APPGUARD
The Malware Disruptor

Mitigating Supply Chain Risk:

Protect Your Organization Even When Your Software Supply Chain is Compromised

WHITE PAPER

SUMMARY:

The recent SolarWinds supply chain attack serves as a strong reminder that we are all part of someone's supply chain, and every chain has a weak link. This paper outlines how supply chain attacks unfold and the steps you can take to prevent becoming a victim of the next supply chain exploit by adopting a zero trust solution.

The Supply Chain Threat

If you are in the security industry or responsible for keeping your organization's assets secure from breaches, you've likely read about the recent SolarWinds attack. This is not the first high visibility supply chain attack and certainly won't be the last. Hackers realize that supply chain attacks, when successful, provide a domino effect: by compromising just one vendor, attackers can gain access to all of that vendor's customers.

Supply chain attacks are particularly dangerous. In a supply chain attack, attackers infiltrate trusted third-party applications that have access to your systems and data – without you or the vendor knowing. With no control over a third-party organization's security posture and practices, yet dependent on their offering, enterprises are faced with a difficult security dilemma - how to protect against these types of attacks?

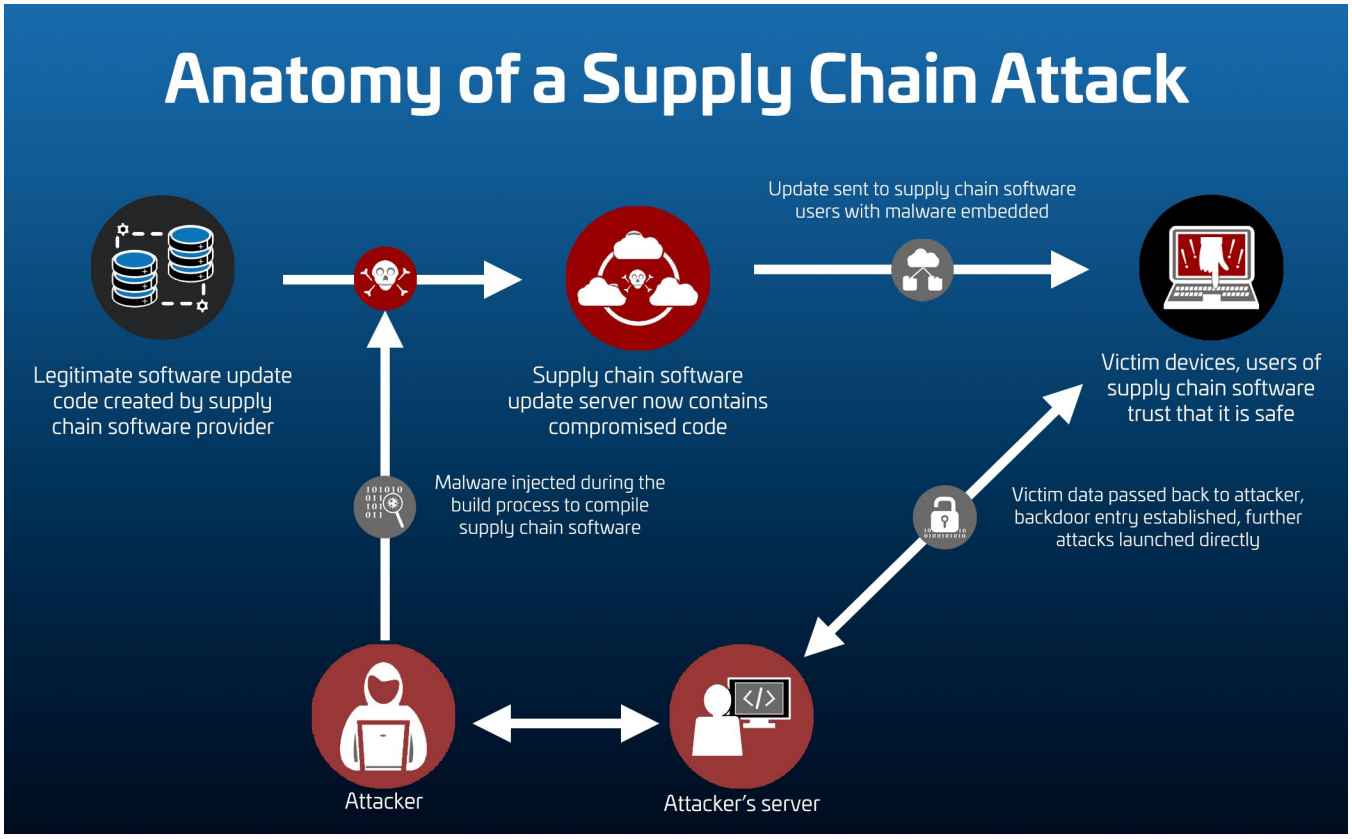
In the case of the SolarWinds attack, the severity of the attack cannot be overstated, and unfortunately the chance of similar attacks on the horizon are fairly certain. The SolarWinds attack was likely the most dramatic to date due to its unprecedented scale. While the full impact of the attack won't be known for months, we already know that by the end of 2020 more than 18,000 organizations and several U.S. government agencies were impacted, as submitted in a report by SolarWinds to the SEC in December 2020.

