Insight Space

cyber insights programme

nccgroup

How to prevent, detect and respond to a supply chain attack

Technical Viewpoint

Rick Tahesh
Associate Director,
NCC Group

Global. Transformative. Resilient.

How to prevent, detect and respond to a supply chain attack

Supply chains at large organisations often include thousands of enterprises, partners, service providers, contractors and other suppliers. Managing risk across these complex networks is difficult, so there is a huge dependency on trust across global supply chains. However, recent cyber attacks have targeted organisations through their third parties, so relying on trust to provide strong business assurance without strong measures and controls is simply an illusion.

Rick Tahesh
Associate Director, NCC Group

Threat actors can exploit supply chains in various ways, including:

1. **Open-source software**
   Attackers introduce code into builds that get installed or leveraged by organisations' systems.
2. **Third-party software**
   Attackers target third-party systems and compromise them by introducing malware or trojan-ware.
3. **Software development tools**
   Attackers compromise legitimate websites through website builders and other methods.
4. **Service provider data stores**
   Attackers target outsourcing partners and service providers to exploit organisations' data and assets.
5. **Stolen certificates**
   Attackers introduce malicious code under the guise of trusted organisations' certificates.
6. **Firmware attack**
   Attackers target access to firmware and introduce malware to enable them to gain access to organisations' data and systems.

The following example illustrates a supply chain attack using open-source software

A banking organisation partners with an open-source software developer's party.

Threat actors receive intelligence of the banking organisation partnership.

The banking organisation uses the open-source software in one of its applications.

Threat actors compromise one of the developer's GitHub accounts through a phishing attack.

Using the compromised GitHub account, the threat actors insert malicious code into the open-source software library with a trojan horse.

The software library is packaged, along with the trojan horse, for release.

The banking organisation installs the latest release of the open-source software and with it the trojan horse.

Threat actors now have full access to the banking application.

The nature and complexity of supply chains and the tactics, techniques and procedures that threat actors use to exploit them require a broad set of governance and technical cyber security controls to mitigate against such attacks. In this paper, we highlight some of the key requirements that CISOs need to consider to prevent, detect and respond to supply chain threats and attacks.

Prevention

Building resilience against supply chain attacks requires a multi-layered prevention strategy that includes a number of key components.

Help you better understand your supply chain risks by gaining clarity on the services and products that your suppliers provide you with

Awareness

Firstly, it's crucial that you know which entities make up your supply chain pool by conducting a comprehensive discovery exercise involving your procurement, finance, legal, BCM, IT, cyber and other teams from across the business. Then, you can better understand your supply chain risks by gaining clarity on the services and products that your suppliers provide you with, as well as the access they have to your environment and data assets. Finally, you can use this intel to prioritise assurance for those services and products based on their value, criticality and priority to your organisation and the risk attached to the suppliers that support them.

1 in 4

cyber security decision makers do not rigorously audit the results of their suppliers' risk assessments

Assurance

To maintain ongoing assurance around your supply chain, develop a supply chain risk management framework that is supported by supplier assurance policy, processes and controls. This could include roles and responsibilities for key business functions that interact with third parties, and working with your procurement team to integrate their supplier onboarding process with cyber security, BCM, technology, risk and compliance processes.

