International Journal of Multidisciplinary Engineering in Current Research
Volume 1, Issue 1, September 2016, http://ijmec.com/

Understanding and Combating Malvertising Attacks in Malware cybercrime

Krishnachaitanya. Katkam
Asst Prof (CSE)
Kshatriya College Of Engineering
Armoor India
chaitanya.dynamics@gmail.com

Abstract: **Using the systems with defects in operating system design makes computers more vulnerable to malware attacks. Malware developers provide tricks to users to download their malware. Through this one can better understand how sites are tricked and how to prevent it. The present paper covers the discussion of malware practices and enlists several methods to fight against the problem.**

Keywords: **Cyber war, Cybercriminal; Cybercrime; Malware; Malvertising; Vulnerability**

1. INTRODUCTION

Malvertising is introducing harmful advertisements into legal online advertising networks. It is a serious problem to business as well as customers with major consequences. Both advertisers and site publishers are equally responsible for Malvertising attacks. Here, customers are the primary victims as their coputer and files may get infected by clicking on a malicious advertisement or by visiting their site. Deceptive advertisers, agencies running advertisements and compromises to the advertisement suppliers comprising advertisement networks, exchanges and servers causes Malvertising. Users redirect to malware once they click on the main web page containing corrupted or malicious advertisement. This mechanism is popular because it requires less effort and infecting an advertisement is easier than finding vulnerability in site software. To gain fame, attackers place clean advertisements on a trustworthy site and insert spyware or malicious code along with the advertisement for a period of time until the infection is done.

Experts infect the users on networks by developing resistant Malverts and use various techniques to be legal. Cybercriminals are opportunistic and look for weak link in the system to exploit. Substantial growth in online shopping and banking increased phishing and financial malware attacks. Cybercriminals can be discouraged through increased security measures for online sites, providing customer's confidence and ensuring damage can be limited, though all online fraud can not be controlled.

Malvertising tricks have been changed as ways to fight against malvertising have came out. Today these methods are highly developed and elaborated with deceptive techniques. The violent attack by malvertising continues and it is expanding clearly very high. Malvertising is the prominent source of spreading malware. Extensive security policies and procedures are needed to combat the infection and curb the risk of malware. Online advertising is the platform for spreading malware. Advertisements play a major role on the web revenue, therefore significant efforts are made to attract the users. Attackers take advantage of this and redirect the users to malicious sites.

2. MALWARE

Malware is an abbreviation of malicious software. Malware access or damage a computer with/without the knowledge of the owner. Malware is unnoticed by actively hiding and simply by not making feel its presence. It is created as an experiment, fun and prank but malware eventually led to a deliberate damage and destruction of targeted machines.

For some third party's financial benefit, they install malware on your system and perform unwanted tasks. Credit card numbers and data or send fake emails from your email account, infecting other machines on the network. Malware can be installed generally in a number of ways- when you visit a comprised and contaminated website or download so called innocent software. Silent extensions and add-on's infect your internet browser.

Adware, Spyware Zombie, Ransom ware, Financial malware, Virus and Worm, Browser hijacker, Key loggers or any malicious code that infiltrate a computer are the types of malwares. Availability of ample of money through organized internet crime is the cause for the development of malware. It is developed for the profit through forced advertising adware, stealing sensitive information spyware, spreading email spam or child pornography zombie computers, or to extort money Ransom ware, 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 settings to redirect links to other advertising sites or sites which collects web usage information are modified by browser hijacker. Key loggers records every keystroke for misuse.

Trojan Horse is software that comes bundled with other software. An email containing harmless link or attachment can infect a computer potentially. Security loopholes of browser are used by malware to harm your machine. Sometimes websites make users to click on Yes and

International Journal of Multidisciplinary Engineering in Current Research
Volume 1, Issue 1, September 2016, http://ijmec.com/

install software onto their machines, if user click No many error windows will be displayed. Some sites tell you that using a certificate makes your site safe which is not true.

Due to internet based social networking sites, cybercriminals use an unprecedented revolution in connectivity. Some of the common methods are placing pages on social media sites containing links to drive by download, propagating malware, concealing malicious JavaScript, breaking into social media sites, and doing spear phishing. It is a mere misconception that you get infected only by clicking on the advertisements. Online advertisements are not hosted on the website or just as an image but they appear to be an image.

