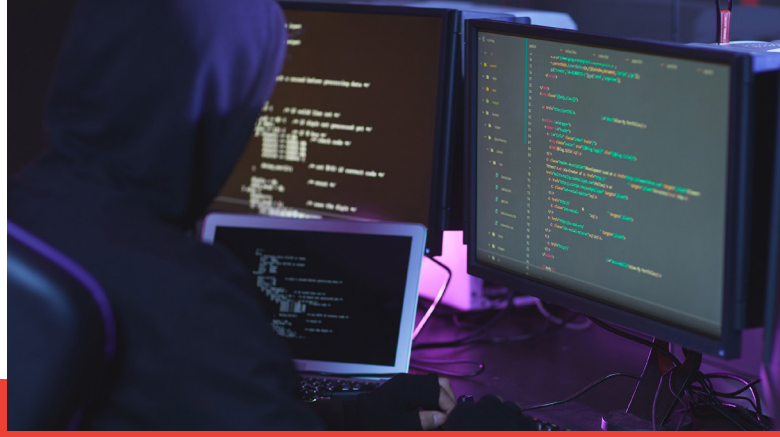
The Rise and Imminent Fall of the N-Day Exploit Market in the Cybercriminal Underground



Malicious actors gain access to exploits via the cybercriminal underground, which hosts an active market for exploits for both unpatched (zero-day) and patched (N-day) vulnerabilities. Over the past two calendar years, we scoured underground forums for exploits requested by buyers as well as those offered by sellers. We share our findings in our research paper, which also covers the life cycle of exploits and the emergence of service-based models in the cybercriminal underground.

KEY FINDINGS

The age and status of an exploit affects the demand for it. A zero-day exploit could fetch a high price in the underground — typically over US$5,000. As soon as it becomes an N-day exploit — that is, once the affected vulnerability is patched — its price decreases drastically.

Some older exploits remain relevant in the underground. Malicious actors still find uses for N-day exploits, even those for vulnerabilities that have long been patched. Sellers occasionally offer older exploits as a bundle to make them more attractive to potential buyers.

Exploits for Microsoft products had both the highest demand and the highest supply. No doubt because of their widespread use, they accounted for at least 47% of exploits requested and at least 51% of exploits sold by users on cybercriminal underground forums. Microsoft Office alone made up 21% of exploits requested and 23% of exploits sold.

Service-based models have led to a shift in the exploit market. Subscription services let exploit sellers offer prepackaged exploit tools and builders to less technically inclined customers. Similarly, the access-as-a-service model provides customers access to corporate networks via remote desktop protocol without the customers' having to set up complicated infrastructure.

SECURING ORGANIZATIONS FROM EXPLOITS VIA VIRTUAL PATCHING

The best way for organizations to thwart exploits is to continuously update their systems with the latest security patches. However, especially in the case of large organizations, this could take plenty of time and resources. Virtual patching can help shield organizations while they work to update their systems, by implementing security policies designed for specific vulnerabilities and exploits.

Learn more about our findings on the exploit market in our research paper at https://bit.ly/exploitmarket.

TREND MICRO | research