Zero-day Attacks and Countermeasures

Nafin Mahmoud
Computer Science and Engineering
Qatar University
Doha, Qatar
nm1913152@qu.edu.qa

Talha Abdullah Punjabi
Computer Science and Engineering
Qatar University
Doha, Qatar
tp1903446@qu.edu.qa

Abrar Shahriyar Hossain
Computer Science and Engineering
Qatar University
Doha, Qatar
ah1912955@qu.edu.qa

***Abstract*— Nowadays, skilled attackers can uncover flaws in any networked application. A zero-day attack is one of the most serious threats for any business; many of these attacks go unreported, therefore the problem spreads swiftly before any response. For personal benefit, attackers utilize these vulnerabilities to steal sensitive data or cause harm to systems. Even if firms have safeguards in place to fight against known threats, a zero-day attack can occur out of nowhere. A zero-day attack poses a significant threat to an organization's security. Recent malware outbreaks have put enterprises' security systems at risk. This results in assaults such as botnets, crypto jacking, APT, and so on. The concept of a zero-day attack and the steps involved in carrying it out these attacks are outlined. Discussions about how to detect and thereby avoid successful zero-day attacks have also been summarized and discussed.**

Keywords—zero-day attacks, countermeasures

I. INTRODUCTION

One of the biggest threats that exist among any organization is the Zero-day attack. Zero-day attacks are ones that occur because of the discovery of new vulnerabilities in a system. Zero-day attacks pretend to be a basic risk to the association's system as the unknown vulnerabilities can be exploited. It is hard and challenging to predict the nature of the attack due to the unknown vulnerability [1]. This attack occurs before the developers have a chance to patch the flaw. Since there are no updates for the zero-day vulnerability, the chances of the attack to be successful is high. This attack can be used to harm assets or steal sensitive information from the system. The patches to fix these vulnerabilities can even take up to weeks, which gives ample time for the attacker to cause enough damage to the individual, system, or the organization. In general, the persistent fear of a zero-day attack in a computer system or application is known as a zero-day attack [1]. The prevention of zero-day attacks is one of the most pressing security challenges that modern businesses confront. To protect organizational assets, zero-day malware must be recognized, destroyed, and deleted. The purpose of security analysis is to understand the attack so that defenses can be built to safeguard the organization's network.

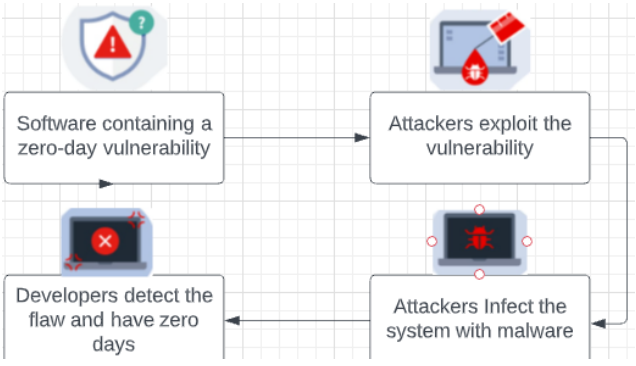

Fig. 1. Overview of a Zero-day Attack

A. *Types of attackers*

Attackers who hack to acquire an advantage can launch zero-day attacks. They can be classified into different types of attackers based on their motives.

1) Cyberwarfare Attackers: Cyberwarfare is an attack that takes place in cyberspace, which is an environment where information is transmitted via network. [2]. Attackers utilize cyber-attacks against a nation to cause physical harm, such as loss of life, through causing damage to assets. This is a threat to national security, and it is carried out to bring down information networks by attacks such as denial-of-service attacks, propaganda campaigns, or even economic disruption. A recent cyberwarfare incident in Iran was caused by malware introduced through a Universal Serial Bus (USB) device, resulting in significant harm to nuclear weapon manufacture [3].

2) Hacktivists: Group of cyber-attackers who get together to carry out cyber-attacks for political, social, cultural, or religious benefits. They deface or leak information from organizations to communicate a message and raise awareness for a cause they support [4]. Carding forums are frequently used by them. Tor, for example, improves the anonymity of user activity on the black web, allowing criminals to share compromised information and benefit from it in a fraudulent manner. [4].