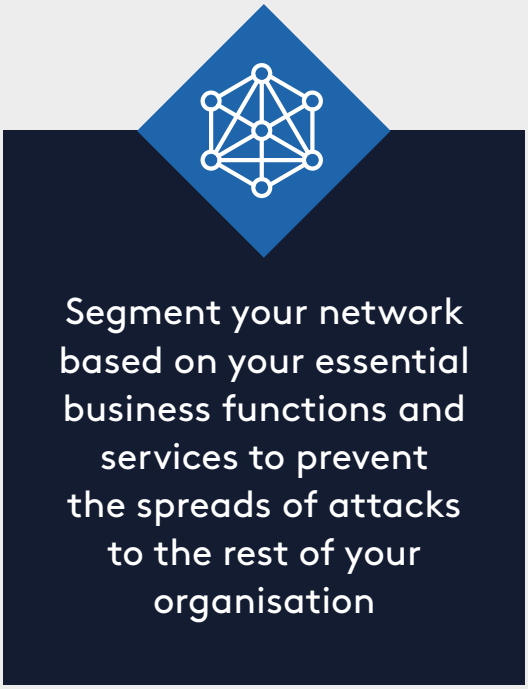
According to our global survey of 1,400 cyber security decision makers, one in four do not rigorously audit the results of their suppliers' risk assessments. This should be a non-negotiable, so ensure that the right to audit and appropriate security reporting measures are included in any RFIs, RFPs and contracts, alongside security requirements and clauses.

Finally, you should assess your vendors and suppliers regularly with a focus on high-risk providers. Adopt different approaches to assessments that commensurate with the risk profile of suppliers, such as tailored security control questionnaires supported by evidence gathering, pen testing, input from vulnerability scanning tooling, certification and other assurance reporting measures.

Isolation and segmentation

Threat actors can infiltrate a supplier before moving through the chain until they reach their target. Excessive privileges and permissions make supply chain attacks much easier, so adopt least privilege access controls, always assigning least privilege to your suppliers, software processes and employees. You should also segment your network based on your essential business functions and services to prevent the spreads of attacks to the rest of your organisation.

Implementing security-by-design by ensuring secure and safe software and application development practices at the supplier end as well as your own should also fix known software vulnerabilities and support the operation of secure applications.



Detection

Timely detection of supply chain attacks rely on comprehensive coverage of suppliers' connections and activities across your networks, systems and applications. Consider monitoring through a Security Operations Centre (SOC), which can detect and respond to incidents in real time. You should also introduce automated security controls to break off suppliers' connections in case of access violation or attempted breach. For ongoing detection, test your software applications and network using pen testing and vulnerability scanning regularly, and frequently apply integrity checks on new, updated or patched software to detect any changes to software code that could indicate a malicious attack.

Respond

Responses to incidents and breaches in your supply chain should be built into your organisation's incident response plan. This plan should ensure that security incident reporting clauses are part of your suppliers' legal and contractual agreement with your business. Similarly, ensure you have an agreed media and stakeholders' communication plan with your suppliers, to effectively manage public and stakeholders' relations following any major security breaches.

Finally, develop appropriate incident response play and run books, based on up-to-date real-world scenarios, to handle and respond to incidents from within the supply chain. Regularly test those plans and scenarios with your key suppliers and partners to keep everyone updated and well-practiced for incidents.

Conclusion

Our research shows that supply chain attacks have increased by 51% in the past six months. Despite this, many of the organisations that we spoke to planned to invest in new third-party software, hardware and SaaS security products in 2022, which could increase the third-party threat vector for malicious actors. All of this makes it crucial for technical decision makers to act now to prevent, detect and respond to this growing threat.

Top five actions to prevent, detect and respond to supply chain attacks

1. Be aware of your critical assets, the suppliers that support them and the risks to the business if they were compromised.
2. Maintain ongoing supplier assurance with policy, processes and controls including security requirements in RFI, RFP and contracts and ongoing security assessments.
3. Adopt least privilege access controls for third parties, segment your network and implement security-by-design.
4. Implement a Security Operations Centre (SOC) to continually monitor, detect and respond to indicators of supply chain attacks.
5. Integrate supplier management into your incident response plan, including real-world scenarios and communication plans following an incident.

Global. Transformative. Resilient.

To discuss how we can help you address legacy security issues to build your organisation's cyber resilience, speak to our team today.

www.nccgroup.com

About NCC Group

NCC Group exists to make the world safer and more secure. As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With circa 3,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss how we can help you address legacy security issues to build your organisation's cyber resilience, speak to our team today.

www.nccgroup.com

UNI104675