**Topic :Zero-Day Attack and countermeasures**

**Students:**

Talha Abdullah Punjabi -201903446

Abrar Shahriyar Hossain -201912955

Nafin Mahmoud - 201913152

**Introduction:**

Zero-day attacks are ones that occur because of the discovery of new vulnerabilities in a system. 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.

Diagram

Description automatically generated

Figure 1- Overview of a Zero-day Attack

**Types of Attackers:**

1. **Cyberwarfare Attacker** – 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.
2. **Hacktivists** – Group of cyber-attackers who get together to carry out cyber-attacks for political or social advantage. They deface or leak information from organizations to communicate a message and raise awareness for a cause they support. A recent example came from a group called Void, which threatened to destroy key American infrastructure by exploiting a zero-day vulnerability. In the end, they caused a significant damage to the company and even sought a large sum of money for not revealing sensitive company information.
3. **Cyber criminals** – 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. An attack on Acrobat Reader that bypassed the sandbox anti-exploitation protection and sold information to intelligence agencies for large sums of money through contactors.

**Important Terms**

1. **Zero-day vulnerability –** A vulnerability in a software or hardware that is not known to developers.

Timeline

Description automatically generated with medium confidence

Figure 2- TimeLine of Zero-Day vulnerability

1. **Zero-day exploit –** An exploit is a method of gaining system access by exploiting a vulnerability.

**Who are susceptible to Zero-day Attacks?**

• People who use a vulnerable system, such as an operating system, via which hackers might gain access to their systems.

• Big organizations or enterprises

• Individuals with access to critical business data

• Governmental organizations

• Threats to national security

**TimeLine of Zero-day Attack**

Diagram

Description automatically generated

Figure 3- Timeline of Zero-Day Attack

**Negative Impacts by Zero-day attacks**

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. 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.
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. 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.
6. **Watering-Hole Attacks –** Zero-day vulnerability can lead to attacks such as watering-hole attack. 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 Prevention**

* **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 (4). 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.
* **Reducing surface of attack:** Decreasing the parts of a system that may be susceptible to attacks can
* **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.
* **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.
* **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.
* **Examination of systems for any unexpected or suspicious activity:** Before deploying an attack, attackers try to discover vulnerabilities using different tools like fuzzers (5), 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.
* **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.
* **Having security as one of the primary concerns 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.
* **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.
* **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.
* **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.

**C Mitigation**

* **Encouraging system users to have their systems updated after every major security patch:** After a vulnerability is detected an 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.
* **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 to remove the reported vulnerability possibility.
* **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.

**Positive Impacts caused by Zero-day Attacks**

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.

**A Case study: Zero-day attack that happened in the Middle East - 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. 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:

1. The software was induced into a controller computer at the plant.
2. The program collected and transmitted data about the plant's computers and how they are configured to the agencies.
3. 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.
4. The worm disrupted the working of the centrifuges and forced them to spin fast or slow, resulting in the destruction of some of them.
5. 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.

**III. COUNTERMEASURES AND TECHNIQUES AGAINST ZERO-DAY ATTACKS**

A. **DETECTION**

There is no network on earth connected with internet which does not have vulnerability against zero-day attack. Any device connected to web is in danger of zero-day attack. Internet Detection System, 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 host-based technique, once the attack reaches the susceptible application and is executed, host-based solutions detect the attack at the system level [2]. 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 [2].

Zero-day attacks can take various forms to trick any system in order to launch a successful attack. Trojans, worms, viruses, and some other malwares can be the appearance of zero-day attacks. Both host-based and network-based techniques are used in order 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 the some of the network-based zero-day attack detection techniques. Each of the techniques have its own way to deal with certain form of attacks. The explanation of different techniques is discussed in 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 between the normal activity in a network against 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 [3]. 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-base detection technique 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 [2]. Since the limit of the system determines the quality of detection, the adjustment of detection parameters need 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 activity. 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 [3].

**2. Signature-Based Detection Technique**

It is another network-based technique which is exercised by anti-virus companies. Signature-based approaches are used to detect polymorphic worms and identify their new appearances on each new contamination [4]. 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. [1]. Anti-virus software companies update their libraries by constantly adding newly identified signatures of different viruses, worms, and malwares. These signatures are later used against incoming traffic to find out any viruses in network which matches with the records. The signature-based technique is further divided into three categories which are semantic-based signatures, vulnerability-driven signatures, and content-based signatures [3]. The disadvantage of this technique is that it is always a step behind zero-day attack. To tackle a zero-day attack, the signature libraries need to have the signatures of attack beforehand. An attack can happen with a virus which 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 updated library and last recorded library before attack.

**3. Behavior-based technique**

The behavior-based technique is based on the flow of traffic throughout a network. It predicts the flow of 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. 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 server. Later it will analyze the different viruses or worm’s 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 which was not an attack. This could lead to unnecessary cautions and financial loss of an organization. False negative is the byte patterns which were identified as unharmful but turns out to be a malicious malware or virus. The damage possible by false negative 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 [4].

**4.Hybrid-based technique**

This technique is the 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 weakness, hybrid techniques are most effective to confront attacks.

A hybrid model proposed by [3] can be used to cover up weakness of some techniques. The model combines both signature-based technique and behavior-based technique to detect threats by monitoring 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 [3].

Diagram

Description automatically generated

Figure - Hybrid Model of Zero-day attack

**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. Broadhurst, Roderic & Woodford-Smith, Hannah & Maxim, Donald & Sabol, Bianca & Orlando, Stephanie & Chapman-Schmidt, Ben & Alazab, Mamoun. (2017). Cyber Terrorism: Research Review: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology. SSRN Electronic Journal. 10.2139/ssrn.2984101.
2. Astudillo, Darwin & Riofrio, X. & Tello Oquendo, Luis & Merchan-Lima, Jorge. (2021). Zero-day attack: Deployment and evolution. VIII. 38-53.
3. 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.
4. Cuppah,D., G,A. & Hanumanthappa, M. (2020). Design and Analysis of a Hybrid Security Framework for Zero-Day Attack.
5. Akshaya, Swathy & Ganapathi, Padmavathi. (2019). A Study on Zero-Day Attacks. SSRN Electronic Journal. 10.2139/ssrn.3358233.