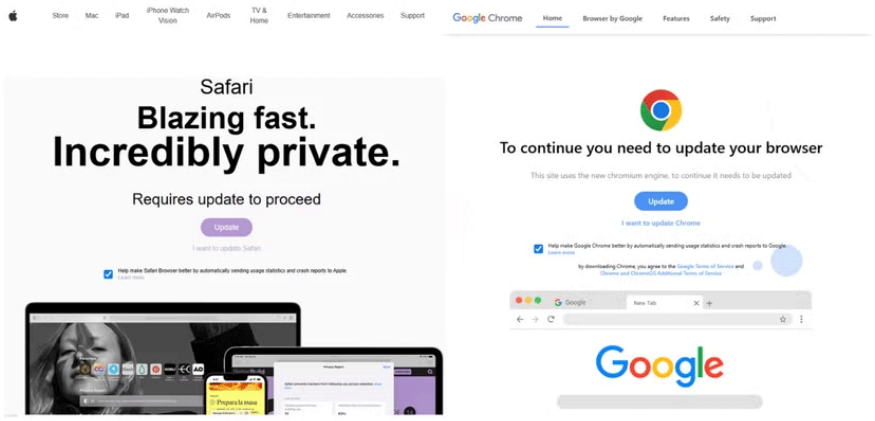
New FrigidStealer Malware Spreads Through Fake Browser Updates on Macs

It may come as a surprise to some Mac fans, but cybercriminals are still actively looking for ways to attack macOS.

It may come as a surprise to some Mac fans, but cybercriminals are still actively looking for ways to attack macOS.

New FrigidStealer Malware Spreads Through Fake Browser Updates

A new malware strain, FrigidStealer, was recently discovered by Proofpoint and highlighted by AppleInsider.



This malware is designed to steal information from users' Macs. Using compromised websites that appear legitimate, criminals will redirect you to a fake browser update page. As you can see in the image, the pages look legitimate at first glance.

If you click the Update button, the DMG file will download to your Mac. The installation instructions also look very official—when you follow them, they will bypass Gatekeeper, which is a Mac security feature that warns you that an app is unsigned and untrusted.

The final step of the 'installation' requires you to enter your Mac password. Proofpoint explains what happens after execution:

Once executed, FrigidStealer uses Apple and osascript script files to prompt the user for their password, then collects data including browser cookies, files with extensions related to password documents or

cryptocurrencies from the victim's Desktop and Documents folders, and any Apple Notes the user has created.

All that data is then sent to another compromised website.

Mac users still need to stay up to date on security

One of the biggest draws of Apple products, including Macs, is their focus on security. But as this social engineering campaign shows, bad actors can sometimes create a believable scenario that can fool someone.

There are several ways you can protect yourself from this very scary malware. First, be careful about the files you download from online sources. While Gatekeeper is a great feature of Macs, it can sometimes be bypassed, like FrigidStealer. If you're worried, there are a few quick websites that will tell you whether a link is safe before you download it.

Another way to stay protected at all times is to use antivirus software. Instead of spending money, you can find some great free antivirus options for your Mac.