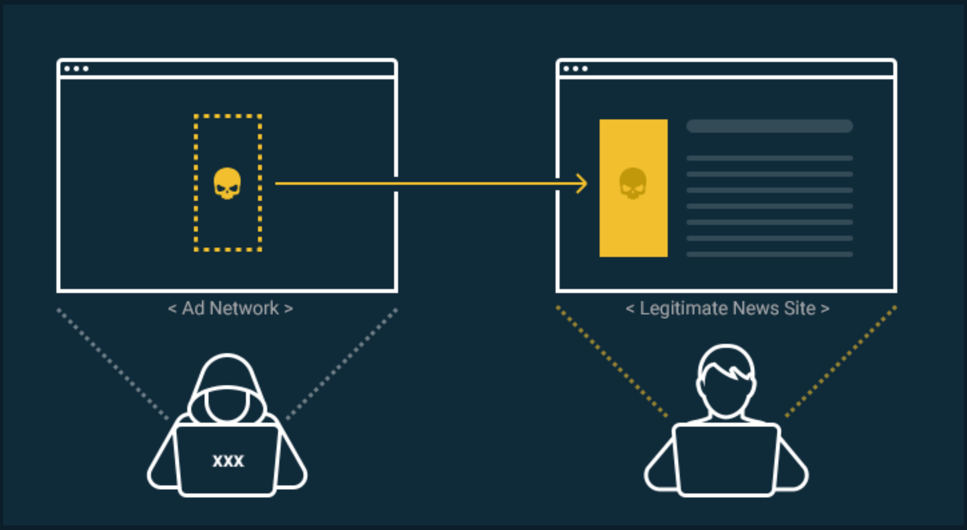
BitDentify

What is Malvertising?

Malvertising (malicious advertising) is the use of online advertising networks to spread infected ads across popular and trusted websites.

These ads will appear on your favorite news site or in your social networks, the look legitimate but will redirect victims to corrupt webpages or install malware on their computer.

How does Malvertising work?



The online advertisement industry is a huge and complex machine with many entities communicating and sharing data.

Publishers and advertisers buy and sell ad space on ad exchanges (known as inventory), advertising networks supply ads across a wide range of websites while ad servers store and deliver online ads. The complexity of these systems makes them ideal targets for a clever hacker.

This is a simple explanation on how a malvertising attack works:

1. A cybercriminal buys ad space on a website or from an ad network.

2. The cybercriminal uploads an infected ad to be displayed in the space they bought, cleverly masking it to look legitimate.

3. The infected ad is displayed on a website you visit, the attack happens when you either:

a. Click the ad, or...

b. Load the website with the ad, many infected ads can attack on their own without the need for a click.

Types of Malvertising

The first example of malvertising was identified in 2007, based around a specific Adobe Flash vulnerability and used to exploit sites like Myspace and Rhapsody. Today malvertising has adapted to the new and complex media landscape, utilizing a myriad of techniques to serve you malware.

Since then malvertising has become more common on all platforms, and increasingly **drive-by downloads** that don't require any direct interaction has become the norm.

Steganography

Steganography is an ancient technique of concealing secret messages in texts or images. Cybercriminals use this technique to hide malicious code within images in ads, in many cases neither advertising networks nor users can tell the difference between real or malvertising ads.

Polyglot images

Just like Steganography, Polyglot images contain malicious code, but also scrips used to execute that code and start the attack. Without the need for external scripts to extract the malware package, Polyglot images are a more potent and dangerous version of Steganography.

Tech-support scams

In this scam, the hackers try to make you believe there is something wrong with your computer. The Tech-support scam ads will install a form of browser-hijack malware that disrupts normal functions, and then tell you to call a number to resolve those issues.

When you call the number to resolve the issues you will be connected to a scammer that try their best to separate you from your money and personal information.

Scareware

Like the tech-support scams, scareware tries to frighten you with popups saying your computer is infected with viruses, promoting you to take action immediately.

You are prompted to download their fake cybersecurity/antivirus software that either collects information about you or infects your computer with malware.

