Trustwave®

2021 Network Security Report

2020 was an unusual year. The COVID-19 pandemic created enormous challenges for businesses worldwide and cybersecurity challenges were prominent among them. As employees transitioned to working from home, this created new vulnerabilities in systems designed for a centralized, in-office workforce. There was a subsequent spike in cybercriminal activity, as bad actors hastened to take advantage of the situation, along with an increase in malware attacks and other network security threats.

Our internal and external network vulnerability scanning systems inspect servers for insecure configurations that could increase the risk of a successful attack. This research is based on scans of millions of servers worldwide, and their findings provide insight into which network vulnerabilities occur most frequently. In this Network Security Roundup, we'll take a look at some of the biggest network security trends of the past year. We'll also discuss the risks that arose when organizations took a band-aid approach to securing remote work.

The remote access trend: VPN Vulnerabilities

Early in the year, the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an alert strongly urging organizations to update Virtual Private Networks (VPNs). While this alert specifically mentioned a vulnerability that was made public in 2019, there were numerous reports of active exploitation of multiple VPN and gateway platforms throughout 2020. After the abrupt shift to work-from-home in March, malicious actors were targeting unpatched VPN vulnerabilities more frequently. Some of the most serious vulnerabilities that we detected on our customer networks include:

- Pulse Secure Connect Arbitrary File-Reading Vulnerability (CVE-2019-11510)
- Citrix Application Delivery Controller (ADC) and Citrix Gateway Directory Traversal Vulnerability (CVE-2019-19781)
- F5 BIG-IP Network Balancer Remote Code Execution Vulnerability (CVE-2020-5902)

The Pulse Secure Connect arbitrary file-reading vulnerability was patched in April 2019, but 8 months after the patch was released, attackers behind the REvil ransomware gained access to the currency exchange Travelex's network through this flaw. The attackers demanded $6 million to restore the company's data.

In early 2020, SANS published an update reporting that there had been an increase in scanning activity for versions of the Citrix Application Delivery Controller and Citrix Gateway vulnerable to CVE-2019-19781. This vulnerability could give an attacker employing a crafted Web request direct access to local networks behind Internet gateways without the need for a local account or authentication. The vulnerability was trivial to exploit. Although Citrix released an advisory about it on December 16, 2019, patches were not made available for another month despite the bug's severity and its wide impact.

F5 disclosed a critical vulnerability in the BIG-IP Traffic Management User Interface (TMUI) in June of 2020. This vulnerability allowed remote code execution and attempts to exploit it were observed in the wild within days. CISA observed broad scanning to detect presence of this vulnerability across federal departments and agencies. The vulnerability was particularly notorious because it could enable the compromise of any application behind the interface.

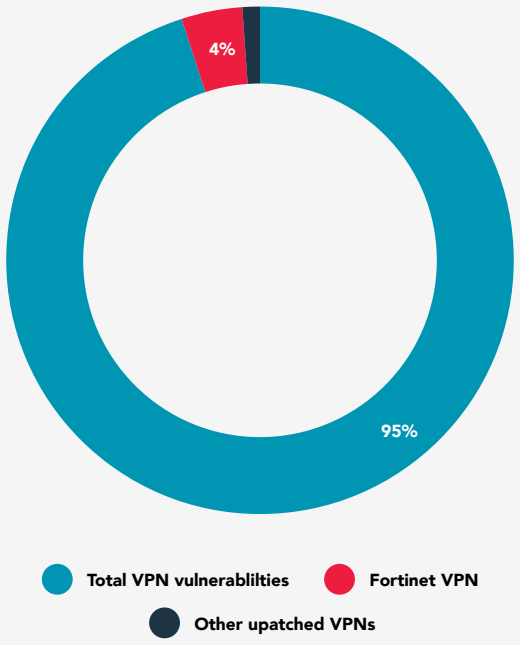

Figure 1: VPN Vulnerabilities detected on scans

As Figure 1 shows, at the end of the year, 5% of VPN solutions remained unpatched and were still vulnerable to several of the most prominent VPN CVEs, including those highlighted above. Some had yet to be patched for a two-year-old Fortinet FortiOS SSL VPN path traversal vulnerability (CVE-2018-13379). Exploitation of this flaw could allow an attacker to access contents of the 'sslvpn_websession' session file to steal login credentials.

