SOPHOS
Cybersecurity evolved.

Minimizing the Risk of Supply Chain Attacks: Best Practice Guidelines

In December 2020, news of a cyberattack on IT monitoring company SolarWinds pushed supply chain cybersecurity attacks into the spotlight, but they are far from a new phenomenon. In fact, worryingly, nearly one in 10 ransomware victims (9%) stated that the attack found its way in via a trusted third-party supplier, according to Sophos' 2020 survey of 5,000 IT managers across 26 countries[1].

But what is a supply chain attack exactly, and how do they work? More importantly: what can you do to protect your organization from the impact of a supply chain attack?

These questions and more are answered in this paper.

[1] *The State of Ransomware 2020 – Sophos, 2020*

A Sophos Whitepaper. April 2021

What is a supply chain attack?

Organizations are often reliant on some form of third-party supplier to manage all or part of a particular business function, such as your IT infrastructure. While enabling third-party suppliers to connect to your network does have business benefits (freeing up in-house resources, for example), it inherently introduces security risk – namely vulnerability to supply chain attacks.

In a supply chain attack, rather than infiltrating you directly, attackers instead exploit the access that trusted third-party suppliers already have to your systems to gain a foothold in your environment. Once they're in, they can conduct all sorts of malicious activity.

Having just a single supplier connected to your network introduces the risk of a supply chain attack. On average, however, small and mid-sized organizations report having at least three suppliers who can connect to their systems[2]. Securing these connected suppliers creates substantial challenges and increased workload for IT teams. To compound the challenge, supply chain attacks are notoriously difficult to detect, let alone defend against, as they can come from any part of your supply chain.

Types of third-party suppliers

Professional services and IT service providers are two of the most common third-party suppliers that can connect to an organization's network.

Professional services

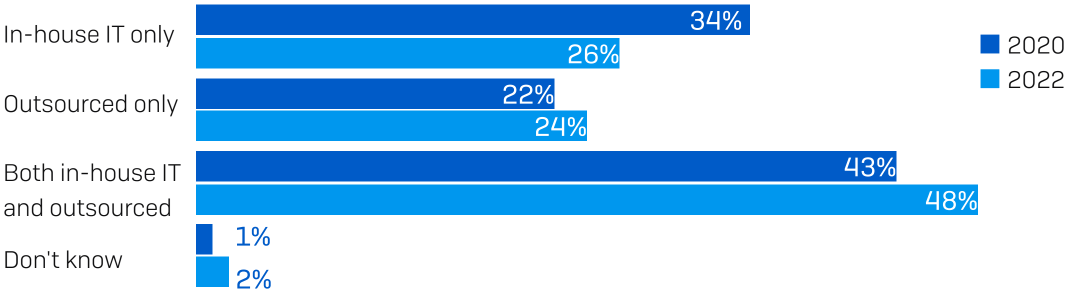
Professional services are often employed by organizations to independently manage business functions (or parts of them) when they don't have the specialized skills and knowledge required internally. Take for example an accountancy firm that needs to have access to sensitive financial data (through software) to provide the client with the analysis and insights they have been employed to deliver. As you can imagine, a successful cyberattack on such an organization could be devastating for its portfolio of clients.

IT service providers

IT service providers are external organizations entrusted with the running of a company's IT infrastructure and/or IT security. Often known as managed service providers (MSPs) or managed security service providers (MSSPs), they are frequently targeted in supply chain attacks.

They're particularly attractive targets for attacks because they hold the keys to many different customer organizations. With the number of organizations outsourcing their IT security set to rise to 72% by 2022[3], the security posture of these third parties is of paramount importance to your own.

How IT security is delivered: Now and 2022



2,3 Cybersecurity: The Human Challenge – Sophos, 2020

Types of supply chain attacks

While supply chain attacks differ in terms of how they are delivered, the principles and endgame for attackers are often the same – to infiltrate a trusted third-party supplier and abuse the trusted access to implant malware, steal intellectual property, or spy on internal communications.

