ActZero

TechTarget | Custom Media
White Paper

6 Steps to Secure Your IT Supply Chain

Cybercriminals are always looking for shortcuts to more easily attack businesses and maximize profit from hacking activities. Increasingly, smart cybercrooks are finding that if they can target a common, critical piece of IT infrastructure—whether software, hardware or remote cloud service—they can accomplish more with less effort.

This is the heart of an IT supply chain cyberattack: leverage a single backdoor in a piece of the IT supply chain that many, many companies use to compromise all their systems nearly at once.

In response, organizations need to put in the hard work to take a layered approach to minimize the risk that attacks against their IT suppliers will open them up to devastating breaches. This means not only taking preventative action to add better governance and security around the IT products and software code they use in their environments, but to also prepare layers of defense for when successful IT supply chain attacks provide attackers with footholds into their environments.

Organizations need to put in the hard work to take a layered approach to minimize the risk that attacks against their IT suppliers will open them up to devastating breaches.

This paper looks at some actionable, proven steps enterprises should take—right now—to better secure their IT supply chain against relentless and innovative attempts to leverage security gaps in those supply chains.

SolarWinds Solarigate compromise example

In the past few years, we've seen numerous examples of how IT supply chain attacks can play out in the real world. For example, Iranian state actors utilized vulnerabilities in industrial control systems to spy on other countries.[1] And the widespread exploitation of a flaw in a common open source component was directly tied to the massive Equifax breach in 2017.[2]

But we don't need to look very far back to find one of the most prime examples of how IT supply chain weaknesses can expose everyone to a lot of residual risk. The SolarWinds Solarigate compromise illustrates that software and hardware IT supply chain attacks are on the rise

1 "Iranian Cyber Espionage Group Targets Suppliers of Industrial Control Systems," Control Risks, Jan. 21, 2020

2 "How Hackers Broke Equifax: Exploiting a Patchable Vulnerability," Forbes, Sept. 14, 2017

as criminals perfect this technique for casting a broad, yet targeted net for cybervictims. SolarWinds is not the first and definitely will not be the last of these incidents, but to date, it offers the most clear-cut example of how all-encompassing an IT supply chain cyberattack can be across the technology world.

SolarWinds is an IT vendor that produces a suite of tools, called Orion, that is used by tens of thousands of businesses and federal agencies to manage their IT networks. SolarWinds officials explained in January that attackers managed to compromise the company's development environments to quietly install backdoor code into its products.[3]

The backdoor then gave attackers the keys to the kingdom within SolarWinds customer environments.

The fallout is ongoing and will snowball in 2021 and beyond. What we know now is that potentially 18,000 organizations were impacted by the attack. This includes heavy hitters like Microsoft, FireEye and the U.S .Department of Homeland Security, which all admitted they were successfully compromised by attackers using the SolarWinds Sunburst backdoor.[4] In fact, widespread zero-day attacks against a Microsoft Exchange server component by Chinese state actors have also been tied to the compromises of Microsoft source code that was triggered by the SolarWinds debacle.[5]

This is no isolated or singular incident. The lesson for IT practitioners from SolarWinds should be to expect more of the same. They should expect attackers to use sophisticated techniques like implanting backdoors in software that many organizations use; with the discovery of the SolarWinds incident, it should become clear that the widespread assault on the IT software supply chain is an inevitability. Attackers are perfecting their tactics against software and hardware suppliers by the day, manufacturing their own zero-day exploits defenders will be unprepared for.

3 "New Findings From Our Investigation of SUNBURST," SolarWinds, Jan. 11, 2021

4 "SolarWinds: What Hit Us Could Hit Others," Krebs on Security, Jan. 21, 2021

5 "China's and Russia's Spying Sprees Will Take Years to Unpack," Ars Technica, March 6, 2021

Why securing your IT supply chain is crucial

Historically, IT environments have always consisted of a number of platforms, software and systems from a range of vendors. But in the cloud and IoT era, and especially in a time of digital transformation, the external IT pieces provided by third-party suppliers have grown more interconnected and vulnerable to attack than ever before.

