Special Report

The Rise of Malvertising

CYPHORT™

Introduction

The practice of injecting malicious advertisements into legitimate online advertising networks with the intent of compromising users and their devices—or malvertising—is a serious problem that has very quantifiable consequences to businesses and consumers. As outlined by a study conducted by the Association of National Advertisers, ad-fraud will cost global advertisers around $6.3 billion dollars in 2015. Much like advertisers, site publishers can be blamed for malvertising attacks. If a user is infected, chances are he or she will have second thoughts about returning to the site. Obviously, consumers are the most direct victim, as their computer and contained files may now be infected by clicking on a malicious ad or, in some cases, by simply going to a site they visit frequently.

To better understand malvertising, it is important to understand how it occurs, how sites are "tricked", its pervasiveness and what can be done to prevent it.

How Malvertising Occurs

Malvertising campaigns are launched through deceptive advertisers or agencies running ads or through compromises to the ad supply chain including ad networks, ad exchanges and ad servers. Websites or web publishers unknowingly incorporate a corrupted or malicious advertisement into their page. Once a user lands on the main web page, they are redirected to copying viruses or spyware.

This is done through a variety of tactics, sometimes simply imitating Adobe™ Flash file downloads, or other well known application updates. This form of malware delivery is a popular form of delivery for attackers because infecting an ad is easier and requires less effort than finding a vulnerability in a high-demand, popular web site, and it allows for broader distribution.

Very often, attackers will place “clean” advertisements on trustworthy sites in order to gain a good reputation. Once that has been achieved, they insert a malicious code or spyware behind the ad for a limited period time and remove the code once an infection has been launched. The attackers are accustomed to tricking the networks by making “armored” malverts, where they use various techniques to appear legitimate to the analysts, but infect the users nonetheless. For instance, they will enable the malicious payload after a delay of several days after the ad is approved. Another way is to only serve the exploits to every 10th user, or every 20th user who views the ad.

A common misconception is that you must click on ads to get infected, which is sometimes true, but often not. Online ads appear to be an image hosted on the website, but they’re neither hosted on that website nor just an image. Ad networks, which are not under the control of the host website, decide which ad to send you, but often don’t actually deliver the ads. Instead, the ad networks instruct your browser to call a server designated by the advertiser.

Ads often deliver files and entire programs to your browser. To infect, HTML-based JavaScript or Flash-based ActionScript covertly routes your browser to a different server that hosts an exploit kit. Flash is scary because it embeds sophisticated logic into the ad, which manipulates your browser as the ad is displayed. Ads can be instructed to only attack at particular times and geographies. Some examples are delaying the attack until after the ad network examines and approves the ad or until major holidays, when web traffic is higher and off time for advertising personnel to promptly remove ads.

How Malvertising “Goes Live”

Combating malvertising is difficult due to the large layered setup of the bidding platforms currently in place. With specific schemes such as real-time bidding, malicious advertisements can remain hidden for extended periods of time. Real-time bidding is a process many advertisers use to serve ads. Here’s how it works: When a user visits a website a bidding request among the affiliates of the advertiser is triggered

to determine who will get to see meta-data about the visiting user. This metadata can include geographical location, browser type and web browsing history. The affiliates then automatically bid on this impression. The highest bidding advertiser gets to display their ad.

It is common practice to outsource the advertising on websites to third-party specialists. These companies re-sell this space, and provide software, which allows people to upload their own advertisements, bidding a certain amount of money to 'win' the right for more people to see them. The ad networks get millions of ads submitted to them, and any one of those could be malvertising. They try to detect and filter malicious ads from their systems, but it is challenging. The potential damage is high, as ad networks have a very deep reach and can infect many people quickly. Verifying user agents and IP addresses also is a common strategy used by the malvertisers to hide from analysts and automated malware detection.

The attackers can implement various targeting strategies for malware infection, which appear normal in the context of advertisement, but essentially evade certain security detection. The use of redirection via HTTPS makes it harder to analyze the origin of attack because even if a security company has the recorded network traffic, it is impossible to decrypt and trace the origin of the malware redirect.

Evolution of Tactics and Deployment

Malvertising tactics have changed as ways to combat the problem have emerged, with attackers initially exploiting weak advertisement management panels. Today, methods have become more sophisticated and elaborate with deceptive techniques that are most often only noticeable at the client side. Malvertising was first identified by security experts in 2007, and the growing breadth of online advertising has led to an explosion in this form of online exploitation.

In 2009, one of the most notable malvertising events occurred when the banner feed of The New York Times was hacked for the weekend of September 11 to 14, causing some readers to see advertisements that told them that their systems were infected and instructed them to install malicious software in disguise. According to spokeswoman Diane McNulty, "the culprit approached the newspaper as a national advertiser and had provided apparently legitimate ads for a week." The onslaught of malvertising continues, and its expanse is clearly evident:

- According to Online Trust Alliance research, by 2013 malvertising increased to over 209,000 incidents and generated over 12.4 billion malicious ad impressions, which is more than four per each person using the Internet.
- Cisco's Annual Security Report found that online ads were the second-most common source of Web malware encounters, accounting for 16% of incidents.

According to Cyphort's own data, we can see 300% increase in malvertising.