Phishing attacks

One of the most common attack vectors utilized by supply chain attackers are phishing emails. Attackers target trusted third parties with phishing emails to compromise and gain access to their networks, and then use them as a springboard to infiltrate their clients' systems.

Compromised software update

In more sophisticated supply chain attacks, hackers infiltrate the infrastructure of a software company or distributor and insert malicious code into software update packages. The third party then distributes these updates to their clients, unknowingly infecting them in the process. As you can imagine, the consequences can be devastating, particularly if the organization has a large portfolio of customers. The December 2020 SolarWinds attack is a perfect example of this type of attack.

Supply chain attack case study: SolarWinds

In late 2020, it was discovered that the supply chain of IT management firm, SolarWinds, had been compromised. This discovery created headlines across the globe, thrusting the vulnerability of supply chain security into the spotlight. It is thought to have impacted over 18,000 of their customers.

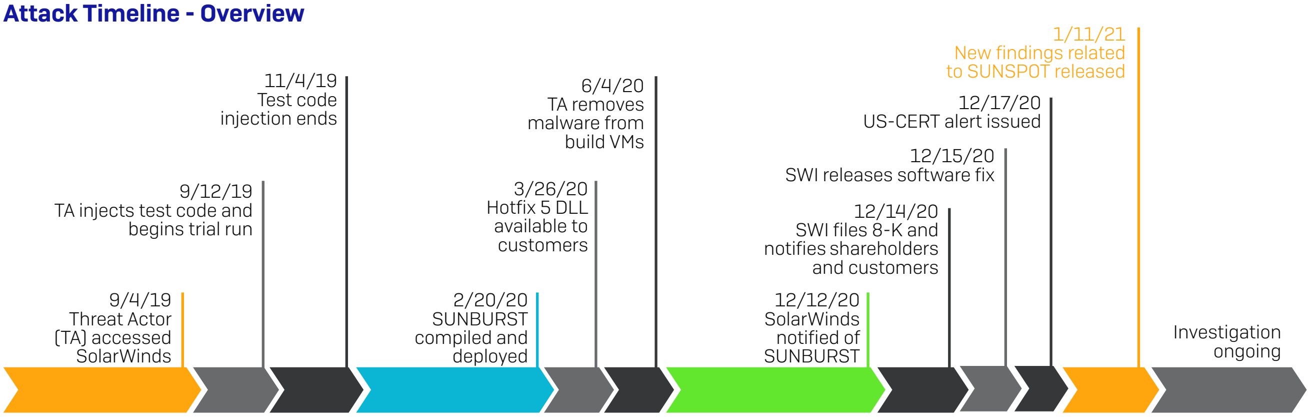
It is important to note that as of the date of publication, April 2021, the investigation into the SolarWinds attack is still ongoing and may change.

How did the attackers pull it off?

In a nutshell, hackers managed to insert malicious code into SolarWinds' infrastructure monitoring and management platform Orion. This malicious code was then unwittingly sent out to customers by way of a standard software updates. It is reported that in the region of 18,000 customers (including many Fortune 500 companies and U.S. government agencies) installed the updates, leaving them vulnerable.

Worryingly, indications of foul play were suspected by SolarWinds as far back at September 2019 as seen in the timeline below. This suggests both that the move was calculated and that the threat actors exercised extreme caution, seeking to trip as few alarms as possible in their intrusion. You can read Sophos' in-depth analysis of how the Sunburst malware variant evaded defenses here.

Attack Timeline - Overview


9/4/19 Threat Actor (TA) accessed SolarWinds
9/12/19 TA injects test code and begins trial run
11/4/19 Test code injection ends
2/20/20 SUNBURST compiled and deployed
3/26/20 Hotfix 5 DLL available to customers
6/4/20 TA removes malware from build VMs
12/12/20 SolarWinds notified of SUNBURST
12/14/20 SWI files 8-K and notifies shareholders and customers
12/15/20 SWI releases software fix
12/17/20 US-CERT alert issued
1/11/21 New findings related to SUNSPOT released
Investigation ongoing

All events, dates, and times approximate and subjects to change, pending completed investigation

SolarWinds - https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

What has been the impact of the attack?

