2021 Cybersecurity Zero-Day Gamechangers: SolarWinds, ProxyLogon, & Kaseya Breaches

4 Imperatives Executives & IT Teams Must Face

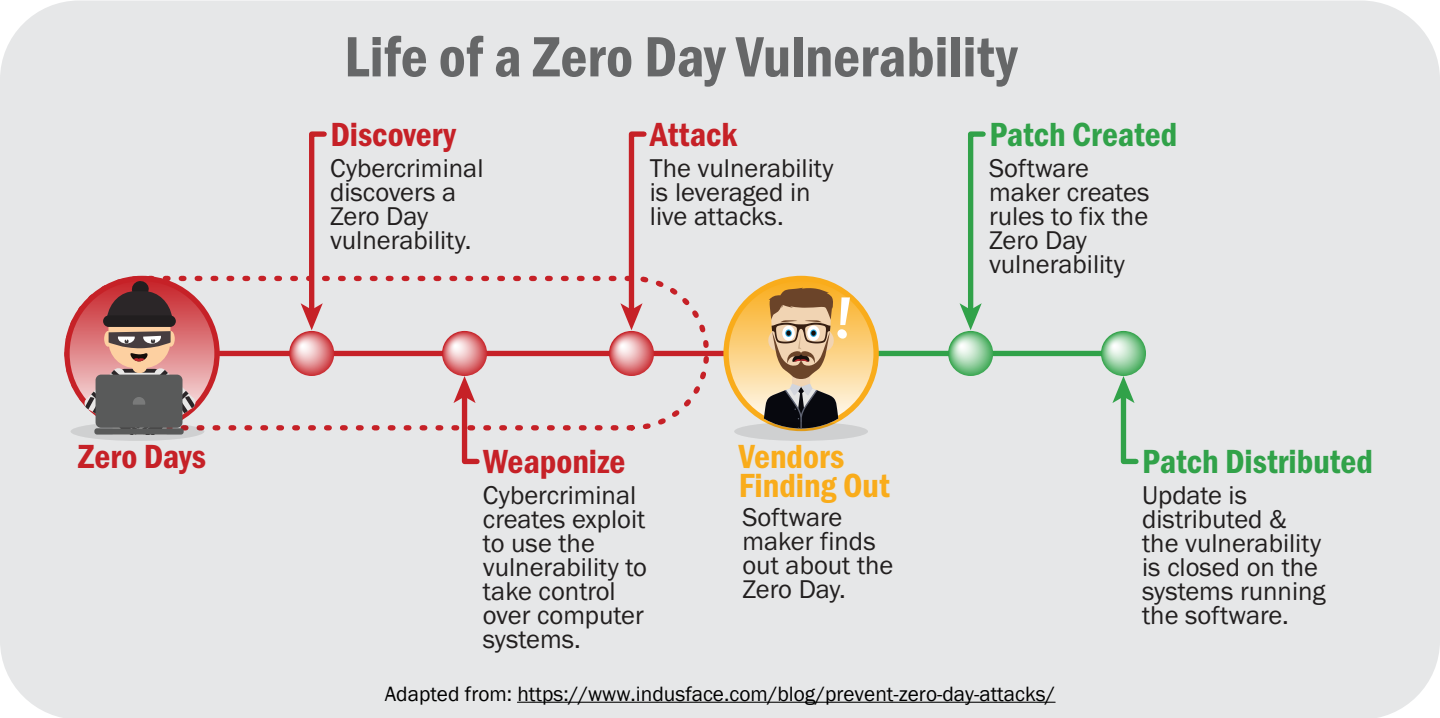
Authors: Jason Ingalls, Cyrus Robinson, Janine Byas

INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452

In 2021, a series of cyberattacks using unknown vulnerabilities, called Zero-Days or 0-Days (pronounced “oh day”), changed the risk management calculations of operating Information Technology (IT) for businesses across all industries, government agencies, and critical infrastructure organizations in the United States. These Zero-Day vulnerabilities were unknown to exist by anyone except the criminals and nation-state-sponsored threat actors that used them to gain access, steal data, and in some instances, cripple operations. 0-Day vulnerabilities are especially challenging to defend against because they are inordinately difficult to detect in production IT systems, and until the vendor responsible for fixing the security flaw identifies it and produces a patch, the vulnerable systems must be guarded against exploitation and compromise. Enter the rising trend in cybercrime - attackers going through your vendors’ unknown vulnerabilities to get to your business’ critical data, perform espionage, target opportunities to grind operations to a halt, and ransom access for payment.

