John Kyle Razon November 29 2021

BS Info Tech IV

What is a zero day exploit

Software programs often have vulnerabilities. These are unintentional flaws, or holes in software programs that could hypothetically be taken advantage of. For example, there may be a flaw that allows a cybercriminal to gain access to otherwise secure data. Software programmers are often on the lookout for these vulnerabilities. When they discover a vulnerability, they analyze it, come up with a “patch” to fix the vulnerability, then issue that patch in a new release of the software.

Types of perpator

Corporate spy – a person hired by an organization to break into another organization’s specific computer and steal its proprietary data and information, or to help identify security risks within their own organization. The hiring of a corporate spy is called corporate espionage.

Cracker – someone who accesses a computer or network illegally, with the intent of destroying data, stealing information, or any other malicious action. A cracker usually has advanced network skills. Cyberextortionist – a person who uses e-mails as their drive force for extortion. A cyberextortionist usually performs actions, such as threatening to expose confidential information about a company, unless they are paid a certain sum of money.

Cyberterrorist – someone who uses the internet or a network to destroy or damage computers for political reasons. Cyberterrorists are also associated with cyberwarfare, which is described as an attack whose goal ranges from disabling a government’s computer network to crippling a country.

Hacker – a person who accesses a computer or network illegally. Some hackers make a claim or justify their intent for hacking, are to improve security.

Script kiddie – someone who has the same intent as a cracker but does not have the technical expertise, so in turn use pre-written hacking and cracking programs to breach computers or networks. Unethical employee – employees may break into their employer’s computer or network maybe either to simply exploit a security weakness or to seek financial gains from selling confidential information. Some employees may just want revenge.

**Category of Exploit**

**Known exploits**have already been discovered by cybersecurity researchers. Whether the known exploit is due to a vulnerability in the software, OS, or even hardware, developers can code patches to plug the hole. These patches are released to users as security updates. That’s why it’s crucial to keep your devices updated.

**Unknown exploits** or zero-day exploits, in contrast, are created by cybercriminals as soon as they discover a vulnerability, and they use the exploit to attack victims on the same day. When a zero-day exploit attack happens, software developers and cybersecurity researchers have to scramble to figure out how the exploit works and how to patch the vulnerability.

Some exploits have led to such massive cyberattacks that they’ve become nearly household names.

**Types of Exploit**

**EternalBlue**

[EternalBlue](https://www.avast.com/c-eternalblue) is one of the most famous — and most damaging — exploits out there. Originally developed by the NSA, EternalBlue was stolen by the Shadow Brokers hacking group and then leaked in March 2017. Although Microsoft discovered the leak and issued a security update to patch the vulnerability, many people and organizations failed to apply the patch in time. This allowed hackers to proceed with some of the most damaging cyberattacks in history, including WannaCry and NotPetya.

**WannaCry**

[WannaCry](https://www.avast.com/c-wannacry) was the stuff of nightmares: a [wormable attack](https://www.avast.com/c-computer-worm) that used the EternalBlue exploit to spread exponentially across computer networks, infecting 10,000 machines per hour in 150 countries. As ransomware, WannaCry encrypted computers, rendering them inaccessible — a huge issue for the national health services, governments, universities, and large corporations that WannaCry hit. Although WannaCry is no longer active, other exploits can still take advantage of EternalBlue to attack Windows users running outdated software — so make sure yours is updated.

**Petya and NotPetya**

[Petya](https://www.avast.com/c-petya) and its amusingly named successor, NotPetya, were ransomware strains (NotPetya also relied on the EternalBlue exploit). The Petyas caused huge damage by encrypting computers’ master file table (MFT), rendering the machines completely unusable. And while there were ransom demands made, NotPetya could not be decrypted. So even if the users and organizations paid up, they never received anything in return. Experts estimate that Petya strains of ransomware caused over $10 billion in damage as they blew through banks and other corporations.

**BlueKeep**

[BlueKeep](https://blog.avast.com/what-is-bluekeep) is an exploitable vulnerability in Microsoft Remote Desktop Protocol (RDP) that can allow attackers to log in to a victim’s computer remotely. Microsoft raised the alarm about BlueKeep in May 2019, and issued a patch even for outdated operating systems such as Windows XP. That unusual step demonstrates the potential severity of BlueKeep: as it's another wormable exploit, many security researchers feared that BlueKeep would lead to the next devastating worldwide cyberattacks. As of this writing, BlueKeep has yet to amount to much, but it’s still important to patch your system so you won’t be caught in any future attacks.