3) Cyber Criminals: The reality is that continuous amalgamation of technology in everyday life is creating an environment for attackers to be motivated to do cybercrime. [5] Attackers who carry out cyber-attacks to attain monetary gain. They attempt to make a profit by carrying out attacks such as ransomware, selling information, and so on.

B. *Vulnerabilites*

Vulnerability is present in most software whether it high or low. Zero-day vulnerability is a vulnerability in a software or hardware that is not known to developers. According to the National Vulnerability Database (NVD), the reported number of vulnerabilities doubled in the years 2017, 2018 and 2019 [6]. Software vulnerabilities often is a result of glitch. Zero-day exploit gains system access by exploiting a vulnerability [6].

Examples of Zero-day vulnerabilities
CVE-2017-8759- SOAP WSDL Parser Code Injection
CVE-2017-0261- EPS "restore" Use-After-Free
CVE-2017-0262-Type Confusion in EPS
CVE-2016-4117 Flash Zero-Day Exploited in the Wild
CVE-2016-0167 Microsoft Windows Zero-Day Local Privilege Escalation
CVE-2016-1019 Security Advisory for Adobe Flash Player
Adobe Flash Zero-Day: CVE-2015-3113APT3
CVE-2015-2424 Microsoft Office Zero-Day CVE-2015-2424
CVE-2015-1701 Adobe & Windows Zero-Day exploits

Fig. 2. Examples of Zero-day vulnerabilities

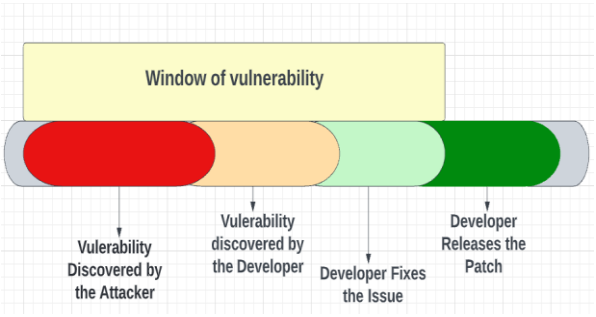

Fig. 3. Timeline of zero-day vulnerability

The above shown figure 3 depicts the timeline of zero-day vulnerability and the window risk for attacks and damages possible.

Zero-day attack cause significant harm to people who use a vulnerable system, such as an operating system, large businesses or enterprises, individuals with access to sensitive corporate data, governmental institutions, or pose a threat to national security. The longer the time takes for a patch to be installed after an attack, the higher will be the chances for an attacker to achieve his evil goal.

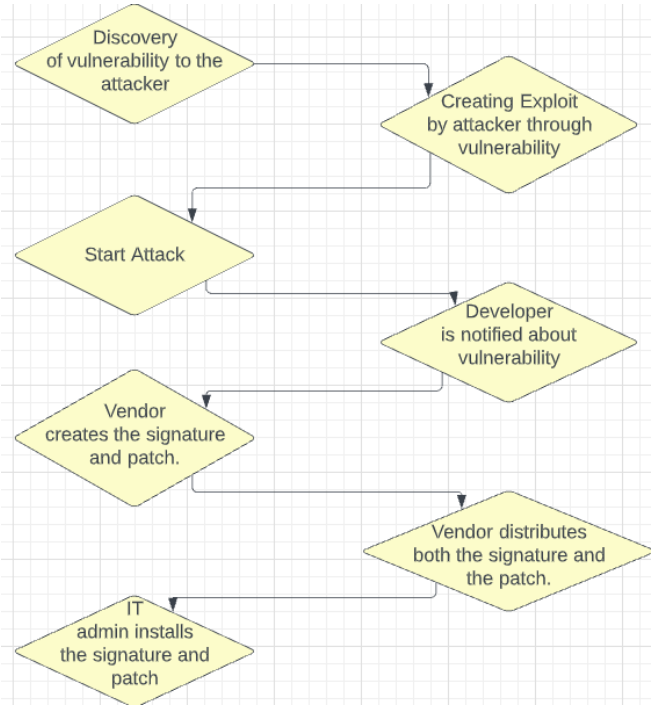

Fig. 4. Timeline of zero-day attack [7]

