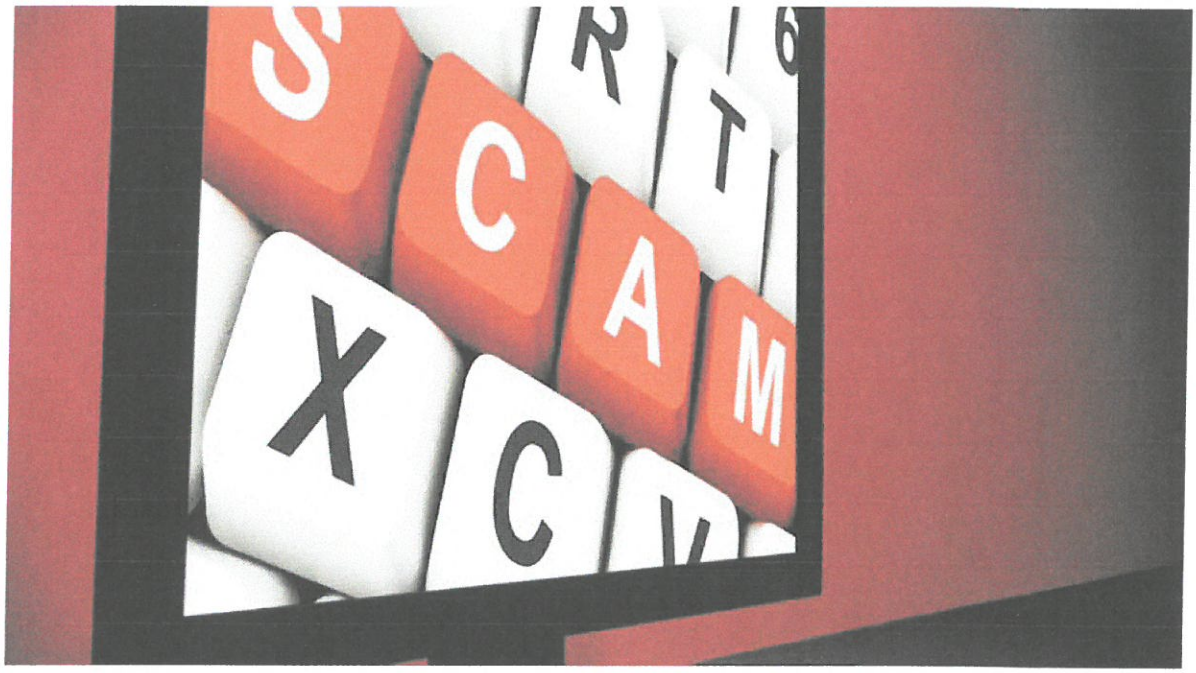
HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-10

GOOGLE ADS LEAD TO MAJOR MALVERTISING CAMPAIGN



1. Background:

Fraudsters have long been leveraging the shady corners of the internet to place malicious ads, leading users to various scams. However, every now and then we see a campaign that goes mainstream and targets some of the world's top brands.

As a case in point, we recently uncovered a malvertising chain abusing Google's ad network to redirect visitors to an infrastructure of tech support scams. Unsuspecting users searching for popular keywords will click an advert and their browser will get hijacked with fake warnings urging them to call rogue Microsoft agents for support.

What makes this campaign stand out is the fact that it exploits a very common search behavior when it comes to navigating the web: looking up a website by name instead of entering its full URL in the address bar.

2. What is Malvertising?

Malvertising — or **malicious advertising** — is a relatively new cyberattack technique that injects malicious code within digital ads. Difficult to detect by both

internet users and publishers, these infected ads are usually served to consumers through legitimate advertising networks. Because ads are displayed to all website visitors, virtually every page viewer is at risk of infection.

Malvertising attacks can be complex in nature, leveraging many other techniques to carry out the attack. Typically, the attacker begins by breaching a third-party server, which allows the cybercriminal to inject malicious code within a display ad or some element thereof, such as banner ad copy, creative imagery or video content.

Once clicked by a website visitor, the corrupted code within the ad will install malware (malicious software) or adware on the user's computer. The attacker may also redirect the user to a malicious website and leverage spoofing or social engineering techniques to advance the attack.

Malvertising attacks may also execute an exploit kit, which is a form of malware that is designed to scan the system and exploit vulnerabilities or weaknesses within the system.