The remote access trend: Videoconferencing Platform Vulnerabilities

As offices closed and remote workers began using videoconferencing platforms at unprecedented scale, there was a sharp spike in cybersecurity attacks targeting Zoom, Microsoft Teams, Cisco WebEx and similar platforms. At the same time that cross-platform video conferencing service Zoom became a household name, it also became a popular target, attracting widespread scrutiny of its security practices. There were reports that Zoom was leaking data to Facebook through Facebook's software development kit (SDK) on Apple platforms running iOS, as well as buzz about Zoom calls being vulnerable to eavesdropping because Zoom did not actually enforce end-to-end encryption in video conferences despite claims that it did.

One malicious practice that's received a great deal of attention is "Zoom Bombing," in which videoconferences are hijacked by disruptive trolls. The FBI issued a warning about teleconference hijacking after multiple reports of such incidents. Another Zoom security issue that's come to light involves a UNC Path Injection issue within the Zoom Windows Client. Zoom initially allowed Windows networking UNC paths to be converted into clickable links within chat messages. This enabled attackers to steal the Windows credentials of users who clicked on the link.

In addition, were reports of a wormable, zero-click vulnerability in Jabber, which was subsequently patched by Cisco. This flaw, identified as CVE-2020-26085, has a CVSS score of 9.9 out of 10, making it critical in severity. It can allow attackers to execute arbitrary code remotely through specially crafted Extensible Messaging and Presence Protocol (XMPP) messages. The attack would proceed by initiating the transfer of a malicious .exe file and forcing the victim to accept it using cross-site scripting (XSS), which would then be employed to run the code on the victim's machine. Cisco WebEx had additional, less severe vulnerabilities as well. One of these – CVE-2020-3419 – allows a ghost user to join a session. This ghost user would then have access to the shared screens, the teleconference's audio content, and the chat, possibly allowing sensitive information to be leaked.

The team at Spiderlabs discovered and reported on further vulnerabilities in Cisco Webex as well as some in Microsoft Teams.

More Windows Vulnerabilities

Microsoft Windows had its fair share of vulnerabilities in 2020. The year started off with Microsoft disclosing a critical vulnerability dubbed **"Curveball"** or **"ChainofFools."** Discovered by the NSA, this certificate validation vulnerability affects Windows 10 and Windows Server 2016/2019 along with applications that rely on Windows for trust functionality. The vulnerability makes it possible for malicious actors to spoof certificates that rely on Windows CryptoAPI for signature validation. It can enable attackers to bypass trusted network connections and deliver executable code while masquerading as trusted entities. After the exploit was made public, malware with spoofed Microsoft certificates was uploaded to VirusTotal, a leading threat intelligence library.

In March 2020, a critical vulnerability in Windows 10 was mistakenly disclosed by Microsoft before a fix had been published. Codenamed SMBGhost or **EternalDarkness**, CVE-2020-0796 is a fully wormable vulnerability so dangerous that it merited the rarest CVSSv3 rating – a perfect 10. The vulnerability, in Microsoft's Server Message Block version 3.1.1, could enable arbitrary code execution if a malicious data packet were sent to the server. A Shodan search conducted in early January 2021 indicated that over 100K machines were susceptible to attacks exploiting this flaw (Figure 2).

Another wormable vulnerability with a perfect CVSSv3 score of 10.0, codenamed SIGRed, was made public in July of 2020. CVE-2020-1350 is a remote code execution vulnerability affecting Microsoft Windows DNS server versions 2003 to 2019. Attackers who exploit it can gain Domain Administrator rights for the server in question, potentially giving them direct access to an organization's corporate infrastructure.

