Malvertising

The exposure to threats while surfing online is massive. Even if a person is extremely careful about the legitimacy of the websites, he/she visits, accidental infection of malware is still possible. As legitimate websites can also infect your systems and compromise the organization's network. The reason is Malvertising.

What is Malvertising?

Malvertising, or malicious advertising, is the use of online, malicious advertisements to spread malware and compromise systems. Generally, this happens through the injection of malicious code into ads that may appear on legitimate websites. Malicious actors then pay legitimate online advertising networks to display the infected ads on various websites, exposing every user visiting these sites to the potential risk of infection. In addition to its huge attack surface, it is also very problematic for organizations to identify exactly which ad is malicious because the ads change dynamically on a webpage, which means that one visitor may be infected, but the others who visit the exact same webpage, may or may not be infected.

Malvertising vs. Adware

Malvertising and adware are often confused with one another, as they both use advertising as a cover for malicious software. Malvertising refers to the code that is embedded in a malicious ad that a user may download after visiting a single webpage. Adware is a program that is constantly being run on their computer and affects every webpage they visit.

What are the modes of malware transfer?

There are mainly two types of malvertising:

1. **Click to download –** The user is enticed to click on the ad for the malware to interact and infect your system. For example, pop-up ads for misleading downloads, such as fake anti-virus programs that install malicious software on the computer.
2. **Drive-by downloads –** This is more harmful as an infected ad only has to finish loading before it will harm your computer.

History of attack

This attack was first recorded in late 2007 / early 2008 which was based on a vulnerability in Adobe Flash and affected several platforms. Since then it has been prevalent all around the world infecting several users.

- In 2011, Spotify faced a malvertising attack which used the Blackhole exploit kit which delivered malicious payload to a victim's computer – this was one of the first occurrences of a drive-by download.
- In 2013, Yahoo, with monthly ad visits of 6.9 billion, was the victim of a major malvertising campaign. It was based on Cross-site scripting (XSS) attack which infected users' machines with the ransomware, 'Cryptowall', placing a ransom of up to $1000 in bitcoins, to be paid in 7 days, to decrypt the data.
- In 2017, RoughTed, a malvertising campaign, was reported. A noteworthy point is, it was able to bypass ad-blockers and evade many anti-virus protection programs by dynamically creating new URLs.

What can be done to prevent the attack?

1. When browsing the Internet, make sure to **close browser windows when not in use**, since this will minimize the number of ads displayed and minimize the likelihood of a malicious ad appearing.
2. Users must not completely rely on ad-blockers. Since, not all ad blockers stop all ads. And some websites might not run properly if an ad blocker is turned on.
3. Users **must avoid visiting unreliable sites** like online dating sites, sites offering Flash games, torrent sites, etc. that attackers consider as potential business pages.
4. Where possible, users should **disable the use of Flash** or **set it to 'require user interaction'** in order to run.
5. Some obvious clues like poor grammar or spelling should be a potent indicator to detect a malicious ad.
6. Users should be extra careful while net surfing and **report any suspicious occurrence of ad to the Information Security Team @** it.securityincident@nha.gov.in