The Adverse Effect of Watering Hole Attack in Distributed Systems and the Preventive Measures

Glory V. Umoh, M.Sc
Nnamnso P. Paul, M.Sc.
Department Of Information Technology,
SRM University, Kattankulathur - 603203
Kancheepuram Dt, Tamil Nadu, India.

Abstract **- This paper focuses on a simple, yet impactful crimes that occurs in the virtual world as opposed to physical attack such as war, that may lead to system crash if not notice on-time. It describes the Watering Hole technique and how it works; this technique is used in targeted attacks that aim to gather confidential information and intelligence from organisation, identifying the attack and what impact it creates. In addition, the Watering Hole Attack (WHA) is very effective, so we find preventive measures of terminating it, so that it will not invade the system.**

Keywords **- Hacking , cracking, threat, victim, zero-day attack.**

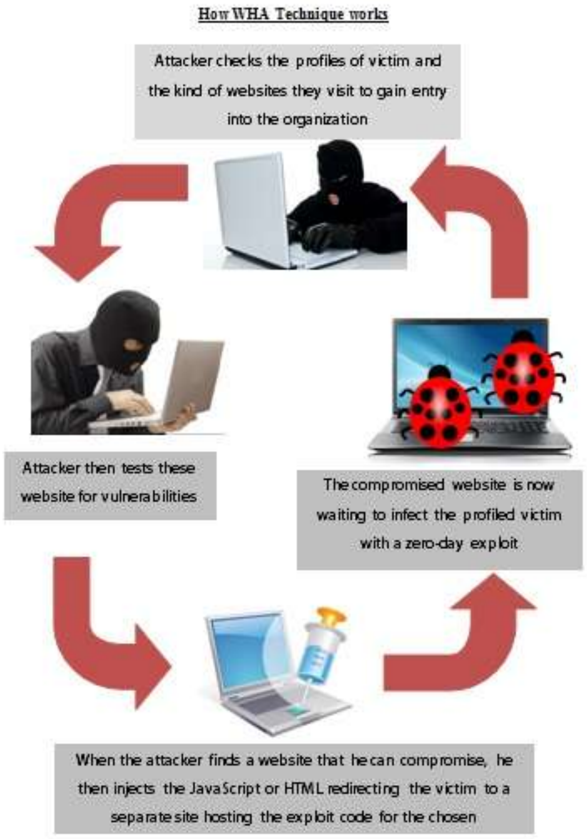
I. INTRODUCTION

Watering hole attacks are becoming an increasingly trending threat to the society at large, based on current researches.

Watering hole is a form of computer hacking and cracking whereby attacks observes websites and injects malware on to the website, the visitor or the victim might be a prominent company, organisation, region, industry, institution or any frequent visitor to a particular website. It is just like a predator waiting reflexively near a water source to ensnare prey, attackers compromise a site likely frequented by their intended victim.

Watering hole is a computer attack strategy identified in mid 2012 by RSA security in a campaign known as VOLTO. The goal of watering hole attacks is not to serve malware to as many systems possible, instead, the attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims.

II. HOW WHA TECHNIQUE WORKS


How WHA Technique works
Attacker checks the profiles of victim and the kind of websites they visit to gain entry into the organization
Attacker then tests these website for vulnerabilities
The compromised website is now waiting to infect the profiled victim with a zero-day exploit
When the attacker finds a website that he can compromise, he then injects the JavaScript or HTML redirecting the victim to a separate site hosting the exploit code for the chosen

III. WHO ARE THE TARGETS OF WHA

WHA techniques are used to target attack and congregate confidential information and intelligence from the under-listed organizations. The congregated information are later used to instigate more damaging attacks against the affected organizations.

A. Top Business Firms

The attacker can inject malware code secretly into commercial organisation that operates on profit basis, through selling goods or services to consumers' website and obtain the following information to attack back.

- Financial record of the business
- Information flow in the business
- Processes operation
- Style of work or apparatus used
- sales
- Shipments
- Purchase and inventories
- Source of income
- Losses or expenditure .etc.

B. Non-Governmental Organizations (NGOs)

This are organisation that may be funded by governments, businesses, foundations , private Individuals or run primarily by Volunteers. It may be susceptible to inject malware to the Website and obtain the following information to attack back …..

- The objectives and goals of the organisation
- Financial record
- Sources of fund
- Contribution from volunteers
- Organisation standards
- Mission and activities, etc.

C. Governmental Organizations

This are legal entity that undertakes commercial activities on behalf of the Government. Whose site may be vulnerable and can easily be attacked by Watering Hole to congregate the following information:

- Government budgets
- National archives and record of administration
- Salaries of workers
- Governmental rules and procedures
- Model code of conduct for employees
- Business proposal, etc.

D. Financial Institutions

This is an establishment that focuses on financial transactions, such as investment, loans and deposits, Examples of such Institutions are banks, trust companies, insurance companies and investment dealers. Attacker can inject malware code secretly into the Establishment's website and obtain the following information to attack back

- Customers Information
- Financial record
- Filing System
- workers and customers profile
- stacks of unopened bills
- Goals and objectives of the institution
- Commitment and exemptions of trade
- Negotiations of services, etc.

