Digital Security
Progress. Protected.

Zero-day threats

What is a zero-day?

The term "zero-day" refers to a new, previously unknown vulnerability in a computer system or program. This flaw can be caused by a bug, a system glitch or a design error.

The name "zero-day" comes from the fact that no patch yet exists to mitigate the vulnerability being exploited, as neither the product manufacturer nor the security community are aware of its existence.

Although a zero-day vulnerability can be discovered by accident, they're typically found by expert hackers seeking to find, exploit and monetize them.

When a zero-day vulnerability hasn't been identified or patched before a criminal finds and starts using it, it becomes a zero-day exploit or zero-day attack.

Zero-day exploits can be used in a variety of ways. Common examples include:

- **Creating backdoor access to networks without a password**
- **Installing malicious programs such as ransomware or spyware**
- **Taking control of computers remotely**
- **Stealing or tampering with data**

These attacks can continue for months, weeks and even years without being discovered.

Because these types of threats are so difficult to detect, they can also be extremely valuable. While less common than in previous years, zero-days are often bought and sold on the dark web. In May 2020, for example, cybercriminals listed two Zoom zero-days for sale.

Examples of zero-day attacks

The most famous zero-day exploit is Stuxnet, a computer worm that was used in targeted attacks on supervisory control and data acquisition (SCADA) systems. Discovered in 2010, Stuxnet leveraged zero-day flaws in the Windows OS to eventually target centrifuges used to produce enriched uranium. It is widely believed to have substantially damaged Iran's nuclear program.

Another well-known zero-day exploit targeted the Ukrainian city of Kiev in 2016, creating an hourlong power blackout. ESET researchers discovered that malware (which they named Industroyer) had been used to leverage a security vulnerability in a Ukrainian power substation. It then leveraged that weakness to create a backdoor into the industrial systems control and shut down the entire power grid.

Why you need protection against zero-days

Zero-day exploits are particularly dangerous because they're launched on the same day a system vulnerability in your system is discovered. Because the exploit is known only to the attacker, signature-based malware detection won't be able to recognize and block it.

Once the vulnerability is discovered, then a patch will need to be created. Even when a patch is released, it won't be effective until a user or organization updates their software. That's why security experts emphasize the importance of updating software and devices each time a new patch is released.

How to protect against zero-day attacks

Basic rules:

- **Keep all your software, including operating systems, patched and up to date.**
- **Be sure to update your laptops, phones and other devices as patches or updates are released.**
- **Use a reliable, multilayered endpoint security solution.**
- **ESET endpoint security products include LiveGrid®, a malware protection system that identifies and analyzes suspicious files and automatically shares updates to all global endpoints.**

However, the most effective defense against zero-day exploits and other threats is advanced detection and analysis via cloud-based sandboxing:

ESET LiveGuard Advanced (ELGA)

ELGA detects and blocks zero-days by quickly analyzing new files in a cloud sandbox to fully understand their behaviors. Your entire organization is protected as soon as the file is submitted so malware never reaches your users, network and endpoints.

Via machine learning and behavioral analysis, ELGA will identify the file's true purpose while keeping it quarantined. Based on its behavior, the file will either be released or deleted—all within minutes of the initial detection.

Learn more about ESET LiveGuard Advanced

eset Digital Security
Progress. Protected.