What is malvertising? How to prevent malvertising?

Attackers are attempting to compromise web browsers and browser plugins. Malvertising, which uses third-party ad networks to embed attacks on legitimate websites, is becoming increasingly common. To learn more about what malvertising is and how to prevent it, please continue reading the article below from TipsMake.

Malvertising is not advertising, but rather software that can easily compromise systems when users click on links that redirect to malicious websites.

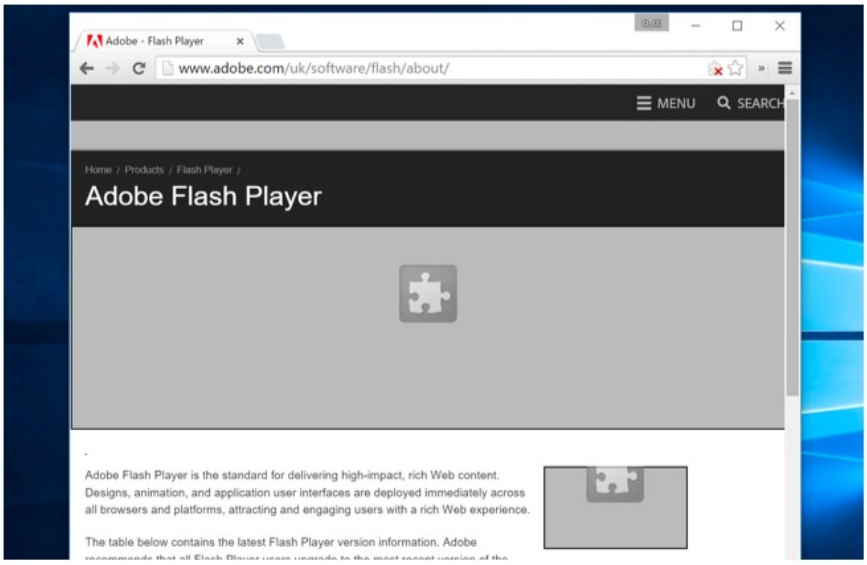
This article from TipsMake will answer your questions about what malvertising is and ways to prevent it.

1. Web browsers and plugins are under attack.

There are two ways attackers can compromise a user's system. One is by tricking the user into downloading and running malicious software or something similar. The second is by attacking web browsers and plugins such as Adobe Flash, Oracle Java, and Adobe PDF reader. These attacks exploit security vulnerabilities in the software to force the user's computer to download and run malware.

If the system is vulnerable—because an attacker exploits a zero-day vulnerability in software that the user hasn't installed or updated with security patches—the user only needs to access a website containing malicious code to allow the attacker to infiltrate and infect the system.

These malware programs often take the form of malicious Flash objects in Java applets. Clicking on the link will redirect users to malicious websites to compromise the system.



2. What is malvertising?

Instead of trying to trick users into visiting a malicious website, malvertising uses ad networks to spread malicious Flash objects and other malicious code to other websites.

The attackers upload Flash objects and other malicious code to advertising networks, paying the network to distribute this malware as legitimate advertisements.

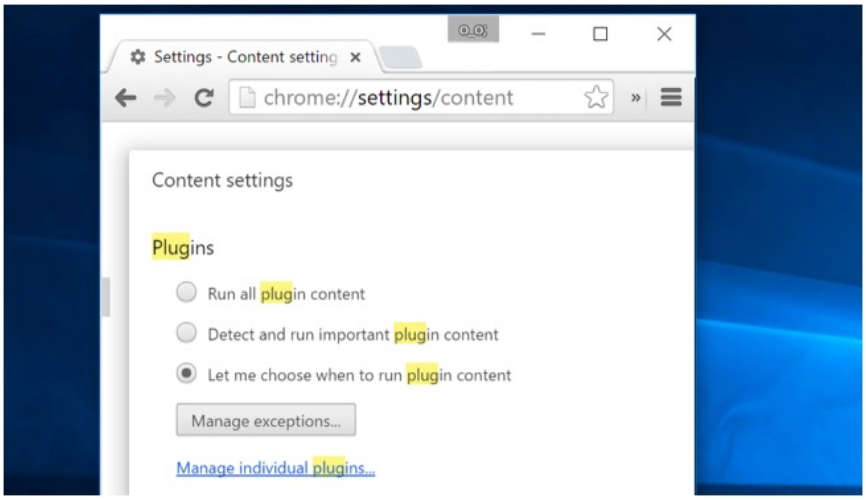
Users can access a website, and the ad script on that website will download an ad from the network. The malicious ad then attempts to compromise the user's web browser. This is precisely how an attack using Yahoo's ad network to serve malicious Flash ads worked.

It's the core of malvertising – exploiting vulnerabilities in the software users are using to infect legitimate websites. Besides malvertising, users can also be infected in a similar way by clicking on links on malicious websites. Security vulnerabilities are the core issue here.

3. Ways to prevent Malvertising

Even if your browser doesn't reload ads, TipsMake still recommends applying some of the following tricks to protect your browser and system from common online attacks:

- Enable the Click-to-Play plugin: Make sure you have enabled the Click-to-Play plugin in your web browser. When you visit a website containing Flash or Java elements, they won't automatically play unless you click on them. Most malicious ads use this plugin.



