IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Malware Analysis And Possible Solutions Of Malvertising

Arya P Pillai
Assistant Professor
MES AIMAT

Nayana Habeeb
Assistant Professor
MESAIMAT

Jibin N
Assistant Professor
MES AIMAT

Abstract.

A malicious program with a motive of attacking the computer operations and data is called a malware. Viruses Trojans, spywares, backdoors, adware, worms, rootkits, bots etc are examples for the malware. Malvertising is a type of attack where you insert a piece of malicious code into the online advertisement which redirects to some other websites to do some harmful actions. In this digital era the online advertisement has a greater impact in the revenue of business. So, it is essential to find way to identify and remove or reduce the malware through the advertisements. Hence in this paper the authors discuss about various attacks and damages that happens through Malvertising and the possible solutions to stop these attacks. In the first section of the paper, we discuss the cyber security in the context of Malvertising. Next , we present the current situation in digital marketing in terms of the malicious advertisement. Finally, the paper discusses some methods that helps to stop this attack

Keyword: Cyber Security, Malicious code, Malvertising, online marketing, digital advertisements

INTRODUCTION

Today Internet plays an important role in every one's life. It is one of the significant instruments for communication. As the Internet is growing, cyber-attacks is also increasing day by day. Air India had reported the recent cyber-attack on 21st May 2021.The personal details of about 4.5 million customers were hacked including passport, credit card details, birth dates, name and ticket information .It was disclosed that the cyber attackers had access to the system for a period of 22 days.

Different types of cyber-attacks are there such as MITM attacks, Phishing attacks, Whale-Phishing attacks etc. The most common type of cyber-attack is Malware attack, where it executes unconstitutional

activity on the victim's system. Malware is a threat to the operations in business. It can access the important business data, client information without any knowledge of the user.

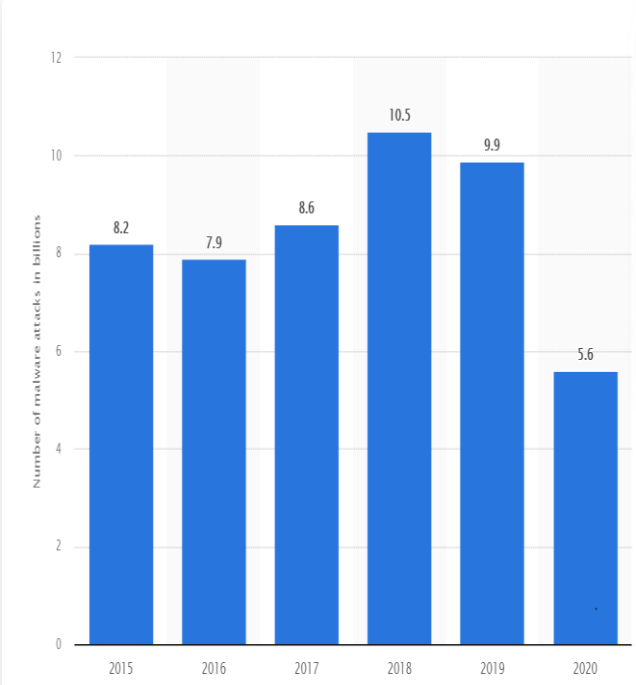
Malware is a software, which is developed to damage computers, networks, client, servers etc. It is a multiple of several software types including viruses, spywares, and ransom ware. It is as much powerful that it can hack confidential information such as border attacks, surgical strike etc.

A massive power outage occurred in Mumbai on October 2020 as a result of Chinese cyber campaign against India. This power grid failure resulted in power outages, stopping trains on tracks and hit the economic activity hard. An expert Malware analyst can easily construct unknown file formats and data patterns .They examine and identify different physical and virtual medium to spread malware into the network and computer systems. The malicious program is spread over Internet through different downloads, which is automatically getting to the system without users' knowledge.