3. MALVERTISING

Malvertising means malicious online advertising. Advertising on web have became essential for companies to promote and for customers to learn about their products. This helps cybercriminals for spreading virus and spyware. This is a very serious threat to online community. The two methods of malvertising are: First, Criminals act as trustworthy and place clean advertisements on trusted sites that host third party advertisements and gain good reputation by running for a period of time. Then comes the attack by inserting a virus or spyware behind the advertisement to produce mass virus infection. Second, By hacking trusted sites and injecting viruses cybercriminals turn legal advertisements into malicious.

The other ways are: Drive-by Downloads, Social Engineering, infected Content Delivery Networks, malicious Flash banners and hidden I frames. Malvertising targets millions of Internet users accessing respective sites and put on the malicious advertisements on the sites. These sites fox users to copy 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. They prefer this because distribution of malicious advertisement content is quick, it is on large scale and free of charge, no need to pay for bandwidth.

Advertising networks decide which advertisement to send you and instructs your browser to call a server designated by the advertiser. They 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 Java script or Flash based Action Script which cautiously routes your browser to a different server that hosts an exploit kit.

Social engineering tricks you to click on a link to open the malicious website. Cybercriminals purchase advertising space and install malware in the advertisement. Simply visiting these websites is enough to infect your device.

Ransom ware Scare ware and fake antivirus use social engineering using popup similar to that of computer through which communicating System Warning and Threats found or Your computer are infected. In anticipation of click ok to remove virus you click on the message which allow you to download malware on your system. Search engine is close tie up with advertising and 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.

Attackers use hidden I frames to hide objects that spread malware. I frames load dynamic content for advertising which are used 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. The reason advertising flash banners are used extensively to spread infections is advertising flash banners are widespread so attacks are also widespread.

4. COMBATING MALWARE AND MALVERTISING

We can fight against Malware and Malvertising by being careful and alert about email attachments, being cautious while surfing, 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. If the concerned business adopt comprehensive measures, the risks from malvertising and social media based attacks can be reduced considerably. For this, the users have to be educated about ensuring social media safely, use strong passwords and different passwords for different accounts. Threats are blocked by using intrusion prevention systems. Avoid visiting sites dedicated to shopping, sports, gaming and pornography. Restrict use of social media applications and controlled use of Web

5. APPLICATIONS BY EMPLOYEES

Malvertising is most favorable for Cybercriminals to selectively target the Internet users with sophisticated attacks. Strict vigilance and following best practices by everyone involved the web property owners, Advertising networks, and web surfers can combat malvertising successfully.

some preventive measures to combat dangerous threat of Malvertising:

- 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.

- 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 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.

CONCLUSION

Malvertising is the malicious online advertising to spread malware. It is growing rapidly. It is a continued, silent and unnoticed threat that is always taking different forms. Cybercriminals generally use malvertising or social media based attacks to exploit common web activities. They are attacking with increased aggression and sophistication day by day. To steal financial and other data, Malvertising is placing malicious advertise on legitimate website to spread viruses and spyware and drive downloads of fraudulent applications. Users must take care of monitoring, inspecting and analyzing advertisements delivered to them. It is difficult to identify friend and enemies on the web. Aggressive offense is the best defense against Malvertising.

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-
[4]. Malware Wears Costumes, Too",https://www.nh.gov/doit/.../resources/.../nl2015-10-malware-costumes.pdf
[5]. "Combat Malvertising, minimize your risk & protect yours reputation with RiskI Q for Adds", https://www.cdn2.hubspot.net/hub/250381/...pdf/.../RiskIQ_Ads_Datasheet_2014.pdf
[6]. "Top 5 Malware Trends for 2014 and How to Combat Them", https://www.ncbpinc.com/collateral/Webroot-Executive-Brief-01-22-14.aspx

KRISHNACHAITANYA.KATKAM completed MTech CSE from JNTU Hyderabad Having 9+ years of experience in Teaching. At Present Working as a Asst Prof in Kshatriya College Of engineering Chepur,Armoor. Interested in MOBILE COMPUTING,COMPUTER FORENSICS, COMPUTER NETWORKS.