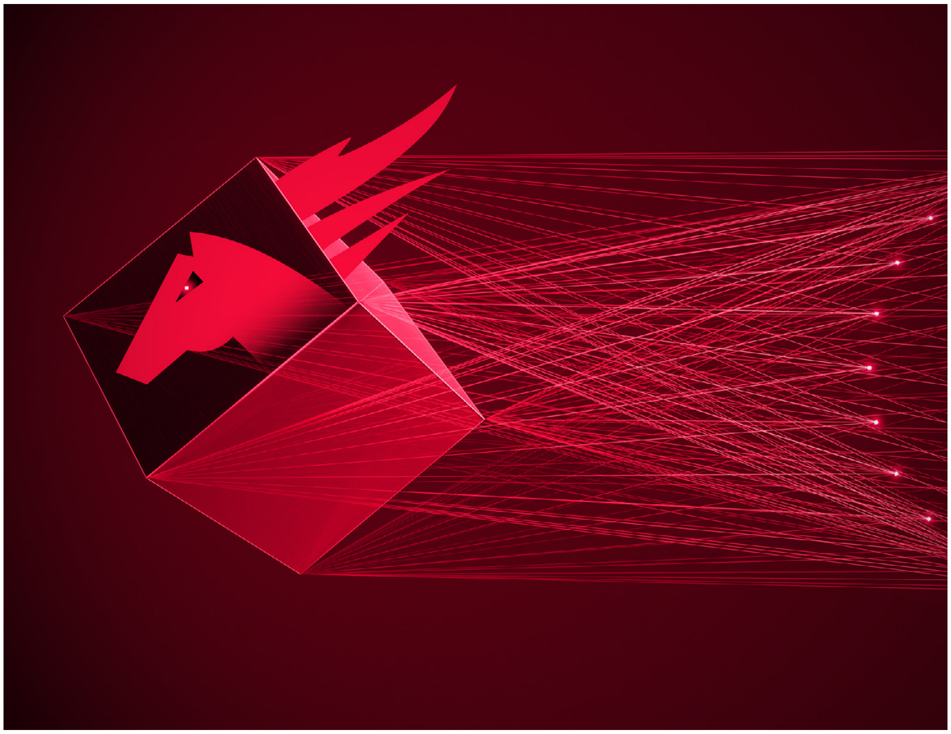
Supply Chain Attacks: Cyber Criminals Target the Weakest Link

By Threat Hunter Team

Table of Contents



Supply chain attacks have been occurring for several years, but they made major headlines at the end of 2020 due to what became known as the "SolarWinds hack". Thousands of organizations were affected when the update mechanism for SolarWinds' Orion software was compromised in order to deliver a backdoor Trojan known as Sunburst (Backdoor.Sunburst). Information about this attack campaign emerged in December 2020, with the activity thought to have been ongoing since at least March of that year.

Supply chain attacks, such as the SolarWinds hack, are indiscriminate, infecting all users of a compromised software, even though attackers may only be interested in a handful of them. In the case of SolarWinds, additional malicious activity was seen on the networks of a small subset of the original victims.

The SolarWinds hack is reminiscent of similar supply chain attacks of recent years that had a large number of victims, such as the CCleaner attack. In that incident a compromised software update led to millions of devices becoming infected, even though the attackers were only interested in a handful of machines.

A compromised software update is just one way of carrying out a supply chain attack, with several other methods of compromising victims also leveraged by attackers carrying out these attacks. This paper will go through the different types of supply chain attacks, detail some notable examples, contemplate why this is a growing issue for businesses, and what the future might hold in this space.

Some of the key areas covered in this white paper include:

- Updated metrics about the number of Symantec customers impacted by the SolarWinds supply chain attack, and an in-depth examination of this significant cyber incident
- A case study, including previously unpublished information, about a supply chain attack that has been linked in public reports to the North Korea backed Lazarus APT group
- How publicly reported supply chain attacks increased fivefold between 2016 and 2020
- Whether or not multi-stage supply chain attacks are something your organization needs to worry about
- Why and how malicious actors might leverage a supply chain attack to target your business, and steps your organization can take to reduce its risk

Software Supply Chain Attacks Explained

Software supply chain attacks really started to take off around 2017, with at least one supply chain attack publicly reported every month in that year, while less than a handful of these types of attacks had been reported in the preceding few years. In the Internet Security Threat Report 23 (ISTR 23), we defined a software supply chain attack as the following:

> *"Inserting a Trojan into an otherwise legitimate software package at the regular distribution place; this can be at the creation phase at the vendor, third-party storage location, or by redirection."*

This definition largely stands to this day, with supply chain attacks having become increasingly frequent since their growth in popularity began in 2017. Supply chain attacks are useful for attackers as they can allow them to infiltrate even well-guarded organizations if they are able to compromise the software of one of the organizations' trusted partners. The typical attack scenario - as seen in the SolarWinds hack and the CCleaner incident - involves the attacker replacing a legitimate software update with a malicious version in order to distribute it quickly and surreptitiously to intended targets. Any user applying the software update will automatically have their computer infected and will give the attacker a foothold on their network.