Trustworthy Apps Can't Always Be Trusted

The SolarWinds attack is yet another reminder that even trustworthy applications cannot be fully trusted. Hackers have honed their craft and know how to successfully infiltrate the source code of applications, allowing them to gain full access to software vendors' and end customers' data. Vendors who are compromised unwillingly transmit the malware to their customers.

Supply chain attacks are stealthy – often using multiple attack vectors that bypass existing security defenses. In the SolarWinds case, malicious code was embedded in digitally-signed binaries, ensuring cryptographic safeguards at customer organizations failed. When SolarWinds updated its product, the hidden code was included in the update package - granting it access to third-party servers and data.

While the SolarWinds attack is arguably one of the most significant state-sponsored hacks we've seen in years, it is not an isolated event. Given today's digital era, and the world's dependency on software to run businesses and governments, organizations must prioritize their security initiatives to ensure they can effectively defend against supply chain attacks.



> *So what can an organization do when they have little choice but to trust the security of supply chain vendors, but have no control over how those vendors manage their security?*
>
> *Use security software that implements policies that treat supply chain activity like anything else. Even the most trustworthy applications cannot be fully trusted.*

Supply Chain Attacks Outsmart Traditional Endpoint Protection Tools

Unfortunately, supply chain attacks have proven their ability to undermine the methodologies used by most endpoint protection tools. Since traditional anti-virus and next generation anti-virus tools detect breaches by identifying known malicious code, or code that is not on their trusted default list, malicious code embedded in popular enterprise software is not detected by these tools.

In the case of the SolarWinds attack, the adversaries disabled the Endpoint Detection and Response (EDR) tool on the initially compromised host so they could do some 'noisy' actions - including planting malware that operated quietly and mimicked legitimate operations to evade detection. When finished with the 'noisy' activity, they restarted the host and the EDR. Since supply chain malware leaves no trackable file for EDR tools to detect, the SOC personnel thought nothing of a single endpoint's absence in the EDR platform reports for a short period of time while it was disabled. For months, the malware ran without detection by the EDR.

Fortify Your Supply Chain Security With AppGuard

So what can an organization do when they have little choice but to trust the security of supply chain vendors, but have no control over how those vendors manage their security? Use security software that implements policies that treat supply chain activity like anything else. Even the most trustworthy applications cannot be fully trusted.

AppGuard is uniquely suited as a defense against supply chain attacks because it is designed to apply controls that render exploited applications harmless, even when undetected, with the assumption that everything is likely to be compromised at one point or another. Since AppGuard is focused on controlling the high-risk actions which must be executed in order for an attack to have any measurable effect, its protection is equally as strong regardless of where the attack is coming from - including trusted third parties.

AppGuard is the only software on the market that applies zero trust principles within the endpoint.

AppGuard doesn't strive to distinguish good from bad or normal from abnormal - among infinite possibilities. It simply restricts behavior to what is allowed, applying zero trust principles within endpoints. AppGuard focuses on normal behaviors of the operating system and employs a combination of pre-launch, containment, and isolation controls to defeat malware techniques without having to recognize malware or its effects. Unlike Endpoint Detection and Response tools that generate alerts that require humans to investigate, AppGuard's effectiveness is not dependent upon humans reacting to alerts. Instead, those that adopt AppGuard can rest easy knowing that any activity outside an application's "swim lane" is blocked.

AppGuard vs. Supply Chain Risk: Mitigating the Threat

AppGuard enforces multiple policy approaches which combine to create unparalleled protection from the most common attack vectors. It segments the file system into trusted and untrusted areas with different allowed actions and launch capabilities, isolates risky actions, and applies a patented ability for a child process to "inherit" the rules applied to its parent process (therefore allowing the policies to adapt to context). This allows AppGuard to offer a powerful "middle ground" - applying zero trust principles without compromising operational integrity. As noted previously, this is particularly powerful in a supply chain scenario since policies continue to be applied uniformly without consideration that a "supply chain" application should be entitled to a higher level of trust, leaving the enterprise equally protected regardless of the source of the attack. The following are examples of how AppGuard's policy principles apply in a supply chain attack scenario:

Prohibited Launch Controls

With AppGuard, launch controls are placed on the operating utilities which have the administrative access and functionality to perform high risk activities that malware would use to achieve its goals, like data theft, system control, or installation of backdoor

access. Such utilities can only launch in certain specific instances (generally, by applications marked as PowerApps in AppGuard's management system). Out of the box, AppGuard has default restrictions applied to most living off the land binaries (LOLBAS) and those restrictions can be adjusted if necessary, for operational needs.

