ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
August 2015,
Vol. 8, No. (2):
Pgs. 124-130

Website Injection for Fraudulent Activities and Ways to Combat

T. VENKAT NARAYANA RAO[1] , JELLA SHRUTHI[2] and THAKKALLAPALLY SNEHA[2]

[1]Computer Science and Engineering, Sreenidhi Institute of Science and Technology, India.
[2]Computer Science and Engineering Sreenidhi Institute of Science and Technology,
Ghatkesar, T.S, India.

(Received: May 10, 2015; Accepted: August 15, 2015)

ABSTRACT

Now a days , web injection exhibits in different modes, but basically occurs when malicious and unwanted actors tamper directly with browser sessions for their business profits. Malware's are injected through ad networks into websites. How an individual play different roles in this kind of tampering browsers is being discussed. The consequences of malware attacks are explored, as these are new trends in website attacks and describe types of malware you need to watch out on your site. Finally, this paper discusses solutions for reducing malware threats and also includes some best practices for protecting website and business.

Key words: Malware, Spyware, Cybercriminals, Spammers, Ransomware.

INTRODUCTION

With the Internet becoming the governing network for advertising and marketing, online advertisements are more and more used for illegal purposes such as scamming, propagating malware, click frauds, etc. Malware, in short the malicious software, is any type of software that is used to interrupt computer operation, provide access to private computer systems, or gather sensitive information[1]

Malware is defined by its malicious intent, which acts against the user requirements, and does not include software that causes accidental damage due to some deficiency. Bad-ware is the term sometimes used, which is applied to both true malware and unintentionally harmful software.Both business and academia have been working on this threat, by studying ads to identify their malicious content. However, malicious ads often use code packing and obfuscation techniques to elude detection[2]

Another complicated situation is pervasiveness of ad syndication, it is a model in where an ad network vends and resells the spaces it acquires from publishers to other ad networks and advertisers. Ad syndication increases the chances of posting malicious content on other Web site.

It licences a malicious ad network to distribute ads directly to a user's browser, without the need of acquiescing them through the more

trustworthy ad networks and originators from whom it gets the ad space. Malware may be furtive, which is intended to steal content or spy computer users for an prolonged period without their knowledge, 'Malware' is a term that is used to refer a variety of forms of adversary or intrusive software, which includes worms, computer viruses, ransomware, Trojan horses, adware, scareware, spyware, and many other malicious programs. Malware has many forms – scripts, executable code, active content. In non-malicious files, Malware is often hidden as, or enclosed in. According to the law, malware is a computer contaminant[3]

Spyware or other malware is sometimes found embedded in programs supplied officially by companies, e.g., which can be downloaded from websites, that appear valuable or eye-catching, but may have, for example, additional unknown tracking functionality that collects marketing statistics.

Role of Cyber criminals

There are several steps for criminal money-making schemes to work were the criminals need to focus in their works. The criminals should have adeptness, talent and responsiveness to continually elude defences and avoid apprehension by law enforcement. The following are various roles cybercriminals fill to create a effective crime[4]

Exploit writers

Exploit writers are hackers who are specialists in noticing vulnerabilities in software and also creating exploit packs which are noting but a group of vulnerabilities packaged together. Then these exploit pack is sold to less technical criminals. And these technical criminals use on websites and also in email attachments to insert malware on unpatched computers[5,7]

Translators

The language quality that is used in many lures, spam emails, and social engineering attacks has improved vividly in recent years. The teams behind these attacks are investing in services to improve the number of victims.

Bot herders

The zombie computers that are used for creating a botnet are infected by bot herder, which the criminals use for DDoS attacks, spamming, proxying and other computing needs of the criminal underground.

Based on geography and type of bot needed by the purchaser the bot herders segregate and sell or lease computers.

Money mules and mule managers

Financial criminals need people on the street to walk into banks and transfer funds or deposit checks. Mule managers concentrate in hiring people who are down on their fluke, or prepared to look the other way when asked to help commit financial scam. Many mules are trapped into helping by work-at-home scams and other guises intended to fool them into assisting.

Partnyo'rka owners

Partnyo'rka or "partner network" is affiliate marketing schemes set up to stimulate low-level criminals to spread information about Canadian pharmacy offers, forged luxury goods and other spammed or services or goods. The commissions are paid by Partnyo'rka operators to their minions for each sale. Partner network owners encourage their schemes with spam in emails, blog comments, mediums, conversations, and social media, as well as website poisoning. [6]

Tool providers

For spreading spam and malware a group of people write tools. Cybercriminals can purchase toolkits, CAPTCHA solvers, exploits and a host of other tools designed to spam every online service from $20 to many thousands of dollars.

