Digital Security
Progress. Protected.

Zero-day exploits are on the rise—but why?

Zero-day vulnerabilities take advantage of new, previously unknown vulnerabilities in a computer system or program. They are particularly dangerous because attacks can go on for months or even years without being discovered. This gives criminals ample time to steal data, create backdoor access to networks, take control of computers and more.

Worse, recent reports note that zero-days are more common than ever.

In 2021, Google's Project Zero report detailed the detection of 58 in-the-wild zero days, more than twice the previous record of 28 detected in 2015. Over the same period, Mandiant Threat Intelligence identified 80 zero-days exploited in the wild, which is more than double the previous record volume in 2019.

Opinions differ on the root cause of the increase. A Google researcher cited better detection methods and an increase in disclosures as two reasons for these record numbers.

But the potential for enormous profits is another explanation of why these exploits have hit an all-time high.

An MIT Technology Review article reported that a zero-day vendor named Zerodium will pay up to $2.5 million for a zero-day exploit that provides control over an Android device. In turn, Zerodium sells that exploit to someone else—but not necessarily the software vendor involved, for them to patch it. Instead, they may simply sell to the highest bidders, including governments and private industry.

Experts also point toward the expansion of technologies like mobile, cloud and Internet of Things. More systems and devices online obviously lead to more software flaws that can be exploited.

The bottom line? Organizations need to make sure that zero-day exploits become harder to execute. That means investing in better cybersecurity.

The most effective defense against these exploits is advanced threat detection via cloud-based sandboxing. Unlike signature-based detection, cloud sandboxing can protect against previously unknown threats like zero-day exploits and ransomware.

By executing and analyzing files in an isolated environment, this technology identifies threats and blocks them before they can spread to your endpoints and users.

Companies can also harden their overall security with the following best practices:

- **Implementing multilayered security with the ability to detect, protect and respond**
- **Conducting regular cybersecurity awareness training for all employees**
- **Committing to regular system updates and prompt patching of any vulnerabilities**

Learn more about zero-day threats on this resource page

Get started: Talk with one of our experts