C. Past attacks

1) Wannacry: WannaCry, a very aggressive new strain of self-replicating ransomware, infected hundreds of thousands of computers around the world in May 2017 and held victims to ransom [14]. The attack was successful due to the carelessness of people about updating their computers periodically. Hackers utilized the opportunity to attack the outdated machines and most of the machines were run by Windows operating system. It used a zero-day exploit produced by the National Security Agency (NSA) codenamed EternalBlue, which was disclosed by the unknown hacker organization The Shadow Brokers [15]. Most of the victims had no knowledge about phishing and fell into trap of the attackers' phishing emails.

2) Operation Clandestine Wolf: Adobe flash player was targeted in this operation by attackers. They exploited the vulnerability of the flash player. When Adobe Flash Player analyzes FLV files, the attack makes use of a zero-day vulnerability and this operation was reportedly conducted by a Chinese outfit known as APT3 [15].

3) Russian doll: This is another attack that exploited the vulnerability of Adobe Flash Player. In April 2015, FireEye Labs discovered a Russian doll APT operation [15]. In an attempt to obtain access to sensitive information, the threat actors used two zero-day vulnerabilities. At first, to deploy a virus to the target system, the malware utilizes an Adobe Flash Player vulnerability. The targeted user will be directed to a website controlled by the attacker after being deceived into clicking on a malicious link. Later by using Windows local privilege escalation vulnerability, the attacker gains access to the targeted user's system permissions. Afterward, the attackers proceed to steal data from the victim.

4) Hurricane panda: For compromise and persistence, Hurricane Panda employs the China Chopper webshell [15]. The operations begin with the compromise of web servers and the deployment of Chopper webshells, followed by the escalation of privileges utilizing a previously undisclosed vulnerability in the local privilege escalation tool. It raises attacker privileges to system user privileges, then spawns a new process with these access permissions to conduct commands, often intelligence-gathering activities.

5) Dark leech attack: Dark leech is the codename of an operation that began in 2012 and contaminated thousands of Apache servers. Dark leech relates to an Apache module that was used to distribute malware and was accessible on the black market. The campaign attacked mainly on web servers. The dark leech campaign successfully infiltrated over 40,000 online servers [15].

6)Stuxnet: One of the cyber weapons employed against Iranian nuclear facilities was Stuxnet. Stuxnet was built with rootkits, four zero-day exploits, and a worm [8]. This was developed by attackers to be inserted into a conventional industrial control system. Stuxnet's purpose was to slow down rather than destroy the facility's production. The strategy was prepared in the following order: [8]

a) The software was induced into a controller computer at the plant.

b) The program collected and transmitted data about the plant's computers and how they are configured to the agencies.

c) Using this information, the agency created a worm that attacked the plant's computers. The new program was induced into the plant's computer controller.

d) The worm disrupted the working of the centrifuges and forced them to spin fast or slow, resulting in the destruction of some of them.

e) New variants of worms were created and caused different faults in the plant's operation.

The entire event ended up causing substantial damage to the Iranian production facilities. The Iranians attempted to secure the plant in response to the attack. Even after that, new

attacks were being carried out that posed a threat to the Iranian production facilities.

II. IMPACT OF ZERO-DAY ATTACKS ON SECURITY OF ORGANIZATIONS AND SOCIETY

A. Negative Impacts

1) Data Theft: Zero-day attacks can be used by attackers to gain access to a company's or organization's critical and sensitive data [16]. This information could be sold to others for profit on criminal websites or sold to criminals for nefarious purposes.

2) Identity Theft: Attackers use unauthorized control over the victim's network, websites, or programs. They can also inject in the victim's device any malicious malware or virus that can cause permanent damage to the device [16].

