Zero-Day Vulnerability: The Unknown Threats to Your Data

The internet is a dangerous place for your data. Even though your business ticks all the cybersecurity boxes, it certainly doesn't mean you are completely secure. There's still a chance your defenses could be breached.

Most businesses dismiss it as bad luck. However, these incidents are not just bad luck, but carefully orchestrated attacks called -zero-day attack. Their origins can be traced back to the dark web, where hackers buy information that enables them to break through vulnerable software.

Victims of zero-day attacks lose revenue and reputation, without ever knowing the real reason for it.

What Is a Zero-Day Vulnerability?

A zero-day vulnerability is a security flaw in the software that is known to the software vendor, but with no patch in place to fix the flaw.

The time between discovering the flaw and releasing a patch is the sweet spot for hackers to launch zero-day attacks (exploits). It's like a thief sneaking in through a backdoor that was accidentally left unlocked.

Why Are Zero-Day Attacks Dangerous?

Zero-day exploits are usually reserved for high-value targets, such as financial and medical institutions, due to their high success rate. The reason is two-fold.

Firstly, a vulnerability is kept confidential for as long as possible by limiting communication to hacker forums via the dark web. Secondly, it takes an average of 59 days for vendors to roll out patches.

The result? The likelihood of a successful attack with maximum impact.

Here are a few types of zero-day attacks:

- ***Account Takeover (ATO) Attacks.*** Exploit malware can take unauthorized control of your system and can be used in malicious ways, like installing other malware and sending phishing messages to your contact list for example.
- ***Watering-Hole Attacks.*** These attacks target websites that attract a high number of visitors. The malware sits on the webpage and spreads within seconds of users dropping on the website. The aim is to infect as many visitors as possible before the vulnerability is detected.
- ***Zero-Day Wednesday.*** Hackers take advantage of Microsoft's monthly security update cycle by timing new attacks just after Patch Tuesday – the second Tuesday of each month when Microsoft

releases its patches. It could be a month before Microsoft has a chance to respond to such attacks, giving hackers ample time to wreak havoc.

The Anatomy of Zero-Day Vulnerability

Typically, a zero-day attack involves targeting a software system with malware. Malware enters the existing system and prevents it from performing its default functions.

Stuxnet, also known as the world's first cyberweapon, is a great example of a zero-day vulnerability. This malware was used to disrupt an Iranian nuclear plant. Here's how it happened:

1. Attackers infiltrated Windows computer systems looking for vulnerabilities
2. Stuxnet then deployed four different zero-day vulnerabilities in the Microsoft Windows OS
3. The vulnerabilities passed from Windows to the nuclear control systems (not Windows OS supported)
4. The malware manipulated the frequency of the centrifuge (sped it up and then slowed it down). As a result, the centrifuges were destroyed
5. Stuxnet was undetectable. Iranian monitoring systems never picked up the malware, making it appear as though systems were operating normally

How Are Zero-Day Attacks Discovered?

While zero-day attacks are near impossible to detect, IT professionals have come up with four basic methods to discover zero-day attacks:

Statistical Analysis

This involves machine learning to collect data from previously detected exploits to create a framework for safe system behavior. Granted, using historical data to detect real-time exploits has limited effectiveness. However, it does help in analyzing the likelihood and potential source of an attack.

Signature Analysis

Past attacks are compared with current data patterns to determine potential threats. Machine learning is used to analyze and create signatures for existing malware, which are used to detect previously unknown vulnerabilities.

Behavior Analysis

Behavior detection looks for suspicious patterns. It studies the behavior of the hacking entity and its interaction with the site under attack. If the pattern differs from the usual, it could be a sign of a zero-day attack.

Hybrid Analysis

All three approaches are combined into a single scoring system to determine the likelihood of a breach. It's one of the best ways to discover a zero-day attack since it takes advantage of all three techniques while mitigating their limitations.

Protecting Your Business Against Zero-Day Exploits

Protecting your business against a zero-day attack is an uphill battle, but not an impossible one. Cybersecurity professionals are working together to fight such attacks, with Zero Day Initiative (ZDI) a step in that direction.

The ZDI was created to encourage the reporting of zero-day vulnerabilities privately to vendors by financially rewarding researchers so that vendors can come up with a patch before the exploit occurs. It has helped vendors and their clients protect their profits and credibility from public scrutiny.

However, it's impossible to prevent zero-day attacks completely. No business can protect all its systems and SaaS applications against zero-day attacks, regardless of whether it is Office 365, G Suite or Salesforce. The attacks are only going to get bigger and bolder, as experts believe the frequency of zero-day attacks will rise to one per day by 2021, as opposed to one per week in 2015.

Zero-day attackers come for your data from every direction possible, and they come at you hard. One small loophole and your data could be gone forever.

A disaster recovery strategy is your ultimate response strategy against zero-day attacks.

Spanning's comprehensive disaster recovery strategy keeps your Office 365, G Suite and Salesforce data safe from attack from all directions, ensuring business continuity at all times.

References:

- https://securityboulevard.com/2020/06/zero-day-vulnerability-the-unknown-threats-to-your-data/
- https://www.cynet.com/cyber-attacks/zero-day-attack-prevention/
- https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html
- https://www.forcepoint.com/cyber-edu/zero-day-exploit