Spreading malware through an already established distribution channel allows attackers to compromise a large number of computers in a short period of time, especially if the compromised software has an automated update mechanism. Added to this, supply chain attacks are often difficult for the average user to spot, or for security software to stop. The compromised update is downloaded from a legitimate, trusted domain that generally has the required permission to perform network connections and execute downloaded binaries. In some cases, the downloaded binary even has a valid digital certificate.

Malicious actors that leverage supply chain attacks rarely want or need access to all the machines that they compromise through the Trojanized update process. However, the initial access allows them to carry out reconnaissance on infected machines before they identify those they are interested in. They generally then deploy a second-stage payload onto machines of interest. Supply chain attacks can also allow attackers to carry out a certain amount of targeting. For example, if they compromise a software that is known to be used in a certain sector or country. This is what we saw in the NotPetya attack in 2017. The entry point in that attack was a compromised accounting software widely used in Ukraine. The self-propagating nature of NotPetya, however, meant that it quickly spread beyond its originally targeted geography and caused widespread havoc.

When we consider the level of access that successful supply chain attacks can provide to compromised networks, it is easy to understand why they are being increasingly used by sophisticated attack groups.

How Attackers Compromise the Supply Chain

There are a few attack methods that cyber attackers use to carry out software update supply chain attacks, with the most common method being compromising a third-party supplier directly. Basically, attackers go after a weak link in the targeted company's supply chain. This normally means compromising a software supplier, but could also mean compromising a managed service provider (MSP) or IT provider in order to gain access to their clients' networks. We have seen some targeted attack groups, like Cicada (aka APT10), targeting MSPs.

Compromising a software vendor is the most straightforward path for an attacker wanting to carry out a supply chain attack, though it can be complex to achieve depending on the level of security the vendor has in place on its own systems.

If the attacker succeeds in compromising the software vendor, they can then switch the update package with a modified malicious version. One way to achieve this is by compromising the web server where the update packages are hosted, which may be achieved by exploiting a vulnerability in the content management tool. But the ultimate aim for the attacker is to get access to the vendor's development environment, which may be achieved through a successful spear-phishing attack against a developer, credential theft, or through another vector.

If they achieve elevated enough access, the attacker may also be able to acquire digital certificates that also allow them to code-sign the Trojanized update. This results in the malicious update having a legitimate and trusted digital signature that cannot be distinguished by the user, making the attack almost impossible to detect. While this type of attack is difficult to conduct, and would require a high level of skill from the attacker, it is also the most difficult to detect, and therefore highly effective.

Most of the high-profile software supply chain attacks of recent times - including SolarWinds, CCleaner, NotPetya, and ASUS - were achieved by the attackers being able to Trojanize the software update before it was delivered to customers.

Other Ways of Carrying Out Supply Chain Attacks

Another common way of carrying out supply chain attacks is by hijacking third-party hosting services, such as GitHub, for example. Not all software vendors host software on their own infrastructure, many use cloud storage, while others use service providers like GitHub. Open-source projects are particularly likely to use service providers like GitHub and so are particularly susceptible to being compromised in this way.

One way of compromising open-source projects is to make subtle changes to the source code that attackers may then be able to exploit, however, these kinds of changes could be discovered if the project is reviewed. Another method is to steal the credentials of someone, most likely a developer, with the requisite permissions to upload new binaries. Developer account credentials are very valuable to cyber criminals.

We saw several examples of attackers attempting to infect open-source software in 2020 in the hopes it would be used by developers and integrated into their projects. In December 2020, Sonatype reported that it had discovered two malicious packages uploaded to the RubyGems repository, where anyone can upload code written in the Ruby programming language. These malicious packages contained a clipboard hijacker that the attackers used to attempt to steal cryptocurrency from infected machines. In another incident in the same month, the security team behind the "npm" repository for storing JavaScript packages removed two malicious packages that contained code that could install a remote access Trojan (RAT) on the computers of developers who downloaded the package. The malicious packages were downloaded around 100 times before they were discovered. Underlining the threat to open-source projects, the security team at npm said that since August 2020 it had seen an increasing number of purposely malicious data-stealing libraries uploaded to its repository. As mentioned, developer account credentials are highly valuable to cyber attackers.

In May a significant supply chain attack targeting developers who use GitHub was revealed. A new malware called Octopus Scanner was used to compromise 26 open-source projects hosted on the platform. The malware had been built to insert backdoors into NetBeans projects without the owners of the projects being aware. The malware would then insert a backdoor into any repository or project the compromised code was used in.

Domain Hijacking

Domain hijacking is another form of supply chain attack. This could involve, for example, attackers compromising a domain registrar to change the registered name servers for a given domain, or even transfer the whole domain. Or they could attempt to compromise a DNS server to change the domain resolution to a different IP address under the attacker's control. An even simpler way of doing this is to simply buy a legitimate domain – this is possible if the owner of the domain forgets to renew, something that has happened to some domains owned by some well-known companies in recent years. Taking over a domain could allow attackers to redirect users to malicious websites, to steal their information, or push Trojanized updates onto their machine.

