Mphasis
The Next Applied

Fake Google Chrome Update Popups Aim for Hundreds of Websites

Date: 7th June 2024 | Severity: High

Summary

Fake Browser Update campaigns are known for their deceptive tactics used by hackers to trick users into downloading malicious software. These campaigns typically involve injecting malicious code into a website, which then displays a popup message urging users to update their web browser. Clicking on the provided link usually results in downloading malware, such as a remote access trojan or an infostealer.

One of the most notorious examples of this type of malware is SocGholish. However, our research team has been tracking a new campaign that has been active since late April 2024. This campaign follows a similar pattern but includes some unique characteristics that make it particularly concerning.

Attack Vectors

- The infection process for this new fake browser update campaign begins with the injection of malicious code into vulnerable websites. Once the website is compromised, visitors are presented with the following misleading popup message a few seconds after the webpage loads.
- The message, written in poor English, reads: Warning Exploit Chrome Detect. Update Chrome Browser and includes a large blue Update button. The pop-up is displayed even to users who are not using the Chrome browser, highlighting its deceptive (and amateurish) nature.When a user clicks on the Update button, they are redirected to one of several malicious URLs designed to initiate a malware download
- The malicious code injected into compromised websites is designed to execute a popup message using the following legitimate WordPress plugin: Hustle – Email Marketing, Lead Generation, Optins, Popups This plugin is commonly used for creating popups and opt-in forms, making it an ideal tool for attackers to exploit.

Indicator of compromise

INDICATOR TYPE	INDICATORS
URLs	• hxxps[:]//photoshop-adobe[.]shop/download/dwnl.php • hxxps[:]//brow-ser-update[.]top/download/dwnl.php • hxxps[:]//tinyurl[.]com/uoiqwje3
Domain	• brow-ser-update[.]top • photoshop-adobe[.]shop
IP address	• 185.196.9[.]156

Recommendation

- Employ a "use it or lose it" policy on your website. That means regularly review all plugins and remove any components that you don't recognize or aren't in use.
- Generate strong and unique passwords for all of your accounts, including admins, FTP, database, and hosting.
- Regularly monitor your website and check for suspicious activity or unexpected website admin users.
- Consider using 2FA and restricting access to your WordPress admin and sensitive pages to allow access to only trusted IP addresses.
- Always keep your website software patched and up-to-date, including your core CMS, plugins, themes, or any other extensible components.
- Use a web application firewall to help prevent vulnerability exploits, malicious code, and hack attempts.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://blog.sucuri.net/2024/06/hundreds-sites-targeted-by-fake-chrome-update-pop-ups.html
- https://cybersecuritynews.com/beware-of-fake-google-chrome-update/
- https://securityonline.info/beware-of-fake-google-chrome-update-pop-ups-malicious-campaign-targets-hundreds-of-websites/