ISSN No. 0976-5697

Volume 7, No. 2, March-April 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks

Dr.P.B.Pathak
Assistant Professor & Head, Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded
Maharashtra, India

Abstract: Defects in the operating system design and running the same operating system with too much permission to users, on all the computers from network makes computers more vulnerable to malware attacks. Malware developers trick users to download their malware. By studying how Malvertising occurs, how sites are tricked and how to prevent it, one can better understand Malvertising. The present paper covers the essential discussion of Malware, Malvertising and the attack methods used to distribute malicious advertisements and enlists several measures to combat the problem.

Keywords: Cyberwar; Cybercriminal; Cybercrime; Malware; Malvertising; Vulnerability

I. INTRODUCTION

Malvertising is injecting malicious advertisements into legal online advertising networks to compromise users and their devices, is a serious problem with considerable consequences to businesses and customers. Advertisers and site publishers both are equal responsible for Malvertising attacks. Customers are mostly victim, since their computer and files may get infected by clicking on a malicious advertisement or, by simply visiting their frequent visiting site. Malvertising are usually enforced via deceptive advertisers or agencies running advertisements or by compromises to the advertisement suppliers comprising advertisement networks, advertisement exchanges and advertisement servers. Once user lands on the main web page containing corrupted or malicious advertisement they are automatically redirected to malware. This malware delivery mechanism is popular because finding vulnerability in the site software is difficult compared to infecting an advertisement and requires less effort. To gain a good reputation, attackers place clean advertisements on trustworthy sites, and then they insert a malicious code or spyware along with the advertisement for a limited period time and subsequently they remove the code once an infection is done. Habituated attackers trick networks to infect the users by developing resistant Malverts and apply various techniques to appear legitimate. Cybercriminals are opportunistic and always look for weak link in the system that can be exploited. Substantial growth in Internet shopping and online banking due to its popularity, increased phishing and financial malware attacks. Increased Security measures for online sites helping customer's confidence, ensuring damage can be limited and cybercriminals can be discouraged, though all online fraud can't be conquered.[1,3]

Malvertising tactics have changed as ways to combat the Malvertising have emerged, with attackers initially exploiting weak advertisement management systems. Today, methods have become more sophisticated and elaborate with deceptive techniques. The assault by Malvertising continues, and its expanse is clearly very high. Malvertising are rapidly becoming one of the prominent sources of spreading malware. There is an urgent need of extensive security policies and procedures to combat and curb the risk of infection due to malware. Online advertisements provide a convenient platform for spreading malware. Advertisements provide significant revenue on the web so the significant efforts are being put into attracting users to them. Malicious agents take advantage of this skillful attraction and then redirect users to malicious sites that serve malware.[4,2]

II. MALWARE

Malware is an abbreviation of Malicious Software. Malware gain access or damage a computer not necessarily in the knowledge of the owner. Malware remains unnoticed, either by actively hiding or by simply not making its presence felt. Malware includes viruses, worms, and Trojan horses. Destructive malware utilize popular communication tools to spread, including, worms sent through email and instant messages, Trojan horses dropped from web sites, and virus from infected files downloaded. Malware exploits existing vulnerabilities on systems making their entry quiet and easy. Malware was originally created as experiments, fun and pranks, but eventually led to vandalism and destruction of targeted machines. [2]

Malware gets installed on your machine and performs unwanted tasks, often for some third party's financial benefit. Malware can range from being simple irritating pop-up advertising to causing serious computer assault and potential damage by stealing sensitive information like passwords, credit card numbers and data or send fake emails from your email account, infecting other machines on the network. Malware can transmit information about your Web browsing habits to advertisers or other interested third party. Malware can be installed on a computer, with or without knowledge of owner, in a number of ways generally when you visit a compromised and contaminated website or download seemingly innocent software. Malware can infect your internet browser via silent extensions and add-on's.[5,7]

There are various types of malware like Adware, Spyware, Zombie, Ransomware, Financial malware, Virus and worm, Browser hijacker, Keyloggers, or any type of malicious code that infiltrates a computer. Malware development is on the rise

due to the availability of ample money through organized internet crime. Malware is developed for profit through forced advertising adware, stealing sensitive information spyware, spreading email spam or child pornography zombie computers, or to extort money Ransomware, financial malware, scans a computer system for financial transactions information. Virus and worm replicates and spreads, damages a computer, deletes files, reformats hard disk, or consumes computer memory, browser hijacker modifies browser settings to redirect links to other advertising sites, or sites which collects web usage information, and keyloggers records every keystroke for misuse.