E. Colleges

The attacker can inject malware code secretly into colleges' website and obtain the following information to hit back

- Fees and other charges portal
- Financial record
- Student's results
- Staff and student's profile
- Course forms
- Registration form, etc.

IV. IMPACTS OF WHA

Companies like Facebook, Microsoft and Apple have been a victim of Watering Hole Attack. This attacks aimed at companies that are popular and they target these companies in an inexplicit way that uses a discrete site as an attack vector.

This attack can lead to loss of confidentiality – where the companies' profile, private and secret documents are leaked and accessed secretly by an attacker, which they can use to harm or attack the victim.

V. IDENTIFYING WHA

Attackers can identify Watering Hole site by injecting malware into a frequently visited site. But this process is not easy with professional websites with high-security settings or parameters.

The following are the techniques used by the attacker to inject malware and gather information from a frequently visited site

A. *Tracking Services*

Tracking services technique involves the use of automated tracking process either by marketing or ads to identify traffic patterns and accesses information provided by a visitor while surfing.

In a normal manner, the visitor will provide information as required from the website, unconsciously to the user that there is a tracking services that collate all the information and forward to the attacker.

Tracking services techniques provide the attacker with the complete information about an organization's frequent access site and access policies. This technique is not transparent to the user.

B. *Set Trap*

This technique gives the attacker information about a site and guides to access a target. The targets are mostly site with less security or companies whose security are not strict. The attacker sets s trap by injecting a malicious code on the vulnerable sites and waits for users/victim to visit the sites and carry out normal practice.

When the victim visits the site, the injected malicious code traps and redirects the victim's page or browser to a malicious site so that the victim's computer can be assessed for vulnerabilities and attack.

VI. WHY IS IT EFFECTIVE?

The attackers subsume procedure to evade the targeted organizations, protection or firewalls in order for the Watering Hole Attacks to be successful. This may come in form of human error.

The main aim of Watering Hole is not to distribute malware to the distributed system, the attackers utilized on well-known and trusted sites to be visited by their targeted victims. This give rise to Watering Hole technique effective in delivering its planned payload.

Watering Hole Attacks can also incorporate zero-day feats that target unpatched susceptibility, and the victims are left with no resistance against this feats.

VII. PREVENTIVE MEASURES OF WHA TECHNIQUES

The following are some preventive measures of WHA techniques from attacking a vulnerable sites:

A. *Frequent Software Update:*

It is advisable that organizations should be updating their software to the latest patches from the authorized vendors in other to avoid WHA from tracking the old patches and capitalised on it.

B. *Detection of Network Traffic:*

Organization should implement security measures to prevent attack arising from malware generating traffic while communicating with the server from increasing rapidly. Technologies such as Trend micro Deep Discovery, Kaspersky Internet Security can help detect such suspicious network traffic and terminate the communication which results at redirecting the victim to another website.

C. *Interaction with well Known Advanced Persistent Threat(APT) Activities:*

With the help of big data analytics, companies or organizations can be aware on whether they are affected by a targeted attack by interaction in the wild cybercrime activities with what is happening in an organization network.

Organization should build their own private local intelligence so that their document can be protected from the targeted attacks.

VIII. CONCLUSIONS

Nowadays the distributed system is susceptible to different kinds of attack. Watering Hole is one of the attacks that are used to gain dominance in competitive areas. The more competitive advantage the organization have, the more frequent the attack.

Watering Hole Attack is used to test frequently visited sites for vulnerabilities, then inject malicious codes as trap which is not visible to the victim. As soon as the visitor visits the site, the injected malicious code redirects the victim's system to malicious site, and hijack information using zero-day attack which are used to infiltrate the site and attack.

It is not harmful to the victim(user), rather, to the organization or company whose site are vulnerable and lack rigid security measures to stop such attack.

Finally, knowing about the Watering Hole and implementing the preventive measures will significantly improve the security of information in the organization/company's website.

REFERENCES

[1] B. Donohue, *" Watering Hole Attack Targets Automotive, Aerospace Industries"*, September 2014

[2] Internet Explorer Zero-Day Used in Watering Hole Attack: Q&A, Symantec Security Response Symantec Employee, Dec 2012.

[3] M. Michael., *" Why Watering Hole Attacks Work "*, March 2013. Available: https://threatpost.com/why-watering-hole-attacks-work-032013/77647#sthash.8WthZOip.dpuf.

[4] New Internet Explorer 10 Zero-Day Discovered in Watering Hole Attack, Symantec Security Response Symantec Employee, Feb 2014 .

[5] O, Robert., *" Watering Hole Attacks: Tips on outsmarting Hackers "*, May 2014.

[6] W. Gragido, "*Lions at the Watering Hole – The "VOHO" Affair*", *The RSA Blog*, EMC Corporation, July 2012.

[7] A. S. Tanenbaum and M. V. Steen, "*Distributed Systems: Principles and Paradigms*", 3rd ed., Prentice Hall Press, 2013.