3) Reputation damage: The attacker can acquire access to the victim's device or system, which he or she can then use to post or produce publicly to harm the victim's reputation. They can also reveal that the company's security systems are vulnerable, allowing many additional attackers to target the same system and increase the harm.

4) Financial Loss: Zero-day attacks can bring systems to a halt for hours or even days. These can result in financial loss, particularly in large corporations [16]. Financial losses can also arise when developers or patch manufacturers attempt to investigate, respond to attacks, and recover. Large organizations can still make a comeback unlike small or new organizations, which may even shut down.

5) Legal fines: If the owner cannot prove that a cyber-attack on the system was caused by a security violation or breach rather than security negligence. Organizations may face significant fines or penalties because of these attacks [16].

6) Watering-Hole Attacks: Zero-day vulnerability can lead to attacks such as watering-hole attack [16]. The attacker finds an exploit in the most used web pages by the victim and try to gain access to the victim's network and computer.

B. Positive Impacts

Although, Zero-day attacks are just attacks, and hence lead to loss of data, infrastructure, etc. There is a good aspect to these attacks as well. Firstly, once these attacks are known to the public, other developers can quickly patch these vulnerabilities and hence preventing their software, hardware, or firmware from being exploited. Secondly, when an exploit is discovered, there is a time limit under which a developer must produce a solution as quickly as possible, which is why it is referred to as zero-day. This in turn, leads to skilled individual being deployed to patch these vulnerabilities and, as a result, educate others regarding such vulnerabilities.

III. COUNTERMEASURES AND TECHNIQUES AGAINST ZERO-DAY ATTACKS

To tackle zero-day attacks, security measures always need to be on alert. A blueprint of measures to take before, after, and during an attack must be prepared and updated periodically. Since zero-day attacks are unpredictable, even the best defense system can collapse if it is not updated for a long time. Plans need to be made by taking all financial, data, and human factors into consideration. Based on the timeline, the countermeasures can be divided into three parts: detection, prevention, and mitigation. A detailed discussion on each of the parts is provided in the forthcoming segment.

Fig. 5. Timeline of countermeasures

A. Prevention

1) Regularly updating browsers, servers, and systems with the most up-to-date security measures: Browsers that are used by regular users on their day-to-day life can contain zero-day attack vulnerabilities. One such zero-day vulnerability was patched by Mozilla for their Firefox browsers in 2022, which had a "use-after-free" memory corruption bug. Attackers could use this bug for overwriting data, execute code remotely or lead to crashes [17]. These patches are only applied to the users if they have the latest version of their browsers installed. For this reason, it is important to have user applications up to date.

2) Reducing surface of attack: Decreasing the parts of a system that may be susceptible to attacks can reduce the possible vulnerabilities.

3) Controlling of access to systems: Access to systems should be controlled using firewalls and whitelisting. Attackers exploit lenient access limiting to systems to discover vulnerabilities. Allowing access to only specific users reduces the chances of an attack.

4) Controlling file access to non-whitelisted programs: Enforcing user access rules to files and data in a system helps in reducing exploits against the system. Attackers can no longer run programs that access files and directories which need higher privileged user permissions.

5) Usage of the most advanced and high-valued security software: Security is something that should never be compromised. Zero-day attacks have a short time window to act upon, and so security software should be advanced to that level of prevention. Antivirus solutions that rely on file signatures to detect malware are ineffective against zero-day attacks. They may still be beneficial since, once a vulnerability is publicly disclosed, antivirus vendors will quickly append the vulnerability to their malware databases, making the antivirus effective against the threat. Still, organizations should have better protection against zero-day attacks. One such protection solution is NGAV or Next-Generation Antivirus. These anti viruses use analytics related to behavior and can detect abnormal behavior, to detect chances of an attack. Upon detection, processes related to the behavior are blocked to ensure safety.

6) Examination of systems for any unexpected or suspicious activity: Before deploying an attack, attackers try to discover vulnerabilities using different tools like fuzzers [9], which can send various payloads for detection. This may cause unexpected behavior in systems, which can be detected and analyzed. So, monitoring for such behaviors gives an

insight about any possible exploit discovery of the system which reduces chances of zero-day attacks.

