LESSONS FROM LOG4SHELL

In early December, alarm bells were being sounded. A vulnerability enabling remote code execution had been discovered in a widely used, open-source software library designed for logging security and performance data in Java. The vulnerability in Apache's Log4j (since designated as "Log4Shell") seemed to open the door to potentially devastating cyberattacks across all sectors. Jen Easterley, head of CISA, would describe Log4Shell in an early interview with US broadcaster CNBC as "the most serious vulnerability" of her decades long career in cybersecurity. WIRED magazine declared it "excruciatingly clear that Log4Shell [would] continue to wreak havoc across the internet for years to come".

And yet, here we are at the end of January 2022. Exploitation of Log4Shell has been consequential, no doubt. It appears to have been deployed by the Chinese-speaking threat group HAFNIUM and the Iran-sponsored PHOSPHORUS, not to mention being used by criminal hackers for crypto mining. However, exploitation has been nowhere near as ubiquitous, successful, or devastating as the initial predictions led us to fear. The storm has been tempestuous, but the sky has yet to fall in.

Why is this? There are two probable contributing factors. The first is that Log4Shell can only be exploited indirectly via the application's embedding the library code and so can be surprisingly difficult to take advantage of. To act on a vulnerability of this kind, threat actors must first scan for vulnerabilities across the whole stack, application-by-application. They must then determine on a case-by-case basis what the custom malicious code string required for exploitation will need to be. The second reason is that the community response to Log4Shell has been swift, robust, and well-coordinated. Enterprises were quick to conduct targeted, risk-based patching for high-priority applications connected to the internet, update security controls, and step-up monitoring for potential exploitations. Security agencies in both the public and private sphere swiftly raised the alarm and went on to provide a substantial support network to the community.

Some might conclude on this basis that the initial fears about Log4Shell were overblown. But it's not at all clear that this is so. In fact, it's difficult to calibrate just how concerned we should have been about this vulnerability. It may be that the window for exploitation of Log4Shell on major applications is closing. But we shouldn't lose sight of just how sobering the discovery of this vulnerability is. For one thing, it's sure to be with us for some time. Legacy applications which are not updated or whose manufacturers are no longer solvent will be vulnerable to Log4Shell indefinitely. For another, it's highly unlikely that this sort of issue will be unique to Log4j. There are countless other widely used, ostensibly benign open-source and commercial software libraries which could be ripe for weaponization in a similar vein.

This highlights just how dependent we can become on multi-purpose code packages for which we lack a good level of visibility. This points to a need for a much greater understanding of our dependencies on code and for the containment and segmentation of application sets. Log4Shell may not have been a reckoning, but it should at the very least be considered a stark warning and a salutary reminder of the growing importance of supply chain security

BEYOND blue

NEWSLETTER

February 2022

In early 2022, the world continues to reel from the emergence of one of the most important cybersecurity events in recent memory.

In this first edition of the Beyond Blue newsletter, we consider some of the takeaways from the emergence of Log4Shell. We also shine a spotlight on key themes set to dominate the security landscape in 2022, outline key priorities for ensuring compliance with Operational Resilience regulation, consider the limits of the EU's draft AI regulation, and reflect on the value of practice to cyber incident response.

David Ferbrache, OBE
Managing Director

SECURITY SPOTLIGHT FOR 2022

Key themes to watch in the coming year

CONTINUOUS ASSET MANAGEMENT

One of the critical lessons to be learned from the Log4J fallout is the importance of technical teams knowing as much as possible about IT assets. The more comprehensive and real-time this knowledge of the complete technology stack and the underlying dependencies between its components, the more secure enterprise networks will be. We expect to see enterprises placing a heavier emphasis on IT teams continuously tracking, monitoring, and governing IT assets in the name of security hygiene in 2022.

SUPPLY CHAIN MANAGEMENT

As awareness grows of the sheer number of entry points for ransomware attacks, there is an ever-greater focus on mapping and protecting the attack surface. This poses significant challenges for enterprises with dependencies on complex and extensively distributed supply chains. We expect to see a greater emphasis in 2022 on enterprises charting their supply chain dependencies and working with all their supply chain partners in a collaborative and transparent way to improve their overall security posture and reduce risk.

ZERO-TRUST SECURITY

As enterprise organisations continue their mass migration to the cloud and simultaneously find a substantial portion of their workforce operating remotely, network perimeters are becoming ever harder to define. This is fast making traditional firewall focused security models obsolete For this reason, we expect 2022 to see a substantial acceleration in organisations moving towards what Google has dubbed a zero-trust security model in which authentication and authorisation procedures serve as the principal means of defence

APPLICATION AND API SECURITY

The 2021 LinkedIn data breach brought home for many the importance of application security. This colossal "data scrape" – which affected some 700 million users – was caused by vulnerabilities in LinkedIn's API. With more and more applications being built in-house, there is a greater imperative for developers to add security features customised to each application's functionality which would be left unaddressed by the standard controls. We predict 2022 will see an increased emphasis on these concerns.

SECURITY ANALYTICS PLATFORMS

Incident Response and Vulnerability management will be a central concern in 2022, with a particular focus on the ability of organisations to isolate critical incidents and vulnerabilities. Central to these efforts will be the growing number of organisations embracing security analytics tools such as Extended Detection and Response (XDR) (for continuous visibility and threat detection) and Security Orchestration, Automation and Response (SOAR) (for security management, integration, and automation). When used closely together, these tools will provide vital security advantages.

