Advancement in Robust Cyber Attacks-An Overview

Nikunj Pansari

Department of Information Technology

Krishna Institute of Engineering and Technology, Ghaziabad

Abdul Kalam Technical University, (India)

Dhruwal Kushwaha

Department of Information Technology

Krishna Institute of Engineering and Technology, Ghaziabad

Abdul Kalam Technical University, (India)

ABSTRACT

Cyber-attacks usually are quite costly for the victims in terms of their loss of information, materials and confidential documents with added auxiliary consequences of it. These attacks are capable of leveraging any system or network specifications and thus cause more harm to them than ever intended. Artificial Intelligence(AI) is a boon to the human economy, as well as the recent development in the science and technology. But, when attackers use it for exploiting their attacks, it can be quite catastrophic for the victim. Internet of Things(IoT) makes our life smart and easier, but if IOT could be combined viewed as a Ransomware, what grievous damage it can cause is also unignorable. Sandboxing technology has become increasingly useful for detecting and evading malware infections. Some famous attacks like phishing, SQL-injection, and DOS/DDOS can be also beneficial for forming the primary path for an attacker to initiate. When an attack like Meltdown and Spectre penetrates into the hardware, it becomes extremely undecidable for the victim to respond.

Keywords-*artificial-intelligence, cyber-attacks, IOT, meltdown, ransomware, repercussions, sandboxing, spectre.*

I.INTRODUCTION

Organisations always try to improve or enhance their security to a maximum, to deny the attackers to steal any kind of confidential information or data. Continuous Advancement is technology leads to definite development. This principle is true, not just for a country or organization but also for the cyber-attacks to occur.

The attackers could use more renowned and advanced method for leveraging the security of any system. When an attackers try to use Artificial Intelligence(AI) for initiating their attacks on the victims, it becomes quite troublesome for victims to recover from it. Sandboxing-technology proves to be the useful tool for inspecting and detecting malware infections. It could potentially define the report of the malicious patches in it. Internet of Things(IoT) makes the world and the people(users) smart. Ransomware is quite harmful when effective to its extent. When this combination of IOT and Ransomware are built, it results in the alarming state for the users.

Famous cyber-attacks are often lethal, but if countermeasures are implemented properly, then the system or network can be secured from any kind of such attacks also. Phishing is often trying to make the users believe into an environment, which looks absolutely real, but offers very less assistance for the users could identify it properly. SQL-Injection does the same kind of work of other attacks, specifying its domain of gaining unauthorized access to the user's login credentials or other personal information. DOS/DDOS attacks bring out the users for denying the services that were being offered to them earlier, by various flooding mechanisms.

When cyber-attacks are dealt with, focus defines purely on the software-based attacks only. Now, there are some hardware-based attacks which actually tries to eat up the information or services provided through that operating

system or the processors. Meltdown and Spectre attack basically, tries to break down the isolations between the series of layers of the user application and the operating system.

II.AI-Powered Attacks

Traditionally, cybersecurity has proved to be the major and most essential part of any system, whereby the attackers or intruders are being kept under the illusion for being modifying or unauthorized access of the anyone's information or data. However, the attackers would continue to perform their malicious work or either hire someone to do it for them. [1]

Artificial Intelligence in combination with Cyber-security, utilizes machine learning and its algorithms to get understanding of any “norm” of defined system, and then regularly use to check about the deviation from that particular set norm. This is used by the enterprise for breaching updates and accordingly react to it. Obviously, some of the utilities are duly valuable enough to be put at risk, even with a slight degree of error or with a very efficient or intelligent system. [1]

As Artificial Intelligence(AI) is proving to be main limelight for distributing, developing, gathering and imparting major useful and beneficial services and facilities for the future as well as the present with the support of persistent-automation. When hackers or attackers start using the AI for attacking or generating all their malicious attacks, then it becomes a source of unmanageable vulnerability. [1]

III.Sandbox-evading Malware

Security researchers, mobile detection marketplace and usually the antivirus companies use the Malware sandboxes. These groups usually encounter with the difficulty of environment-aware malware which changes its state and functioning if it encounters it is being carried out in an analysis environment. [1]