Formjacking

Formjacking is a term we use to describe the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of e-commerce sites.

The malicious code can just be injected directly onto the targeted website, but in many instances formjacking cyber criminals use supply chain attacks to gain access to websites. Formjacking (or card skimming) attacks have been around for a long time, but they really took off in the final quarter of 2018. Supply chain attackers aiming to carry out formjacking attacks would often target the networks of third-party companies whose products were used on e-commerce sites to manage analytics, for website support and other services. In one high-profile attack, formjacking attackers were able to gain access to Ticketmaster's website when code used in a third-party company's chatbot, which was used for customer support on Ticketmaster websites, was compromised.

The third-party companies targeted by formjacking criminals were generally much smaller than the actual target company. Smaller companies tend to have less stringent security measures and are easier to compromise than the network of a well-known brand.

Supply chain compromise was so important in formjacking attacks that incidents of formjacking accounted for a significant proportion of the supply chain attacks we saw in 2019. There doesn't appear to be as many public reports of formjacking attacks leveraging weak parts of the supply chain in 2020, although there are still some incidents. This could be for a few possible reasons:

- The attacks have occurred but haven't yet been publicly revealed
- Website owners have learned from the incidents of recent years and have improved security on their e-commerce sites by removing third-party code from checkout pages
- Formjacking isn't the "on-trend" cyber crime it was in 2018 and 2019, with the criminals behind it having possibly moved on to other types of cyber crime
- Cyber criminals are injecting malicious code directly onto targeted websites rather than carrying out the compromise via supply chain attacks.

However, the use of third-party code on a website still opens up a business to the possibility of being compromised via this code. Businesses should reduce their exposure by ensuring third-party code is not present on pages where personal information is gathered, such as checkout or login pages, and by monitoring any code changes in their environment.

SolarWinds: A Significant Cyber Intrusion

Undoubtedly, one of the most high-profile software supply chain attacks of recent years is also one of the most recent. News of the SolarWinds hack broke in December 2020 and it remained in the headlines for many weeks as investigators discovered more details about the hack. The investigation into this incident is likely to continue well into 2021 with many questions about it still to be answered.

These attacks became public when security firm FireEye disclosed details of them in December. The campaign had been underway since at least March 2020 and any user of the SolarWinds Orion software who had downloaded an update in that time was believed to be impacted - with this amounting to approximately 18,000 organizations. The Trojanized update delivered a backdoor Trojan called Sunburst to affected machines. A subset of these initial targets was then identified by the attackers for further compromise.

Symantec had identified 4,167 customers by the end of January 2021 that had received the first-stage Sunburst backdoor. We also identified a small number of organizations where one of two second-stage payloads were deployed. These second-stage payloads are Backdoor.Teardrop and Backdoor.Raindrop. Initial analysis had uncovered only the first backdoor - Teardrop - but further research by Symantec investigators led to the discovery of a second backdoor - Raindrop - which was used for lateral movement on some victim networks.

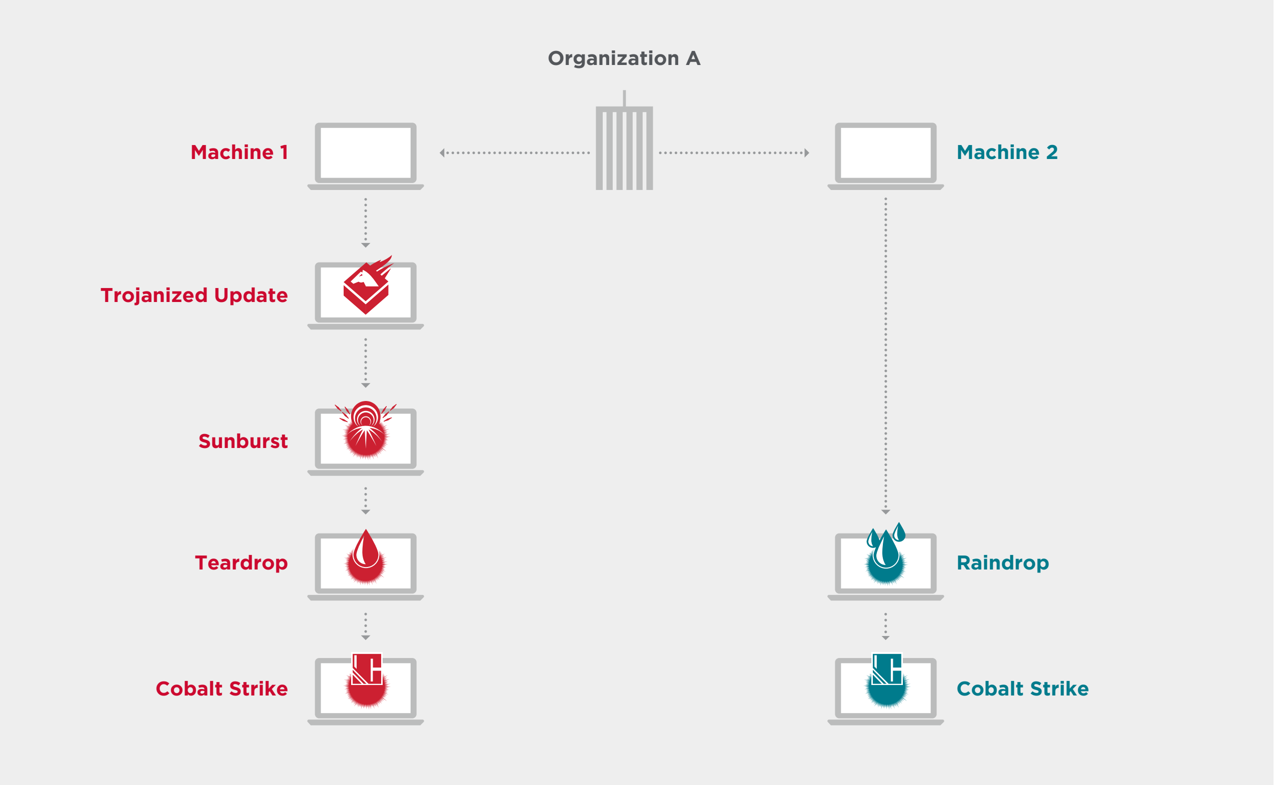
The compromise of the software occurred when an existing SolarWinds DLL called SolarWinds.Orion.Core.BusinessLayer.dll was modified by the attackers to include an added class. This malicious class could:

- Set delay time before execution (in order to avoid being detected if the software was run in a sandbox)
- Collect and upload system information
- Download and run code
- Iterate the file system
- Create and delete files
- Calculate file hashes
- Read, write, and delete registry entries
- Reboot the system

The second-stage malware, Teardrop, was used to deliver the Cobalt Strike commodity malware. Cobalt Strike was observed connecting to a command and control (C&C) server. The attackers attempted to obtain credentials, and they also used the Adfind tool to query Active Directory. The attackers appeared to be looking to gain elevated privileges - such as domain administrator- so they could access the domain or move laterally through the network.

Raindrop - the other second-stage malware observed - also delivered a payload of Cobalt Strike. Raindrop is very similar to the aforementioned Teardrop tool, but there are some key differences between the two. While Teardrop was delivered by the initial Sunburst backdoor, Raindrop appears to have been used for spreading across the victim's network. We have seen no evidence of Raindrop being delivered directly by Sunburst, rather it appears elsewhere on networks where at least one computer has already been compromised by Sunburst. We have only seen Raindrop activity on a small handful of machines so it does not appear to be as widely deployed as Teardrop.

Figure 1. Example Teardrop and Raindrop Activity in a Compromised Organization



The motivation behind the attack is speculated to be cyber espionage by many. Public reports have said that there is some evidence of the attackers accessing email on targeted networks, but the extent of any spying or exfiltration of data isn't clear.

The speculation and discussion in the infosecurity and wider community since this attack took place has been wide ranging, with one U.S. politician describing it as "the greatest cyber intrusion, perhaps, in the history of the world." And the impact of the attackers behind this attack wasn't just felt by SolarWinds customers - with as many as 30% of those affected reportedly not customers of SolarWinds. How the attackers initially accessed SolarWinds systems is not yet established. However, Microsoft did also reveal in December that the hackers that targeted SolarWinds had also accessed its corporate network, but said it had "found no indications" that its systems were used to attack others. However, SolarWinds itself is now reportedly investigating if Microsoft's cloud was the hackers' initial entry point into its network, although this is said to be just one of a number of theories being investigated.

If this turns out to be the case then it looks like this may have been a multi-stage supply chain attack: where one company was targeted to gain access to another company, and to then gain access to that company's customers. However, that is just in the realm of theory at the moment. One thing is for certain though, investigations into this attack are unlikely to finish anytime soon with many questions still to be answered - such as who is behind this attack? And of course, establishing the initial entry point. The U.S. government has speculated that the attackers behind this attack are Russia state-sponsored actors, but definitive evidence of this assertion has not yet been published.

This attack has also thrown into sharp focus the extent to which many businesses - from the small to the very large - rely heavily on cloud services, and the complications that can create when it comes to keeping your network safe.

Symantec has published multiple blogs and podcasts about this attack, which can be accessed in the Further Reading section at the end of this paper. Our investigations into this attack are also continuing, with the safety of our customers' networks always our primary concern.

Other High-Profile Supply Chain Attacks

NotPetya

The NotPetya attack occurred in 2017 and is one of the most high-profile software supply chain attacks of recent times. NotPetya ended up compromising thousands of computers around the world and causing billions of dollars in damage. M.E.Doc, a tax and accounting software widely and primarily used in Ukraine, was identified as the initial insertion point of NotPetya into corporate networks. Analysis of the attack revealed that the attackers used stolen credentials to modify the configuration of the M.E.Doc web server, allowing them to redirect any request for updates to a malicious server under their control. This is how they downloaded the NotPetya malware onto compromised computers.