In a supply chain attack, if the hijacked application attempted to run one of these utilities to do its work, it would not be able to do so unless the application was already intentionally given the express ability to do so. It is unlikely that this would be the case in most real-world scenarios, and even if it was, AppGuard's additional policy rules would then block the attack at a different stage in its life cycle.

Using SolarWinds as an example, wscript.exe was a prohibited utility used in a critical part of the attack's activity. AppGuard's prohibited launch controls block wscript.exe from launching in the manner that it did with SolarWinds and would have thwarted the attack.

Scripts, executables, and DLLs from high-risk locations such as your Downloads folder and other common temporary directories are usually only allowed to run a program signed by a source which is placed on a trusted publisher list. Although a supply chain application is likely to be marked as a trusted publisher, this policy rule is still an effective additional protection when combined with AppGuard's other rules. Its presence requires a malware writer to be perfectly precise in how they deliver the attack, and one mistake will render the attack harmless. In combination with the requirements created by AppGuard's other policy rules it makes it extremely difficult for the malware to execute to completion.

In the case of SolarWinds, some binaries were launched and signed by SolarWinds – but some were launched from SolarWinds' Orion product yet not signed at all. The latter would have been blocked and would render part of the attack null, undermining its ability to complete.

Containment of High-Risk Applications

AppGuard's containment policy blocks risky applications from making alterations or reading/writing to memory on system resources, with exceptions available for specific needs. This allows some applications that would normally be prohibited from launching to instead run with restrictive controls that prevent them from being used to achieve command and control of the system. By default, most supply chain applications' child processes would be placed in a category that is contained, putting strong restrictions on its ability to complete such actions outside of its normal operations.

> *"AppGuard, with its Zero Trust premise, is a crucial element in any effective supply chain defense. It is 'origin-agnostic', blocking execution of malware emanating from a 'trusted' source in your information architecture akin to that which occurred during the SolarWinds attack."*
>
> **Mark Kelton**
> **Former Director Counterintelligence, CIA**

Inheritance of High-Risk Policy

Once a process tree is marked as "high-risk", all of its subsequent processes are also marked as high-risk. This allows the policy to quickly adapt in real time to thwart new and unseen behaviors that might ultimately be from a new type of attack.

In the case of SolarWinds, this could stop attempts to try to run Cobalt Strike (originally a pen testing tool, but also now used by attackers to create a "beacon" on a system) to connect back to the attacker's network.

Isolation policy over LSASS

Isolation policy blocks access to memory and control over high value system resources, with only specific exceptions allowed for operational necessity as configured by an administrator. Local Authority Security Service (LSASS) is one example of a core Windows security process which holds administrative credentials and is subject to Isolation because it is a high value target for credential theft.

In the case of SolarWinds, credentials were stolen from LSASS in order to access other folders throughout the enterprise infrastructure. There would be no reason for a specific LSASS access exception to have been created for SolarWinds, so AppGuard would have blocked this attempt in its infancy.

> *AppGuard is the only solution on the market that applies Zero Trust principles **within** the endpoint.*

These examples demonstrate the benefit of AppGuard's true preventative techniques, applying redundancies and roadblocks to the dangerous activities that malware will attempt to execute in the process of an attack.

When most endpoint protection vendors attempt to recognize and react to malicious behavior, they are often fooled when such activity originates within a trusted supply chain application. AppGuard's preventative approach is different. It restricts activities within endpoints that can allow malware to execute a successful attack, placing roadblocks across various potential attack stages. This approach ensures that even when the attack has not yet been detected there are protections actively blocking it from success. Supply chain attacks are difficult to detect because the malicious application is trusted. AppGuard provides protection without detection - even against those as sophisticated as the SolarWinds attack.

Outsmart Supply Chain Attacks with the Right Defense

The recent SolarWinds supply chain attack serves as a strong reminder that we are all part of someone's supply chain and every chain has a weak link. Even trustworthy applications cannot be trusted. The SolarWinds incident demonstrates the significant impact software supply chain attacks can have, and the fact that most organizations are unprepared to prevent and detect such attacks. Organizations must adopt a Zero Trust approach to ensure endpoints and third-party software are free from malicious content. Those that do not are more dependent on finding needles in detection haystacks. The latter approach did not protect enterprises from the SolarWinds attack. Now, more than ever, companies must put in place defenses that will protect them from their most trusted applications, should they be compromised.

About AppGuard

AppGuard is a cyber security company on a mission to set a new standard: true cyber protection for all. AppGuard's patented technology prevents compromises before they happen by disrupting malware activity from causing harm without having to recognize it. Unlike detection-based solutions, AppGuard outsmarts malicious actors to ensure businesses can do what they need to do, and malware can't do what it wants to.

APPGUARD
The Malware Disruptor

www.appguard.us | sales@appguard.us