Guide to Zero-Day Exploits

While you've taken steps to secure your network and sensitive data, you're still at risk of a Zero-Day vulnerability. Maybe you've heard the term before but don't have a deep understanding of how Zero-Day exploits work. Or perhaps, you know about Zero-Day exploits but need actionable insights on how to prevent them.

This guide provides an overview of Zero-Day exploits, how they happen, how to detect and identify a Zero-Day attack, and ways you can protect your organization.

The Basics: What is a Zero-Day exploit?

A Zero-Day exploit is an undisclosed application vulnerability that could be exploited to negatively affect the hardware, applications, data or network. The term "Zero-Day" refers to the fact that the developers have "zero" days to fix a problem that has just been exposed and may have been already exploited. Hackers seize on that security vulnerability to launch a cyber attack on the same day a weakness is discovered. Basically, the vulnerability is exploited before a fix becomes available.

Zero-Day exploits can be leveraged by threats such as viruses, polymorphic worms, Trojans, and various types of malware. All can be bought, sold, and traded. Hacker groups often post Zero-Day exploits as organizations under attack scramble to release patches against the security holes.

How does a Zero-Day exploit happen?

There are several ways a Zero-Day exploit can occur. In most cases, attackers use exploit code to take advantage of a Zero-Day vulnerability. In some cases, the exploit can also be a part of an email or an attachment.

Steps attackers take for a Zero-Day attack usually involve the following phases:

1. **Looking for vulnerability**: Attackers search through code looking for vulnerability. In some cases, Zero-Day exploits are sold (and purchased) by hackers.
2. **Vulnerability determined**: Attackers find a hole in the software or OS system that is unknown to the original developers.
3. **Exploit code created**: Attackers create the exploit code.
4. **Zero-Day exploit launched**: Armed with their exploit code, the attackers plant a virus or malware.

Zero-Day attacks occur because of a Zero-Day vulnerability window that exists between the time a threat is discovered and the time a security patch is released. A patch (aka "code fix") can be released to combat the threat after it has been discovered by the good guys. Sometimes the fix can take hours, but in other cases, it can take days or even weeks.

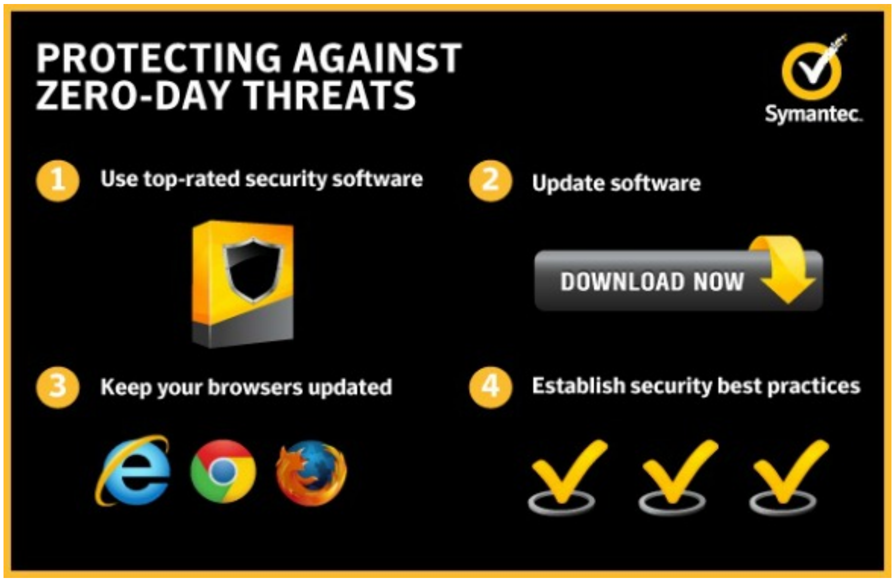
Sometimes an individual who discovers a Zero-Day vulnerability notifies the developer about the risk. But not all discoveries are altruistic. Frequently, hackers with malicious intent find the vulnerability. These hackers can use a Zero-Day vulnerability for their own purposes or sell the exploit on the underground hacker market.

How do you detect a Zero-Day attack?
Detection techniques for Zero-Day exploits include:

- **Statistical-based:** This approach to detecting Zero-Day exploits in real time relies on attack profiles built from historical data.
- **Signature-based:** This detection approach is dependent on signatures made from known exploits.
- **Behavior-based:** This model defense is based on the analysis of the exploit’s interaction with the target.
- **Hybrid-based:** As the name suggests, this approach is a blending of different approaches.

The traditional approach for detecting Zero-Day exploits often involves relying on disparate network and endpoint protection technologies, which may cause gaps in the security system. Unfortunately, this may not be enough to combat attackers using advanced attack methods. Detecting advanced targeted attacks requires an integrated, multi-layered approach.

How can you prevent Zero-Day exploits?


PROTECTING AGAINST ZERO-DAY THREATS
Symantec.
1 Use top-rated security software
2 Update software
DOWNLOAD NOW
3 Keep your browsers updated
4 Establish security best practices

Zero-Day vulnerabilities can leave you susceptible to Zero-Day attacks with disastrous results to your business. We know this sounds a little daunting—and it is—but you can take proactive and reactive security measures.

- **Use top-rated security software.** Be sure your security software doesn't just cover known threats because Zero-Day attacks are, by definition, attacks not yet known.
- **Update software**. Software updates often contain security measures against any intrusion. Be sure to have your software updated regularly.
- **Use updated browsers**. Browsers are favorite targets for Zero-Day attacks. Updates to browsers are often automatic, but make sure your browsers are all updated as they often contain patches to vulnerabilities. Check for specific browser update instructions.
- **Establish security best practices**. Make sure you set an example of personal online security best practices and have all your employees do the same.

How Symantec helps fight Zero-Day attacks?

Symantec is addressing the needs of organizations to accelerate detection and prevention of Zero-Day attacks. However, organizations of all sizes need to stay constantly vigilant to the developing tactics and methods used by attackers. Zero-Day vulnerabilities are not only an industry-wide concern, but also an issue for all of us as collective end-users.

Overall, education, preparation and a swift response to Zero-Day vulnerabilities need to be a company-wide concern—from the top executives, board members, and IT security teams to all employees. As a leader in global security, Symantec is uniquely positioned to provide the technological solutions and actionable insights to help you strengthen your organization's security posture today and on future horizons.

Looking for more insights? Be sure to follow the Symantec Monthly Threat Report