Picture credit: Adobestock

BREAKING THE CHAIN

Phil Robinson *investigates why it is that supply chain attacks are still on the rise*

The MOVEit attack by the Clop ransomware gang proves just how devastating software supply chain attacks can be. The dependency on shared software can see a single attack compromise a multitude of customers, with Emsisoft finding 1,841 organisations have disclosed that they have been breached (according to Wired). And it's a vulnerability that seems to keep accruing victims, much like we saw with Log4j which continues to be a long-tail vulnerability. Research from Sonatype indicates that almost two years after a patch was issued for Log4j, the software continues to be unpatched, with 23 percent of downloads in September 2023 still exhibiting the vulnerability.

These attacks follow in the wake of the infamous SolarWinds attack in March 2020 that saw attackers deploy malicious code via the Orion IT performance monitoring and management software used by more than 30,000 organisations of which 18,000 were breached. The update installed a backdoor, providing the attackers with privileged access to highly sensitive data on the customer's network but also access to their partners and customers as well, enabling the attack to expand and move on to other networks. Infecting US government departments and companies including Microsoft, Intel, Cisco and Deloitte as well as cyber security vendors such as FireEye, the attack was seen as a catalyst for reform and focused efforts on improving supply chain security.

Gartner predicts that in 2025, 45 percent of organisations worldwide will have experienced attacks on their software supply chains

So why are we still seeing more attacks as evidenced by the MOVEit and Log4j examples? Gartner predicts that in 2025, 45 percent of organisations worldwide will have experienced attacks on their software supply chains, up three-fold from 2021, suggesting that the problem, if anything, is getting worse. This is in part due to the renewed efforts of nation state actors and organised criminal gangs who can see for themselves how effectively these attacks are and their ability to scale, but they are also difficult to stop due to the way code is now developed and shared.

Software supply chain attacks typically exploit a vulnerability in the code or use malware to gain unauthorised access during the development phase. With respect to the latter, there are numerous techniques that threat actors can use to compromise the developers themselves or target open source code libraries or public software repositories. For example, attacks can engineer package/repository managers or proxies to retrieve a malicious package.

Techniques include dependency confusion attacks, whereby the package is given the same name as one in an internal repository in a public repository, typosquatting which sees just a couple of characters changed in that name and brandjacking, which is the impersonation of a well-known branded package. As these attacks can take place after a code review and given that the code is often shared, issues can be easily propagated. Other times it's the software development kit that is compromised or even the controls that are designed to check the integrity of the software, such as code signing or hashing.

The tactics, techniques and procedures (TTPs) used are varied, but have been documented in a number of frameworks. In the Cyber Defense Report: Software Supply Chain Attacks, Sean Cordey provides a useful overview of these ranging from the MITRE ATT&CK framework to the Common Attack Pattern Enumeration and Classification (CAPEC) framework to ENISA's Supplier-Customer Supply Chain Framework. The latest framework to try and tackle the issue is the Open Software Supply Chain Attack Reference (OSC&R), which was published over GitHub in March 2023. It takes the TTP approach of the MITRE ATT&CK framework, but specifically focuses on the supply chain and can be used in concert with a supply chain risk management programme.

These frameworks all document the ways in which attackers attempt to infiltrate the supply chain together with the end goal. But why are supply chains so susceptible? It's now rare for an organisation to build and control its systems inhouse, so inevitably services are bought or outsourced. In fact, one of the most vulnerable aspects of this partner supply chain is the Managed Service Provider (MSP). Provided with privileged access to customer networks, MSPs have been seen as the weak link in the chain when it comes to protecting critical national infrastructure, which is why the government is taking steps to bring them within scope of the National Information Security (NIS) directive.

For most organisations downstream of code development, the only option is to use automated solutions to look for vulnerabilities and to attempt to vet their third-party suppliers. Assessments should be carried out as part of the procurement processing prior to onboarding and regularly throughout the span of the contract. But alarmingly just over one in ten businesses review the risks posed by their immediate suppliers (13 percent), and the proportion for the wider supply chain is virtually half that (8 percent), according to the Cyber security breaches survey 2023.

Similarly, the UK Government's Cyber Security Longitudinal Survey Wave 2 found fewer than three in ten businesses (26 percent) have formally addressed the potential cyber security risks associated with their suppliers or partner organisations. Very large organisations were the most proactive (42 percent) in assessing supplier-related cyber risk followed by large organisations (34 percent) while those in the mid-tier trailed at 25 percent. These organisations used a variety of approaches, ranging from stipulations within the contract to supplier questionnaires, via external accreditations such as ISO27001, by adding supplier risks to the risk register or logging data flows with suppliers on data protection registers, according to the Cyber Breaches Survey.