IT depends more and more on software as a service (SaaS) rather than homegrown software. Whether software is internally developed, a commercial off-the-shelf product or a cloud service, almost all of it tends to be composed of a patchwork of different readymade componentry and APIs, both closed and open source. In fact, according to recent figures, the average enterprise software today contains 203 different third-party code dependencies.[6]

Whether at the level of code, application, platform or even hardware, dependency on other companies' technology opens up organizations to risk. At each juncture, these suppliers of the building blocks of the modern IT environment offer potential threat avenues of exposure to hackers, opening their products to compromises like SolarWinds Orion.

As attacks against these building blocks increasingly become a key part of threat actors' playbook, taking proper steps to secure the enterprise's IT supply chain is crucial to maintaining an effective cybersecurity program. Ideally, organizations should be doing that in such a way that they aren't reactively responding to every headline-inducing supply chain attack but instead have all of the protections and defenses in place to know their risks are already mitigated in numerous layers. Here's what it takes to start moving toward that state.

STEP ONE: Inventory and manage IT assets

Organizations need to know quickly when a named vulnerability like Ripple20[7] or a highly impactful backdoor like SolarWinds Sunburst affects their infrastructure. This can't happen if IT and business leaders don't have a thorough understanding of what is running in their environments and which service providers can connect to or are closely integrating with the enterprise's systems.

6 "The 2020 State of the Octoverse," GitHub, December 2020

7 "Ripple20: 19 Zero-Day Vulnerabilities Amplified by the Supply Chain," JSOF, 2020

Documenting and continuously keeping tabs on the configuration state of the hardware and software asset portfolio prepares organizations to quickly identify where the risk of IT supply chain attacks may occur. This can be a tall task when done manually, so leveraging an automated tool is crucial here.

When paired with regular cybersecurity risk assessments, IT asset inventories can also help security strategists understand where best to reconfigure or add security controls to their architecture to mitigate supply chain risks.

STEP TWO: Monitor third-party risk

A big part of IT supply chain security is keeping tabs on how much risk vendors are introducing to the environment. The U.S. Department of Defense's Cybersecurity Maturity Model Certification and audits of providers' CMMC levels can help provide point-in-time snapshots of vendors and service providers.

For more continuous views, particularly in the case of cloud services, some enterprises may consider using a third-party risk management platform to keep tabs on the state of security at vendors and other partners that connect to the organization's systems or handle its data regularly. This works best when companies use that feed to integrate third-party risk management into vendor management practices, with a focus on working with suppliers to drive down the risks that SaaS and cloud services introduce to the enterprise's environment.

STEP THREE: Address software supply chain hygiene

As organizations work to secure their application layers from IT supply chain attacks, software hygiene will play a big part in the process. For commercial and SaaS software, this starts with strong vulnerability and configuration management practices, aided by the asset inventory discussed above. Supplementing this with rigorous audits and penetration tests can ensure that known and unknown flaws in the software and configurations are dispatched quickly.

In the meantime, for companies engaging in internal development or extensive integration and customization of their software ecosystems, software supply chain management practices are crucial. This starts by developing and managing a bill of materials to thoroughly understand the library and component dependencies—open source or otherwise—that software utilizes under the hood.

Stepping up the maturity of code repository management and offering greater governance over the components and APIs that their developers can pull from can help organizations make significant headway in reducing software supply chain risks.

Too many companies today have very flat networks that make it easier for the bad guys to use a breached foothold to tap into the most sensitive systems and data.

STEP FOUR: Segment the network

When supply chain attacks do get through, many threat actors find it trivial to move laterally from their first point of incursion on the network—be it a supplier's compromised platform or software—into a more sensitive part of the network.

Too many companies today have very flat networks that make it easier for the bad guys to use a breached foothold to tap into the most sensitive systems and data. If enterprises want to limit the blast radius of IT supply chain attacks, they've got to make it harder to traverse the network. This is why network segmentation is such a crucial step for minimizing the impact of supply chain attacks.

While it might be beneficial to plan ahead for micro-segmentation or zero-trust initiatives, organizations don't need to get hung up on these multiyear initiatives before they can start reaping the benefits of segmentation.

