A STUDY ON WHA (WATERING HOLE ATTACK) – THE MOST DANGEROUS THREAT TO THE ORGANISATION

N.Krithika

P G Scholar, Department Of CSE, Sri Ramakrishna Engineering College, Coimbatore, India
krithikanatarajan22@gmail.com

Abstract: This paper deals with the survey on the serious threat to the organization (i.e.) WHA (WATERINGHOLE ATTACK). There are number of attacks in real world. Detecting and removing threat is one of the challenging tasks to the individual as well as to the organization. The Criminals, hacks frequent visited sites and inject a malicious code in to that specific sites. We describe how the WHA emerges, what are the root causes and necessary ways to prevent them in future.

Keywords: WHA (watering hole attack**), RTA (**remote access Trojan**), SQA (**Sequential Mining Approach)

1. INTRODUCTION:

Waterhole attack is one of the computer attacks. It targets mainly on a particular group of organization, industry and region. In this waterhole, the attacker guesses which website the group repeatedly uses and infects them with the malware. The indirect nature of this attack could be known by a desire that infect a specific site of weak links. [2] The main aim of the hackers is to hack the particular group / company. The main idea in this waterhole attack is that hackers insert any malicious code into the email / spam, employees or users ignore them. So that avoid this hackers uses a new technique called as waterhole attack where they insert a malware into frequently visited site to the company, organization (Individual / group) PC.

The general survey is conducted on the recent works related to the watering hole attack. [3] The earliest survey of this year tells that the attackers target on the energy sector where they infused light out exploit kit (EK) into the website of thirty Nine Essex street LLP. After which if any browser connected to a malicious page on the site would be probed to establish a finger print of client machine. After that Remote Access Trojan (RAT) was installed, in order to hack the complete detailed of the targeted machine.

The recent attack involves in US department of Labor [17]. Cisco identifies the suspicious Get request made to www.sellagreement.com. A malicious or infected site which are recently linked with Department of labor attack. First, the victim visits one of the sites called www.sbc.net [17]. This sites loads malicious content and their purpose is to scan the victim machine for Antivirus Software. After they collect data, the victim machine phones home its configured data. If the system is running a vulnerable piece of software, an exploit is delivered. The vulnerabilities found are phoned to home back along with cookies.

2. HOW WHA WORKS:

Hackers target the organization by using hacking tools, where the employees use the sites frequently. [12] The attacker's uses common internet tracking tools such as add this and kiss metrics to identify the sites that users frequently visited. The figure depicts the working flow of WHA

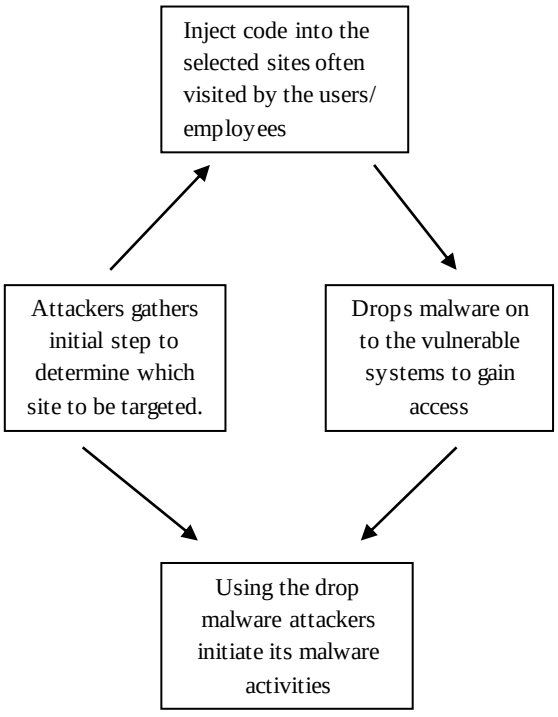

Figure 1: Working Principle Of WHA (Watering Hole Attack)

Hackers insert malware on to the specific sites and wait for the user to visit. Once the user visited the site, hackers identify the vulnerabilities by outdated antivirus & browser. [12] Using Drive by download technique, the attackers don't need user to click or download any files. A small code is downloaded automatically in the background depends on the users access rights, by this the attacker can gain the information such as information of the customer, internet protocol address. After which exploit is delivered to the targeted machine. Attackers access the targeted information by stealing the intellectual property for gaining access to the information. Insert malware into the source code of the site that the user visited, and steal data to commit fraud or sell the information to the criminals for gaining money.