- Google published Fighting Bad Advertising Practices on the Web — 2014 Year in Review report, in which half a billion bad ads were filtered and disabled 2014,000 malware websites

According to Cyphort's own data, we can see 300% increase in malvertising. Through our research, we have found examples of malvertising in highly-visited sites:

Gopego.com

In February 2015, Cyphort Labs detected malvertising campaign originating from the Indonesian gadget and technology site Gopego.com. In this case, the malicious advertisement redirected users to other malicious links and eventually downloaded CryptoWall, which encrypts user files, then demands victims pay $500 using Bitcoin in order to receive the decryption key that allows them to recover their files. It also displays a countdown of 168 hours (seven days) to pay the ransom. If the victim does not pay, the price will increase to $1,000.

The attack served an exploit package embedded in a flash file, including exploits which target four vulnerabilities. Among them, the notorious CVE-2015-0311, which hit affyield.com. The final payload is a variant of CryptoWall version 3.0 (also known as Crowti). Similar to its predecessor, it uses RSA-2048 algorithm to encrypt files on the hard disk. It also drops the following already well known files in each of the affected directories, which contained instructions on how to pay the ransom .

Once it finished encrypting files, the malware visits the url http://paytoc4gtpn5czl2.torpaysolutions.com/hkmxYL and demands victims to pay US$500 using Bitcoin in order to receive the decryption key that allows them to recover their files. It also displays a countdown of 168 hours (7 days) to pay the ransom. If the victim does not obey, the price will increase to USD $ 1,000 after the countdown. –

The ransomware program provided users with links to several Tor gateways leading to CryptoWall decryption services hosted on the Tor network. There have also been reports that this new version of CryptoWall uses I2P (Invisible Internet Project) anonymity networks to carry out communication between victims and controllers to hide from researchers and law enforcement officials.

Huffington Post

In January 2015, Cyphort discovered a compromise of the AOL Ad-Network that led to major websites displaying malvertising, such as HuffingtonPost.com, FHM.com, theindychannel.com, LAWeekly.com and weatherbug.com . These attacks were the work of the Kovter gang, which also launched malvertising campaign on YouTube in recent months. Kovter is an ad-fraud Trojan that simulates user visiting pages with ads, which by automatically 'clicking' online advertisements, generates revenue for the ad-hosting website. All these requests are made in the background and game the system while the victim is none the wiser.

When a user opened the Huffington Post web site, several scripts were executed from the advertising network to show ads. One of these scripts loads an external function through HTTPS from Google AppSpot, and this function loads another redirect through HTTPS. And only then did the user receive the redirect to malware payload. This method made it harder to analyze the origin of attack because even if a security company has the recorded network traffic it is impossible to decrypt and trace to the origin of the malware redirect.

Researchers observed two bugs being exploited: CVE-2013-2551, a use-after-free vulnerability in Microsoft Internet Explorer, and CVE-2014-6332, a Windows OLE Automation Array vulnerability in Microsoft Internet Explorer. In the end, the exploit kit downloaded a Kovter Trojan used for advertising click fraud. The attack required no user interaction, meaning users were infected if they simply navigate to the affected site and their browsers or plugins were vulnerable.

Combatting Malvertising Attacks

Malvertising is likely to become the most favorable vector for cyber criminals to conduct sophisticated drive-by attacks on Internet users with some degree of selective targeting. For example, they can choose hosting sites to target victims by industries and interest groups; they can further select individuals by geo locations and client machine types, and so on. These allow them to be selective in targeting and be stealthy against common detection tools. Combatting malvertising requires vigilance and best practices from all parties involved, the web property owners (hosting sites), ad networks, and web surfers. Only a secure ecosystem can provide a sustainable and safer cyber space.

- Advertising networks should use continuous monitoring that utilizes automated systems for repeated checking for malicious ads.
- Scans should occur early and scan often, picking up changes in the complete advertising chains instead of just the creative impressions.
- Ad networks should leverage the latest security intelligence to power their monitoring systems to stay up to date with global threat.
- Individuals should avoid “blind” surfing to reduce their exposure to drive-by infection. Keeping your computer system and security software patched timely will go a long way in protecting you when you do have to venture in the “dark night.”

What we do

Cyphort enables security teams to quickly and accurately determine the existence and severity of an advanced targeted attack with threat priority-based mitigation techniques. With Cyphort’s Advanced Threat Defense Software Platform, you can detect advanced persistent threats and immediately contain advanced malware with superior visibility, flexibility, and scalability across your entire network.

About Cyphort

Founded in 2011 by a team of security experts, Cyphort advanced threat defense goes beyond malware detection to reveal the true intent of the attack and the risk to your organization with prioritized and expedited remediation. Our software-based approach combines best-in-class malware detection with knowledge of threat capabilities and your organizational context to cut through the avalanche of security data to get at the threats that matter and respond with velocity, in hours not days.

CYPHORT, Inc.
5451 Great America Pkwy
Suite 225
Santa Clara, CA 95054
P: (408) 841-4665
F: (408) 540-1299

Sales/Customer Support
1-855-862-5927 (tel)
1-855-8-MALWAR (tel)
1.408.540.1299 (fax)
Email: support@cyphort.com