'Fingerprint' security flaw ramps up malvertising campaigns

What is Malvertising?

Malvertising is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. Malvertising is attractive to attackers because they can be easily spread across a large number of legitimate websites without having to directly compromise those websites.

Malvertising using fingerprinting

Fingerprinting, in computer science terms, means any data set that can be used to make a unique identification. According to a Malwarebytes report entitled **“**Operation Fingerprint”, exploit kit authors are using advanced “fingerprinting” to preselect and pursue specific victims without any user interaction. Malvertising through the use of fingerprinting is done by first inspecting the file and folder fingerprints of the system to determine if you are a legitimate user or not and then make the decision to ignore the system or download more malware to further exploit it. This fingerprinting technique helps in determining whether the system contains any antivirus software, virtual machines or is it a honeypot that needs to be avoided or does it belong to any security researcher. This can be accomplished by enumerating the local file system and looking for files or folders that may indicate that the system falls into one of those categories. A security researcher, Jerome Segura, from Malwarebytes stated that the main reason behind this way of attack is not to infect more people but to avoid being discovered and to have malicious campaigns last longer. A variety of campaigns take advantage of this security flaw. According to Malwarebytes, the most common Angler-based campaigns include:

- **Fake companies**: Stolen websites are rebranded to appear as legitimate companies, and while XMLDOM-based fingerprinting is not in evidence, these websites have custom filters for those who see malicious code and those who only see benign adverts. An

Apache server component known as the .htaccess file can be tailored to specify who is given the malicious redirect -- and who isn't.

- **Custom SSL campaigns**: Cyberattackers have leveraged the CloudFlare infrastructure to hide a malicious server's IP address, which also connects to clients via the SSL encryption protocol. In one campaign, the server checked to make sure traffic was legitimate before launching a redirection channel to Angler. The fingerprint code was lodged within the fake advertiser's JavaScript but if Kaspersky's Virtual Keyboard plugin was detected, the redirect was aborted to avoid detection.
- **Custom URL shortener campaigns**: The security found one such campaign which hid the fingerprint payload within a .GIF image served over HTTPS. The firm says this was designed to throw off security researchers on the scent, and in addition, the campaign also used shortened URLs to make the infection chain more complex.
- **DoubleClick Open Referer campaign:** The last and most sophisticated, Malwarebytes observed attackers using fingerprint payloads hidden within .GIF images but with an added layer of encoding provided by keys issued once per IP address and embedded within JavaScript.

All of these campaigns have similarities. They all use ad-based domain names and URLs, interim redirector systems, once-per-IP deliveries and, of course, served the Angler exploit kit in the end. The campaigns also implemented fingerprint codes to check for the presence of security products. If none were found, the Angler redirect took place.

Internet explorer vulnerability

If a victim is using Internet Explorer 10 or below, they may be susceptible to malvertising due to a vulnerability in Microsoft Internet Explorer's XMLDOM ActiveX control. The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier allows remote attackers to determine the existence of local pathnames, UNC share pathnames, intranet hostnames, and intranet IP addresses by examining error codes. As a result, this vulnerability allows attackers to search through local file systems on unpatched systems to find "fingerprints" belonging to those that malware operators want to avoid, such as IP addresses and geolocation tags. By adding these checks at the starting point of a chain of infection, only victims who are suitable for compromise will be redirected to an exploit kit.

Why malvertising is a very serious threat?

- No one expects to get infected with malware when they visit trusted sites like YouTube.
- If a victim even realizes a device has been infected, the forensic trail usually goes cold at the site that served the malicious ads. This is because site operators often have no knowledge of malware on their own domain. Ad networks rotate content extremely fast and ads can be purchased with stolen or obfuscated account information and funds, so even when a malicious ad is pinpointed in an investigation it can be practically impossible to prove who actually placed the malicious ad order.
- The Interactive Advertising Bureau (IAB) and Ernst & Young issued a joint report estimating the annual cost associated with a triad of fraudulent practices. They estimated a loss of over $1.1 billion to malvertising. Lost ad dollars starve digital publishers of much needed revenue and marketers of money intended to drive sales.
- Once a malware infiltrates a system,
  - It can inject spyware that allows bad actors to follow the end user's key strokes and thereby copy login data for their financial accounts.
  - It can introduce ransomware (viruses that lock a computer until its owner pays a bounty).
  - It can load nuisanceware that interferes with the proper functioning of a computer or network.
  - It could be a form of malware that either takes over a page or redirects the user to a domain that he or she does not wish to visit.
  - It can infect a computer with a bot, which consumes bandwidth and slows down Internet use.
- The most obvious outward symptom of a malware infection is that the computer may crash, reboot spontaneously or slow down without any logical explanation.

How can we defend against malvertising?

- Always update the installed software when prompted to do so.
- Use reliable anti-virus software.
- Install a software firewall solution or make sure the default firewall is activated.
- Use a safe browser such as Mozilla Firefox or Google Chrome and tighten the browser security settings.
- Avoid the installation of web browser "toolbars".
- Avoid peer-to-peer file sharing programs.
- Practice safe browsing techniques such as not clicking on suspicious links and/or attachments sent via email or spread via social networks, and avoid illegal or unsafe websites.
- Enable Click-to-Play Plug-ins**:** When you visit a web page containing a Flash or Java object, it won't automatically run until you click it. Almost all malvertising uses these plug-ins, so this option should protect you from almost everything.
- Use MalwareBytes Anti-Exploit**.**
- Disable or uninstall Plug-ins you don't frequently use, including java**:** This will reduce your attack surface, giving attackers less potentially vulnerable software to target. You shouldn't need many plug-ins these days. If Adobe Flash is successfully erased from the web along with Java malvertising will become much more difficult to pull off.
- Consider avoiding firefox until electrolysis is done**:** Other browsers like Google Chrome, Internet Explorer, and Microsoft Edge all take advantage of sandboxing technology to prevent browser exploits from escaping the browser and doing damage to your system. Firefox has no such sandbox. A recent malvertising exploit targeted Firefox itself using a zero-day. Sandboxing techniques built into Firefox could have helped prevented this. However, if you do use Firefox, using MalwareBytes Anti-Exploit would have protected you.

References:

http://www.wired.com/insights/2014/11/malvertising-is-cybercriminals-latest-sweet-spot/

http://www.zdnet.com/article/fingerprint-security-flaw-ramps-up-malvertising-campaigns/

http://www.infosecurity-magazine.com/news/malvertising-develops-advanced/

http://betanews.com/2016/03/02/malvertising-fingerprinting/

http://www.technewsworld.com/story/83192.html

http://yourbusiness.azcentral.com/happens-malware-enters-computer-20376.html