As Information Security is introducing innovative technologies with rigorous performance, the volume of sophisticated malware attack is also increasing.2020 is a tumultuous year with a consistent increase of malware attacks with newly unfolds vulnerabilities. The Malware attackers exploit the fear of COVID-19 to cause the victim to fall in cyber-attacks. The attackers released several mobile applications related to COVID-19 updates and information. Several phishing UPI accounts were introduced which leads to cyber-attacks. The widespread of COVID -19 is becoming a right set of circumstances for the attackers to spread malware or to introduce new cyber-attacks.

The way people approach to media has completely changed by the advent of internet. In these competing worlds, as more companies are coming forward with new innovative strategies, to get maximum reach most of the organisations go for digital marketing and E-commerce. As the number of advertisements included in the website increases, the revenue from it will also on the upper side. When people use the internet services, they will also get in touch with the ads displayed. It can be considered as a relationship between people who advertise the content and the one who publish it. This trust is destroyed by the activities of cyber criminals by injecting malicious contents into the virtual ecosystem by the means of malvertising(malicious adverts served through legitimate ad networks. Here the perpetrators inject malicious code into online advertising networks and it will redirect the users to malicious websites and the rest is history. The famous websites which are already used for malvertising are Spotify, London Stock Exchange and The Network Times. Even though a lot of efforts had already put forward to minimize its actions ,malwares are found everywhere.

Graphical representation of malware attacks



The above bar graph depicts number of malware attacks from 2015 to 2020. In the most recently reported period, 5.6 billion malware attacks were carried out, down from 9.9 billion attacks in the previous year.

2. Background and related work

There are a lot of work related to Malvertising that focus mainly on the digital advertisement ecosystem to explore all the vulnerabilities. .Liu et al. [6] founded a browser-based tool that can provides detailed measurements of the existence of different ad targeting strategies. Likewise, Barford et al. [7] developed a Web crawler to collect display ads to determine whether user profile is a factor or not in injecting malwares. Some papers suggest that most of the operations are low-cost and highly effective compared to other malware dissemination techniques such as spamming and social networking [8]

The various methods involved in malvertising includes[10]

- **Malware in ad calls** — pushing the ad through third parties and affecting the systems
- **Malware injected post-click** — Redirecting to several url's when user click some websites and ending up with some disasters
- **Malware in ad creative** — Inserting malwares through graphical content and data like images, videos, banners etc.
- **Malware within a pixel** — inserting malwares in a code embedded in ad call
- **Malware within video** — There are only limited protections in the video players and will display malicious url at the end.
- **Malware within Flash video** — videos with flash are easily vulnerable to malwares.
- **Malware on a landing page** — Even on some trustful landing pages,there will be malicious contents to redirect users to infected urls.

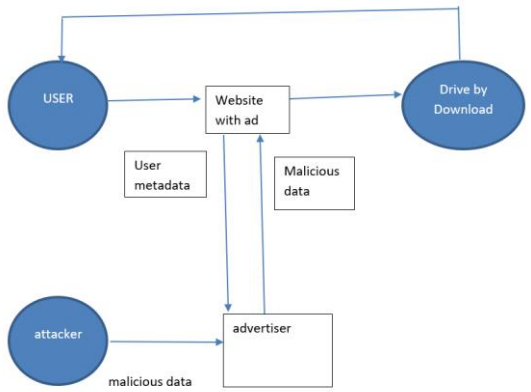
3. Methodology

It is very difficult to mitigate the effects of malwares unless there is combine efforts from publishers and users. The end users can contribute by using antivirus software, using Ad blockers, avoiding use of flash and java and updating browsers and plugins regularly. Publishers can mitigate its effects by taking care of delivery paths and adding additional security features, scanning intermittently to detect malwares and unwanted sites, showing only specific types of files rather than entire JavaScript, employing firewalls to block malicious code.