Software that comes bundled with other software is often called a Trojan Horse. E-mail containing apparently harmless link or email attachment can infect a computer potentially. Malware can exploit security loopholes in your browser to assault your machine. Sometimes websites trick users into clicking Yes and installing software onto their machines, if user clicks No, many error windows are displayed. Some sites tell you that using a certificate makes your site safe which is not the case. Some malware provide no uninstall option, and installs code in unexpected and hidden places like the Windows registry or modifies the operating system, making it more difficult to remove.[10,5]

III. MALVERTISING

Malicious online advertising is Malvertising. Advertising on the web have become essential tools for both companies and customers, to promote and learn about their products, respectively. Cybercriminals are increasingly using them as instrument for spreading virus and spyware. Useful and legitimate advertisements go malicious and harmful, to damage your data, steal your personal details or even control your computer remotely. Malvertising poses very serious threat to the entire online community. There are two common methods used by cybercriminals to spread viruses and other malware through advertisements on the Internet. First, criminals act as trustworthy companies and place a series of clean advertisements on trusted sites that host third party advertisements, gains good reputation by running for some time. Then comes attack by inserting a virus or spyware in the code behind the advertisement to produce mass virus infection. Second, Cybercriminals turn legitimate advertisements into malicious advertisements by hacking trusted sites and injecting viruses. In both the cases, once the damage is done they remove the virus.[3,9]

There are still other various ways of implementing Malvertising for destruction like Drive-by Downloads, Social Engineering, infected Content Delivery Networks, malicious Flash banners and hidden iframes. Malvertising operates by, targeting millions of Internet users accessing the respective sites, once the malicious advertisement is put into place. The user clicks on the advertisement to visit the advertised site, and instead either is directly infected or redirected to a malicious site. These sites fox users to copying viruses or spyware. Cybercriminal hacks an advertisement delivery server, or signs a fraudulent contract to upload an advertisement with malicious content which in turn enters into, advertisement network database and subsequently served to customers to push them in danger. Cybercriminals prefer this mechanism since distribution of malicious advertisement content is quick, is on large scale and free of charge, no need to pay for bandwidth. Cybercriminals distributes malware hidden within an advertisements, executables embedded on a webpage, or bundled within software downloads.

Cybercriminals exploit an unprecedented revolution in social connectivity due to Internet based social networking sites. Placing pages on social media sites containing links to drive by downloads, propagating malware, concealing malicious JavaScript, breaking into social media sites, and doing spear phishing are some common methods adopted by Cybercriminals to carry out social media based attacks. You must click on advertisements to get infected is mere a misconception. Online advertisements are neither hosted on that website nor just an image, though appear to be an image. Advertising networks decide which advertisement to send you, sometimes it instructs your browser to call a server designated by the advertiser. Advertising networks are not under the control of the host website so instead of actually delivering the advertisements, it deliver files and programs to your browser, to infect HTML based Javascript or Flash based ActionScript stealthily routes your browser to a different server that hosts an exploit kit. [6,1]

Malvertising through drive-by downloads occur when a program is downloaded onto your device without your permission. Cybercriminals purchase advertising space and install malware in the advertisement, difficult believe is malicious advertisement, and not legitimate, the malware hidden in the advertisement will automatically download onto your device. Social engineering tricks you to click on a link to open the malicious website; malware can be installed on your device. Simply visiting these websites is enough to infect your device.

Ransomware Scareware and fake antivirus use social engineering using popup similar to that of from computer, communicating System Warning and Threats Found or Your computer is infected. Click OK to remove the virus, in anticipation that you'll click on the message, which allows the malware to be downloaded on to your computer. Fake antivirus malware most commonly uses the technique of scary warning messages to convince you to buy the malware. Fake antivirus is malware that pretends to be real antivirus software once you buy and install the fake antivirus; it infects your computer with malware instead of cleaning it. Search engine's close tie up with advertising also help malicious agents in attracting users to particular sites from which users can be redirected to a malicious site to put you in problem.

