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

**Students:**

Talha Abdullah Punjabi -201903446

Abrar Shahriyar Hossain -201912955

Nafin Mahmoud - 201913152

**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.

Diagram

Description automatically generated

Figure 1- Overview of a Zero-day Attack

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 Attacker** – 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.

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].

Timeline

Description automatically generated with medium confidence

Figure 2- TimeLine of Zero-Day vulnerability

Figure 2 shows 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.

**TimeLine of Zero-day Attack**

Diagram

Description automatically generated

Figure 3- Timeline of Zero-Day Attack [7]

**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.

**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 [8]**

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 [8]. 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.

**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. (2020) Constructing Cybersecurity: Power, Expertise, and the Internet Security Industry. Manchester: Manchester University Press.
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].