This rampant use of 0-days is a sea change from years past, when organizations who possessed knowledge of these hidden vulnerabilities were loath to use them except in very strategic ways. For example, the Electronic Freedom Foundation’s exposé on Chinese espionage against the Uyghur diaspora identifies previously unknown vulnerabilities in the Apple iOS operating system that were used against dissidents to spy on them. This report was an early indicator (2019) of changing policy by nation-state threat actors to more frequent use of 0-days.[1] It is the nature of cyber offense and defense that tools and weapons proliferate rapidly.[2] Therefore, the current use of 0-Days by criminal gangs is a natural progression from the known nation-state-sponsored use of them only two years ago.



Adapted from: https://www.indusface.com/blog/prevent-zero-day-attacks/

1 “Watering Holes and Million Dollar Dissidents: the Changing Economics of Digital Surveillance”, retrieved in July 2021 from https://www.eff.org/deeplinks/2019/09/watering-holes-and-million-dollar-dissidents-changing-economics-digital

2 “Understanding the Proliferation of Cyber Capabilities”, retrieved in July 2021 from https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities

An analysis of three different, recently devastating attacks leveraging 0-days indicates that the bar for effective cybersecurity risk management must be raised across the board. Here, we review the SolarWinds, ProxyLogon, and Kaseya attacks - each possible because the attackers had knowledge of an otherwise unknown vulnerability in trusted software.

SolarWinds

The SolarWinds hack was initially discovered in late 2020. However, exploitation of the vulnerability continued into 2021 and was of such magnitude that many users of the software (over 100 individual organizations, including 9 Federal agencies) had some indication of unauthorized access and data theft.[3] This attack leveraged a supply chain compromise that allowed suspected Russian government-sponsored hackers to gain access to any IT network that the SolarWinds application servers were installed in. Because SolarWinds was a trusted, administrative application with privileged access to data, servers, and networks, the attackers gained unfettered access to all assets that SolarWinds managed. Many organizations had to rebuild their IT environments from scratch, per guidance from the Cybersecurity and Infrastructure Security Agency (CISA).[4]

ProxyLogon

In the days following the March 2, 2021 disclosure by Microsoft of a series of 0-day vulnerabilities that had been leveraged by the HAFNIUM threat actor, over 30,000 organizations were attacked.[5] This resulted in unauthorized access and theft of email accounts, webshell malware installations, and even ransomware and cryptojacking attacks.[6] The HAFNIUM criminals demonstrated awareness of the threat advisory and rapidly escalated their exploitation of the Exchange vulnerabilities, dubbed "ProxyLogon" vulnerabilities, to create the largest impact possible once disclosed. In this instance, it is important to note that many organizations completely ignored or were unaware that a patch was available. The FBI carried out an extraordinary effort to leverage the same vulnerabilities to remove web shell backdoors from ProxyLogon-compromised Exchange Servers.[7] This highlights a Catch 22 of disclosing 0-days, even with a patch available; publication of a vulnerability can create massive impact as attackers rush to reap reward before their opportunity is lost, as organizations also rush to apply the fix.

Kaseya

Kaseya, a Remote Monitoring and Management (RMM) software tool used by hundreds of IT Managed Service Providers (MSPs), was leveraged by the REvil threat actor group to deploy ransomware and encrypt the computers of up to 1,500 companies on July 2, 2021.[8] This brazen use of several 0-day vulnerabilities in the Kaseya VSA application is another example of suspected Russian nationals targeting trusted software in order to deliver malware at-scale and ransom victim environments. These attackers, as with the SolarWinds incident, relied on privileged access and risky, vendor-recommended configurations. As a result, many downstream victims were affected due to the widespread use of the tool. The capabilities that RMM tools provide IT companies also allow for essentially carte blanche access to any environment it is installed in. MSPs do not always have the expertise necessary to configure these tools the most securely.

3 "White House now says 100 Companies hit by SolarWinds hack, but more may be impacted", retrieved in July 2021 from https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies

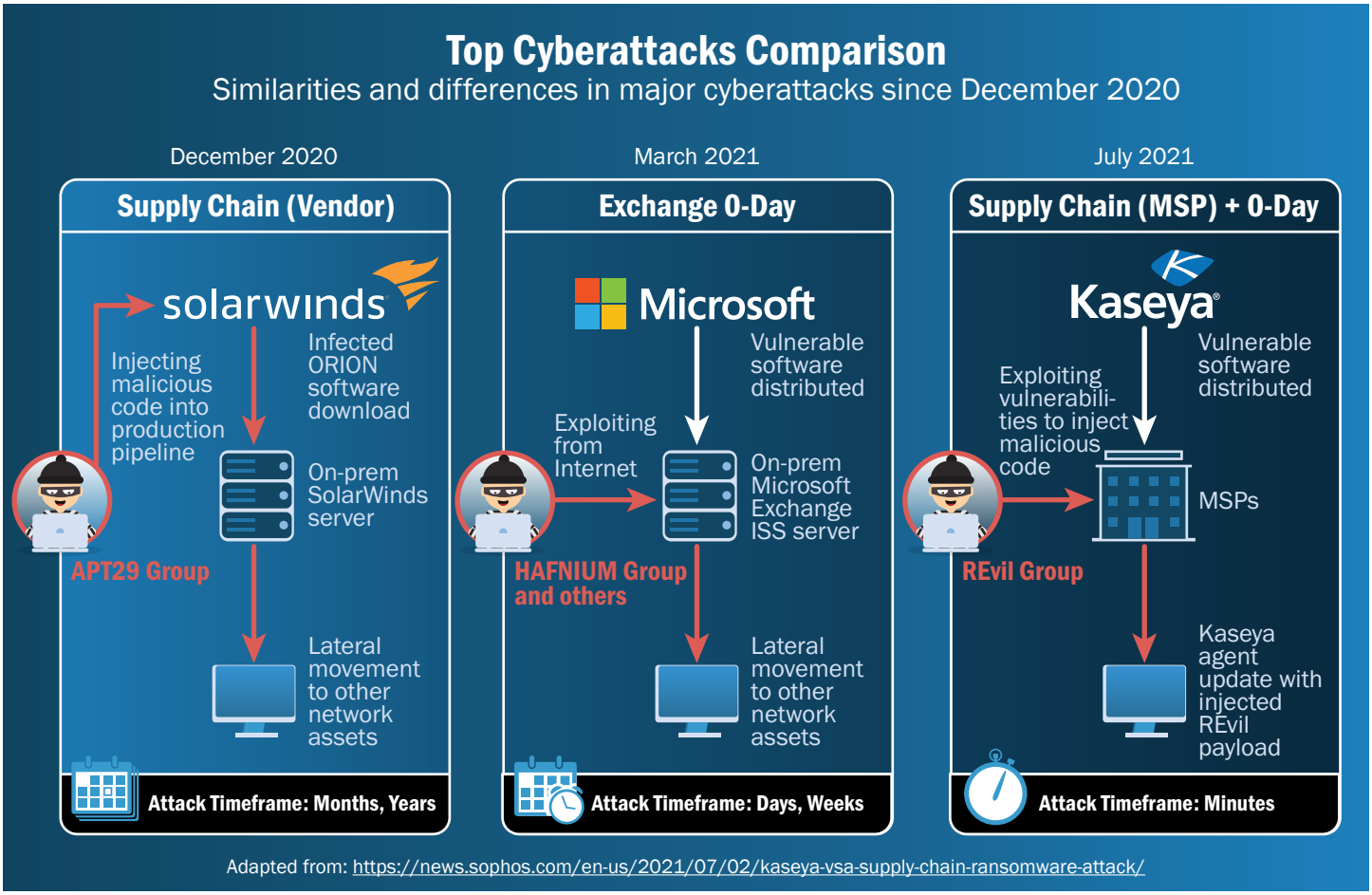
4 "Emergency Directive 21-01", retrieved in July 2021 from https://cyber.dhs.gov/ed/21-01/

5 "HAFNIUM targeting Exchange Servers with 0-day exploits", retrieved in July 2021 from https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

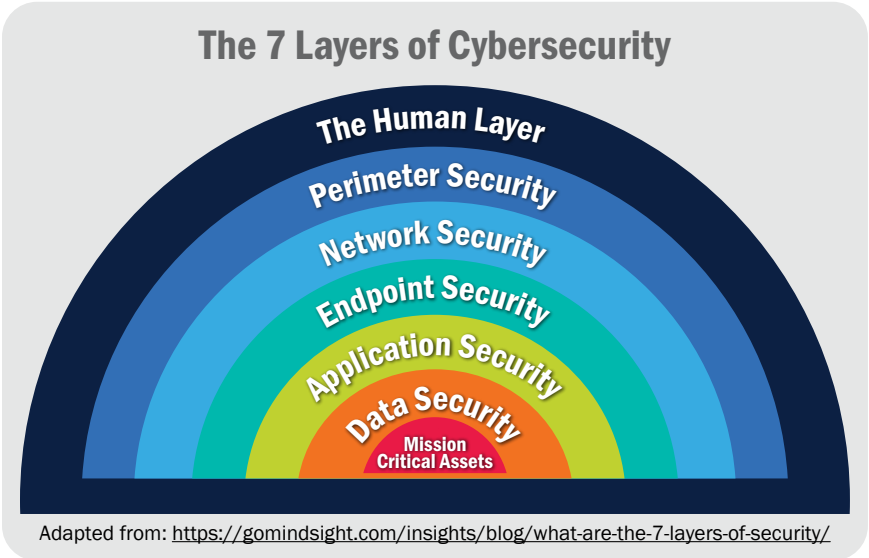
6 "Analyzing attacks taking advantage of the Exchange Server vulnerabilities", retrieved in July 2021 from https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/