The impact of NotPetya may not have been as severe had it not been for the fact the EternalBlue and EternalRomance exploits were incorporated into the threat as one of its means to propagate itself. These exploits allow for self-propagation, meaning that NotPetya was able to spread widely, and beyond the initially targeted devices and networks. The targeting of M.E.Doc to carry out the supply chain attack, which is primarily used in Ukraine, indicates that the targets of NotPetya were probably based in that country. However, its ability to self-propagate meant that it ultimately spread to many other countries, including the U.S., Russia, and many countries in Europe, and led to widespread disruption.

CCleaner

The CCleaner compromise also occurred in 2017, and underlined the indiscriminate nature of software supply chain attacks. It's estimated that more than 2.2 million computers installed the Trojanized software update, but secondary activity was only observed on as few as 40 machines. The compromised version of the software would transmit the infected computer's name, IP address, a list of installed software, a list of active software, and list of network adapters to a third-party server located in the U.S. It appears that once the attackers received this information they then decided whether or not to launch second-stage malware.

The small number of computers that received the second-stage malware indicates that the attackers were only interested in a small subset of CCleaner's users. However, this attack does underline that supply chain attackers are quite happy to infect as many devices and networks as necessary to get them to their desired target(s).

ASUS

A similar attack to CCleaner occurred in 2018, when it was revealed that tech giant ASUS's automated software update system had been hijacked to deliver malware. As many as half a million devices were affected in this supply chain attack, with the attackers seeking to target users who were identified by their network adapters' MAC addresses. The list of MAC addresses was hardcoded into the Trojanized samples and used to identify the intended targets of the hack.

This supply chain attack started in June 2018 and continued through to at least late October that year. The Trojanized updates contained a form of backdoor program that attempted to connect to an attacker-controlled domain. The updates were signed with legitimate ASUS digital certificates, which helped the attack go undetected for a significant period of time.

These examples show that large companies need to be aware of software supply chain attacks not only because their third-party suppliers could be targeted as a means to get onto their systems, but because they too could be targeted to gain access to the systems of their customers.

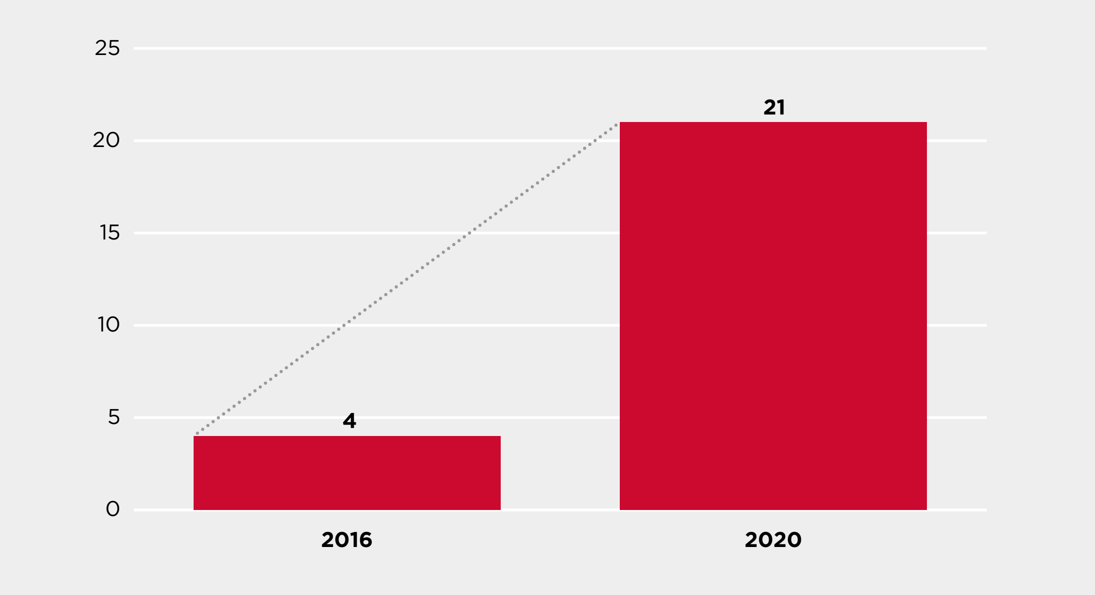
Why are Supply Chain Attacks Increasingly Popular?

Supply chain attacks have increased in prevalence over the last few years. Back in 2015 and 2016 there were just a handful of supply chain attacks – we detailed in the ISTR in 2018 that there were approximately four publicly reported supply chain attacks in both those years. This increased in 2017 when there were approximately 13 supply chain attacks reported, while a jump occurred in 2018 and 2019, driven primarily by the popularity of formjacking.