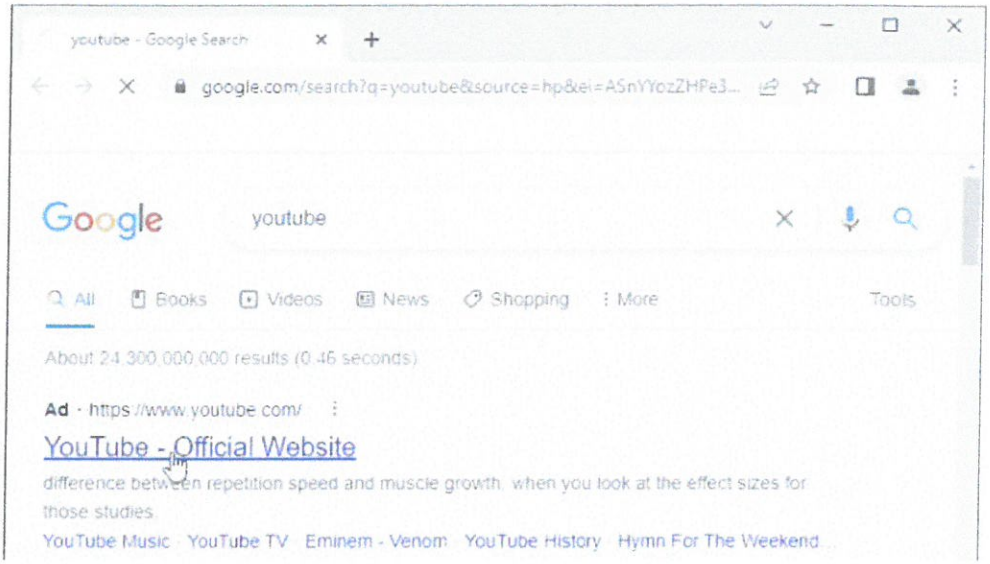
Upon installation, the malware delivered via malvertising attacks operates as any other form of malware. It can damage files, redirect internet traffic, monitor the user's activity, steal sensitive data or set up backdoor access points to the system. Malware may also be used to delete, block, modify, leak or copy data, which can then be sold back to the user for ransom or on the dark web.

Though somewhat less common, it is possible to conduct a malvertising attack without having the user interact with the ad. These attacks include:

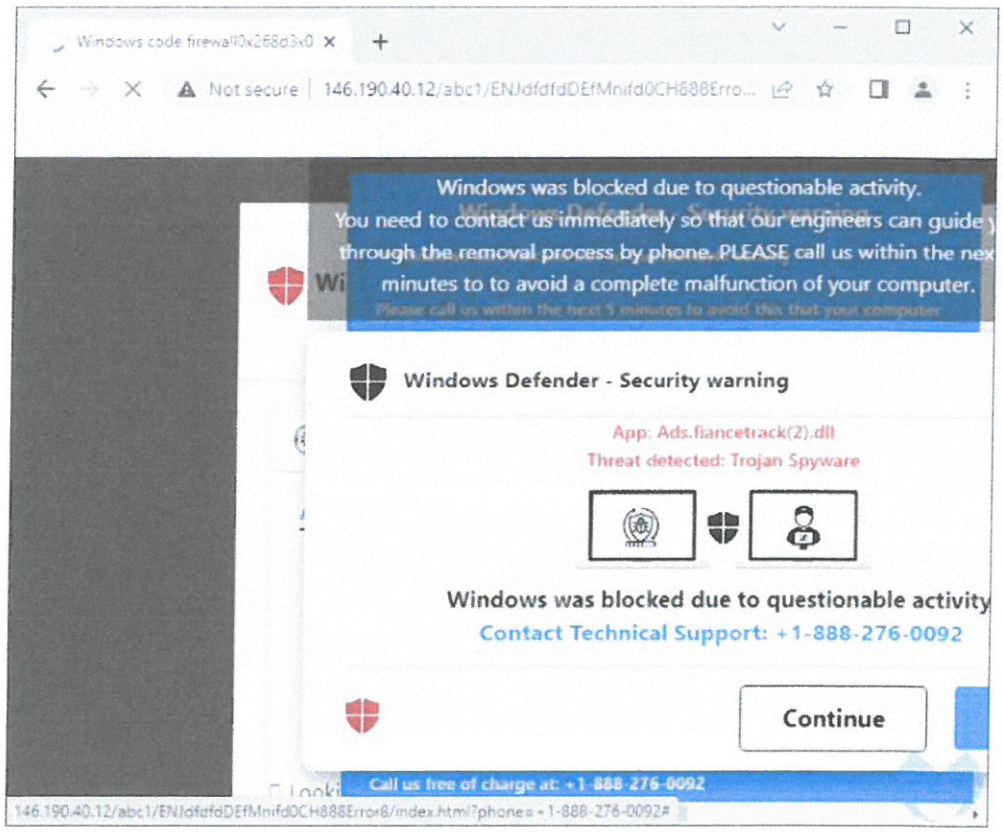
- A "drive-by download," which exploits browser vulnerabilities to install infected files on the system while the user is passively viewing the ad.
- A forced redirect of the browser to a malicious site.
- Executing Javascript or Flash to display unwanted advertising or malicious content.