2.1 Tracking Services:

Hackers identifying tracking service (i.e.) when users without their knowledge provide all the information by simply surfing the internet. [12] By doing this automated tracking methods used by marketing and ad tracking services identify the traffic patterns. There tracking service silently capture all the data's without users knowledge. This shows that which sites employees are accessing frequently and this allows the information for the attackers to enter into the companies browsing and cloud services. If when a user visits the site, the code that redirects the users browses to malicious site, so that the user machine can be assessed for vulnerabilities.

3. HOW TO DETECT THE WHA:

WHA can be detected by technique called as Sequential Mining Approach (SQA). SQA aims to find sequential patterns in time-ordered data [19]. Its quality can be measured by two factors called **support** and **confidence**. Support is a pattern proportion of various sequences in which pattern occurs [19]. Confidence is the ratio between the supports. For detecting WHA we need low support and high confidence patterns.

4. WHA PREVENTION:

For protecting against the WHA, use an updated version of antivirus. Use Google chrome or Firefox with add-ons or extensions like security enhancers that would ask for the user permission before redirecting. Always check for the latest information security news sites for the latest threats.

Standard malware defenses are one of the answers for protecting against WHA [13]. Once the malware is in browser, it captures all the passwords and sensitive information. To prevent these attacks, enterprise can remove / disable the targeted software which includes JRE, Flash, Adobe Reader & IE from system at risk. [13] To keep attackers from redirections, Secure the DNS registration and name servers.[13] Look for third party content and plan to disable them.[13] Use web application firewall with cross site scripting, command injection & SQL injection rules in deny mode.

4.1 Correlating well known Advanced Persistent Threat (APT) activities:

Organizations have to correlate and associate with wild cybercrime so that we can get up to date news above the hacking activity. And thus we can recovery / prevent from this type of attack.

5. CHALLENGES:

Visibility is one of the significant challenges for enterprises [18]. It has always been an issue for enterprises with multiple offices and security resources from different vendors. As many website moves to SSL by default in order to protect and user privacy. This gains importance to the attackers where they hide their attacks from security solutions.

6. CONCLUSION AND WAYS TO AVOID IN FUTURE:

Since the technology are developing rapidly a way to protect our data also increases people should be aware of the attacks / threats and how to come out of it. Follow the security measures and awareness to avoid with in future. By creating awareness enterprises wide and regular threat testing technique tools like **Data Breach Response Toolkit** (DBRT) by **Global Digital Forencies** (GDF) has one of the top priorities to avoid with in future call 1-800-868-8169 for more information about DBRT.

REFERENCES

1. https://en.wikipedia.org/wiki/Watering_hole_attack
2. http://searchsecurity.techtarget.com/definition/watering-hole-attack
3. http://www.networkworld.com/article/2451341/security0/how-to-protect-against-watering-hole-attacks.html
4. http://www.securityweek.com/chinese-attackers-hacked-forbes-website-watering-hole-attack-security-firms

5. https://www.symantec.com/content/en/us/about/media/pdfs/b istr_18_watering_hole_edits.en-us.pdf
6. https://www.scmagazine.com/watering-hole-attacks-are-becoming-increasingly-popular-says-study/article/542694/
7. https://www.scmagazine.com/watering-hole-websites-present-largest-innovation-for-targeted-attacks/article/543771/
8. https://www.scmagazine.com/us-department-of-labor-web-page-serves-watering-hole-attack/article/543538/
9. https://www.scmagazine.com/hackers-leveraging-ie-zero-day-used-watering-hole-attacks-to-compromise-users/article/542679/
10. https://www.scmagazine.com/new-watering-hole-attack-plants-malware-at-news-sites-to-spy-on-chinese-dissidents/article/543726/
11. http://www.infoworld.com/article/2614643/security/watch-out-for-waterhole-attacks----hackers--latest-stealth-weapon.html
12. https://www.skyhighnetworks.com/cloud-security-blog/watering-hole-attacks-protecting-yourself-from-the-latest-craze-in-cyber-attacks/
13. https://zappytech.wordpress.com/2013/02/23/watering-hole-attacks-an-increasingly-common-technique/
14. http://searchsecurity.techtarget.com/tip/Defending-against-watering-hole-attacks-Consider-using-a-secure-VM
15. https://blogs.akamai.com/2013/09/defending-against-watering-hole-attacks.html
16. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web_attack/137/watering-hole-101
17. http://blogs.cisco.com/security/watering-hole-attacks-an-attractive-alternative-to-spear-phishing
18. http://www.networkworld.com/article/2451341/security0/how-to-protect-against-watering-hole-attacks.html
19. https://content.pivotal.io/blog/sequential-pattern-mining-approach-for-watering-hole-attack-detection