Malware writers

Developers are the heart of the whole cybercrime operation to go on. Most of the malware developers don't distribute their wares directly, and also sell their services to the operators of organized cybercrime operations.

Purpose

With the rise of broadband Internet access, malicious software has been designed to gain huge profits. The majority of common viruses and worms have been designed in such a way that they take control of users computers for illicit purposes. Infected "zombie computers" are used to send the

spammed mail, and to host illegal data like child pornography or distributed denial-of-service attacks as a form of extortion[8]

Programs are designed in a way so that they can monitor users' web browsing, exhibit unwanted advertisements, or transmit affiliate marketing returns are called spyware. Like viruses Spyware programs do not spread; instead they are generally installed by exploiting security holes. They can also be wrapped with user-installed software, like peer-to-peer applications. Ransomware affects an infested computer in some way, and stresses payment to converse the loss. One can generate payment using click fraud, making it appear that the computer user has clicked an advertising link on a site, producing a payment from the advertiser. It was predicted in 2012 that about 60 to 70% of all active malware used some kind of click fraud, and 22% of all estimated ad-clicks were fraudulent. Malware is commonly used for criminal commitments, but can be used for sabotage, often without direct benefit to the perpetrators.

How Cybercrime Works

The main reason behind malware is to gain profits. Cybercriminals use many techniques to monetize their activity. To do their work, cyber criminals must take many steps for the entire process.

The first step for cybercriminals is to identify the victims. There are the six primary ways where the Cyber criminals catch unaware victims in their nets and compromise their computers for criminal commitments.

Spam

Initially with email spam the monetization of malware was started. Profitable practices for many criminals include fake watches and Russian brides. Although spam rate have begun to go down, spammers send billions of messages every day with a hope that at least a small section will make it past spam filters and persuade a few people with

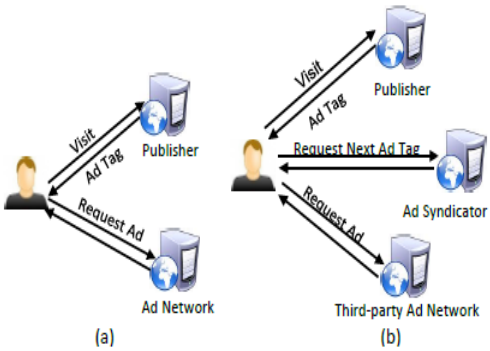

Fig: 1.1: (a) Direct delivery; (b) Ad syndication.

Table. 3.1: Classification of mal-Advertisements

Type of maliciousness	#Incidents
Blacklists	4,794
Suspicious redirections	1,396
Heuristics	309
Malicious executables	68
Malicious Flash	31
Model detection	3

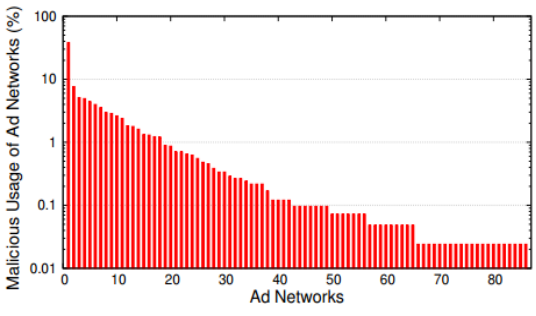

Fig. 3.1: Malvertising distribution from selected ad networks

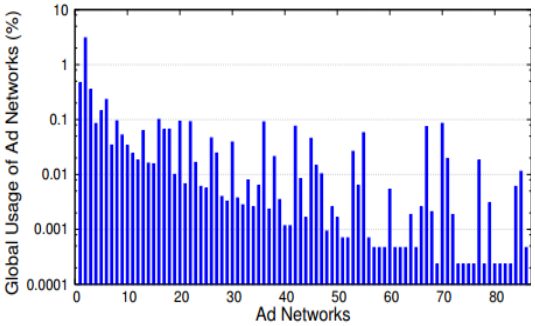

Fig. 3.2: Distribution of advertisements from selected ad networks

their guard down to make a purchase. Malware is attached and sent with more or less messages, in this way it is largely moved to the web.

