The Life of a Zero Day

WHITE PAPER

NYOTRON
SECURING THE WORLD

"Open Sesame!"
– *Ali Baba and the Forty Thieves (One Thousand and One Nights)*

Zero Days Live Longer Than Expected

RAND Corporation's report from 2017 called *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* is fascinating. Although it is 133 pages long, you will not have to spend your whole weekend to get through it. The most striking findings of this research are right up-front, particularly this surprising insight:

> "Zero-Day exploits and their underlying vulnerabilities have a 6.9 year life expectancy, on average."

This is 2,521 days after the initial discovery to be precise. Hence, the reference to "Thousands of Nights" in the study's title. In fact, 25% of zero-days will survive more than 9.5 years according to the research. This data suggests that the time between the discovery of a vulnerability by a researcher (for any purpose, including private use or resale to government entities or gray/black markets) to public disclosure and patch availability is dramatically longer than most in the industry have thought.

By the way, the definition of a vulnerability that RAND uses is "a software, hardware, procedural, or human weakness that may provide an attacker with an open door with which to exploit." The RAND research focuses solely on software vulnerabilities. There is high likelihood that hardware vulnerabilities "live" for much longer periods of time (and, in many cases, forever) than software vulnerabilities due to the inherent difficulty of "patching" hardware.

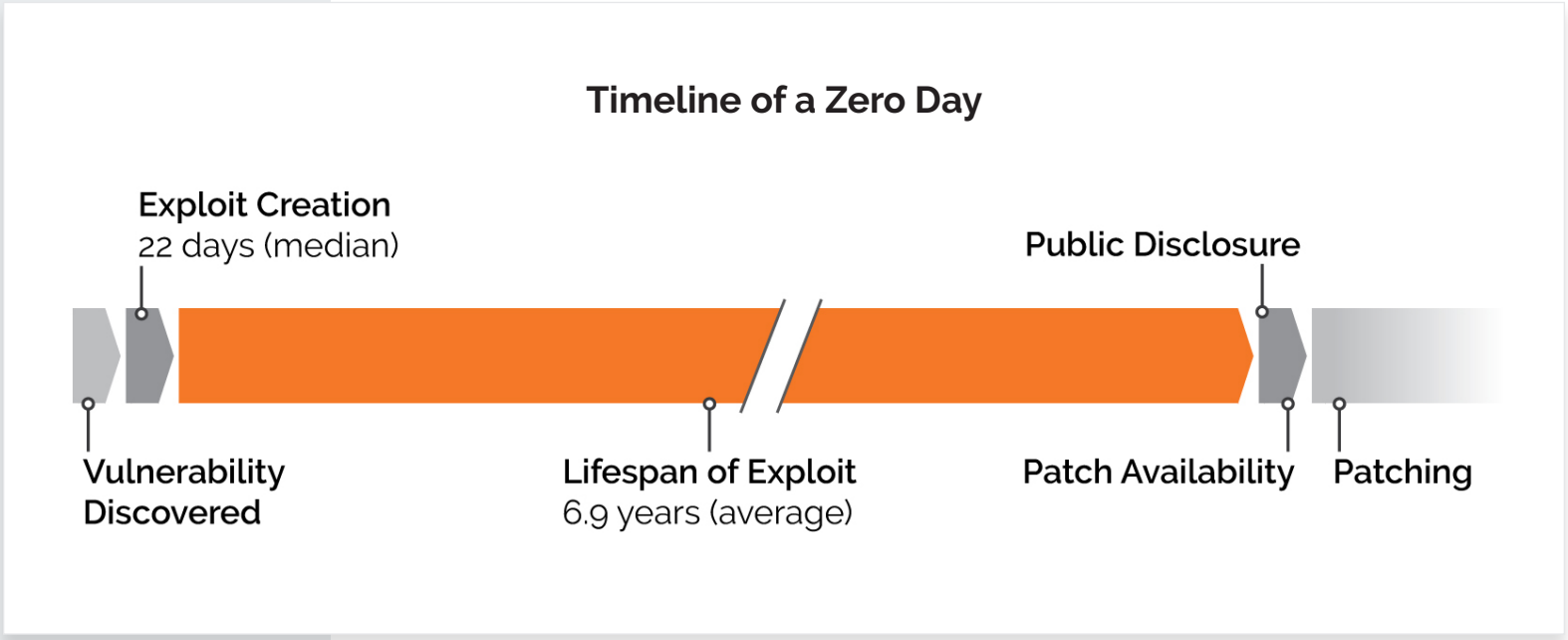
We have all heard about infamous examples of advanced nation-state sponsored malware such as Stuxnet (with its four zero-days) that survived for an estimated five years prior to being discovered.[1] However, these are thought to be exceptions rather than the rule. However, according to RAND Corporation researchers, we should not be surprised by vulnerabilities that survive for up to 10 years or even longer.

[1] "Stuxnet" (https://en.wikipedia.org/wiki/Stuxnet). *Wikipedia*. Retrieved 2018-03-30.

