Zero-Day Exploits

Threat: **Exploits**

Author: **Jeffrey Farnan** Date Originally Published: **May 3th, 2022**

1. SUMMARY

- A zero-day exploit is when an attacker leverages a zero-day vulnerability to attack a system. A zero-day vulnerability is best described as a flaw in software or hardware which is taken full advantage of by malicious actors. Cybercriminal groups use zero-day exploits strategically targeting medical or financial institutions, or government organizations, who remain vulnerable until a fix is developed and deployed.

2. DEFINITION OF A ZERO-DAY

- The term "Zero-day" refers to a computer vulnerability either known or unknown. It's the period of time between discovery of the vulnerability to when a fix is developed and made available.
- A zero-day vulnerability is a previously undisclosed computer software flaw that attacks silently before security teams are aware of it. Once they find the problem they have "zero days" to fix it because they're already at risk.
- The term "exploit" is code which takes advantage of a software vulnerability or security flaw. This exploit is usually written by malicious actors.
- There are there main ways to think of a zero-day:
    - **Zero-day vulnerability**: A software weakness that can be exploited and is found by attackers before the manufacturer knows about it.
    - **Zero-day exploit**: The method an attacker uses to gain access to the system using that zero-day vulnerability.
    - **Zero-day attack**: When bad actors use a zero-day exploit to get into a system to steal data or cause damage.

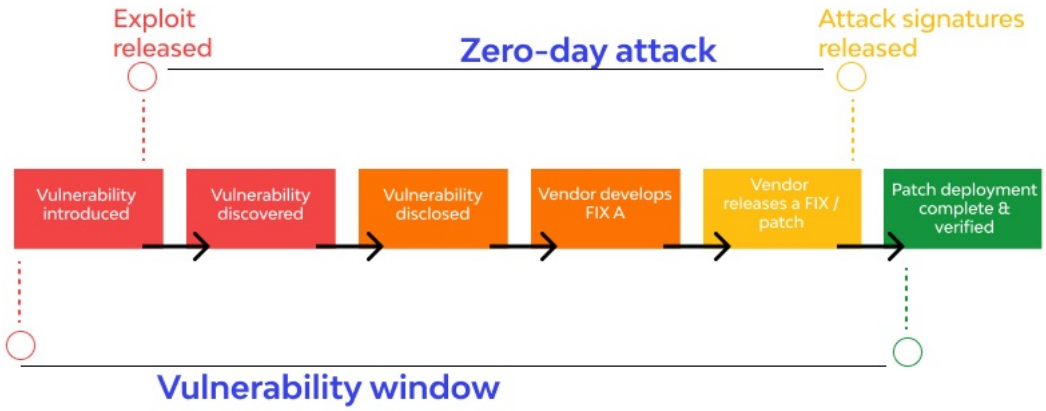
3. HOW ZERO-DAY EXPLOITS WORK

- Manufactures and software developers diligently check their products for flaws before being released but sometimes mistakes happen or weaknesses were not strengthen before release. This allows bad actors who are dedicated in the pursuit of weaknesses or loopholes to exploit these for their own gain.
- The exploit itself is written specifically to take full advantage of this vulnerability.

- A zero-day vulnerability can exist in the wild for months before being detected. During that time, attackers can get away with stealing or copying data and damaging sensitive systems until the software manufacturer implements a fix.
- Malicious actors often sell information on zero-day vulnerabilities on the dark web for large sums of money. As long as the only people who know about these exploits are attackers, they remain a threat.

4. ZERO-DAY TIMELINE

- Zero-day attacks occur during the vulnerability window that exists in the time between when vulnerability is first exploited and when software developers start to develop and publish a counter to that threat. Security experts have divided this timeline of zero-day exploitation into seven steps:



- **Stage 1 – Vulnerability Introduced:** The software developer writes the code, the software is tested it works correctly and is released. The team behind this software release don't release that the code contains a vulnerability.
- **Stage 2 – Exploit released:** A malicious actor tests this software for vulnerability's or any kind of weakness which can be exploited to their benefit. The actor writes a piece of code to exploit this weakness and deploys this exploit code.
- **Stage 3 – Vulnerability discovered:** The vendor is made aware of the vulnerability but a patch is not immediately available.
- **Stage 4 – Vulnerability disclosed:** The vendor or security researchers publicly acknowledge the existence of the vulnerability.
- **Stage 5 – Antivirus signatures released:** If attackers create zero-day malware to exploit the vulnerability antivirus vendors can quickly recognize its signature and provide protection against it. There are other ways to exploit the vulnerability, systems may remain vulnerable.
- **Stage 6 – Security patch developed:** The vender develops a patch to address the vulnerability. The time it takes to provide this patch is determined by the complexity of the problem and how high a priority it is in its development process.
- **Stage 7 – Security patch deployment completed**: The patch is complete and now released to the public. The release of the patch does not provide and immediate fix because it can take some time for users to deploy it. Organization and individuals should enable automatic updates to get patch fixes immediately.

6. POTENTIAL CUSTOMER DEFENSE

To detect this type of threat, you need to implement proactive, in-depth security strategies. Below are a few practices and tools you can use to ensure that your systems are defended against zero day attacks.

- **Regularly update your systems:** Organizations and individual users should enable automatic software updates and pay attention to update notifications.
- **Endpoint Protection Platforms**: Deploy Endpoint Protection Platforms (EPPS) are security platforms designed to layer protections over your endpoints.
- **Secure Your Network:** Create a secure network that is resilient against zero day attacks by:
    - Monitoring data and comparing current activity to an established baseline you can detect abnormalities caused by zero-day attacks. A zero-day attack leaves digital footprints in both data and on the network.
    - Back-up – critical systems and establish recovery and incident response plans.
    - Enforce software / internet use policies and train users to identify security risks.
- **Website Scanner:** Run a free website scanner on a regular basis to check for malware and vulnerabilities. Since the best weapon is a great offense, patch any new vulnerabilities before someone else does.
- **Web Application Firewall:** Deploying a web application firewall (WAF) on the network edge to review incoming traffic and filter out malicious inputs that could target security vulnerabilities is one of the best ways to prevent zero-day attacks.

Research Sources:

- https://www.socinvestigation.com/how-a-zero-day-exploit-works-attack-timeline-and-defense-techniques/
- https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
- https://uk.pcmag.com/security/139414/what-are-zero-day-exploits-and-attacks
- https://www.cynet.com/zero-day-attacks/5-ways-to-defend-against-zero-day-malware/
- https://www.varonis.com/blog/zero-day-vulnerability