Our research focus on generating a method for analysing large volume of advertisements and there by destroying malware injected ads. In this hectic world as the greater number of peoples are using the internet, it is really inevitable to find a solution to this rising phenomenon. The existing techniques are not so flexible but also expensive[11].

The figure demonstrates the way malicious contents are injected into websites.

Fig :Representation of malware contents getting into websites



The security mechanism can be divided into 2 different phases.First phase based on avoidance or protection and the second phase deals with its detection.In the former view ,it explains about analysing each link with or without malicious content and in cooperating complex algorithms to avoid all the malwares to a greater extent.

All the advertisements are accumulated in a special storage space[9]. So, by first method plans are made to scan the entire repository using internet of things along with recording its complete course of action like its activity from start to end until user exits the webpage. All these details will be stored and encrypted using triple AES algorithm. If any of the path which is recorded already is found to be suspicious it will be discarded completely.

The second method includes, strengthening the security procedures of website administrators by rebuilding existing algorithms and adding extra security features. Since they constantly troubleshoot the websites for detecting malwares, it must not be vulnerable. So, steps are taken to equip the system with extra checking and recovering techniques and in cooperating blockchain mechanisms.

After successfully implementing both these phases ,the problems can be controlled to a greater extent and avoid risks and revenue loss by means of malvertising.

Conclusion

This research paper discusses about various cyber attacks and malware attacks and some methods to tackle the issues . In the first section of the paper, the author discusses about the cyber security in the context of Malvertising. Next , we present the current situation in digital marketing in terms of the malicious advertisement. Finally, the paper discusses a systematic method to defend such attacks

References

[1] A. Zarras, A. Kapravelos, G. Stringhini, T. Holz, C. Kruegel, and G. Vigna, "The dark alleys of madison avenue: Understanding mallicious advertisements," in ACM SIGCOMM Internet Measurement Conference (IMC), 2014.

[2] J. DeBlasio, S. Guha, G. M. Voelker, and A. C. Snoeren, "Exploring the dynamics of search advertiser fraud," in ACM SIGCOMM Internet Measurement Conference (IMC), 2017.

[3] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang, "Knowing your enemy: Understanding and detecting malicious web advertising," in Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12, (New York, NY, USA), pp. 674– 686, ACM, 20..12.

[4] X. Xing, W. Meng, B. Lee, U. Weinsberg, A. Sheth, R. Perdisci, and W. Lee, "Understanding malvertising through ad-injecting browser extensions," in International Conference on World Wide Web (WWW), 2015.

[5] S. Ford, M. Cova, C. Kruegel, and G. Vigna, "Analyzing and detecting malicious flash advertisements," in Annual Computer Security Applications Conference, 2009.

[6] B. Liu, A. Sheth, U. Weinsberg, J. Chandrashekar, and R. Govindan, "Adreveal: Improving transparency into online targeted advertising," in Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks, HotNets-XII, (New York, NY, USA), pp. 12:1–12:7, ACM, 2013.

[7] P. Barford, I. Canadi, D. Krushevskaja, Q. Ma, and S. Muthukrishnan, "Adscape: Harvesting and analyzing online display ads," in Proceedings of the 23rd International Conference on World Wide Web, WWW '14, (New York, NY, USA), pp. 597–608, ACM, 2014.

[8] C. Huang, M. N. Sakib, C. Kamhoua, K. A. Kwiat, and L. Njilla, "A bayesian game theoretic approach for inspecting web-based malvertising," IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2018.

[9] What does Advertisement inventory mean? Small Business, Retrieved from: http://smallbusiness.chron.com/advertisinginventory-mean-35920.html

[10] The Rise of Malvertising, Cyphort, 2015, Retrieved from: http://go.cyphort.com/Malvertising-Report-15-Page.html

[11] Shubham Kumar," Malvertising: A case study based on analysis of possible solutions", Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017) IEEE Xplore Compliant - Part Number: CFP17L34-ART, ISBN: 978-1-5386-4031-9