Virtual machines are used by the sandboxes. This system can be easily being gettable, by scrubbing the vendor-specific drivers, BIOS versions, processes and other showing the VM-revealing indicators. On the other hand, the more enlightened sandboxes, part away from the virtualization-based systems and emulation-based systems towards bare-metal hosts. [1]

Sandboxes operate on a simple principle-detecting the file, if it is malicious or not depending on its observed behavior in a controlled environment. The sandbox allows the malware to perform all of its malicious operations and records the resulting behavior. After the due course of time, the result of the system is examined by halting the analysis and looking or determining typical behavior patterns which are more malicious. Sandboxes are able to detect targeted or zero-day malware because the detection is not based on algorithms. [1]

IV.Ransomware and IOT

To increase ease-of-use and advanced security features, IOT devices are generally designed smartly, but they typically don’t offer consumers the option to upgrade or apply patches when there are issues.IOT is on the verge of revolutionizing healthcare and other domains. [1]

Additionally, proper security concerns are standard to be implemented, so many vendors adopt convenience over it e.g. using default credentials in their products, which are easy for an attacker to compromise. Due to this approach, an evident violation of the known practices in product development, which leads to making these devices more vulnerable to attacks. When the security of the products is considered, IOT device manufacturers usually operate largely without regulation, standards or oversight –thereby defining an ideal situation for the attackers to exploit. [1]

Now, when this IOT starts to combine with the ransomware, the impact of it is quite alarming as it enables the attackers to access others data on their devices, also thereby, allowing for disruption of certain useful services for the consumers. It can create a situation having real, physical and potentially dangerous implications if the combination could interfere with the different functionality of device itself. [1]

For instance, a smart thermostat affected by the ransomware could significantly increase the heating in summers

or could be absolutely turn off down in winters unless any ransom is paid. While this might be only an annoyance for most people, it could prove harmful to some vulnerable victims. Another instance could be that a smart lock similarly infected through the ransomware could potentially lock up the people in or out of their houses or can make it permanent open, allowing the attackers to steal easily and effectively, all the belongings of the house. Also, huge disruption can be caused due to infection of smart bulbs, smart fridges and basically any of the smart device operated the system. [1]

V.Famous Attacks

There are certain well-known cyber-attacks, which are constantly a source of worry for all users, but appropriate countermeasures, if followed properly can easily, make it fail.

5.1. Phishing

Phishing is the type of attack, wherein the attacker uses certain techniques and methods to deceive the victim into providing some confidential information, that indeed needs to be protected. The techniques could include certain spoofing attacks and social engineering method to leverage the security of information of victim. [4]

Now, the confidential information could include bank account details, personal credentials, credit card number, password, and pins, etc. It means the security of all these is just disappeared, from a single attack. [4]

There are various ways for phishing, one such include creating a fake page of a website. The fake page of the website should look exactly the same as the original one, to trick or deceive the user to click on it, thinking it as a real one. [4]

The ways by which this can be initiated or performed are-

5.1.1.1. Using Static IP

Fake website page can easily be created by using tools for cloning the website, to make it look exactly the same as the real one. As, we all know that, all these attacks are being performed in Kali Linux because it provides all these tools inbuilt. So, we have to open the SET (Social Engineering Toolkit) option from Start menu, then we have the to perform the steps for cloning the website. [4]

Steps for cloning the website-

5.1.1.1.1. Select Social Engineering attack.

5.1.1.1.2. Then, select website based vectors.

5.1.1.1.3. Finally, select site cloner for creating a replica copy of the website.

After this process, user's IP address is used to make a static link to the website that is to be cloned. After that, websites to be cloned is written and a fake page of the exact website is being created in very short time. Now, it can be used to find out the user's login credentials easily. [4]

5.1.1.2 Dynamically using tools

Certain tools are available which help in making the exact replica of the website page. Now, basically, the attacker has to create the fake website page UI on it, using the features provided in the tools. After that the age is created, the attacker can use certain settings to direct the page's login details and user's credentials to his mail-id or his system. [4]

5.1.2. Countermeasures of Phishing Attacks-[4]

5.1.2.1. Phishing Scams Alerts, Add-ons/Extension.

5.1.2.2. Educating the people about the consequences of Phishing and how to get secure from it.

5.1.2.3. Domain-specific passwords should be auto-generated.

5.1.2.4. Random passwords are generated and stored in the database using Web Browser's PWD Database.

5.1.2.5. Use of Virtual keyboards for more security.

5.1.2.6. 2FA: A two-way Authentication process.