Formjacking criminals didn't appear to be leveraging supply chain attacks as frequently in 2020 as they had been in previous years. In 2020, there were approximately 21 publicly reported supply chain attacks. As the SolarWinds and CCleaner attacks demonstrate, just one supply chain attack can lead to thousands or even millions of compromised machines. Many of these attacks were sophisticated and appear to have been carried out by experienced cyber criminals or nation state groups. They include the SolarWinds hack, as well as attacks by advanced persistent threat group Cicada (aka APT10).

Supply chain attacks show how ever-changing the cyber security landscape is and the importance of staying up to date with what is occurring on the cyber crime landscape. Software supply chain attacks increased more than fivefold between 2016 and 2020, going from being a relatively niche issue, to a problem that organizations of all sizes need to be alert to and aware of.

Figure 2. Supply Chain Attacks Increased Fivefold in the Space of a Few Years



So, why have supply chain attacks soared in popularity among both cyber criminals and nation state actors?

Malicious actors may leverage supply chain attacks for a variety of reasons:

- Supply chain attacks are often used **to infiltrate well-protected organizations** where other infection vectors may have failed. Attackers find the weakest link in the organization's supply chain.
- These types of attacks **can allow for fast distribution of malicious software**, with a large number of machines infected in a short period of time. The number of infections can grow quickly as users update their software, and especially if automatic updates are enabled.
- Supply chain attacks **can allow for the targeting of specific regions or industries**, by Trojanizing a software that is used by a specific sector or region. The NotPetya attacks were an example of this, with 96% of machines affected by the initial Trojanized software update being in Ukraine.
- These attacks **can allow for the infiltration of air-gapped networks**. Sysadmins may copy the software update to the isolated network or install it from a removable drive. If the software itself is Trojanized then the malicious actors can gain access to the separated network.
- It can be **difficult for victims to identify where their system was compromised** as the attacks emanate from trusted processes. This can help attackers conceal their identity and make it more difficult for teams investigating the incident.
- Depending on the software that they Trojanize, **the attack may automatically provide an attacker with elevated privileges** on the target system. The attackers are able to achieve all this without deploying any sophisticated or noisy malware or exploits.

The attackers who carry out supply chain attacks – particularly those who hijack third parties to compromise software updates – are generally sophisticated actors. They require the skills to first compromise the third-party supplier, which may be considered the “weakest link” in a large company’s supply chain, but this doesn’t mean compromising them is easy. To make their attack as convincing as possible attackers will also need to procure or fake a digital certificate. But the appeal of supply chain attacks for attackers is also clear – well-executed supply chain attacks are difficult to stop and hard to detect, until it may be too late.

Case Study: Probable Lazarus Attack Leverages South Korean Software

In November 2020, ESET published a report detailing a supply chain attack campaign aimed at victims in South Korea. This campaign abused the legitimate WIZVERA VeraPort software to deliver malware to victim organizations. WIZVERA VeraPort is a software that is legitimately used in South Korea to install security software. ESET attributed this activity to the North Korean APT group Lazarus. Symantec’s initial investigation into this activity uncovered activity consistent with that reported by ESET, but Symantec has not attributed this activity to any named group.

Symantec’s telemetry showed at least one victim in South Korea in the heavy industry sector that was infected with malware as a result of running WIZVERA VeraPort software. ESET had not specified the sector of any of the targets it saw infected. It is unclear which website the victim machine was visiting that required VeraPort, but the signed downloader was delivered from a compromised website related to the rail transport sector. The attackers quickly moved laterally in the infected organization, utilizing a large variety of tools, including dual-use, hacking tools and malware, and ultimately deploying file-uploading tools in an attempt to exfiltrate data, including Outlook mail archives and video. Information about this post-compromise activity has not previously been publicly reported.

Activity Summary

The signed initial downloader was downloaded from a compromised website and launched by VeraPort.

Symantec then observed various malware and a large variety of hacking tools being deployed on the infected network. These were used to move laterally through the infected network and eventually to attempt to exfiltrate data from infected machines. The attackers made extensive use of living-off-the-land tactics and off-the-shelf hacking tools.

Table 1. Malware and Hacking Tools Used by the Attackers

Malware	Hacking Tools
Dropper	Remote command utility that uses WMI
DLL Service Creator	Open-source proxy tool
Loader	Pentesting tool used for man-in-the-middle (MitM) attacks
	File enumeration too ‘everything[.]exe’
	Active directory tool ‘adfind.exe’

PowerShell was also used to download multiple executables. The command line tool Curl was used to download ‘GIF’ files that were then decoded as executable files using Certutil. Two file uploaders were eventually deployed and used to exfiltrate AVI video files, PST files (an Outlook archive format), and a .DAT file. At least one of the infected machines had Autodesk installed on it, indicating it may be used in engineering or design.

While Symantec has not attributed this activity to a named actor, the infection vector, along with multiple artifacts, including file paths and commands used by the attackers, were consistent with the activity reported by ESET. ESET attributed this activity to Lazarus.

