ZERO-DAY ATTACK

What is zero-day attack?

A zero-day attack is a type of cyber attack that exploits vulnerability in software, hardware or firmware that is not known to the target. The attacker uses a zero-day exploit, which is a method or code that takes advantage of the vulnerability, to compromise the system or data before the target can fix it giving the name zero-day attack.

The attackers use a **zero-day exploit** or method to attack systems (un-patched as well as unidentified) with **zero-day vulnerability** (software vulnerability discovered by attackers before the vendor has become aware of it). The attack is as fast as a movie piracy. s

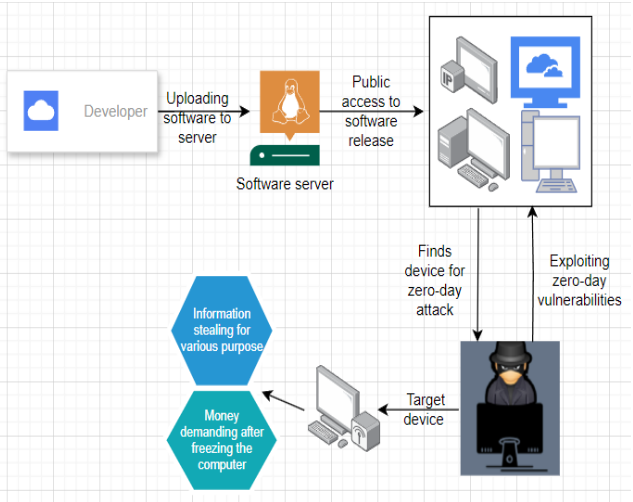
Developer
Uploading software to server
Software server
Public access to software release
Finds device for zero-day attack
Exploiting zero-day vulnerabilities
Information stealing for various purpose
Money demanding after freezing the computer
Target device

Fig 1. Flow of Attack

BEWARE of ZERO-DAY ATTACK

Zero-day attacks are dangerous because they can bypass the existing security measures and cause damage without being detected. They can target any system or device that has a security flaw, such as software, operating systems, servers, routers, etc. Zero-day attacks can have various goals, such as stealing information, installing malware, disrupting services, or gaining unauthorized access.

How the attack occurs!

The attacker has many ways to invade a target's devices. It is better to remember them so that it will be hard to fall as a victim. The types and process is given in the following diagrams.

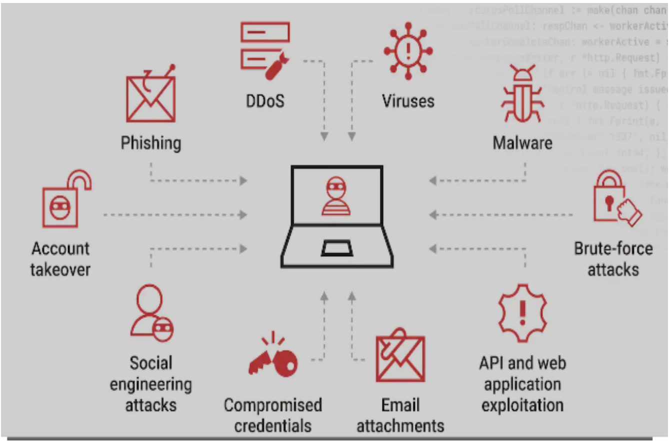

Fig 2. Weapons of Attack

What are the sign of the zero-day attack?

When the attack is done, the computer shows some irregular indicator which was never shown before. Understanding these attack sign can help to reduce the impact of the data.

- Unusual network activity, such as increased traffic, unauthorized access, etc.
- Unexpected system behavior, such as crashes, freezes, or errors.
- Suspicious files or processes, such as unknown executables and malware.
- Security alerts or warnings from antivirus notifications, firewall logs, etc.

How to prevent zero-day attack?

There are some methods that can reduce the attack surface for potential zero-day exploit.

Zero Trust Security Model – In Zero Trust security no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. In this model, authentication and authorization are discrete functions that cyber security teams perform before allowing access to networks and system. This model has three main tenets: risk awareness, lease privileged access, and continuous access verification.

Software up to date: Keeping software and systems up to date with the latest versions that reduce the attack surface for potential zero-day exploits.

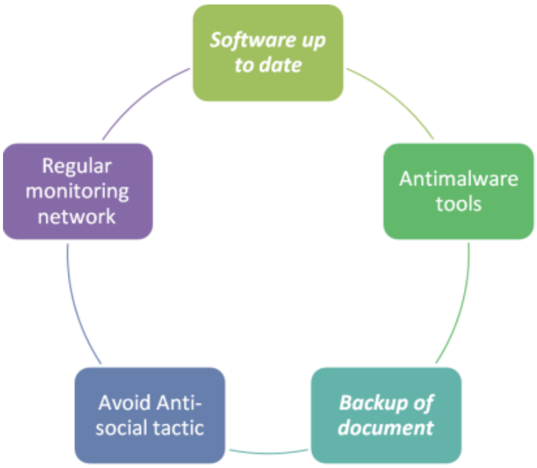

Fig 3. Various Preventive Measures of Zero day Attack

Antimalware tools: Antivirus software can help identify and remove known malware signatures, while firewall can help to block unauthorized access and communication.

Backup of every document: Implement a backup and recovery plan for data and systems can help to restore data and systems in case of a successful zero-day attack that causes data loss or system damage.

Remember anti-social tactics: phishing emails, suspicious attachments, rogue websites or pop-ups.

Regular Monitoring Network: Monitor your network and system activity for any anomalies or indicators of compromise.

Recent cases of zero day attack

In 2023, 10 popular platforms that have been seen the zero day attack are Fortra GoAnywhere, Barracuda Email Security Gateway, Progress SoftareMovelt Transfer, VMware tool, Microsoft windows and Office, WebP/Libwebp, Apple iOS and iPadOS, Atlassian confluence, Citrix NetScaler ADC and NetScaler Gateway, Cisco IOS XE. These popular platforms were exploited and affected millions of people.

What steps should be taken to zero-day attack?

There are some steps which will be helpful to survive the attack:

- Disconnect device from the internet and any other networks to prevent the attacker from accessing data or spreading the malware.
- Update software and system as soon as possible.
- Scan device for malware and remove any suspicious files or programs.
- Restore data from a backup if you have one.
- Review security practices like ISA, WASA and policies and implement any necessary changes like strengthen passwords, enable multi-factor authentication, use encryption
- Avoid clicking on unknown links or attachments, etc.

For better result it's a must to follow the prevention and even if your computer is affected you should immediately report in cybercrime.gov.in or contact the helpline number 1930 within 24 hours for reducing damages.

Fig 4. Toll Free Number

References:

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

https://www.imperva.com/learn/application-security/zero-day-exploit/

https://cloudkul.com/blog/impact-of-zero-day-attacks-on-a-companys-productivity/

https://www.techtarget.com/searchsecurity/feature/10-of-the-biggest-zero-day-attacks-of-2023