5.1.2.7. TMP Chip: Trusted Computing Mechanisms.

5.1.2.8. There could be Encrypted Key Exchange process, which could prevent the dictionary attacks.

5.1.2.9. Check for ‘https' instead of ‘HTTP' in the link.

5.2. SQL-Injection

SQL-Injection basically uses certain malicious SQL-queries to execute the attack on the victim's website. These queries usually grant the access to the attacker as an admin, as the attacker provide some queries (figure 5.2.2.) to the login details to fool the database server of the website. Hence, the server does not understand the instruction and thus get the access. [2][3][5][6] The main point to note here, is that how will the attacker protect himself for revealing his identity. Now, one of the way for it.is to use a TOR browser. This Browser makes the IP of the attacker anonymous, thus being able to attack perfectly. [2][3][5][6]

5.2.1. SQL- Injection Countermeasures [2][3][5][6]

5.2.1.1. Intrusion Detection System(IDS) and Intrusion Prevention System(IPS) can also be used. E.g.: -SNORT can be used.

5.2.1.2. The privileges of the user’s connection to the database should be checked appropriately.

5.2.1.3. Using strong passwords for Administrative accounts.

5.2.1.4. Admin privileges, by default, should be avoided.

5.2.1.5. Secure hashing algorithms such as SHA256, MD5, etc. should be used.

5.2.1.6. The input field should be sanitized and validated.

5.2.1.7. Entries containing Binary data, comment characters, and escape sequences should not be accepted.

5.2.1.8. There are a few of the tools available for reviewing the source codes.

Username	Password	SQL Query
admin	' or '1'='1	SELECT * FROM users WHERE name='admin' and password='' or '1'='1'
admin	' or 1='1	SELECT * FROM users WHERE name='admin' and password='' or 1='1'
admin	1' or 1=1 -- -	SELECT * FROM users WHERE name='admin' and password='' or 1=1-- -'
admin	' or '1'='1	SELECT * FROM users WHERE name='admin' and password='' or '1'='1']

Username	Password	SQL Query
admin	' or ' 1=1	SELECT * FROM users WHERE name='admin' and password='' or ' 1=1'

Fig- 5.2.2. [3]

5.3. DOS/DDOS Attack

Denial of Services(DOS) attack is executed, when the attacker wants to exhaust or limit the resources or services of the victim's system. Network Congestion situation occurs and the attacker sends huge volumes of traffic to the victim's system. Attackers use the vulnerabilities of the website for attacking. In this attack, large no. of HTTP requests is being sent in a very small amount of time which ultimately leads to exploitation of the website. [7][8]

Distributed Denial of Services(DDOS) attack uses multiple systems to attack while making it more difficult for security. All the procedure of the attack remains the same as DOS attack. A DDOS attack is quite hard for detection since, because of the limitations of the network components. [7][8]

Now, these attacks could include TCP SYN flood, Ingress/Egress filtering, IP Traceback, Smurf, UDP flood, traffic shaping and traffic analysis. All the recent DOS attacks are very dangerous for a large organization because their whole work is halted and they become inaccessible to customers and their associated partners. [7][8]

VI. Meltdown and Spectre Attack

Meltdown and Spectre are used for exploit of critical vulnerabilities or disadvantages of modern processors. These are responsible for bringing out the information stored currently on the computer. [9]

Meltdown is a kind of hardware-based attack because it interrupts the isolation between the two important components of a computer system i.e. the operating systems and the user applications. It facilitates the access of memory, information, and contents of other operating systems and the programs. The unpatched operating system running on a computer having a vulnerable processor, then that might be dangerous as it is highly prone to the leaking of information. Not only personal computers but the cloud infrastructure are also a victim of it. So, there are software patches to disrupt meltdown attack. [9] [10]

Spectre is more an application-based attack because it leverages the segregation between different applications. It initiates by giving an error-free program, which becomes a bait for getting the information. This reasonably increases the chances of attacks and thus the applications become more prone to being a prey themselves. This attack is more dangerous for being exploited than Meltdown and is also difficult to diminish. Thus, for this attack also, there are some Software Patches which facilitate an ease from this attack. [9] [11]