OPERATIONAL RESILIENCE COUNTDOWN

For many people in the Operational Resilience world, Christmas will already feel like a distant memory. With the March 2022 compliance deadline drawing ever closer, many teams will have turned their attention to navigating the governance journey that comes with regulatory responses.

Many operational teams will have lived and breathed Operational Resilience for the last 12 months, helping to scope Important Business Services, collect data to justify Impact Tolerances and modelled impacts of Scenario Testing. What some teams may be starting to realise as they summarise their hard work in the Self-Assessment plan their journey up through their organisations' various committees, is that, for some of the stakeholders you will encounter along the way to that elusive Board approval, this may be the first time their engaging in the Operational Resilience world (despite your team's best efforts).

Teams should not underestimate the time and effort required to educate and get these key stakeholders comfortable with what they are being asked to approve. Building in contingency time for challenge, additional one-to-one sessions, and worst-case stand offs with these stakeholders as they understand the ramifications of the suggested Impact Tolerances and Scenario Testing results on their business, teams and budget is advised, to mitigate the risk of missing that March deadline.

62 DAYS TO GO

CHRIS BAARS ON PRACTICE MAKING PERMANENT

I'm a big sports fan. So, when the first lockdown arrived and we were all faced with a glut of possible distractions, I was drawn to *The Last Dance*, a critically-acclaimed ESPN documentary series about the renowned basketball team the Chicago Bulls and their dominance of the NBA in the 1990s. I was struck by many things about this series. It's a great story; one about passion, commitment, teamwork, and peerless talent. But, above all else, I was fascinated by the bravura brilliance of Michael Jordan. Those familiar with Jordan's remarkable legacy will understand why. However, it wasn't his wealth of accomplishments that grabbed my attention; it was his relentless drive to succeed. Jordan's remarkable achievements were due in no small part to the fact that he practiced harder than anyone else out on the court.

The idea that practice is vital to success in sports is age-old. Professional sports teams wouldn't even consider turning up to play competitive games without having first put in the hours to ensure they were on fighting form. So, why is it that practicing isn't seen as anywhere near as vital in the world of cyber incident response? After all, the consequences of "losing the game" are far higher.

(cont.) A successful cyber incident exercising program can be achieved in a multitude of ways. But however you proceed, the key is to ensure your incident responders and managers get the opportunity to practice skills they are unlikely to use on a regular basis, but which could prove decisive in a critical security incident. It's one thing to test your team's responses, quite another to facilitate their practicing them.

A wide variety of scenarios can be designed to assist. Crucially, by putting the responders and managers outside their comfort zone you are creating this all-important practice platform for improvement. Practice through exercising allows us the benefit of a safe environment and the ability to adjust the severity, difficulty and cadence of the scenario to reflect the current skill level of those taking part. By practicing in this way, skills can be improved and honed to the point that they become permanent assets ready to use at any time.

In the case of Michael Jordan practice near enough made him perfect. In the world of cyber security, we don't need to aim that high. But wouldn't we all settle for practice making permanent?

CHRIS BAARS

PRINICPAL CONSULTANT

Chris is a passionate and experienced Cyber Security, Incident Management and Exercising professional. Prior to joining Beyond Blue, he created A.P Moller Maersk's Cyber Security Operational Readiness and Exercising Department in the wake of the 2017 NotPetya attack.

FUTURE FOCUS

CAN THE EU SHAPE GLOBAL AI REGULATION?

The publication of the EU's draft regulation on AI in April of 2021 was an important milestone. It marked the first attempt by a major liberal democratic world power to set out market-friendly standards for the sale and use of high and limited risk AI systems. It is also the first such framework published in alignment with the G20's 2019 AI principles. This will come as a relief to those who fear that the exponential proliferation of unregulated AI applications in emerging digital technologies risks a repeat of recent failures on the part of global regulators to get ahead of fast-moving technology trends with proportionate legal protections. It will also foster hopes amongst other liberal democratic states that the EU can use this regulatory framework to help shape global norms for AI in line with their shared values.

The significance of the EU single market to global trade near enough guarantees these regulations will play some role in shaping the field of AI the coming decade. But there are limitations on this.

For one thing, following the publication of the National Security Commission's report on Artificial Intelligence and NIST's AI risk management concept paper, the US Department of Commerce has recently signalled that it too will soon launch its own regulatory framework. As well as being more influential than any EU counterpart (given the relative size of the US economy), US regulation will likely lean more heavily into protections against anti-competitive market practices than into the rights and welfare-based concerns at the heart of the EU proposals.

There will still likely remain a high degree of convergence between the US and EU proposals. But the emphasis is likely to differ. Secondly, there is the fact that most EU economies will continue to be heavily dependent on trade with China. This will place a significant strain on the EU regulatory framework. China is not only fast-approaching being the world leader in AI development and production, but they are also hard at work developing their own, less transparent approach to AI regulation in alignment with the G20 principles. Whatever shape this takes, it is unlikely to align closely with the EU's focus on the "fundamental rights of natural persons".

Ultimately, the impact of the EU's AI regulation will depend on how member states respond to these challenges.