Figure 2: Shodan Results for SMBGhost CVE-2020-0796 in Jan 2021

Around August 2020, another privilege escalation vulnerability surfaced. This one, dubbed ZeroLogon and identified as CVE-2020-1472, exploits the Netlogon Remote Protocol (MS-NRPC). This is a zero-day elevation-of-privilege vulnerability that makes it possible for an attacker to spoof a domain controller account and then use it to steal domain credentials, take over the domain, and compromise all associated Active Directory identity services. Exploits were soon released, and by November Microsoft researchers were also able to identify that, in a few cases, attackers had leveraged the ZeroLogon vulnerability to access resources within organizations that were still running unpatched domain controllers, even though a patch had been available for a month.

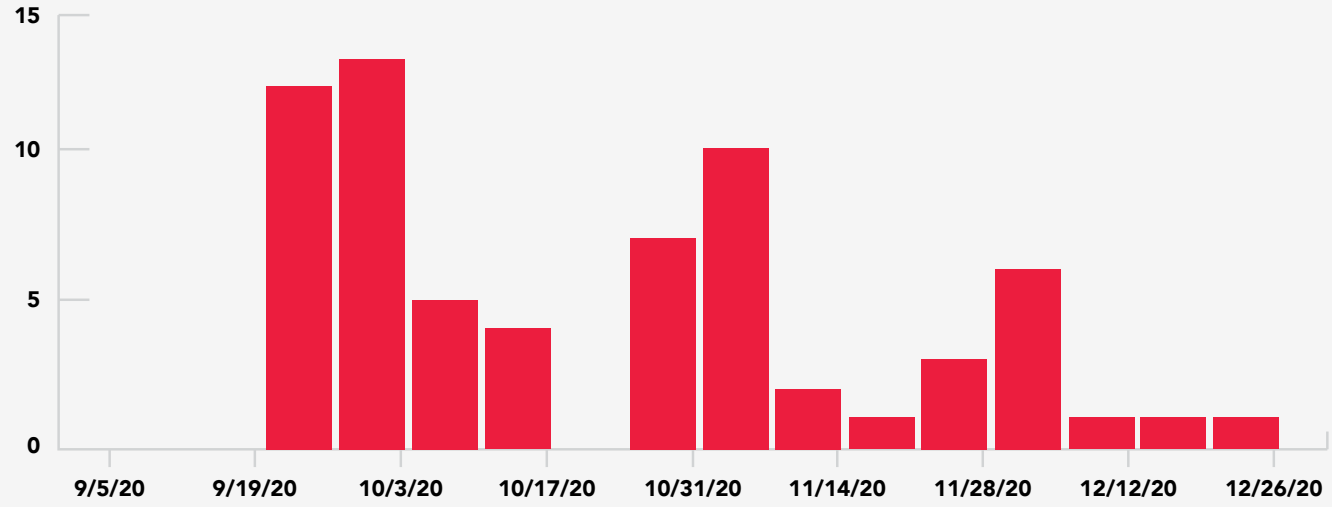

Figure 3: Remotely detecting Zerologon through internal scanner on the same LAN

Our scanners have the unique ability to detect this vulnerability without authentication if the scanner is on the same local area network (LAN) as the vulnerable host. As Figure 3 shows, we queried a sample of scan data from customer networks and observed a number of machines vulnerable to this critical flaw.

Cyberpandemic: Solarwinds Supply Chain Hack

The year ended with the most severe hack of 2020 and what was probably the most crippling and devastating breach of the decade. On December 8, FireEye disclosed that hackers had stolen red team tools and internal threat intelligence data from the firm. Days later, on December 13, reports surfaced that there had been a suspected nation-state-level cyberattack targeting SolarWinds Orion, a network monitoring tool. Various corporations and U.S. government agencies including the Departments of Commerce, Homeland Security, and Energy were among the victims of this supply chain attack. The hackers planted a malicious backdoor into code distributed in a routine software update. The malware, dubbed SUNBURST, was disseminated to approximately 18,000 SolarWinds customers. It granted the attackers the ability to modify, steal and destroy data on the customers' networks. FireEye also released countermeasures intended to reduce the effectiveness of the stolen red team tools, along with a list of CVEs that the tools were designed to exploit.