7) To safeguard the system, numerous security systems are to be deployed on different tiers of the network: Security systems carrying out different monitoring activities as well as vulnerability detection should be used on several layers of the network to prevent attacks from any layer.

8) Having security as one of the primary concerns as an organization while developing a system or software: One of the most important prevention measures is to keep security in mind throughout the development phase of a system or a software, which helps keep the chances of introducing vulnerabilities low after release. Since zero-day attacks exploit the human error, being more careful in the aspect of security will result in fewer errors, which in turn will decrease vulnerabilities. Organizations must consider security as something intrinsic to the way of their operation, having teams that discuss responses to zero-day attacks and other attacks [13].

9) Educating employees on the symptoms of vulnerabilities and typical security threats, as well as how to respond to them: Security awareness is a must for any individual working with a system, since anyone can be the target or cause of a vulnerability. Employees of organizations should be aware of security patches for their system and should take measures to apply them as soon as possible to reduce vulnerabilities.

10) Prepare a proper response and recovery plan in the event of an attack: Even after taking measured steps to prevent zero-days attacks, no one can guarantee that there is no further exploit. For this reason, plans covering steps like preparation, identification, containment, eradication, and recovery should be made to tackle any unfortunate case of zero-day attacks to reduce losses.

11) Set up a cybersecurity team to monitor system security on a regular basis, if possible: For consistent monitoring and exploit detection, organizations should have their own dedicated cybersecurity team.

B. Detection

There is no network on earth connected to the internet which does not have vulnerability against zero-day attacks. Any device connected to the web is in danger of a zero-day attack. Internet Detection Systems, Anti-virus, and several different techniques are used in a corporation or system to identify threats. But these are not enough to detect new vulnerabilities in a system. Researchers over the years proposed many techniques to create a strong countermeasure against zero-day attacks. These several proposed detection mechanisms can be grouped by network-based and host-based detection techniques. In the host-based technique, once the attack reaches the susceptible application and is executed, host-based solutions detect the attack at the system level [11]. On the other hand, as attack data travels through the network in the form of packets, network-based solutions detect attacks at the network level [11].

Zero-day attacks can take various forms to trick any system to launch a successful attack. Trojans, worms, viruses, and some other malware can be the appearance in zero-day attacks. Both host-based and network-based techniques are used to nullify the attacks. But because of the simplicity and capacity to function in real-time, network-based intrusion detection systems are the most extensively used. Statistical-based, signature-based, behavior-based, and hybrid-based strategies are some of the network-based zero-day attack detection techniques. Each of the techniques has its way to deal with a certain form of attack. The explanation of different techniques is discussed in the upcoming part of the research paper.

1) Statistical-Based Detection Technique: This technique is widely used in order to detect unfamiliar access in a system. The statistical-based method keeps track of all known historical zero-day vulnerabilities and uses that data to construct profiles that provide new criteria for detecting assaults. This method differentiates the normal activity in a network from the unusual ones. To put it simply, this approach uses its previous profile to identify which network traffic or activities to allow and which traffic or activities to prevent [12]. This technique is effective when an attack is similar to one of the past exploits and its defense tactics adjust the countermeasures based on historical data. However, this method seldom adapts effectively to changes in zero-day exploit data patterns. For every new attack, the system needs to learn the patterns in order to detect exploits successfully. Attackers always come up with new tricks and adjustments to exploit vulnerabilities in a system. Statistical-based detection techniques always need to be up to date to detect those changes. The detection quality is directly proportional to the threshold limitations set by the vendor or security expert employing this technique [11]. Since the limit of the system determines the quality of detection, the adjustment of detection parameters needs to be done carefully. The more a system that uses this method has been online, the more accurate it is at learning or identifying usual activities. For this method to work properly, the system always needs to keep up to date. Any kind of laziness to keep the system up to date will expose the system to all kinds of exploits by attackers. This brings us to the disadvantage of this method which is that profiles built from log information are static and cannot identify zero-day attacks in real-time if they have not been preserved on the log [12].