A vulnerability does not automatically result in damage. An exploit that takes advantage of a vulnerability needs to be created first. An exploit, as used by RAND, is a "malicious code that takes advantage of software vulnerabilities to infect, disrupt, or take control of a computer without the user's consent and typically without their knowledge." Surprisingly, according to the RAND research, almost a third of exploits are developed in a week or less, with the majority developed in under a month from the point an exploitable vulnerability is found.

What Are the Implications of a Long Life?

At its core, the long life span of a vulnerability means that even organizations with industry-leading vulnerability management and patching processes in place are still vulnerable. This is true even if you go through the pain of immediately testing and rolling out all patches of critical and important severity (ranked using Microsoft's rating system). And, if you have ever managed patch management tools and projects, you know how difficult this is, considering change control policies, rollback requirements, off-line and remote systems, rollout issues and more. Moreover, we are not talking about just patching Windows operating systems. We are talking about patching all third-party applications in use within an organization, firmware and all operating systems (macOS, Linux, UNIX, Android, etc.).



After all is said and done, the "bad guys" can still gain access to an organization's environment. Could this ability be reserved for only a handful of nation-state actors? Not so! According to the RAND research, "...any serious attacker can always get an affordable zero-day for almost any target." Although the costs may reach millions for very unique targets and environments, (the so called "unicorn exploits"), most zero-day exploits (i.e., a functioning exploit and not just a vulnerability) can be purchased for anywhere between $30,000 and $100,000 on gray and black markets.

> "Defenders will always be vulnerable to zero-day vulnerabilities..."
> – RAND Corporation

What Should We Do About Zero Day Vulnerabilities with a Long Life Span?

Now that we know that vulnerabilities and exploits are lurking in the darkness for an average of about 7 years and are accessible to most serious attackers, what can we do about it? Or should we first start with the question—should we care? Isn't the human element still the most exploited attack vector? Remember Kevin Mitnick's "The Art of Deception" that discussed how hackers use social engineering to compromise even the most secure systems and organizations?

After decades, we still haven't truly figured out patch management. And then all those pesky fileless attacks that exploit legitimate scripting and administration tools (e.g., PowerShell) have become popular in the last few years. In reality, the majority of commodity malware and opportunistic attacks rely on already known vulnerabilities. Just look at the WannaCry example. Microsoft patched CVE-2017-0144 (EternalBlue) on March 14, 2017 and the Shadow Brokers hacker group leaked the exploit a month later on April 14, 2017.[2] WannaCry ransomware hit almost two months after the patch became available, affecting more than 200,000 computers across 150 countries with estimated damage ranging from hundreds of millions to billions of dollars.

In fact, most exploits are old. Even at the beginning of 2018, nation-state actors still actively used the EternalBlue exploit. According to Fortinet, 90% of organizations the company protects have experienced cyber-attacks during which intruders tried to exploit vulnerabilities that were three years or older. In addition, 60% of organizations were attacked with exploits ten years or older.[3]

[2] EternalBlue" (https://en.wikipedia.org/wiki/EternalBlue). *Wikipedia*. Retrieved 2018-03-30.

[3] Cimpanu, Catalin (August 24, 2017) "90 Percent of Companies Get Attacked with Three-Year-Old Vulnerabilities" (https://www.bleepingcomputer.com/news/security/90-percent-of-companies-get-attacked-with-three-year-old-vulnerabilities/). *BleepingComputer*. Retrieved 2018-03-30.

Overall, unless your organization is in critical infrastructure, defense and intelligence or another mission-critical industry *and* has already reached the highest level of security maturity, you probably should not be losing too much sleep over zero-days. This does not mean you should ignore them either. Per RAND, "defenders may be able to shift the balance in their favor by starting from the assumption of compromise...".

Consider tools such as Endpoint Detection and Response (EDR) to gain deep historical visibility into what is happening on your endpoints. This would allow you to at least have a DVR-like capability to assess what was compromised and taken in case a previously unknown, but exploited vulnerability becomes public and your organization was affected. Additionally, User and Entity Behavior Analytics (UEBA) will attempt to detect anomalies created by the zero-day based exploit or attacker's actions after they have gained access to your environment. Compensating controls for endpoints, such as OS Hardening, Application Isolation or OS-Centric Positive Security should also be considered.

Summary

We live in incredible times, where we trust more of our lives to machines that are becoming ever more powerful. We cannot leave the doors to our "digital kingdoms" wide open. Adversaries, both nation-states and for-profit malicious actors, have access to a seemingly unlimited supply of "all access keys". Our responsibility is to revoke and disable these keys or to at least make that access as difficult as possible through thoughtful defense-in-depth security controls. These controls should not just rely solely on the "next gen" version of a well-known technology. Truly different types of protection and detection technologies need to be layered in order to create the strongest possible defense.

NYOTRON
SECURING THE WORLD

2880 Lakeside Drive Suite 237
Santa Clara, CA 95054
+1 (408) 780-0750
www.nyotron.com