- Using MalwareBytes Anti-Exploit : Essentially, MalwareBytes Anti-Exploit is a user-friendly software designed to replace Microsoft's EMET antivirus, primarily targeting businesses with its ability to eliminate malware and protect user data. While Microsoft's EMET can be used, TipsMake recommends MalwareBytes Anti-Exploit as an anti-exploit program.

Download and install **MalwareBytes Anti Exploit here.**

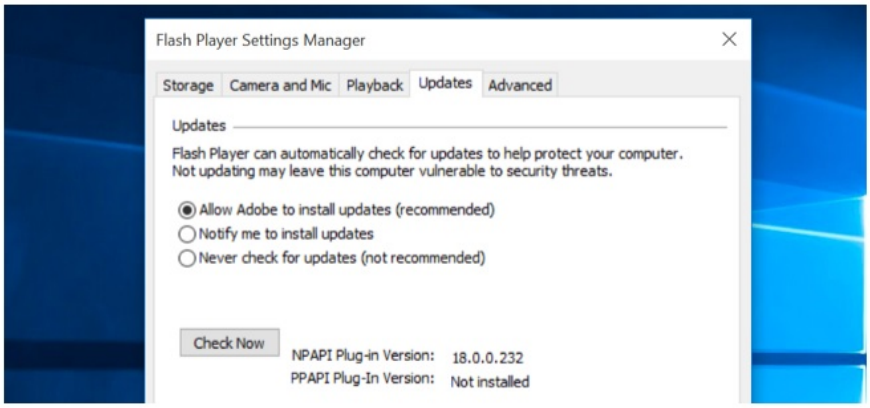
This software does not function as antivirus software. Instead, MalwareBytes Anti-Exploit monitors the user's web browser and tracks the browser exploits being used.

MalwareBytes Anti-Exploit is free software that can run alongside other antivirus programs to protect users from browser and plugin exploits, and even zero-day vulnerabilities.

- Disable or uninstall browser plugins you don't use frequently, including Java: If you don't use browser plugins often, it's best to uninstall them. This reduces the risk of potential software attacks. Additionally, TipsMake recommends disabling or uninstalling the Java plugin, which has several security vulnerabilities.

If Adobe Flash is successfully removed along with Java, it will be more difficult for malicious advertisements to infiltrate and infect users' computers.

- Update browser plugins: Regularly update the plugins you have installed to ensure you have the latest security patches. Both Google Chrome and Microsoft Edge automatically update Adobe Flash. Internet Explorer on Windows 8, 8.1, and 10 also automatically updates Flash. If you are using Internet Explorer, Mozilla Firefox, or Opera on Windows 7, you will need to configure these browsers to automatically update Adobe Flash. Adobe Flash options are available in the Control Panel or in the System Preferences window on a Mac.

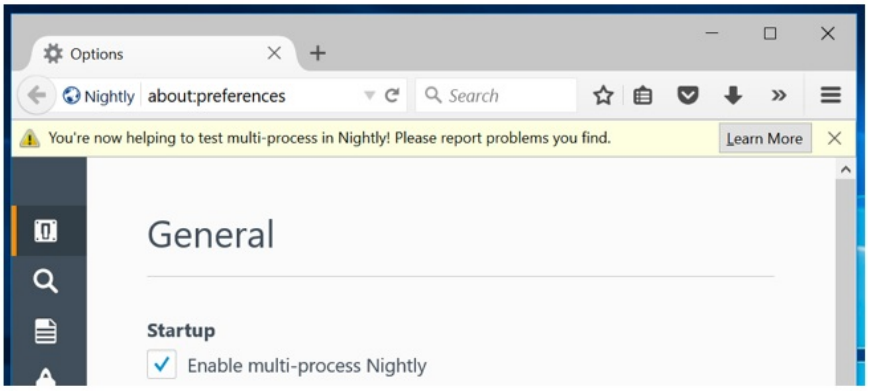


- Update your browser to the latest version: While most malvertising attacks target plugins, a small number also target web browsers. Therefore, in addition to updating plugins, ensure your web browser is also updated to the latest version. If you are using Internet Explorer, make sure Windows Update is enabled and regularly install the latest updates.

- Limit your use of Firefox until Electrolysis is complete : web browsers like Google Chrome, Internet Explorer, and Microsoft Edge all utilize sandbox technology to prevent browser exploitation and unauthorized access to users' systems.

A recent malvertising exploit targets a zero-day vulnerability in the Firefox browser.

Despite years of delays, a sandbox was finally implemented in Firefox as part of the Electrolysis project. The multi-processing feature was included in the stable version of Firefox in late 2015 and is now available in unstable versions. However, this is not enough to guarantee that malicious ad attacks targeting Firefox will not occur.



Therefore, if you are using Firefox to browse the web, TipsMake recommends that you use MalwareBytes Anti-Exploit to protect your device and system.

Currently, almost all malvertising attacks occur primarily on Windows computers. Additionally, recent attacks targeting the Firefox browser have occurred on Firefox for Windows, Linux, and Mac.

The article above from TipsMake has answered your questions about what malvertising is and ways to prevent it. Additionally, if you have any further questions, please leave your comments in the section below the article.

You finished reading the article "**What is malvertising? How to prevent malvertising?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.