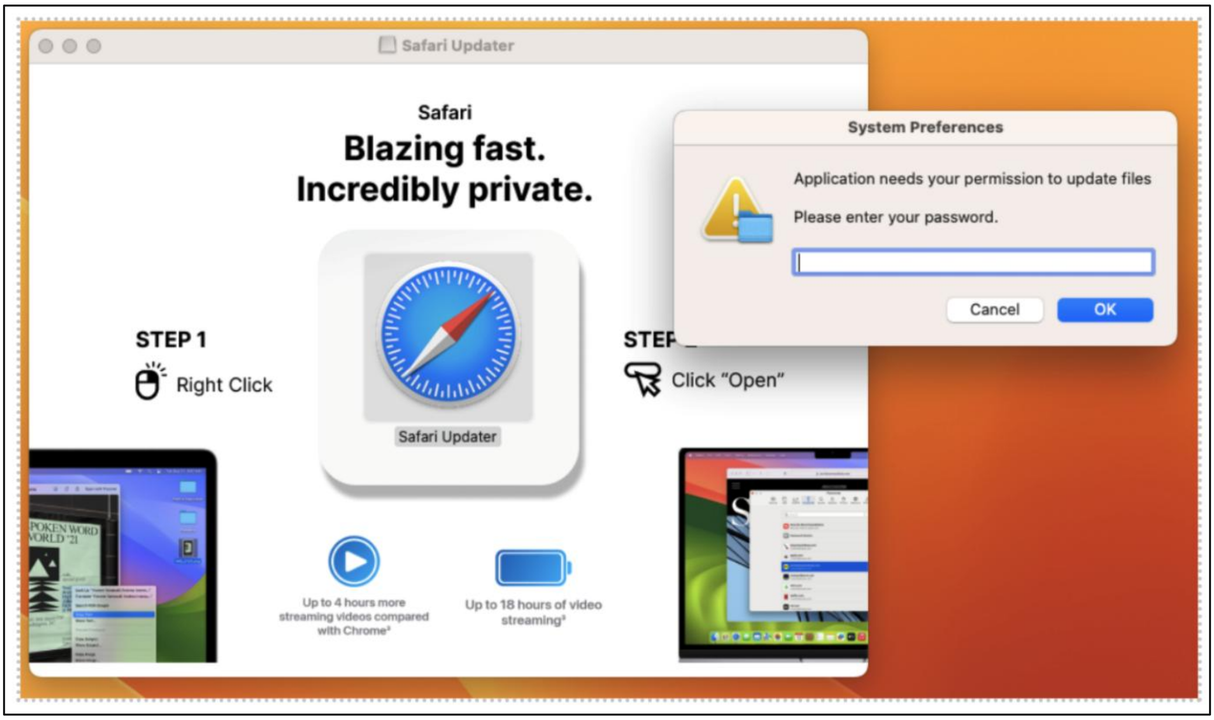
☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google.

by downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service

Figure 1: Fake update lure delivering FrigidStealer via Safari (left) and Chrome (right)

DETAILS OF THE INCIDENT

TA2727 is a financially motivated threat actor known for distributing various malware families via compromised websites with malicious JavaScript injects. The group collaborates with TA2726, a traffic distribution system (TDS) operator that helps distribute malware, and TA569, responsible for delivering SocGholish (FakeUpdates). This campaign spoofs browser update pages to trick users into downloading malware payloads. The latest variant, FrigidStealer, is designed to target macOS users. The activity was detected by the Proofpoint Threat Research Team, which observed new fake update campaigns targeting macOS users in January 2025. The FrigidStealer installer requires explicit user execution to bypass macOS Gatekeeper protections, after which it uses AppleScript to gain elevated privileges.



Application needs your permission to update files

Please enter your password.

Figure 2: Malicious "Safari Updater" with the System Preferences prompt to enter the password

This recent wave of attacks primarily impacts macOS users outside North America, who were previously unimpacted by such campaigns. Additionally, Windows users are being targeted with Lumma Stealer via Hijack Loader (DOILoader), while Android users are at risk of infection with the Marcher banking trojan, posing significant security threats across multiple platforms.

Impact Analysis

The potential impact of this campaign is significant, as FrigidStealer is designed to steal sensitive data, including credentials, browser information, and other private details. Additionally, financial loss is a major concern, as malware specifically targets cryptocurrency-related applications. The malware also compromises system integrity by gaining elevated privileges through AppleScript prompts, allowing it to operate with enhanced access. The exploitation methods primarily involve web injects, where malicious JavaScript code is embedded into compromised websites, and fake browser updates, which deceive victims by redirecting them to spoofed Chrome or Safari update pages.

However, user interaction is required for successful infection on macOS, as victims must manually approve the installation, bypassing Gatekeeper protection.

RECOMMENDED ACTIONS

Immediate Mitigation Steps:

- Block Malicious Domains & IPs at the firewall and endpoint security solutions.
- Avoid Fake Browser Updates – Download software only from official vendor sites.
- Alert Employees & Users about fake update campaigns and suspicious redirects.

Security Best Practices:

- Enable Multi-Factor Authentication (MFA) on critical accounts.
- Use Endpoint Protection Software to detect and prevent malware infections.
- Configure macOS to allow applications only from trusted developers.

For Advanced Security Teams:

- Deploy Threat Hunting Techniques using SIEM/XDR platforms.
- Monitor for Anomalies in browser-based downloads and AppleScript execution.
- Patch & Harden Systems against malicious exploits.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://www.proofpoint.com/us/blog/threat-insight/update-fake-updates-two-new-actors-and-new-mac-malware

https://thehackernews.com/2025/02/new-frigidstealer-malware-targets-macos.html

https://www.hendryadrian.com/an-update-on-fake-updates-two-new-actors-and-new-mac-malware/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com