Phishing

Commonly, attackers use emails for spam promoting products and services. Phishing attacks are delivered through emails, this is the preferred method. These emails pretend to be in the form of emails that come from service providers in order to steal account details and gain access to others company's internal services.

Social media

Many spammers have transferred from email spam to social media spam. In general users more likely click links in commercially motivated spam if it look as if it has come from a colleague or friend from Facebook and Twitter. Curious victims may click on the unsafe links like Breaking news and popular features[9]

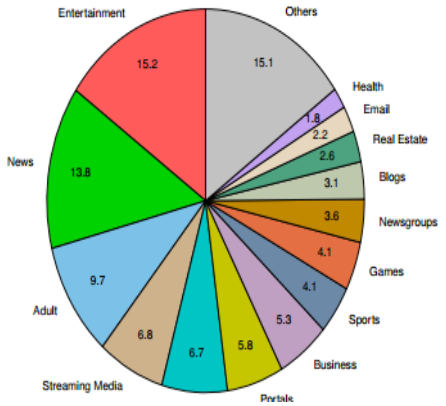

Fig. 3.3: Websites categorization that served malvertisements

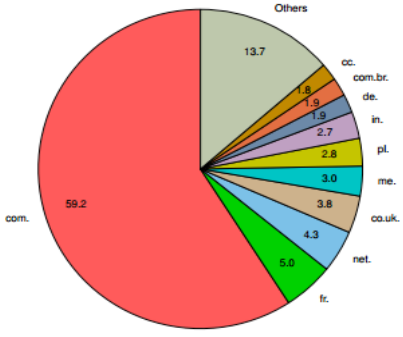

Fig. 3.4: Malvertisements distribution based on top level domains

Blackhat SEO

With the search engines like Bing and Google scammers try to do manipulation, this method is said to be Blackhat SEO or SEO poisoning. This leads to "poisoned" search results about many popular topics, which includes front page results that leads to exploits, malware and phishing sites[10]

Drive-by downloads

By simply visiting the websites containing exploits large numbers of victims are delivered into the hands of attackers. This process is known as drive-by downloads. In a survey it has been observed that 30,000 new URLs every day that expose innocent surfers to a variety of code attempting to exploit vulnerabilities in their browsers, operating systems, plugins and applications.

Malware

Viruses and other malware files still serve their masters well. Compared to the past these attacks are less common today, opportunistic criminals still use malware to infect exposed systems and recruit people's computing devices for their individual purposes[1]

Deceptive Downloads

A specific software component that is malicious try to attract their victims to download and install which is said to be Deceptive downloads. The

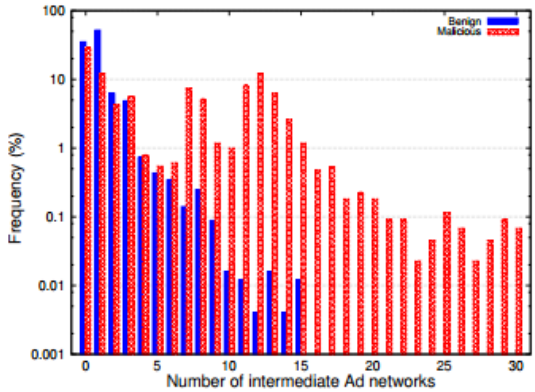

Fig. 3.5: Ad networks involved in ad arbitration for benign and malicious advertisements

main difference between drive-by downloads and Deceptive Downloads is in Deceptive Downloads attackers do not try to find a vulnerability in the victim's browser or browser plugins to download and install a piece of malware, instead they try to deceive the users into performing that procedure willingly. This process happens when user believes that there is some necessary content on the visited web page. And next the victims are informed that to gain access to definite content of the page, they need to install a particular software component or to upgrade their plugins. In this way, instead of the advertised software, the updating/installing procedure installs malware on the user's hosts[2,4]

Link Hijacking

Link hijacking is the processes were the advertisements automatically redirect users to websites that they have not decided to visit. The advertisements are contained within in iframes. However, a malicious script redirects the entire page to a preselected destination by setting Browser Object Model's (BOM) top.