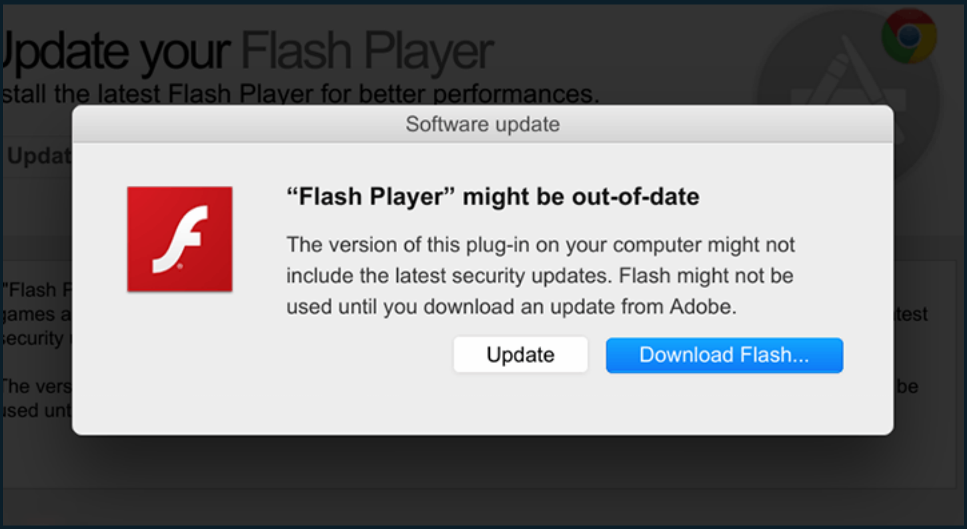
“Get rich quick” schemes and fake surveys

You don’t have to look far to see ads that promises to make you rich if you just complete a medial task, like fill our a form, leave a review or complete a survey. In reality, the only free thing you are likely to get is a computer virus.

Fake software updates

Similar to scareware these ads try to scare you into thinking your computer is at risk since some software is out of date, prompting you to click and download an update. You can be prompted to update your OS or other software you have installed, the update might update your program, but it will also install malware.

How does Malvertising work?



“Flash Player” might be out-of-date

The version of this plug-in on your computer might not include the latest security updates. Flash might not be used until you download an update from Adobe.

With malvertising being often distributed by popular advertisement networks, they make their way to some of the world’s most popular and widely read websites. In recent years malvertising has hit companies like Spotify, MSN, Reuters, The New York Times, YouTube and numerous other websites.

Here are a few of the most prominent examples:

2020 Covid-19 attack
People still using the old outdated Internet Explorer browser was hit with a Covid-19-related malvertising attack, prompting users to click a fake advisory note. The malvertisment installed malware that could steal personal data and passwords of the users.

2019 VeryMal attack

Though short lived, Verymal malvertising attack hit two of the most crucial ad exchanges that supply ads to many top publishing outlets. VeryMal was a steganography-bases attack that targeted Mac users and redirected them to a spoofed website that installed the Shyler Trojan malware, disguised as a Flash update.

2017 RoughTed

With the ability to bypass ad-blockers and evade many anti-virus programs, RoughTed was in a league of its own. Since it had the ability to dynamically create new URL's, it made it particularly difficult to track and deny asses to the domains it was using.

2016 AdGholas attack

Being very cleverly disguised, AdGholas malvertising attack hit Yahoo, MSN and other big-name outlets with fake ads for privacy software. Being steganography-based, the attack redirected users to a malicious landing page that downloaded and installed malware using several Flash exploits.

How to prevent Malvertising

Since malvertising can infect you without requiring clicks or any other interaction, protecting yourself isn't easy. The most thorough step would be to disable ads all together by using an AdBlocker like uBlock Origin with a good browser like Mozilla Firefox.

Use a good antivirus solution

If you're using Windows 10, you don't need another antivirus, and if you're on older Windows systems you can look through this year's AV-tests and choose one of the winners.

Update your software

Vulnerabilities in software is one of the first things hackers look for, malwertising usually takes advantages of these vulnerabilities. Using current and updated software is one of the corner-stones in cybersecurity.

Use a secure browser

Mozilla Firefox is one of the best and most secure browsers out there, and it has an excellent support for plugins.

Use an AdBlocker

An adblocker is a plugin for your browser that, as the name suggest, blocks ads from being shown to you. Using a good adblocker stops malvertising in its tracks, we suggest the adblocker plugin uBlock Origin since it's open source.

Think before you click

Learn how to detect a fake website by learning the telltale signs of spoofing, such as lack of HTTPS, misspell URL's, lack of a privacy policy and incomplete terms and conditions pages. If you are unsure you can always check the website on Googles Safe Browsing checker.

Original post can be found at our homepage:
https://bitidentify.com/blog/what-is-malvertising/