Both these attacks can find vulnerabilities in older versions of processors as well as modern processors. Intel, AMD, ARM are some of the processors affected due to it. It suits perfectly to the example of 'an optimization gone wrong'. [9] [10]

6.1. Meltdown attack basically initiates with following 3 stages

6.1.1. It focuses on the operating system and different address space basics. It means how the address is being defined or allocated for different processes. This address space basic also considers the inter-relationship between different processes. [9] [10]

6.1.2. It considers the hardware part of the system. It means basically an 'Out-of-order execution', where a defined sequence of instructions is being set, but the processors do not follow these and thus an order different from the defined is executed. Attackers can easily take the advantage of it. [9] [10]

6.1.3. The micro-architecture is evaluated for looking the cache memory. This cache memory becomes a source or path for attacking. The attackers perform a timed-side channel attack, which makes him accessible the memory address which is hidden for confidential purposes. [9] [10]

VII.CONCLUSION

A Sustainable challenge to the users is the threat of the cyber-attacks, that they might encounter with. Proper countermeasures are provided, for the each of the attacks, so that the exploitation level by the attackers could be reduced largely. Now, these exploitations can be further improved, by implementing or carrying out more secure and user-friendly services of the applications or websites. Advancements in the cyber-attacks do not fully signify that the users are the sole victims of the attack, rather technology also facilitates the attacker to redefine their actions to make the attack more troublesome. Phishing, SQL-Injection, and DOS/DDOS attack are just executed by the attackers if they try to persistently break the isolation between the users and their services of the system. On the other hand, users have to become more secure, knowledgeable and intelligent in order to identify such attacks before happening, then it could be curbed largely. Hardware-based attacks can be controlled using the introduction of certain software security patches against the exploitation.

VIII. ACKNOWLEDGEMENTS

We would like to express our heartiest gratitude to all the preceding papers authors. These papers and references provided us with all the appropriate knowledge and determination for all our sincere efforts. Also, it would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to all of them. Our family members were the most important sort of encouragement for us to define this paper. We would like to thank our parents, for their love and guidance in whatever fields we choose to pursue. They are our ultimate role models.

REFERENCES

[1] https://www.csoonline.com/article/3250086

[2]Salem A. Faker, Mohamed A. Muslim and Harry S. Dachlan, A Systematic Literature Review on SQL Injection Attacks Techniques and Common Exploited Vulnerabilities, *International Journal of Computer Engineering and Information (VOL. 9, NO. 12, December 2017, 284–291).*

[3]Zainab S. Alwan, Manal F. Younis, Detection and Prevention of SQL Injection Attack: A Survey, *International Journal of Computer Science and Mobile Computing (Vol.6 Issue.8, August- 2017, pg. 5-17).*

[4] Anu Yadav and Jatin Gemini, The Security threat in Cyber World – cybercrime as PHISHING, *Advances in Computer Science and Information Technology (ACSIT) (p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 3; April-June, 2017, pp. 161-165).*

[5] Sonam Panda, Ramani S, Protection of Web Application against SQL Injection Attacks, *International Journal of Modern Engineering Research (IJMER) (Vol.3, Issue.1, Jan-Feb. 2013 pp-166-168).*

[6] Venkatramulu Sunkari & Dr.C.V. Guru Rao, Defensive Approaches on SQL Injection and Cross-Site Scripting Attacks, *Global Journal of Computer Science and Technology: E Network, Web & Security (Volume 14 Issue 2 Version 1.0 the Year 2014).*

[7] Darshan Lal Meena & Dr. R. S. Jadon, Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches, *International Journal of Advanced Research in Computer Science and Management Studies (Volume 2, Issue 4, April 2014).*

[8] Saravanan Kumaraswamy and Dr.R. Asokan, DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS DETECTION MECHANISM, *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT) (Vol.1, No.5, December 2011).*

[9] https://meltdownattack.com/

[10] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lip, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom; Spectre Attacks: Exploiting Speculative Execution, *Cryptography Research Division.*

[11] Moritz Lip, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg; Meltdown., *Cryptography Research Division*.