LESSONS LEARNED

Bernard Montel *looks back at 2021: a year of turbulence in cyber risk – from lockdown to Log4Shell*

Last year ended as abruptly as it started: January saw a surprise lockdown and return to remote working, bringing added risks in cybersecurity. Businesses readopted with fervour the cloud systems that had seen them through 2020, while still working to comprehend and address the risks this move had introduced. And, after a year of patching problems, 105 zero-day vulnerabilities and a surge in ransomware attacks, Christmas provided no respite as Log4Shell shook the industry.

Over the year, over 40-billion records were exposed by attacks and from that over 1.8-billion files, documents or emails fell victim to bad actors. Attackers throughout 2021 did not limit themselves to digital destruction, and several crossed the chasm from the digital world to the physical. These infrastructure attacks rattled the UK public's faith in fuel and food supply chains, mostly using fairly ordinary means to wreak extraordinary damage.

The global threat and vulnerability landscapes were analysed in a recent, retrospective report by Tenable, aiming to guide business responses and navigation of the modern attack surface. The report calls to attention key evolutions in the attack surface that can put businesses at risk, including supply chains, misconfigurations of systems like Active Directory and interconnection across operational technology (OT) devices, among many others. As businesses across the world revisit their security approach in the wake of last year's constant threat of a breach or attack, multitasking will be key and a forward-thinking, holistic approach to their software supply chain could save them from further exploitation from bad actors.

The brief return to pandemic business operations offered bad actors another opportunity to exploit remote workers, thanks to the adoption of cloud solutions and software leading to an increasingly complex ecosystem. These changes, showing more and more permanence even as the COVID-19 threat subsides, are transforming how we define "the perimeter" when it comes to network boundaries. But exciting as this evolution in digital transformation may be, allowing for a better work/life balance and more diverse, international employee teams, an increase in this hybrid set-up inevitably led to a riskier software supply chain; an element effectively exploited by attackers in 2021. Think back to ransomware attacks and breaches like SolarWinds and Kaseya, which made use of the age-old tactic of daisy chaining vulnerabilities in order to expedite breaches; these are core examples of the insecurity in software supply chains that businesses must rectify.

As mentioned previously, January 2021 saw the industry deal with the aftermath of the SolarWinds attack as nation-state actors, Nobelium, compromised an update protocol for the SolarWinds Orion platform to distribute malware to public and private organisations. Then in the summer of 2021, managed services providers were hit by a similar supply chain incident as remote monitoring and management software from Kaseya was exploited by a large scale ransomware campaign. The campaign, for which a Ukrainian citizen with links to the REvil ransomware group was eventually charged, also leveraged multiple zero-days in its attempt to disrupt networks. Importantly, these attacks groups – like Nobelium, have continued to target supply chains, compromising targets via resellers and service providers which puts connected organisations on the radar of these attackers. Threat actors have exploited new zero days in products from both SolarWinds and Kaseya since their supply chain incidents were disclosed.

Ransomware operators inflicted the most damage in 2021 to the healthcare sector, accounting for 24.7 percent of all recorded breaches

Ransomware attacks increased in both volume and sophistication in 2021, with the Kaseya incident being only one of many such breaches. Last year, ransomware groups leveraged zero-days and legacy vulnerabilities alike to target sensitive sectors like healthcare, education and the physical supply chain. Double extortion became the linchpin of most ransomware groups and a key factor in the record breaking profits for ransomware operators.

Healthcare was the sector upon which ransomware operators inflicted the most damage in 2021, accounting for 24.7 percent of all recorded breaches. Hospitals, doctors' offices, billing companies, dentists, therapists and more were impacted by a variety of threats. One of the most notable healthcare breaches linked to ransomware was conducted by the Conti ransomware group, which crippled Ireland's Health Service Executive in May 2021. As a result of the breach, all IT systems had to be shut down for weeks and services like blood test results and patient diagnostics were severely affected.

In addition to healthcare, the education sector was also heavily impacted by ransomware. An astounding 52 percent of breaches were linked to ransomware attacks, leading to severe ramifications for students, educators and parents alike. Many were impacted through cancelled classes and inaccessible learning platforms, and educators must recognise the uphill battle they face securing and protecting devices in the age of hybrid education. It is not clear whether ransomware operators specifically targeted education organisations, or if these results have grown from opportunistic attacks targeting easy-to-find devices, but no matter the motivation, educators should remain conscious of the trend's consequences.