3. Hijacking Traffic from a Specific User Flow

The threat actors are abusing Google's ad network by purchasing ad space for popular keywords and their associated typos. A common human behavior is to open up a browser and do a quick search to get to the website you want without entering its full URL. Typically, a user will blindly click on the first link returned whether it is an ad or an organic search result.

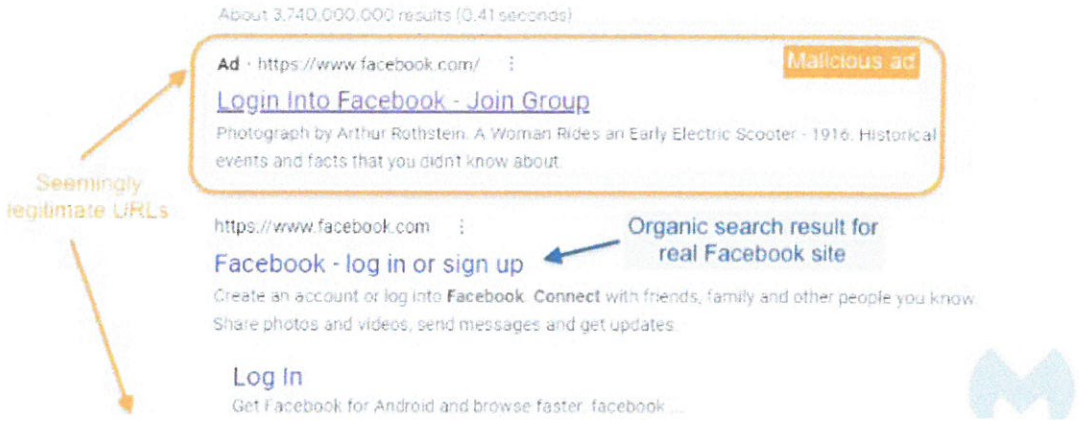


For example, a person wants to load YouTube and typed **'youtube'** instead of entering the full address **'youtube.com'** in the browser's address bar. The first result that appears shows 'www.youtube.com' so the person is likely to trust it and click on it. The victims of these malvertising attacks were simply trying to visit those websites and relied on Google Search to take them there. Instead, they ended up with an annoying browser hijack trying to scam them.



4. Traffic Redirection

Upon clicking the ad search result, the traffic goes to a short of chain of redirects leading to the browser locker. The ad is quite misleading and there is nothing that indicates that clicking on it would redirect anywhere else but to the requested website. As it appears before the top search result on google, it has a guaranteed higher click rate.



5. Recommendations

Malvertising is extremely difficult to detect and avoid for both web users and publishers. This is because of the incredible volume of digital ads being created and the rapid rate at which they are circulated. This means that publishers themselves can often not directly oversee the ad verification and assessment process.

Generally speaking, it is also very difficult for cybersecurity experts to identify exactly which ad is malicious because the ads on a webpage constantly change. Further, most malvertising attacks require the user to interact with the infected ad. This means that not every website visitor will be affected by a malicious ad, which makes it more difficult to narrow down the offending advert.

While it is difficult to prevent infection from a malicious advertisement (malvertisements), users can take steps to reduce their risk.

a. Ensure that all software and extensions, including web browsers, are up to date.

b. Install antivirus software and ad blockers to reduce the risk of running a malicious advertisement.

c. Avoid using Flash and Java or allowing these programs to run automatically when surfing the web.

d. Publishers have a responsibility to protect their visitors from malvertisements. Steps they can take include:

Thoroughly evaluate third-party ad networks that will be responsible for selecting, vetting, and running ads.

a. Scan ad creative intended for display to discover malware or unwanted code.

b. Avoid the use of JavaScript or Flash in ads.

c. Engage a trusted cybersecurity partner to offer customized recommendations based on the organization's digital advertising activity.

Make sure everyone in the organization knows how to avoid malvertising risks. Organizations should invest in educating their employees about basic security practices, such as secure password tips and how to identify phishing emails. This type of education should be conducted frequently because of the ever-evolving threats.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://blog.malwarebytes.com/threat-intelligence/2022/07/google-ads-lead-to-major-malvertising-campaign*
- *https://www.crowdstrike.com/cybersecurity-101/malware/malvertising*