2) Signature-Based Detection Technique: It is another network-based technique that is exercised by anti-virus companies. Signature-based approaches are used to detect polymorphic worms and identify their new appearances on each new contamination [7]. A polymorphic worm is a sort of worm that changes its structure with each appearance or new version. Although the method is used mainly to detect polymorphic worms, it is also utilized to detect viruses and malware in a system. Anti-virus companies have libraries to store all the signatures of viruses found by searching old files and past attacks. A signature is a distinguishing feature of an attack, and it is typically a string containing an implausible date or a hash value. [10]. Anti-virus software companies update their libraries by constantly adding newly identified signatures of different viruses, worms, and malware. These signatures are later used against incoming traffic to find out any viruses in the network which match the records. The signature-based technique is further divided into three categories which are semantic-based signatures, vulnerability-driven signatures, and content-based signatures [12]. The disadvantage of this technique is that it is always a step behind the zero-day attack. To tackle a zero-day attack, the signature libraries need to have the signatures of the attack beforehand. An attack can happen with a virus that is not recorded in libraries. Even if the attack is neutralized by

updating the library just after the attack, most of the damage can be done between the time of the updated library and the last recorded library before the attack.

3) Behavior-based technique: The behavior-based technique is based on the flow of traffic throughout a network. It predicts the flow of the network and gathers information in order to find out any abnormal activities on a network. It acts as a forecast to alert any possible incoming threats. This technique can be implemented using machine learning technology. The machine learning approach will gather all the past information about network activities on the system or machine of a victim along with web servers or servers. Later it will analyze the different viruses or worms' byte patterns which will then help to filter out the network from attacks. But the issue with this method is that it can show a significant number of false positives or false negatives. False-positive is the detection of an attack that was actually not an attack. This could lead to unnecessary cautions and financial loss for an organization. False-negative is the byte patterns that were identified as unharmful but turns out to be malicious malware or virus. The damage possible by false negatives is huge as classified or secret data can be harmed, stolen data can be used against the organization and financial loss will be a lot. For this technique to work, the goal of any tactics used by an organization should be to consistently notice the presence of a zero-day misuse and avoid harm and multiplication of the zero-day misuse [7].

4. Hybrid-based technique: This technique is a mixture of statistical-based, signature-based, and behavior-based techniques. The goal of this method is to combine two or all of the above-mentioned techniques to utilize the strengths of one to compensate for the limitations of the other.

From the time a vulnerability is discovered and exploited until the vendor develops a patch to fix the vulnerability and mitigate the attack, zero-day attacks can be carried out. Massive damage can occur within seconds of such an attack because it is difficult to predict and hard to pinpoint when the vulnerability was discovered. To prevent any zero-day attacks we need to use techniques with the least amount of weakness. But since most techniques have weaknesses, hybrid techniques are most effective to confront attacks.

A hybrid model proposed by [12] can be used to cover up the weakness of some techniques. The model combines both signature-based techniques and behavior-based techniques to detect threats by monitoring the flow of traffic in a network. The system can be divided into six parts which are: Packet acquisition module, Packet extraction, and disassembly module, analysis and evaluation module, signature generation, signature matching, and behavior analysis [12].

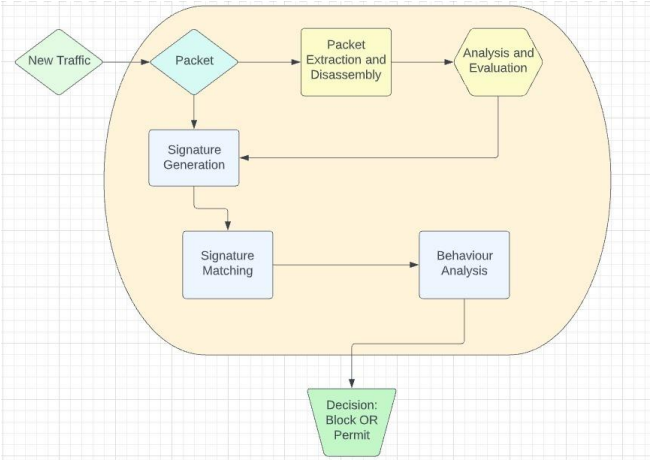

Fig. 6. Architecture of signature-behavior based hybrid technique [12]