THE CONTI RANSOMWARE GROUP CRIPPLED IRELAND'S HEALTH SERVICE IN MAY 2021

In the wake of major attacks on critical infrastructure in 2021, concerns surrounding the security of OT environments have never been higher. Colonial Pipeline, the largest pipeline in the United States, suffered an attack linked to the Darkside ransomware group in May it impacted its pipeline operations. Consumers and businesses alike were affected with drivers facing long lines to purchase fuel, while gas prices climbed to worrying heights. Colonial's CEO later testified before the United States Senate that the attack was due to a legacy VPN account, which lacked multifactor authentication and had not been decommissioned.

Additional risk to critical infrastructure is introduced when security controls and code audits are not in place. A common thread in such risks is the use of insecure protocols such as file transfer protocol and telnet; though they served an important purpose in the past, they can add unnecessary risk running sometimes without a business's knowledge.

The use and re-use of software libraries and real-time operating systems (RTOS) across multiple devices and manufacturers is widespread, making patch management and asset enumeration for these issues tough problems to solve for many organisations. In exceptional cases, mitigations and network segmentation may be the only feasible option for devices that are no longer manufactured or supported by vendors.

Ransomware also took advantage of misconfigurations in Active Directory (AD) in 2021, as threat groups of all kinds exploited this to elevate privilege and traverse networks to further infiltrate target organisations. In fact, when it came to AD, ransomware was responsible for more than half of the breaches analysed; though a small percentage of these were as a result of misconfigured or unsecured cloud databases. Openly accessible cloud databases and overly permissive AD configurations give attackers access to

an organisation's most sensitive information providing valuable fodder for ransoms.

As previously mentioned, 2021 closed with security teams alerted to a critical vulnerability in Log4J dubbed Log4Shell – found in a wide range of services, applications and devices across all industries and geographies. The reason this vulnerability was deemed to be so severe, compared with others, is because it's so ubiquitous. It really does touch so many different types of software and services. It's not as simple as looking for a particular piece of software and checking the version that's being run. Because of the way modern applications and services are written, there can be a number of dependencies that could contain this library, and organisations may not even realise it.

FINANCIALLY MOTIVATED RANSOMWARE GROUPS WANT MINIMAL EFFORT WITH MAXIMUM PROFIT

Threat actors have moved quickly to take advantage of this vulnerability. To date there have been at least 11 publicised attacks that have used Log4Shell. In the UK, the NHS warned that unknown hackers were targeting VMware Horizon deployments with Log4Shell exploits. While unclear if this was connected, ransomware gang NightSky were identified as using Log4Shell to gain access to VMWare Horizon. Meanwhile APT34, another well-known ransomware group, was confirmed as exploiting Log4Shell to distribute a new modular PowerShell toolkit.

Ransomware groups are financially motivated, but want minimal effort with maximum profit. They look for low-hanging fruit such as known but unpatched vulnerabilities, gaps in legacy technologies like VPNs, combined with AD misconfigurations to impact organisations.

But there is hope when it comes to addressing this risk. Organisations can take steps to protect themselves via a holistic security approach. Businesses must examine devices on their network, assessing which controls are already in place to prevent unneeded network access to devices. It is also important to think like employees, recognising the importance that OT devices have in our everyday lives as organisations revisit their security. Hybrid and remote working is not going away – many companies are adopting permanent hybrid models and some are doing away with office spaces altogether – so organisations must redefine their perimeter by examining how cloud and OT assets are secured and integrated within their organisation.

When looking back and learning from 2021, organisations must understand the need to redefine while continuing to protect the evolving perimeter, adopting cloud infrastructure with care and employing security protocols that work across diversified networks. Such care and attention should also be applied to the use of AD addressing misconfigurations. Legacy systems should also be identified and either removed or ringfenced to avoid unidentified attack pathways to exist.

The string of supply chain-related breaches and attacks in 2021 only highlight the need to build on protection for the software supply chain. In fact, 61 percent of security leaders reported that their organisation was exposed to increased risk related to its expanding supply chain in 2021; and though this awareness could make for more action to protect growing corporate networks, for many it was already too late. When assessing events like SolarWinds, Kaseya and finally Log4Shell, businesses must recognise that now more than ever, getting ahead of cyber espionage and ransomware attacks is paramount to security ●

Bernard Montel is EMEA Technical Director and Security Strategist at Tenable. With over 20 years in the security industry, Bernard's expertise includes cryptography, Identity & Access Management, and SOC domains. He has published numerous articles and is regularly invited to speak about cybersecurity – providing insight into current cybersecurity threats, cyber risk management and cyber exposure.

Colonial's CEO revealed the attack was due to a legacy VPN account lacking multifactor authentication that had not been decommissioned