Analyzing malvertisements

Analysis of malicious advertisements is done in this section. Clear description of various aspects of malvertising and how to understand what types of websites are more prone to malvertisements is discussed in this section. Further, investigation is done whether a website is more secure by selecting a trusted ad network to serve the advertisements. Finally, examine if the publishers take the users' security into their consideration and thus, take actions to protect their visitors from being infected[9]

Type of Maliciousness

To investigate to what extent cyber-criminals utilize advertisements to promote their nefarious activities, we analyzed the collected advertisements. For this purpose, the following procedure is used: Initially, retrieve all the analysis reports from Wepawet. Then, examine the reports and look for the existence of specific heuristics like redirects to NX domains or benign websites like Google and Bing, which suggest the utilization of cloaking techniques. Additionally, it has been looked for behaviours (models) that are similar to previously-known malicious behaviors. Next, all the executables and Flash files were validated against VirusTotal. Finally, by using the previously-mentioned blacklists monitoring is done and checked if the content of the advertisement was served by a blacklisted domain. Table 3.1 shows the results of all the misbehaving advertisements that were detected in a span of ten hours across various browsers and applications at random. In general, the survey has identified 6,601 incidents in which the advertisements triggered detection framework. Surprisingly, it was observed that about 1% of all the collected advertisements show a malicious behavior.

Identifying Risky Advertisers

In this step investigation is done whether there is any preference from the side of the malicious advertisers to specific ad networks. Next measure if some ad networks are more prone to serving malicious advertisements than others. As it has been already mentioned, each ad network applies its own policy regarding the acceptance of an advertisement. For instance, some of the biggest ad networks do not allow the promotion of websites infected with malware while others, usually smaller in size, are more tolerant to this[3]

The ad networks are sorted based on the ratio of malicious ads compared to the legitimate ones served. It is observed, that there are some ad networks that are preferred by cyber-criminals, and therefore show more malicious ads. Interestingly, there are ad networks in which the malvertisements underlie more than a third of their global traffic. Figures 3.1 – 3.5 depicts the factual representation of Malvertising distribution and websites interactions with the fraudulent injections.

Although the existence of ad networks that serve malvertisements constitute a threat for the operators of the Web, the size of this risk can only be quantified if we measure the proportion that these ad networks have in the total served advertisements.

Next, three major clusters of websites were created. The first cluster contained the top 10,000 websites from Alexa's one million top-ranked websites, the second cluster the bottom 10,000, and

the third more than 23,000 websites that existed in advertisement dataset and did not belong to the previous clusters. And then measure from which websites the majority of the malvertisements is observed. It is observed that the first cluster served 82.3% of the whole malvertisements, while the second 6.2%, and the third 11.5%. One can consider that the more famous a website is, the better techniques are applied to protect its visitors. However, the recent event occurred in Yahoo! confirm our hypothesis. In detail, when users visited Yahoo!'s website between 31 December 2013 and 4 January 2014, they were aided with malvertisements. Given a typical infection rate of 9%, this incident likely resulted in around 27,000 infections every hour. In order to discover if the top websites receive more malvertisements because they display more advertisements on their web pages compared to the bottom websites, or whether they are simply preferred by cyber-criminals, we measured the number of the total advertisements (both benign and malicious) the previous clusters displayed. The results revealed that the first cluster served 76.6% of the total advertisements, the second 11.6%, and the third 11.8%. These results are close to the previously-mentioned malvertising results. Consequently, we believe that miscreants are not interested from which website their malicious code will be delivered, but they are actually concerned about the total amount of infections they will earn from malvertising[7]

To understand the type of websites that malvertisements are usually targeting, we clustered all the websites we spotted with malvertisement into major categories. Websites that contain entertainment and news content constitute almost one third of the total websites targeted by malvertisement. Interestingly, the websites that contain adult material are ranked third in the preference of miscreants. This fact conflicts with previous studies, which showed that adult content is tied to increased maliciousness[8,1]

Finally, we wanted to see the quota of top-level domains that serve malvertisements. Additionally, it is noticed that the generic top-level domains (mainly .com and .net) compose more than 66% of the malvertising traffic. Given the fact that most of the .com domains have an American-driven orientation, we believe that malvertising are primarily designed to target United States citizens.