The process kicks off by collecting packets from the same flow of traffic and storing it in the packet acquisition module. Later the packets are forwarded to the extraction and disassembly module. All packets are extracted and disassembled before sending it to the analysis and evaluation module. The analysis and evaluation section will use the intrusion detection-based software or device to detect any kind of malware in the packets. The packets will be grouped after deep inspection and the groups of packets will be then forwarded for signature generation. When the signature is generated, it is compared to the signature database, and if it does not match any signature in the database, the traffic is sent to the behavior analysis module for analyzing the traffic flow using the Hidden Markov Model machine learning technique. The Hidden Markov Model (HMM) is a statistical technique used in machine learning and it can be used to understand the nature of observable events that are influenced by internal, non-observable factors. By using this method, if no abnormality is identified in the traffic, it will be allowed to enter the network; nevertheless, if an abnormality, no matter how little, is detected, the traffic will be prohibited from accessing the network.

The above-described hybrid model has some advantages to counter zero-day attacks over signature-based, statistical-based, and behavior-based techniques. Firstly, it is capable to detect anomalies in real-time. Secondly, its detection system can capture attacks before any major harm is done. Finally, it minimizes the downsides of both signature-based and behavior-based techniques.

C. Mitigation

1) Encouraging system users to have their systems updated after every major security patch: After a vulnerability is detected and a new version patching the vulnerability is released, users should be prompted to update their systems as soon as possible to mitigate possible damages done by the prior unsafe version.

2) Reporting and diagnosing unusual activities: After detecting suspicious activity, it should be reported and documented, and measures should be taken accordingly. The system should be modified in order to remove the reported vulnerability possibility.

3) Securing and containing possible sources of an attack: If any user or a network is suspected of carrying out an attack, the user or network access should be revoked in order to

ensure safety. Investigations should also be made to confirm of the suspicion, and actions should be taken accordingly.

4) Having Recovery: As security breaches happening from zero-day attack or any unpatched vulnerability cannot be fully avoided, recovery plays a key differentiating role for organizations [13]. Recovery acts as a strong last line of defense for zero-day attacks.

5) Limiting use of email attachments: Users are probably going to send or accept suspicious email attachments through email networks. For this, it is important to ensure they work on safe situations, where their arrangements should be surveyed and sifted through. In addition to this, disabling HTML messages is a strong protection against zero-day attack attempts, as attackers can cover up malicious code within HTML messages before sending them.[7]

D. Future research track

As zero-day attacks get more aggressive, companies and organizations should be more careful in preventing such attacks. Systems should be security tested before release. Further research should be carried out in order to predict and identify the ways zero-day attacks can be made. At present, the main problems which are open are virtualization, web-based application, cloud computing and others which are not included in common studies related to zero-day attacks. [9]. These are increasing rapidly, which is why it is important to carry out more research on them for preventing zero-day attacks [9]. Although companies have programs for research on them, it is not enough considering the rapid developments and innovations of threat actors, which may result in future unanalyzed problems [9]. Since 2017, there has been an exponential growth in ransomware, which has caused several zero-day vulnerabilities. These losses affected both large and small businesses, almost half of which lost their data and had to pay to retrieve them [13]. Considering this, it is paramount that further research be carried out in detecting and mitigating these attacks.

IV. CONCLUSION

Zero-day attacks are threats that can affect any organization, business, or enterprise. Zero-day attacks can pose new hazards to digitized businesses. Experts believe that these attacks are getting larger and bolder and is expected to rise to a larger extend in the upcoming years. Anything handled over a network is vulnerable to cyber-attacks. Even small and medium-sized enterprises pay to be secure from any such cyber-attacks. Priority must be given to securing data by an organization and being aware of newly discovered attacks and their preventions. Spreading awareness leads to prevention. As a result, it is very important to stay updated with news about newly discovered attacks and exploits. Companies should also pay white hat hackers to break into their security systems. This is also a very effective way for detecting flaws sooner and initiating an instant response to build a patch. Companies, particularly large businesses, should constantly cooperate with a reaction team and have a backup in case of a major fault that is exploited to inflict severe asset loss.

