**Zero Day Attack**

A zero-day attack, often referred to as a zero-day exploit, is a type of cyberattack that takes advantage of a previously unknown vulnerability or security flaw in software or hardware. These vulnerabilities are called "zero-day" because the developers or vendors have had zero days to address or patch them.

In other words, the attackers are exploiting a security hole before the organization responsible for the affected software or hardware even knows about it.

Zero-day vulnerabilities are highly sought after by cybercriminals and state-sponsored hacking groups because they provide a significant advantage. When an attack is executed using a zero-day exploit, there are no available patches or defenses to stop it. This makes it particularly dangerous and difficult to prevent or mitigate.

To defend against zero-day attacks, it's crucial to keep software and systems up to date, use security best practices, and employ advanced security tools and monitoring systems to detect and respond to potential threats.

Additionally, responsible disclosure of zero-day vulnerabilities to software vendors can help protect the wider user community by allowing them to develop and release patches. Some security researchers and organizations follow ethical guidelines for responsible disclosure to ensure that vulnerabilities are fixed in a timely manner.