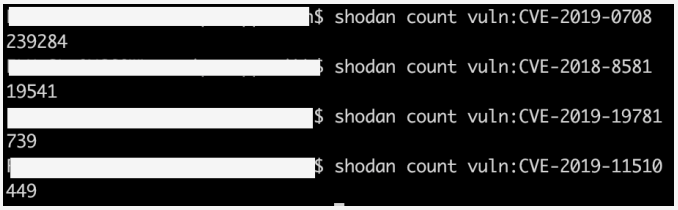

Figure 4: Vulnerable machines found on Shodan.io as of Jan 2021

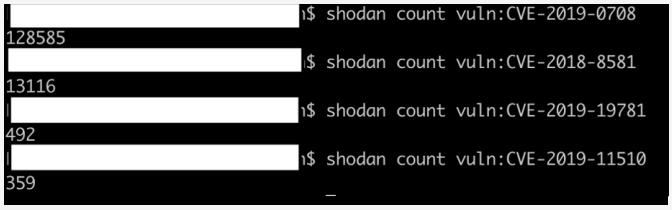

Figure 5: Vulnerable machines found on Shodan.io as of Jun 2021

As shown in Figure 4 and Figure 5, there are a number of vulnerable targets that currently appear on Shodan.io for some of these CVEs. According to a Shodan report executed on January 8, 2021 for CVE-2019-0708 (Bluekeep) over 200K machines remain vulnerable. As of June 8, 2021 (Figure 5) that number has reduced to ~128K If the query is limited to machines running Windows Remote Desktop Protocol (RDP), there are still nearly 30,000 results. The 16 CVEs in the list include several that are described in the article above, including CVE-2019-11510, CVE-2019-19781 and CVE-2020-1472.

In October 2020, the U.S. National Security Agency (NSA) published a report detailing the 25 vulnerabilities being exploited most frequently by Chinese state-sponsored threat groups. Multiple CVEs from the FireEye list also appeared in the report. The most striking aspects of the SolarWinds supply chain attack were that the attackers were highly trained in operational security and used methods to evade detection by security tools or forensic examination. However, there wasn't a single zero-day on the list of vulnerabilities exploited in the SolarWinds attack. In fact, some of the vulnerabilities exploited were more than two years old, with patches that had long been available. It is clear that unpatched vulnerabilities continue to attract cybercriminals' attention. It remains extremely critical for organizations to prioritize proactive patching, especially of vulnerabilities in remote access tools, external web services and components accessible directly over the public internet.

Recommendations: Vulnerability Remediation and Proactive Patch Management

We recommend that organizations adopt a multi-faceted approach for remediation and patching.

- **Asset Management:** Having an up-to-date inventory of assets on the networks provides real time visibility which is important in protecting against the ever-changing threat landscape.
- **Risk Assessment – Vulnerability Prioritization:** Performing a risk assessment of vulnerabilities is critical since time and resources are often limited. A risk assessment aligned with business objectives helps prioritizing vulnerabilities based on the environment. Systems that contain sensitive data, critical business functions, systems directly exposed to the Internet are likely to be higher risk and should be prioritized first.
- **Vulnerability Remediation and Patch Management:** Next comes vulnerability remediation – organizations should define a scan frequency since that helps with streamlining the remediation process. This ties in with proactive patch management. There cannot be enough emphasis on the importance of deploying critical security updates as soon as possible. On average, exploits to critical vulnerabilities surface anywhere from a day to a month and if patching efforts are not timely, it greatly increases the risk of exploitation.
- **Continuous Cycle:** And finally, vulnerability management must be a continuous process that should be reviewed adapted on an ongoing basis in order to effectively mitigate the latest threats.

Looking Ahead: 2021 and beyond

The working-from-home trend will almost certainly continue into this year, so attackers will likely continue targeting remote access services like RDP and VPNs. It's also likely that attacks will grow more sophisticated. The SolarWinds supply chain attack is representative of the more complex attacks and nation-state activity that we're likely to see in the coming years. With more and more companies moving to the cloud, cloud hosting services will be impacted more frequently as well.

Trustwave is a leading cybersecurity and managed security services provider focused on threat detection and response. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries.
For more information about Trustwave, visit *www.trustwave.com.*

Trustwave®