Possible 'Dream Job' Link

During Symantec's investigation into a campaign dubbed 'Dream Job', in which pharmaceutical companies producing COVID-19 vaccines, and security researchers, were targeted, we also observed the VeraPort software being used as a potential vector. The victims in this campaign were targeted through phishing emails and by manipulation on social media, but Symantec researchers also found that attackers may have got onto victim machines:

- From VeraPortmain20[.]exe - which is the WIZVERA VeraPort software
- Potentially from other infected machines on the same network via the Windows Management Instrumentation Command-line (WMIC)

The abuse of the same software and use of a similar technique for lateral movement do raise the possibility that the same actors were involved in both attacks. The Dream Job campaign has been linked by multiple others - including Google and ClearSkySec - to government-backed actors from North Korea.

This attack is also interesting as it demonstrates one of the features of supply chain attacks: that they can allow for the targeting of victims in specific geographies. WIZVERA VeraPort software is widely used by government and banking websites in South Korea, with some websites requiring that visitors have the software installed before they are able to access the sites' services. Compromising this software gives attackers the opportunity to potentially infect a large number of users in South Korea.

Targeted Attack Groups Leverage Supply Chain Attacks

Supply chain attacks are frequently used by advanced persistent threat (APT) groups, like Lazarus and others.

Orangeworm/Kwampirs

We first wrote about this threat in 2018, when we revealed a group we called Orangeworm was using the Kwampirs malware to target the healthcare sector via supply chain attacks.

At the time, Orangeworm had victims in a variety of sectors, including manufacturing, information technology, agriculture, and logistics. However, all the victims in these sectors had links to healthcare, so appear to have been targeted as part of supply chain attacks to achieve the ultimate goal of compromising healthcare victims.

Kwampirs is a remote access Trojan (RAT) that provides the attackers with backdoor access to the affected machine. The malware spreads through an infected network via network shares.

It appears the threat is still active, since in 2020 the FBI released an alert three times warning that malicious actors were leveraging Kwampirs to carry out supply chain attacks. The healthcare sector was highlighted as being of particular interest to them. The FBI first released this warning in January 2020, and then issued it again in February and March, as the COVID-19 crisis ramped up and put pressure on the healthcare sector worldwide.

Chinese APT Groups Leverage Various Means to Carry Out Supply Chain Attacks

A group of seven men were indicted by the U.S. Justice Department in September 2020 for their alleged involvement in hacking more than 100 high-tech and online gaming companies over many years. The Justice Department said the men were part of a targeted attack group called APT41 (aka Winnti), which is believed to have links to the Chinese government. Symantec tracks APT41 as two separate groups – Blackfly and Grayfly – with two of the men named in the indictments appearing to have worked with both groups.

The indictment states that APT41 used phishing emails to target its victims, but the group was also known to leverage supply chain attacks by hacking a software company and modifying its code to gain access to its customers' machines. The group also allegedly created security software and PC utilities that they advertised as being legitimate.

Five of those named in the indictment are resident in China and remain at large, but the Justice Department stated in the indictment that it had been able to seize websites, domains, and servers associated with the group's operations and shut them down, hindering their operations. However, as most of the individuals involved have not been arrested, these indictments are unlikely to fully stop Grayfly/Blackfly activity.

Also in 2020, we observed an attack campaign by another China-linked group – which we call Cicada, but which is also known as APT10. Cicada has been publicly linked by authorities in the U.S. to the Chinese government. In the campaign we reported on in 2020, Cicada was seen targeting Japan-linked organizations in a number of sectors, including the automotive, pharmaceutical, and engineering sectors. We did not see the group Trojanizing software or leveraging Trojanized software as an entry point to targeted organizations, however, we did see managed service providers (MSPs) among the group's targets. Cicada has a history of targeting MSPs, we assume with the aim of gaining access to their customers' networks. The group was also seen targeting a number of companies involved in supplying parts to the automotive industry, as well as targeting automotive companies themselves. These suppliers may have been targeted as a means of gaining a foothold on the networks of their automotive customers.

Attack Groups Targeting the Middle East Leverage the Software Supply Chain

We wrote about Tortoiseshell in September 2019, when we spotted it targeting IT providers in Saudi Arabia, in what appeared to be supply chain attacks aimed at ultimately gaining access to the IT providers' customers. Around 11 organizations were compromised in that campaign.

Elfin (aka APT33), a group we published about in March 2019, also had a focus on organizations in Saudi Arabia. In the campaign we investigated we also saw the group targeting victims in the U.S., but said at the time that these organizations may have been targeted as part of supply chain attacks in an attempt to gain access to organizations in the Middle East. In one instance, a large U.S. company was attacked the same month that a Middle Eastern company it co-owned was also attacked.

There were reports in January 2020 that Elfin was increasingly targeting the suppliers and manufacturers of industrial control systems (ICS) used in electrical utilities, manufacturing, and oil refineries. Indications are that these may have been supply chain attacks aimed at establishing a presence on the suppliers' customers.