Using hidden iframes attackers hide the objects that are used for spreading malware. Iframes can be used to load dynamic content for advertising. This functionality of iframes can be exploited to trigger infections. A Content Delivery Network is a third party advertising server that provides content to different domains across the web. These are the preferred choice for attackers to spread malware by exploiting the web servers. The attackers simply use the servers doing the job of spreading the malware. Flash embeds sophisticated logic into the advertisement, which manipulates your browser as the advertisement is displayed. The reason advertising flash banners are used extensively to spread infections is advertising flash banners are widespread so attacks are also widespread. [9,10]

IV. COMBATING MALWARE AND MALVERTISING

We can combat Malware and Malvertising by being careful and alert about email attachments, being cautious while surfing and staying away from suspicious websites. By installing and maintaining an updated, quality antivirus / antimalware designed to identify, remove and prevent Malware from infecting computer systems or electronic devices by exploiting vulnerabilities. As far as the businesses are concerned if not complete elimination can be reduced considerably, the risks from Malvertising and social media based attacks by adopting comprehensive measures. Educate users about ensuring social media safely and avoiding Malvertising. Use strong passwords with adequate password length, use of special characters and changing password periodically, using different passwords for different account. Use of Intrusion prevention systems can greatly block threats. Avoid visiting sites dedicated to shopping, sports, gaming and pornography. [1,2] Restricted use of social media applications and controlled use of Web applications by employees. Malvertising is most favorable for Cybercriminals to selectively target the Internet users with sophisticated attacks. Successful Combating Malvertising is only possible by strict vigilance and following best practices by everyone involved the web property owners, Advertising networks, and web surfers.[7,8]

Following are some preventive measures to combat dangerous threat of Malvertising:

- Prevention is better than cure so install effective and comprehensive antivirus/antimalware internet protection with safe browsing functionality and keep security patches up to date.
- Scan email attachments prior opening. Open email attachments from expected and trusted source. Delete all unwanted and untrusted messages without opening.
- Don't click on Web links from unknown source. Don't respond to strange messages, files, or web site links, pop up online surveys.
- Scan all files before transferring them to your system. Transfer files from only well known source.
- Block all unwanted outbound communication
- Adopt user education and password policy in businesses to avoid attacks.
- Use Intrusion prevention Mechanism, Deploy application control-content filtering and don't trust too much.
- Install third party applications and software from a trustworthy source only if you really need.
- Don't post confidential, personal and financial information on social media.

V. CONCLUSION

After Cybercriminals generally either use Malvertising or Social media based attack to exploit common Web activities. Malvertising is the malicious online advertising to spread malware. Malvertising is placing malicious advertise on legitimate website to spread viruses and spyware and drive downloads of fraudulent applications to steal financial and other data. Malvertisement is growing at an alarming rate. Malvertising is a continued, silent and unnoticed threat that's always taking different forms. Cybercriminals are attacking with increased aggression and sophistication day by day. Individuals and businesses must take care of monitoring, inspecting and analyzing advertisements delivered to them. It is difficult to identify friend and enemies on the web. The best defense against Malvertising is aggressive offense.

VI. REFERENCES

[1] "The Rise of Malvertising", http://go.cyphort.com/rs/181-NTN-682/images/Malvertising-Report-15-RP.pdf

[2] "How SMBs Can Stop Malvertising and Social Media-Based Attacks", www.mcrinc.com/.../201511_How_SMBs_can_stop_Malvertising.pdf

[3] "2015 A10 Security Predictions", https://www.a10networks.com/sites/default/files/.../A10-WP-21118-EN.pdf

[4] "Optimized Mal-Ops", https://www.bromium.com/sites/.../bromium-report-optimized-mal-ops.pdf

[5] Aditya K Sood, Richard J Enbody, Michigan State University, "Malvertising – Exploiting Web Advertising", https://www.cse.msu.edu/~enbody/CFS_2011-04_Apr.pdf

[6] "Malware Wears Costumes, Too",https://www.nh.gov/doit/.../resources/.../nl2015-10-malware-costumes.pdf

[7] "Combat Malvertising, minimize your risk and protect your reputation with RiskIQ for Ads", https://www.cdn2.hubspot.net/hub/250381/...pdf/.../RiskIQ_Ads_Datasheet_2014.pdf

[8] "Top 5 Malware Trends for 2014 and How to Combat Them", https://www.ncbpinc.com/collateral/Webroot-Executive-Brief-01-22-14.aspx

[9] "Adblock Plus. Surf the web without annoying ads!" https://adblockplus.org, 2014.

[10] https://www.doubleclickbygoogle.com/