7 "FBI blasts away web shells on US servers in wake of Exchange vulnerabilities", retrieved in July 2021 from https://www.zdnet.com/article/fbi-blasts-away-web-shells-on-us-servers-in-wake-of-exchange-vulnerabilities/

8 "Kaseya ransomware attack: 1,500 companies affected, company confirms", retrieved in July 2021 from https://www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-company-confirms/



The special risk 0-days present to IT environments requires careful consideration of how to manage it. Historically, there've not been many available risk management controls marketed as point solutions for 0-days, because of the various ways that 0-day vulnerabilities present themselves. For example, an Endpoint Protection solution that might scan for attempts to perform buffer overruns in application code and prevent such an execution might be helpless against a different technique that leverages a configuration change to an application that allows attackers to escalate their user privileges and pivot to sensitive data. Where possible, it's important to adopt a defense-in-depth strategy to detect and prevent unauthorized activity that may originate from exploitations of such vulnerabilities.



This requires a profound shift in the way organizations think about protecting data and operations. It's time to come to grips with some critical realities:

1 **There is no silver bullet for keeping cybercriminals out.** For those relying solely on antivirus for protection, it's only a matter of time before you experience a breach. Antivirus is critical, but it should be seen as one part of a comprehensive, defense-in-depth strategy for a cybersecurity program. At a minimum, organizations need a layered defense strategy implementing security at all levels: Human, Perimeter, Network, Endpoint, Application, and Data Security.[9] Think of Swiss cheese slices. Each IT tool, employees, and a host of organizational factors introduce weaknesses into your environment. These Swiss cheese holes (vulnerabilities) are apparent and can be easy for hackers to navigate. However, if you stack different slices of Swiss cheese up, although every

slice has its own holes, each layer provides coverage for the layers that precede and succeed it, creating a single, more impenetrable fortification.

2 **Unmanaged security tools are not enough to secure organizations.** The allure of Artificial Intelligence and the marketing promises vendors may make regarding security software and hardware may convince organizations to believe that deploying a specific tool or stack of tools is enough to manage the risk that organizations face. However, no matter how advanced and capable the toolset is, a "set it and forget it" cybersecurity solution is a foolhardy one that promotes a false sense of security that can actually result in increased risk. Unmanaged security tools generate an exhaustive amount of data. Without human-in-the-loop management, tools break and fail to protect. Security tools require careful monitoring, fine-tuning, and meaningful context by a skillfully trained human being.. It is vital to rely on experts who understand how to configure, monitor, and respond to the output of these tools.

3 **There is an imperative for security expertise at the executive level.** Cybersecurity is a governance responsibility that belongs to leadership positions; however, individuals in these roles are often under-equipped to make decisions about security. For midsize to enterprise-class organizations, investing and trusting in a Chief Information Security Officer, Chief Information Officer, or Chief Technology Officer is required to appropriately segregate duties and effectively establish a cybersecurity strategy with controls, policies, and procedures aligned to organizational priorities. The world will have 3.5 million unfilled cybersecurity jobs by the end of 2021 with an average growth rate of 31% for Information Security Analysts.[10] Employing trained security analysts, Information Security Managers, and/or partnering with a trusted cybersecurity provider (different from an MSP) are also serious investments to consider.

4 **Your IT budget is not the same as an investment in the security of your organization.** Paying lip service to regulatory compliance will not protect organizations in today's threat landscape. Traditional antivirus is no match for modern attackers who use more sophisticated techniques. Implementing control standards (NIST, CIS, ISO) and defense-in-depth requires both executive endorsement and monetary investment. Organizations face a choice: Make the necessary investments to build resilient IT systems now, or pay the price in the form of required security control implementation, ransom, litigation, business impact, and fines after a breach has occurred.[11]

The conversation around cybersecurity amongst executives and IT professionals must evolve. Cybersecurity encompasses a large ecosystem that requires its own mastery of the discipline, separate from IT administration. Threat actors, whether nation-state sponsored or independent criminal gangs, are exploiting gaps that result from immature and underfunded security postures - and they are growing in sophistication, targeting more critical infrastructure and services at a break-neck pace and critical scale. It is time to see investing smartly and effectively in cybersecurity, and bringing expertise around it to the decision-making table, as an existential imperative.

9 "What Are The 7 Layers Of Security? A Cybersecurity Report", retrieved in July 2021 from https://gomindsight.com/insights/blog/what-are-the-7-layers-of-security/

10 Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021", retrieved July 2021 from https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/ and, "U.S. Bureau of Labor Statistics: Occupational Outlook Handbook - Information Security Analyst", retrieved July 2021 from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

11 "Pay It Now or Pay It Later - Cybersecurity Always Collects its Dues", retrieved in July 2021 from https://www.linkedin.com/pulse/pay-me-now-later-cybersecurity-always-collects-its-due-rich/

INGALLS INFORMATION SECURITY
Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452