REFERENCES

[1] D. Hammarberg, “Information Security Reading Room the Best Defenses Against Zero-day Exploits for Various-sized Organizations,” 2019

[2] Whiting, A. Payne Constructing Cybersecurity: Power, Expertise, and the Internet Security Industry. Manchester: Manchester University Press, 2020

[3] Malware Affecting Siemens WinCC and PCS7 Products (Stuxnet) - Entries - Forum - Industry Support - Siemens. (n.d.). Copyright Siemens AG - All Rights Reserved. Retrieved December 1, 2020, from https://support.industry.siemens.com/tf//WW/en/posts/malware-affecting-siemenswincc-and-pcs7-products-stuxnet/46366?page=0&pageSize=10 G. L. Sanders, S. Upadhyaya, and X. Wang, ‘Inside the Insider’, IEEE ENGINEERING MANAGEMENT REVIEW, vol. 47, no. 2, p. 8, 2019.

[4] B. Payne, D. C. May, and L. Hadzhidimova. America’s most wanted criminals: Comparing cybercriminals and traditional criminals. Criminal Justice Studies, 32(1):1–15, 2019.

[5] Grispos, G., Glisson, W., & Cooper, P. (2019). A bleeding digital heart: Identifying residual data generation from smartphone applications interacting with medical devices. Paper presented at the proceedings of the 52nd Hawaii international conference on system sciences. Maui, HI, USA.

[6] NVD. National Vulnerability Database. 2020. https://nvd.nist.gov/.

[7] S. Akshaya and G. Padmavathi. “A Study on Zero-Day Attacks,” In Proceedings of International Conference on Sustainable Computing in Science (SUSCOM), pp. 2170–2177, 2019.

[8] Fruhlinger, J. (2017). What Is Stuxnet, Who Created It and How Does It work? [online] CSO Online. Available at: https://www.csoonline.com/article/3218104/what-is-stuxnetwho-created-it-and-how-does-it-work.html [Accessed 28 Feb. 2022].

[9] Xavier et al., 2020, Zero-day attack: Deployment and evolution

[10] Astudillo, Darwin & Riofrio, X. & Tello Oquendo, Luis & Merchan-Lima, Jorge. (2021). Zero-day attack: Deployment and evolution. VIII. 38-53.

[11] Ejiofor, C & Onyejegbu, Laeticia & Emmah, Victor. (2022). Review of Malware and Techniques for Combating Zero-Day Attacks. International Journal of Engineering and Technical Research. 6. 267-275.

[12] Cuppah, D., G, A. & Hanumanthappa, M. (2020). Design and Analysis of a Hybrid Security Framework for Zero-Day Attack.

[13] A. Fagioli, “Zero-day recovery: the key to mitigating the ransomware threat,” Computer Fraud and Security, 2019.

[14] Kristoffer Kjærgaard Christensen & Tobias Liebetrau, A new role for ‘the public’? Exploring cyber security controversies in the case of WannaCry, Intelligence and National Security,2019 34:3, 395-408, DOI: 10.1080/02684527.2019.1553704

[15] K. Radhakrishnan, R. R. Menon and H. V. Nath, "A survey of zero-day malware attacks and its detection methodology," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 533-539, doi: 10.1109/TENCON.2019.8929620

[16] Ritika, S. (2021) What are the Potential Impacts that Zero-Day vulnerabilities Pose to Your Organizations,. https://www.indusface.com/blog/what-are-the-potential-impacts-that-zero-day-vulnerabilities-pose-to-your-organizations/#:~:text=4.-,Loss%20of%20Production%20and%20Productivity,hampering%20employee%20and%20organizational%20productivity.

[17] https://www.qcert.org/node/1843 (retrieved 11 Apr. 2022)