The success of the attack, dubbed Sunburst, gave the actors wide-ranging access to corporate and governmental information systems. It has already resulted in as-yet uncalculated volumes of data theft and concerns the attackers have used the foothold to insert other backdoors into enterprise networks yet to be discovered.

More importantly, the global scale of the attack has highlighted just how unprepared many organizations are when it comes to defending against supply chain attacks.

Poison packages

A less common type of supply chain attack, though one we expect to see more frequently in the future, is what we have coined 'poison packages'. As use of the cloud, Docker, and agile development methodologies grows, so does the use of off-the-shelf components to shorten the development lifecycle. Malicious actors have begun to booby trap some commonly used containers, libraries, and other resources, hoping to get bundled into your end-product.

Guidelines for defending against supply chain attacks

Given the complexity and nature of supply chain attacks, technology alone can't prevent them. Instead, these best practice guidelines are intended to enable you to minimize the risk associated with a supply chain attack.

1. Shift from a reactive to a proactive approach to cybersecurity

SolarWinds was the wake-up call for many organizations across the globe. Once an attack becomes obvious, it is often too late: by the time a criminal drops a payload, they may have already stolen critical data and, often, have had access to your network for days. You need to adopt a new mindset – assume you are always compromised and hunt for the threats before it is too late. There are technologies and services that can support this approach which we'll expand on later in the paper.

2. Monitor for early signs of compromise

During investigations conducted by the Sophos Managed Threat Response (MTR) team, two things stand out as early indicators of compromise: one is the use of credentials for remote access and administrative purposes during off hours; the other is the abuse of system administration tools to conduct surveillance and steal data from the network.

The use of legitimate accounts and your own tools to gain and retain persistence is often referred to as Living Off the Land (LOL). Detecting these behaviors requires vigilance and skill; however, they stand out clearly to a trained security operations analyst, alerting you to the attack before the bulk of the damage has been done. You should either invest in the technology and training needed to monitor for these indicators in-house or engage a managed detection and response (MDR) service provider to monitor on your behalf.

3. Take an audit of your supply chain

It may sound obvious, but taking some time to map out a list of all the organizations you're connected to can be invaluable – there are probably more than you think. In conducting this exercise, you'll quickly be able to identify the weak links (e.g. the organizations more susceptible to cybercrime) and can take further actions to mitigate the associated risks. You can expect to be connected to third-party suppliers such as:

- IT service providers
  - MSP / MSSP
  - Cloud providers
- Professional services
  - Finance
  - Legal
  - Security
  - Janitorial
- Suppliers
  - Materials
  - Services
  - Labor
  - Logistics

Once you've mapped out who you're connected to, you can assess the type of network access they have and what information could be accessed using those credentials. If it is anything more than the minimum, it is time to lock down that access and isolate the access to only the necessary information. Start with the providers who have the most unnecessary access and work your way down.

4. Assess the security posture of your suppliers and business partners

There are many approaches to making an assessment, but one popular approach for large service providers, cloud operators, and payment processors is to determine what types of certifications and audits they are subject to.

For example, a payment processor will be subject to compliance with PCI DSS. If they are subject to PCI DSS level 1 or 2, you should request their report on compliance (RoC) issued by their QSA/ISA. You should review these RoCs on a quarterly basis to assure they are meeting your expectations.

Another popular certification to confirm audits is SOC 2/2+/3 for your cloud service providers. SOC audits assess security controls and mitigations covering five Trust Service Principals: privacy, security, availability, processing integrity, and confidentiality.

Just as with your own security, no number of audits is a guarantee of anything, but it is certainly an indication that the supplier takes security and adherence seriously. Other things you may want to consider or ask for include penetration test reports, and GDPR compliance, or frequency of previous flaws or data breaches.

