Zero-Day

A zero-day (also spelt as 0-day) is a software weakness not known to those who are vendors of the target software. Unless the weakness is resolved, hackers can take control of the system and adverse programs, data, or the computer network itself.

Such attacks are known as zero-day attacks or zero-day exploits.

Zero Day will come under the Science and Technology segment of the IAS Exam.

Definition of Zero-Day

Zero-Day at first was used to refer to the number of days a new software was released to the public, hence ‘zero-day software’ was obtained by hacking into the developers' computer before the software was released.

As time went on, ‘zero-day’ came to be referred to as a series of weaknesses that enabled hacking and to the number of days that the vendor had to fix them. Once the weaknesses became known to the developers, they would apply patches and implement other safeguards to mitigate it.

The longer it takes for the developers to become aware of the weakness in their software, the less chance they have to fix or mitigate it. However, once safeguards have been developed, the chances of the hacking exploit succeeding decreases as more users apply the fix.

Apart from directly hacking the software, the exploit or the weaknesses created can be sold on the dark web for a tidy sum of money.

Zero-day attacks are dangerous as only the attackers themselves will have knowledge about the infiltration in the network. Once they have infiltrated a network, criminals can either attack immediately or sit and wait for the most advantageous time to do so.

Who carries out Zero-Day attacks? Target of Zero-Day Attacks

Who carries out zero-day attacks?

Malicious actors who carry out zero-day attacks fall into different categories, depending on their motivation. For example:

- Cybercriminals – Hackers with the intention of making financial gains through illicit and criminal means.
- Hacktivists – Political activists or social activists with hacking skills in order to bring attention to their cause.

- Corporate espionage – Hacking done to gather sensitive information about corporations
- Cyber Warfare – Countries or political entities using hacking as a method to attack another nation's computer infrastructure.

Their targets include:

- Operating systems
- Office applications
- Hardware
- Firmware
- Internet of Things (IoT)
- Web Browsers

How are Zero-Day attacks identified?

The weaknesses exploited by zero-day attacks can come in the following forms:

- Missing data encryption
- Missing authorizations
- Incomplete algorithms
- Bugs
- Weakness in password security

The above are one of many such weaknesses that can be exploited, although the scope of such attacks keep evolving from time to time. Even so, the extent of the damage caused by such vulnerabilities is only known once they have been identified.

Despite this, there are many techniques with which a zero-day exploit can be identified. Some of them are:

- A database of existing malware can be used to identify the type of zero-day attacks. Although the database is updated extensively and quickly, zero-day attacks are also evolving at a faster rate than before. Hence, there can be a limit to how much the malware database can be helpful

- Certain techniques are developed based on how the zero-day malware interacts with the target system. Rather than examine the code of the files, this method focuses on the interaction with the existing software and will analyse if they result from malicious actions.

- Machine learning is used extensively to analyse data from previously recorded attacks in order to establish a foundation for a safe system behaviour based on data of past and current interactions with the system. The more data becomes available, the more reliable the detection will be.

Incidents of Zero-Day Attacks

Some recent examples of zero-day attacks include:

2021: Chrome zero-day vulnerability

Google Chrome was subjected to a series of zero-day attacks in 2021. The attacks led to the web browser coming up with updates to remove a bug in its JavaScript engine

2020: Attack on Zoom

Zoom, a well-known video conferencing platform, was found to have vulnerabilities. With these vulnerabilities, hackers could access a users' computer remotely in case they were running an older version of the operating system. In case the target had administrative privileges, the hacker could take over their machines completely and gain access to all their files.

2020: Apple iOS Vulnerability

Apple's iOS is considered to be the most secure among all the smartphone platforms in the world. Yet it was subjected to at least two zero-day vulnerabilities, one of which enabled hackers to access iPhone remotely

2017: Microsoft Word Zero-Day Exploitation

Unsuspecting victims inadvertently opened a pop-up window which asked permission to 'load remote content'. Upon clicking 'yes', it exposed the victim's bank accounts.

Frequently Asked Questions about Zero Day

What is the meaning of zero-day attacks?

A zero-day attack (also referred to as Day Zero) is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. The software developer must rush to resolve the weakness as soon as it is discovered in order to limit the threat to software users.

How common are zero-day attacks?

Conventional wisdom in IT security has long taught us that zero-day exploits are rare and that we need to be far more concerned with non-zero-days, which make up the vast majority of attacks

What is a Zero-Day virus?

A zero-day virus (also known as zero-day malware or next-generation malware) is a previously unknown computer virus or other malware for which specific antivirus software signatures are not yet

available. The antivirus scans file signatures and compares them to a database of known malicious codes.