Vulnerabilities Being Exploited Faster Than Ever: Analysis

In 2022, the widespread exploitation of new vulnerabilities was down 15% over the previous year; zero-day attacks declined 52% from 2021; and there were 33% fewer vulnerabilities known to have been exploited as part of a ransomware attack. On the surface, it might appear that things were easier for security teams last year. That would be wrong.

The figures are taken from Rapid7's 2022 Vulnerability Intelligence Report, an annual publication commenced in 2020. The most worrying finding today is the time from vulnerability disclosure to exploitation is decreasing. "A large number of vulnerabilities are being exploited before security teams have any time to implement patches or other mitigations," Caitlin Condon, senior manager of security research at Rapid7, told *SecurityWeek*.

To be precise, 56% of the vulnerabilities in the report were exploited within seven days of public disclosure – a 12% increase over 2021, and an 87% increase over 2020. Resources for triaging and remediating vulnerabilities remain limited, and priorities can be misdirected.

A good example of this was hype emanating from Log4Shell. "Many organizations spent the first weeks (or months) of 2022 working their way down a lengthy list of Log4Shell remediations, taxing IT and security team resources that had already been depleted by shrinking budgets and pandemic exhaustion," notes the report.

But after Log4Shell we had Spring4Shell and then Text4Shell. There was, suggests Condon, "a 4Shell cadence given to new vulnerabilities." This implied they were of the same magnitude

as Log4Shell when they were not. But the C-suite saw these reports and asked the security folks, what are we doing? “It’s kind of hard for the security team to reply, ‘yeah, it’s called 4Shell, but it’s stupid and we’re not prioritizing it,’” said Condon. The result is resources are inadvertently redirected from important vulnerabilities to less important vulnerabilities when the time-to-exploitation of those important vulnerabilities is decreasing dramatically.

Pressed on whether hype is a problem for security teams, Condon replied that it can be. She believes the press in general, and the security press in particular, are a ‘net good’. “But if you’re a researcher on Twitter, and your incentive is to get 2,000 retweets and get hired, that’s a huge incentive to hype it up – and that can put pressure on reporters.” She added that not all security vendors are innocent when their own product can provide mitigation.

Condon believes there are three primary takeaways from the current Rapid7 research. The first is that widespread threats remain high, even though they are down from 66% in 2021 to 56% in 2022’s dataset. “Common payloads dropped during mass exploitation included cryptocurrency miners, web shells, and a variety of botnet malware in addition to an ever more diverse set of ransomware payloads,” says the report.

The second takeaway is the complexity of the ransomware ecosystem and how that affects visibility and statistics. “The vulnerabilities that we could definitively map to ransomware incidents decreased in 2022 by one-third. Why is this happening, when we and many other firms have seen an increase in the overall volume of ransomware incidents?” she asked.

The obvious conclusion is that ransomware groups are leveraging fewer new vulnerabilities than they did in 2021. “That might be part of the equation, but it almost certainly is not the whole story – the diversification of both the ransomware ecosystem as a whole and also the broader cyber

underground comes into significant play here," she added.

The effect is complex. When the number of vulnerabilities used is decreasing and the number of ransomware families is increasing, it means there are more threat actor payloads to track and there are more TPPs to track and attribute. "All of this contributes to likely lower industry visibility, at least in the short term, into ransomware CVE mappings, and lower confidence levels in tracking full attack chains and timelines. Because of the diversification of the ransomware ecosystem and more limited use of new vulnerabilities, we are probably seeing lower competence and visibility into some of these activities."

All of this is complicated by Condon's third takeaway: the time-to-exploit for newly disclosed vulnerabilities. "We believe the time between when a vulnerability is known and when it's exploited is a really critical metric for security practitioners," she said. "They must not only choose what to prioritize but must also justify what they are prioritizing with often very limited resources all the way up their chains and across their organization."

Vulnerability Time to Known Exploitation (Source: Rapid7)

Even considering the statistical disturbance of zero-day

exploits, the time between disclosure and exploitation has decreased steadily over the past three years. “In 2020, 30% of our report vulnerabilities were exploited in the wild within a week of disclosure. In 2021, that went up to 50%. In 2022, 56% of our reported vulnerabilities were exploited within a week of disclosure.”

Some of these vulnerabilities may technically be classified as zero-days or n-days. “There were more than half a dozen examples that were not exploited at the time of disclosure but were exploited within a few days,” she added. But zero-day or not zero-day is not a distinction that Rapid7 is trying to make. It concentrates primarily on the time-to-exploitation.

“And the numbers are not good, which is a tough message for a lot of our customers,” she said. This combination of widespread exploitation, reduced visibility into ransomware incidents, and very short time-to-exploitation on new vulnerabilities is simply increasing the pressure on security teams at a time of increasing burnout already brought on by post pandemic stress and unregulated over-working at home.

Related: Chinese Hackers Exploited Fortinet VPN Vulnerability as Zero-Day

Related: VMware Says No Evidence of Zero-Day Exploitation in ESXiArgs Ransomware Attacks

Related: GitHub Updates Policies on Vulnerability Research, ExploitsRelated: Cyber Insights 2023 | Criminal Gangs

Vulnerabilities Being Exploited Faster Than Ever: Analysis