5. Constantly review your own IT security operations hygiene

While the posture of your suppliers is critical in safeguarding against supply chain attacks, do not neglect your own cybersecurity hygiene. Many organizations ignore it either because they didn't know where to start or they believed they weren't important enough to be targeted through the compromise of a trusted partner. Your cybersecurity practices could mean the difference between a mild inconvenience and a catastrophic data breach.

Enable multi-factor authentication (MFA)

The most common way we see organizations fall victim to supply chain attacks is through the use of stolen, but authorized access. Service providers are all too often provided credentials with the same rights and privileges as internal employees.

That is to say: they aren't required to use MFA, allowing attackers to exploit both credentials stolen through phishing attacks and unauthorized credential reuse by their staff. Because most organizations employ SSO (single sign-on), these credentials can be abused to access all sorts of systems that are unnecessary for the task at hand, expanding the risk of malicious insiders and outsiders alike.

Review supplier access and application privileges

Another common mistake is providing unfettered VPN, RDP, or other remote access technology for third parties to enable them to manage solutions. By unfettered we mean providing access to the entire network instead of segmenting and carefully hardening any necessary remote access tools.

All externally facing tools must require multi-factor authentication, and they should be limited to single hosts or systems. Where additional access is desired, the use of "jump hosts" is recommended to reduce risk and provide additional opportunity for monitoring and logging.

Allowing by default all applications signed by a vendor's software certificate also exposes organizations to supply chain attacks. We have repeatedly seen certificates stolen and abused to sign malware. Security tools should inspect everything possible.

Proactively monitor supplier security bulletins

Monitor all suppliers' security bulletins to be able to quickly deploy patches and mitigations when vulnerabilities are discovered, and keep an eye on the news headlines for your suppliers. When in crisis mode responding to an incident, you may not be very high on their list of organizations to notify. This can allow you to lock down access and begin to investigate whether you are impacted by their situation.

Review your cybersecurity insurance policy (if you have it)

Lastly, if you have cyber insurance, determine whether it covers third-party losses and how to engage the policy, if necessary. Work with your vendors to ensure that your coverage overlaps with any appropriate coverage they may have.

Technology and service enablers

As previously mentioned, defending against supply chain attacks is complex in nature. It is more a case of handling the risk associated with them and softening the blow. Fortunately, there are technologies and services available that are ideally placed to support the mitigation of this risk.

Threat hunting

We mentioned needing to shift to a proactive approach to cybersecurity to safeguard against supply chain attacks. Threat hunting is a key practice that organizations need to adopt to embody this mindset.

Endpoint Detection and Response (EDR)

A key threat hunting enabler is EDR technology. EDR, typically integrated into endpoint protection platforms, combines real-time continuous monitoring and endpoint data, with automated response and analysis capabilities. This enables security teams to swiftly identify and remediate threats.

Sophos Intercept X endpoint includes powerful EDR functionality. Sophos EDR is the first designed for both security analysts and IT administrators alike, giving you the tools to ask detailed questions when hunting down threats and strengthening your IT security operations hygiene. You get access to powerful, out-of-the-box, customizable SQL queries that give you the information you need to make informed decisions.

What's more, Sophos' EDR automated threat identification feature enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.

Learn more about Sophos' EDR capabilities

Managed Detection and Response (MDR) services

The most devastating cyberthreats, like the SolarWinds hack, generally involve human-led attacks. While technology, particularly threat hunting tools such as EDR, has an important role to play, expert operators are still required. Stopping human-led attacks requires human-led threat hunting, and IT managers know this with 48% of them planning to incorporate these practices within the next year[4].

One such human-led approach to threat hunting is engaging with an MDR service. Sophos' award-winning MDR service, Sophos Managed Threat Response (MTR), goes beyond just threat notification; it empowers your IT team with a dedicated team of cybersecurity experts who work around the clock to proactively hunt for, validate, and remediate potential threats and incidents on your behalf.

