International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Combating Cybercrime: A Growing Trend Malvertising and Ransomware

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

Abstract— 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. People across the globe are subjected to extortion on a very large scale. Ransomware is modern and technology enabled way of extortion. Ransomware stops you from using your system or device and holds your system/device or files for ransom. The present paper covers the essential discussion of Malware, Malvertising and the attack methods used to distribute malicious advertisements and also discusses Ransomware all round i.e. What is it? What are various forms of it? How it works? How to prevent it? The paper gives some preventive measures for Malvertising and Ransomware.

Keywords— Cyberwar, Cybercriminal, Cybercrime, Malware, Malvertising, Ransomware, Vulnerability

I. INTRODUCTION

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.[1,5]

Ransomware is a way of direct and large scale revenue generation using Crypto Ransomware and Locker Ransomware. Crypto Ransomware encrypts personal data and files on computer and Locker Ransomware locks the computer or device, preventing victims from using it. Locker Ransomware use payment vouchers and Crypto Ransomware use it's Bitcoins for payment. Ransomware is considered a Scareware as it scares users to pay a fee or ransom. Paying for the ransom does not guarantee that users can eventually be able to access the infected system.[7,11]

II. MALWARE

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.[2]

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.[5].

III.MALVERTISING

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.[3]

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.

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. [6]

IV. RANSOMWARE

Crypto Ransomware finds and encrypts valuable data stored on the computer, making the data useless unless the user obtains the decryption key. The developers of Crypto Ransomware know that data on computers is very important to users and they may be desperate to get their data back, preferring to pay the ransom to restore access and avoid painful consequences. Crypto Ransomware unnoticeably searches for files and encrypts them. Its goal is to stay unnoticed until it can find and encrypt all of the files that could be important and valuable to the user. By this time the victim receives the malware's message that that their data is encrypted. With Crypto Ransomware infections, mostly the affected computer continues to work normally, and users can still use the computer apart from accessing encrypted data. [8,13]

Police themed Ransomware cleverly present their ransom demands as official looking warning messages from a local police. Ransom message claim that the user's computer is locked after the police identified it as being used to visit illegal websites related to terrorism or abuse and that payment of a fine is required to settle the offense and directions for paying it via anonymous, untraceable disposable cash cards. TorrentLocker and CryptoWall malware variants are difficult to beat and grow their disjointed criminal activity into coordinated, improved stealth and effective business operations. Ransomware attack methods advanced in techniques and increased in profit in past few years. The social engineering has increased infection rates considerably. [10,14]

V. COMBATING MALVERTISING AND RANSOMWARE

Following are some preventive measures to combat dangerous threat of Malvertising:[1,4]

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

Ransomware infections can be prevented potentially by adopting following measures. [9,11]

A. Take regular backup of files and data.
B. Ransomware may arrive by exploiting vulnerability so keep security software up to date by applying patches regularly.
C. IT is good practice to access trusted and bookmarked websites.
D. Always be cautious by avoiding downloading email attachments from untrusted sources and clicking on links from email.
E. Use reputed antimalware/antivirus and Scan system regularly.
F. Use strong firewall.
G. Enable popup blocker
H. Disconnect from Internet if received Ransom notice.

VI. CONCLUSION

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. Ransomware forces its victims to pay the ransom through certain online payment methods to grant access to their systems, or to get their data back. Cybercriminals primarily focus on refining existing tools and techniques surely Ransomware is evolving progressively. The present papers talks about rising danger of Cybercrime in the form of Malware, Malvertising and Ransomware and suggest some common preventive measures for Malvertising and Ransomware.

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] Aditya K Sood, Richard J Enbody, Michigan State University, "Malvertising – Exploiting Web Advertising", https://www.cse.msu.edu/~enbody/CFS_2011-04_Apr.pdf
[4] "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
[5] "Top 5 Malware Trends for 2014 and How to Combat Them" https://www.ncbpinc.com/collateral/Webroot-Executive-Brief-01-22-14.aspx
[6] "Adblock Plus. Surf the web without annoying ads!" https://adblockplus.org, 2014.
[7] http://www.trendmicro.com/vinfo/us/security/definition/Ransomware
[8] https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
[9] http://in.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware
[10] https://www.f-secure.com/en/web/labs_global/removing-police-themed-ransomware
[11] Kim Boatman, "Beware the Rise of Ransomware", http://in.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware
[12] CISCO, Inc. Ransomware on Steroids: Cryptowall 2.0. http://blogs.cisco.com/security/talos/cryptowall-2,
[13] SYMANTEC, Inc, "Internet Security Threat Report" http://www.symantec.com/security_response/publications/threatreport.jsp
[14] Krebs on Security, "Inside a Reveton Ransomware Operation" http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/