Study examines 200 real-world 'zero-day' software vulnerabilities

March 9 2017

Zero-day software vulnerabilities - security holes that developers haven't fixed or aren't aware of - can lurk undetected for years, leaving software users particularly susceptible to hackers. A new study from the RAND Corporation, based on rare access to a dataset of more than 200 such vulnerabilities, provides insights about what entities should do when they discover them.

Until now the big question - whether governments or anyone should publicly disclose or keep quiet about the vulnerabilities - has been difficult to answer because so little is known about how long zero-day vulnerabilities remain undetected or what percentage of them are eventually found by others.

The RAND study is the first publicly available research to examine vulnerabilities that are still currently unknown to the public. The research establishes initial baseline metrics that can augment other studies that have relied on manufactured data, findings only from publicly known vulnerabilities, or expert opinion.

Based on the dataset, RAND researchers have determined that zero-day vulnerabilities have an average life expectancy - the time between initial private discovery and public disclosure - of 6.9 years. That long timeline plus low collision rates - the likelihood of two people finding the same vulnerability (approximately 5.7 percent per year) - means the level of protection afforded by disclosing a vulnerability may be modest and that keeping quiet about - or "stockpiling" - vulnerabilities may be a

reasonable option for those entities looking to both defend their own systems and potentially exploit vulnerabilities in others'.

"Typical 'white hat' researchers have more incentive to notify software vendors of a zero-day vulnerability as soon as they discover it," said Lillian Ablon, lead author of the study and an information scientist with RAND, a nonprofit research organization. "Others, like system-security-penetration testing firms and 'grey hat' entities, have incentive to stockpile them. But deciding whether to stockpile or publicly disclose a zero-day vulnerability - or its corresponding exploit - is a game of tradeoffs, particularly for governments."

People who know about these weaknesses may create "exploits," or code that takes advantage of that vulnerability to access other parts of a system, execute their own code, act as an administrator or perform some other action. One famous example is the Stuxnet worm, which relied on four Microsoft zero-day vulnerabilities to compromise Iran's nuclear program.

"Looking at it from the perspective of national governments, if one's adversaries also know about the vulnerability, then publicly disclosing the flaw would help strengthen one's own defense by compelling the affected vendor to implement a patch and protect against the adversary using the vulnerability against them," Ablon said. "On the other hand, publicly disclosing a vulnerability that isn't known by one's adversaries gives them the upper hand, because the adversary could then protect against any attack using that vulnerability, while still keeping an inventory of vulnerabilities of which only it is aware of in reserve. In that case, stockpiling would be the best option."

Of the more than 200 real-world zero-day vulnerabilities and the exploits that take advantage of them analyzed by RAND, almost 40% are still publicly unknown. Ablon and co-author Andy Bogart were able to

determine that 25 percent of vulnerabilities do not survive to 1.5 years and only 25 percent live more than 9.5 years. No vulnerability characteristics indicated a long or short life. However, future analyses may want to examine more closely Linux versus other platform types, the similarity of open and closed source code, and type of exploit class.

The study examined what proportion of zero-day vulnerabilities are alive (publicly unknown), dead (publicly known), or somewhere in between. But boiling the argument down to whether vulnerability is "alive" versus "dead" is too simplistic and could create a barrier for vulnerability-detection efforts, Ablon said. A vulnerability may be classified as "immortal" if it's one that will remain in a product in perpetuity because the vendor no longer maintains the code or issues updates.

Vulnerabilities that are publicly known are often disclosed with a security advisory or patch, but in other cases, developers or vulnerability researchers post online about a vulnerability without issuing a security advisory. Other vulnerabilities are quasi-alive - "zombies" - because, due to code revisions, they can be exploited in older versions of a product.

Once an exploitable vulnerability has been found, a fully functioning exploit may be developed quickly, with a median time of 22 days. That means any serious attacker can likely obtain an affordable zero-day for almost any target, given the typical life expectancies of these vulnerabilities and the short development time. However, most of the price for those wishing to purchase such a zero-day exploit from a developer is driven not by labor but by its inherent value, lack of supply and other factors.

Funding for the study, "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and their Exploits," was provided by philanthropic contributions from RAND supporters, income from operations, and from the RAND Institute for Civil Justice, dedicated to

improving the civil justice system by supplying policymakers and the public with rigorous and nonpartisan research. Its studies identify trends in litigation and inform policy choices about liability, compensation, regulation, risk management and insurance.

Provided by RAND Corporation