ZERO DAY THREATS:
FUTURE-PROOFING YOUR SYSTEM

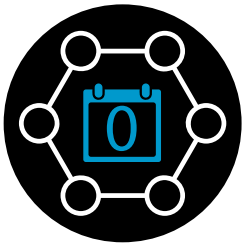
Introduction

Zero day attacks are extremely common and extremely dangerous. When it comes to zero day hacking, 2021 has shattered past records. An average of 80% of successful breaches consist of zero day attacks, according to the Ponemon Institute.

In recent weeks, a high-profile zero day threat, known as Log4j, emerged. Its severity was judged as 10 out of 10, and potentially affects hundreds of thousands of organizations around the world. Since then, federal cyber security agencies and software companies have distributed extensive warnings about related risks.

Although said zero day story has faded from the news cycle, the vulnerabilities' ubiquity continues to threaten organizations, and more importantly, other vulnerabilities just like it could surface at any moment.

In this e-Book, discover what zero day attacks are, why they matter, and how to adopt a prevention-first posture that can mitigate and insulate your organization from zero day threats.

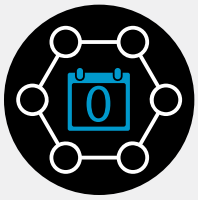


According to the Ponemon Institute, an average of 80% of successful breaches consist of zero day attacks.

What is a zero day attack?

A zero day attack (written as zero day, zero-day or 0-day) relies on a weakness in a software program to gain entry into a network system. Attackers may then deploy ransomware on systems, attempt system takeovers, steal data or engage in other disruptive and harmful behaviors.

Cyber criminals prefer to use zero day vulnerabilities within software programs that maintain wide distribution levels, as this yields a high number of targets that they can exploit. For example, a common cloud application represents a more attractive vehicle through which hackers might launch a zero day attack as compared to an application only used by a subsector of a comparatively obscure industry.



Defining zero day terminology

Key terms related to zero day attacks are often used interchangeably, despite nuanced differences in meaning. To avoid confusion, see the definitions below.

Zero day vulnerabilities: These are weaknesses in software, firmware or hardware that remain unknown to vendors and clients. Zero day vulnerabilities function as the points-of-entry that cyber criminals use to break into systems.

Due to the nature of computer code, it is generally accepted that some code-based products will deploy with these weaknesses or invisible imperfections. In the majority of cases, they're only discovered once a cyber attack has occurred.

Zero day exploits: If a zero day vulnerability is the "door" that criminals enter through, zero day exploits are the crowbars that hackers use to open doors. An exploit refers to the method and/or code used to profit from a zero day vulnerability.

Zero day attacks: These occur when cyber criminals choose to make use of the exploit/s to break into systems.

Zero day targets: Attackers can use zero day attacks to put millions of organizations at risk. Zero day attackers generally seek financial gain from either single organizations or large industry sectors.

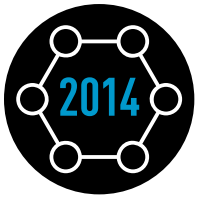
As journalist Nicole Perlroth points out, attackers also routinely leverage zero days on behalf of governments, attacking foreign targets; from federal buildings to public institutions.

It is less common for zero day attackers to go after a single organization without hitting any other targets simultaneously.

Dangers of zero days: For vendors and their clients alike, zero day attacks are dangerous because no one can see them coming. Imagine a robber breaking into a bank through a hidden door, which no one knew existed and that's connected to a former hotel five blocks away. You get the idea.

Examples of famous zero day attacks

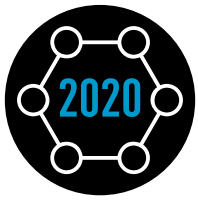
Zero day threats can take a variety of different forms and new zero day threats emerge everyday. The examples below illustrate what they can look like, how they operate, the level of damage that they can inflict, and common mitigation tactics.



In 2014, the Heartbleed bug emerged as a serious flaw in OpenSSL, an encryption software behind a large number of secure communications exchanges on the internet. The bug essentially allowed nefarious persons to identify secret keys, passwords, credit card numbers and personal information transmitted through what were ostensibly private messages.

Attackers leveraged the vulnerability to access internal corporate networks, wreaking internal havoc. Allocating additional resources to corporate security can prevent hackers from gaining entry into systems via zero day vulnerabilities and exploit tools.

In 2017, the EternalBlue vulnerability came to light. Microsoft released patches for this issue, however, multiple devastating attack types were directed towards unpatched computers. Attacks related to this vulnerability caused upwards of $1 billion USD in damages across more than 60 countries. This episode highlights the extent to which patching can protect organizations from harm.



In 2020, a well-known video conferencing provider's software showed zero day vulnerabilities. Video conference calls could be exploited for the purpose of launching cyber attacks. The vulnerabilities enabled exploits related to arbitrary code execution, which allows attackers to run any code or commands on victims' machines. The vulnerabilities have since been patched, and function to further emphasize the importance of patching in averting cyber disaster.

Not all is lost. In the way that your organization can prepare for a natural disaster, your organization can also be prepared for a cyber disaster.

Zero day attack prevention

1. Keep up-to-date regarding the latest zero day vulnerabilities.
2. Implement vulnerability management and patching programs. These ensure that any vulnerable software is updated as soon as possible.
3. Adopt a zero trust approach, limiting credentialed access to systems and sub-system locations to as few individuals as possible.
4. Ensure that all of your endpoints are secure.
5. Implement firewalls, which can monitor traffic across your network and reduce unauthorized access.
6. Ensure that your firm has a data backup system in place. In the event of a zero day attack, backups can facilitate an expedient recovery.
7. Adjust your organization's cloud application security strategy to ensure that it both scales with cloud adoption and can help prevent the next zero day attack. Build automation into cloud security processes.
8. Although alluded to previously, it's worth repeating - Incorporate artificial intelligence into your monitoring and tracking strategies.
9. Invest in threat prevention technologies with high NSS ratings, cutting-edge capabilities, 100% block rates, and few false positives.
10. Finally, consider a consolidated cyber security platform, which can provide you with expanded visibility and control across your entire ecosystem.

Also, be sure to maintain an up-to-date incident response plan. Organizations may want to test-run incident response plans before an actual incident occurs.

Conclusion:

Zero day attackers intentionally operate under-the-radar, but preemptive prevention measures can thwart zero day threats. The key takeaway: Adopting a layered approach to cyber security. Ensure that your organization maintains critical security layers. *Ensure that your organization can detect and remediate zero day vulnerabilities quickly and easily.*

If you would like a free security check up for your organization, or have questions about products, contact your Check Point sales representative. For the latest cyber security news, trends and analyses pertaining to zero-day vulnerabilities and more, visit CyberTalk.org.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com