[4] *Cybersecurity: The Human Challenge - Sophos, 2020*

The Sophos MTR team of threat hunters and response experts will:

- Proactively hunt for and validate potential threats and incidents
- Use all available information to determine the scope and severity of threats
- Apply the appropriate business context for valid threats
- Initiate actions to remotely disrupt, contain, and neutralize threats
- Provide actionable advice for addressing the root cause of recurring incidents

Learn more about Sophos MTR

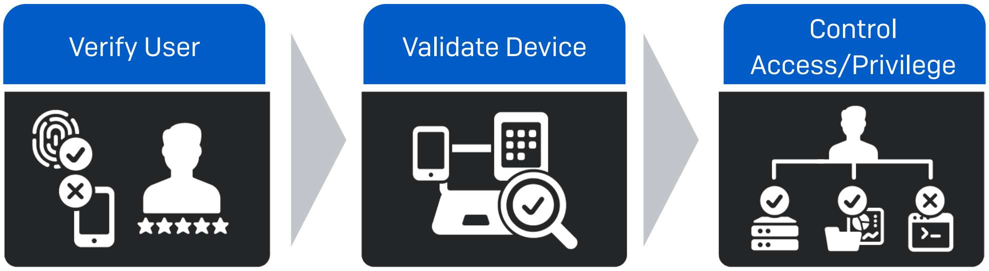
Evolving towards a zero-trust approach to cybersecurity

Earlier, we discussed reviewing your own security posture – in particular, enabling MFA and constantly reviewing both access and application privileges. All of this can be achieved by shifting towards a zero-trust approach to cybersecurity.

Zero trust is based upon the principle of "trust nothing, verify everything," and focusing on protecting resources regardless of where they are physically or digitally. No one vendor, product, or technology will get you to zero trust. Rather, it requires a cultural shift and a lot of different solutions to shift the paradigms by which we secure our resources. However, one steppingstone towards this model is adoption of a zero-trust network access (ZTNA) solution.

ZTNA, as the name implies, is based on the principle of zero trust. It enables users to securely access data from anywhere while providing admins with very granular controls.

ZTNA is all about verifying the user, typically with multi-factor authentication and an identity provider, then validating the health and compliance of the device – checking if it is it enrolled, up to date, properly protected, encryption enabled, etc., and then using that information to make decisions based on policies to determine access and privilege to important networked applications. ZTNA provides a great alternative to remote access VPN as it can offer very granular controls over who can access what – critical in safeguarding against supply chain attacks that rely on supplier access to your systems.



Sophos ZTNA, our new, cloud-delivered, cloud managed network access solution, is currently in Early Access Program (EAP) and will be Generally Available from mid-2021. IT provides protection for any networked application hosted on your on-premises network, or in the public cloud, or any other hosting site. It covers everything from RDP access to network file shares to applications like Jira, Wikis, source code repositories, support and ticketing apps, and beyond.

Learn more about Sophos ZTNA

Conclusion

Given their complexity, it is near impossible to prevent a supply chain-based attack from taking place. However, by following the guidelines in this paper, you can reduce your risk of falling victim to an attack and prevent an attack from significantly impacting your business. In summary:

1. Shift from a reactive to a proactive approach to cybersecurity
2. Monitor for early signs of compromise
3. Take audit of your supply chain
4. Assess the security posture of your suppliers and business partners
5. Constantly review your own IT security operations hygiene

In addition, consider adopting technologies and services such as EDR, MTR, and ZTNA to support your supply chain security objectives.

The threat landscape has evolved, and supply chain compromise is an issue for all organizations, large and small. We're all targets in someone's supply chain – and it's never been more important to minimize third-party supply chain risk.

Learn more about Sophos' industry leading
cybersecurity solutions and expertise at sophos.com

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2021-04-14 (SB-NP)

SOPHOS