Why You Need To Be Aware of Supply Chain Attacks – and How to Protect Yourself

Supply chain attacks are generally leveraged by skilled malicious actors in targeted intrusions. Organizations need to be aware of these kinds of attacks as they could be targeted for the initial intrusion, or following on from the successful compromise of one of their third-party suppliers.

It can be complex to detect and stop a supply chain attack targeted at your business. As we have said, the malware is often delivered to your network via a trusted process and from a trusted vendor, often even with a valid digital certificate, making spotting the malicious activity difficult until it is too late.

However, while supply chain attacks are difficult to prevent, there are some steps that can be taken including:

- **Testing new updates** in small test environments or sandboxes first to detect any suspicious behavior. However, when doing this bear in mind that sophisticated attackers can apply well-known tricks to delay malicious behavior in order to not attract attention during this kind of analysis.
- **Behavior monitoring** of all activity on a system can help identify any unwanted patterns and allow you to block a suspicious application before any damage can be done. This is possible as the behavior of a malicious update will be different to that of the expected clean software.
- The producers of software packages should also ensure that they are able to **detect unwanted changes** in the software update process and on their website.
- Organizations should **reduce the attack surface** by implementing Zero Trust policies and network segmentation, so that if a malicious update is downloaded onto one machine it won't be able to automatically spread to the whole network.

An interesting potential trend to note too, as mentioned in the SolarWinds section of this paper, is the possibility that some supply chain attacks could be multi-stage. For example, attackers are compromising Company 1, gaining access to Company 2's network, but their actual targets are Company 2's customers (Company 3, 4, 5) etc.

Multi-stage supply chain attacks would be a complex undertaking, and would likely only be attempted by highly skilled actors, such as those behind the SolarWinds attack. They would require maintaining a low profile on multiple networks before even gaining access to the targeted network(s). Only sophisticated actors would likely have the skills to carry out these kinds of attacks successfully, and they would need to be highly targeted for them to be worthwhile for the attackers.

As such, multi-stage software supply chain attacks are likely to only ever be a rare occurrence, but if carried out successfully could grant attackers access to highly protected networks that could not be compromised by any other means. Attackers capable of successfully executing such an attack would be highly skilled, meaning they would pose a significant danger to the operations of any organization they would compromise.

Conclusion

The attackers carrying out supply chain attacks, like those behind the SolarWinds hack, are sophisticated and highly skilled actors who pose a significant threat to any organization they compromise. These attacks are also difficult to guard against, as the malware generally makes its way onto targeted networks by abusing trusted processes and relationships. This means that these attacks often aren't detected until a second-stage malware is deployed, at which point the damage may already be done, as attackers have potentially already been on the system for a long time.

One important step organizations can take is to do an audit of their third-party suppliers and who has access to their network. They should minimize access as much as possible, giving only the minimum amount of access and permissions required to third parties. They should also ensure they carry out due diligence with any companies they work with or which supply them with software or support services, to ensure these companies have sufficient protocols and protections in place. However, as the SolarWinds hack demonstrated, this isn't always a guarantee that your organization is protected as even well-established companies like Microsoft and security firms can fall victim to supply chain attacks. It is for that reason that further steps like network segmentation and Zero Trust policies are also important.

How Symantec Solutions Can Help

The Symantec Enterprise Business provides a comprehensive portfolio of security solutions to address today's security challenges and protect data and digital infrastructure from multifaceted threats. These solutions include core capabilities designed to help organizations prevent and detect advanced attacks, including supply chain attacks.

Symantec Endpoint Security Complete

Symantec Endpoint Security Complete (SESC) was specifically created to help protect against advanced attacks. While many vendors offer EDR to help find intrusions, as does Symantec, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.

LEARN MORE

Privileged Access Management (PAM)

PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity.

LEARN MORE

Symantec Web Isolation

Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.

LEARN MORE

Symantec Secure Web Gateway (SWG)

SWG delivers high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.

LEARN MORE

Symantec Intelligence Services

Symantec Intelligence Services leverages Symantec's Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.

LEARN MORE

Symantec Content Analysis with Advanced Sandboxing

Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential APT files and toolkits.

LEARN MORE

Symantec Security Analytics

Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.

LEARN MORE

Further Reading

Blogs

SolarWinds Resources

- SolarWinds: How Sunburst Sends Data Back to the Attackers
- Raindrop: New Malware Discovered in SolarWinds Investigation
- SolarWinds: Insights into Attacker Command and Control Process
- SolarWinds: How a Rare DGA Helped Attacker Communications Fly Under the Radar
- SolarWinds Attacks: Stealthy Attackers Attempted To Evade Detection
- Sunburst: Supply Chain Attack Targets SolarWinds Users

Podcasts

Sunburst: Everything we know about the supply chain attack targeting SolarWinds users

The latest on the SolarWinds hack, a lot of ransomware activity, and healthcare hit hard by cyber attacks

Raindrop: How the additional tool was discovered in SolarWinds investigation

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com