IT'S CLEAR ENTERPRISES ARE NOT BEING NEARLY AS PROACTIVE AS THEY REALLY SHOULD BE

When it comes to regularly assessing suppliers, the numbers dwindle still further. The Longitudinal survey found only 22 percent of all businesses had done so within the last 12 months. Only just over half of businesses (57 percent) say they have requested cyber security information from their supply chains during that time frame. This is partly due to the fact that it can be difficult to request this information in the first place, let alone again, which means assessments post-procurement are much less likely to happen. Managing risk is of course an ongoing requirement for any organisation and should be routinely assessed, but without regular monitoring of suppliers and third parties organisations are effectively ignoring it. According to Gartner more than 80 percent of legal and compliance leaders identified third-party risks after initial onboarding and due diligence.

The Cyber Breaches Survey also found the main barriers to businesses undertaking a formal review of suppliers and/or the supply chain were lack of budget (32 percent), not being able to get the information from suppliers (31 percent) and not knowing what checks to carry out (25 percent). As a result, almost a third (29 percent) said such challenges had prevented them from understanding the potential cyber risks in their supply chain. This indicates supply chain security is problematic because of a lack of understanding of the risk, lack of visibility and poor understanding of what the organisation needs to ask its suppliers to do.

Awareness is growing, however, in part due to the seismic supply chain attacks mentioned at the start of this article but also due in no small part to the efforts of the NCSC, which has been issuing guidance on assessing supply chain risk. In October 2023, it

sought to offer guidance for all regardless of where they are on their supply chain risk journey, from an introduction to the topic to best practices in supply chain management to free e-learning modules on the subject.

The NCSC advocates a five-step plan for addressing supply chain security, beginning with considerations with respect to the organisation and how it evaluates risk and who should be responsible for overseeing supply chain risk before outlining key components when devising the approach and how this should be applied to new suppliers. The approach should be incorporated into both new and existing supplier contracts and regular evaluations carried out to ensure it remains relevant.

THE MAIN BARRIERS TO BUSINESSES UNDERTAKING A REVIEW OF SUPPLIERS IS LACK OF BUDGET

It's worth pointing out that the approach is seen as a two-way street, allowing the business to monitor suppliers for their security performance and to support them to rectify any perceived increase in risk. This ensures that the risk can be addressed before it is exploited or becomes an issue, which is crucial because it can and does happen and can leave both parties not knowing what to do. The Longitudinal Survey found that 12 percent of businesses stopped working with a supplier following an incident. Finally, the evaluation stage is also seen as an opportunity to collaborate with suppliers and to raise issues of concern.

As we've seen, some seek to solve the problem of supplier risk simply by ensuring they meet the requirements of ISO27001. ISO 27001:2022 ensures the business manages information security risk by creating an information security management system and there are provisions in the standard that therefore ensure the organisation's data assets are effectively protected if they are accessible to suppliers. Annex A.5.19 mandates the development of a security policy for supplier relationships, A.5.20 security within supplier agreements and A.5.21 specific ICT suppliers.

Such an approach is helpful for businesses dealing with suppliers that may be larger than they are and are unlikely to bow to individual policies but that's not to mean the business can't implement controls and monitor the relationship, which is wise as it can be used to evidence good practice for managing suppliers and complying with standards.

Going forward, it's heartening to hear of new developments in the space to try to tackle threats such as the OSC&R framework and to see the emergence of sector-specific guidance that aims to help businesses develop their own supply chain risk assessment programmes. But it's also clear from the low numbers evidenced in the latest government surveys that enterprises are not being nearly as proactive as they should be.

Software supply chain attacks do originate higher up the pipeline and checks and balances need to be put in place to ensure the code shared during development does not contain vulnerabilities. But it's also the responsibility of those providing these software services to do their due diligence and also the end customer (ie the business) to have processes in place to hold their suppliers to account. The worry is that without more commitment to supply chain security, and an impetus to put in place a supply chain risk management programme as standard, the attacks we've seen so far will continue and that could have dire consequences for those businesses, governments and economies affected ●

Phil Robinson – Principal Security Consultant at Prism Infosec – has over 25 years' experience in the infosecurity industry and is an (ISC)² CISSP, ISACA CISA, Cyber Scheme Team Leader (CSTL), and a PCI Qualified Security Assessor (QSA).

Fewer than three in ten businesses (26 percent) have formally addressed the potential cyber security risks associated with their suppliers or partner organisations

Picture credit: Adobestock