Ad Arbitration

Website administrators might assume that by using only advertisements from major networks, which are considered trustworthy, they can protect their visitors from potential malvertisements. Inappropriately, this is not the case. There is a practice called ad arbitration, which is widely used by ad networks to increase their revenue. During the ad arbitration process, the ad networks buy impressions from publishers as if they were advertisers, and then start a new auction for these ad slots as if they were publishers. Hence, even if an administrator delegates a portion of her website to a specific ad network, she cannot be sure that the advertisements will be only provided by that particular ad exchange. Although we expected to see a similar behavior in both benign and malicious advertisements, we discovered some cases in which the ad arbitration chain had a much higher length when it came to malvertisements. In some cases, both harmless and malicious advertisements were served directly from the initial ad network. Nevertheless, there were cases in which a specific ad slot participated in up to 15 auctions for benign advertisements and up to 30 auctions for malvertisements. Even though the ad slots that participate in more than 15 auctions constitute only 2% of the malvertisements, we further investigated this phenomenon. Our results revealed that in the initial phases of the auction process, the participants are both popular ad networks and ad networks that we found out being involved in malvertising. However, once the auction process gets longer the last auctions typically happen only among those ad networks that we found to serve malvertisements. An explanation for this could be that smaller and less reputable ad exchanges come into play only when the larger ones failed to obtain an ad slot for a particular arbitration. Interestingly, it is observed ad networks to repeatedly participate in the auctions for the same ad slot. Specifically, it was noticed that the same ad networks buy and sell the same slot several times. Another stimulating fact is the distribution of the ad arbitration chains. Regarding the benign advertisements, the arbitration chain follows a decreasing trend, while, when it comes

to malvertisements, it follows a slightly different model. In absolute numbers, the chain follows the same decreasing trend; however, we observe an increase in the frequency of chains in the middle of our graphs.

Secure Environment

Publishers trust the ad networks as they give favorable advertisements. So they will not protect their ads display environment. Link hijacking i.e. redirecting original to a dissimilar destination, is a weighted attack as several users open multiple tabs for further checking. By this users will be redirected to other malicious websites without knowing that. In HTML 5 by using sandbox attribute of iframes this problem can be solved. But none of the websites use this attribute[10]

CONCLUSION

As long as there is money to be gained criminals will carry on with different methods to take favour of opportunities to take away our pockets. Our fight with cybercriminals can be scary. Many adversaries have plenty of insistences to infect users, their plans need different steps to gain. We just cut the process of chain to eradicate our loss. By simply deploying patches faster and eliminating irrelevant programs will hamper more than 85% of the attacks.

Many attacks will succeed when user's protection is low. By making known to users about these malicious ads and links which are making money from our pockets. Although we have many security tools, users also need to understand the basics to avoid individual and organization loss.

We have to know our loop holes and work together to defend ourselves from losses. Removing the threats through few applications, making user to gain knowledge and restrict attackers.

REFERENCES

1. Miss. Payal P.Kilor, Mr.Pravin. D.Soni, "Cryptography: Realizing next generation information security", *IJAIEM,* **3**(2): (2014).
2. H. Mekky, R. Torres, Z.-L. Zhang, S. Saha, and A. Nucci. Detecting Malicious HTTP Redirections Using Trees of User Browsing Activity. In IEEE Conference on Computer Communications (INFOCOM), 2014.
3. V. Dave, S. Guha, and Y. Zhang. ViceROI: Catching Click-Spam in Search Ad Networks. In ACM Conference on Computer and Communications Security (CCS), 2013.
4. P. Gill, V. Erramilli, A. Chaintreau, B. Krishnamurthy, K. Papagiannaki, and P. Rodriguez. Follow the Money: Understanding Economics of Online Aggregation and Advertising. In ACM SIGCOMM Conference on Internet Measurement (IMC), 2013.
5. Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang. Knowing Your Enemy: Understanding and Detecting Malicious Web Advertising. In ACM Conference on Computer and Communications Security (CCS), 2012.
6. N. Vallina-Rodriguez, J. Shah, A. Finamore, Y. Grunenberger, K. Papagiannaki, H. Haddadi, and J. Crowcroft. Breaking for Commercials: Characterizing Mobile Advertising. In ACM SIGCOMM Conference on Internet Measurement (IMC), 2012.
7. B. Stone-Gross, R. Stevens, R. Kemmerer, C. Kruegel, G. Vigna, and A. Zarras. Understanding fraudulent activities in online ad exchanges. In Proceedings of Internet Measurement Conference, IMC '11, 2011.
8. X. Dong, M. Tran, Z. Liang, and X. Jiang. AdSentry: comprehensive and flexible confinement of JavaScript-based advertisements. In Annual Computer Security Applications Conference (ACSAC), 2011.
9. B. Stone-Gross, R. Abman, R. Kemmerer, C. Kruegel, D. Steigerwald, and G. Vigna. The Underground Economy of Fake Antivirus Software. In Workshop on Economics of Information Security (WEIS), 2011.
10. M. Cova, C. Kruegel, and G. Vigna. Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code. In International Conference on World Wide Web (WWW), 2010.