**Topic: Zero-day attacks and countermeasures**

**Introduction:**

Zero-day attacks are ones that occur because of the discovery of new vulnerabilities in a system. This assault occurs before the developers have a chance to patch the flaw. Because there are no updates for the zero-day vulnerability, the chances of the attack to work are high. This attack is used to harm assets or steal sensitive information from the system. The patches to fix these vulnerabilities can even take up to weeks. Basically, the persistent fear of a zero-day attack in a computer system or application is known as a zero-day attack.

**Types of Attackers:**

Cyberwarfare – Attackers utilize cyber-attacks against a nation to cause physical harm, such as loss of life, through causing damage to assets.

Hacktivists – group of cyber-attackers who get together to carry out cyber-attacks for political advantage

Cyber criminals – people who carry out cyber-attacks to attain monetary gain

**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

**Damage caused 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 or 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.

**Preventing Zero-day attacks**

* Regularly updating browsers, servers, and systems with the most up-to-date security measures
* Usage of the most advanced and high-valued security software.
* Examination of systems for any unexpected or suspicious activity.
* To safeguard the system, numerous security systems are deployed on different tiers of the network.
* Install the most recent versions of anti-virus software and security fixes.
* Educating employees on the symptoms of vulnerabilities and typical security threats, as well as how to respond to them.
* Prepare a proper response and recovery plan in the event of an attack.
* Set up a cybersecurity team to monitor system security on a regular basis, if possible.

**Examples of Zero-day Attack**

1. **Meltdown and Spectre (2018)** – This was an attack that affected billions of computers due to two sophisticated processor weaknesses that were recently disclosed in early 2018. Malicious programs were able to read and access sensitive data from the system's memory because of these weaknesses.

**TO DO: Extract information from this website**

Reference:

<https://www.kaspersky.com/resource-center/definitions/zero-day-exploit>

https://info.capsule8.com/how-to-detect-and-prevent-zero-day-attacks

<https://www.indusface.com/blog/what-are-the-potential-impacts-that-zero-day-vulnerabilities-pose-to-your-organizations/>