Nearly a Quarter of Exploits Sold on Cybercriminal Underground Are More Than Three Years Old

Trend Micro research warns of threat from unpatched legacy vulnerabilities

DALLAS, July 13, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, released new research urging organizations to focus patching efforts on the vulnerabilities that pose the greatest risk to their organization, even if they are years old.

Trend Micro Research found that 22% of exploits for sale in underground forums are more than three years old.

To view a full copy of the report, *The Rise and Fall of the N-day Exploit Market in Cybercriminal Underground* please visit: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the-underground-n-day-exploit-market.

"Criminals know that organizations are struggling to prioritize and patch promptly, and our research shows that patch delays are frequently taken advantage of," said Mayra Rosario, senior threat researcher for Trend Micro. "The lifespan of a vulnerability or exploit does not depend on when a patch becomes available to stop it. In fact, older exploits are cheaper and therefore may be more popular with criminals shopping in underground forums. Virtual patching remains the best way to mitigate the risks of known and unknown threats to your organization."

The report reveals several risks of legacy exploits and vulnerabilities, including:

- The oldest exploit sold in the underground was forCVE-2012-0158, a Microsoft RCE.
- CVE-2016-5195, known as the Dirty Cow exploit, is still ongoing after five years.
- In 2020, WannaCry was still the most detected malware family in the wild, and there were over 700,000 devices worldwide vulnerable as of March 2021.
- 47% of cybercriminals looked to target Microsoft products in the past two years.

The report also reveals a decline in the market for zero-day and N-day vulnerabilities over the past two years. This is being driven in part by the popularity of bug bounty programs, like Trend Micro's Zero Day Initiative, and the rise of Access-as-a-Service – the new force in the exploit market.

Access-as-a-Service has the advantages of an exploit, but all the hard work has already been done for the buyer, with underground prices starting at $1000USD.

These trends are combining to create greater risk for organizations. With nearly 50 new CVEs released per day in 2020, the pressure on security teams to prioritize and deploy timely patches has never been greater – and it's showing. Today, the time to patch averages nearly 51 days for organizations patching a new vulnerability. To cover that gap in security protection, virtual patching is key. It is based on intrusion prevention technology and offers a hassle-free way to shield vulnerable or end-of-life systems from known and unknown threats indefinitely.

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---