If the network is flat or only broadly segmented, enterprises should start with the basics, introducing more (and smaller) traditionally partitioned network segments before making longer term plays for new sophisticated security architectures. Not only does this preventative measure minimize the damage supply chain attackers can inflict when they're successful, but it also reduces the scope of implementing more in-depth security defenses around the most important IT assets. The more sensitive a segment, the more controls an organization can layer around it.

STEP FIVE: Reduce your attack surface

In addition to basic security hygiene practices like patching and vulnerability and configuration management, organizations should consider reducing their attack surface by deploying only the software and functionality they need, reducing the amount of software open for remote access and adhering to least-privilege principles for account access to that software. The less functionality that's running and available for access, the fewer opportunities attackers have to leverage it in their supply chain attacks and lateral movement.

This kind of threat surface reduction can include enabling the software restriction policy in Windows, uninstalling unused software, turning off or uninstalling unused features and functions, and minimizing external communications wherever possible. Similarly, it's important to root out hardcoded passwords and default accounts from systems—particularly within privileged accounts. Organizations should also keep tabs on and minimize remote access. Don't forget about cloud, reverse shell and remote administration points of exposure when doing this work.

The philosophy should be to think of abuse cases rather than use cases and try to limit exposure to them.

STEP SIX: Monitor the environment

Circling back to step one, asset inventorying is so important because it provides the foundation for monitoring the environment on a number of levels. First of all, the inventory will give an organization a blueprint for continuously monitoring versions of software, configuration states and updates that will need to be made in response to supply chain security problems. Second, the inventory helps security strategists understand where to collect data and set telemetry to gain visibility into what is going on within the assets.

Without visibility into those assets, it is difficult to know whether a threat actor is already operating in an environment or to go back and trace an intrusion based on new intelligence.

Thorough data collection of a robust body of logs across the networks and endpoints is vital to forensics and incident response when big supply chain attacks are identified, and ideally, it can arm threat hunters to do more proactive searches for the attacks no one knows about yet.

Organizations should think critically about who or what is monitoring those telemetry feeds and how. If monitoring is carried out by a single analyst poking through the SIEM, odds are that analyst is not going to be able to sift through false positives fast enough to make a difference. AI-backed threat detection will play a role in speeding up detection time and triaging IT supply chain threats and incidents. It should also be stated that it is difficult to know if a threat actor is already operating in your environment without the right visibility into those assets.

Conclusion

Ultimately, organizations can't simply buy their way out of the problems posed by sophisticated supply chain attacks. If it were as easy as buying a tool, that would be the hottest selling security tool on the market. Instead, organizations must roll up their sleeves and get to work, taking the measures described above to reduce the likelihood of an attack landing, as well as speeding up the detection of them via proactive monitoring and rapid response.

ActZero can help organizations cover the most important of these steps. ActZero makes companies more secure by empowering IT and security teams to cover more ground with fewer internal resources. This means companies seeking to wrap their arms around IT supply chain risks can count on ActZero to help them:

- Institute the kind of telemetry and log collection they need to respond to the latest supply chain attacks
- Integrate public and private intelligence feeds into their security functions to stay alert to the latest techniques used by IT supply chain attackers
- Regularly scan IT assets for known vulnerabilities that need mitigation
- Actively monitor the telemetry in IT environments 24/7 for signs of attacks against known and unknown vulnerabilities
- Engage in threat hunting aided by artificial intelligence to respond at machine speed to newly developing IT supply chain attacks

ActZero makes companies more secure by empowering IT and security teams to cover more ground with fewer internal resources.

ActZero combines threat hunting expertise with emerging AI and machine learning technology to help customers identify more vulnerabilities more quickly, proactively recommend and prioritize actions to seal gaps, rapidly contain and remediate threats, and ultimately harden customers' cybersecurity posture. All of this can greatly help enterprises prepare for IT supply chain attacks now and in the future.

ActZero

About ActZero

ActZero challenges cybersecurity coverage for SMB and mid-market companies. Intelligent MDR provides 24/7 monitoring, protection and response support that goes well beyond other third-party software solutions. Our teams of data scientists leverage cutting-edge technologies like AI and ML to scale resources, identify vulnerabilities and eliminate more threats in less time. We actively partner with customers to drive security engineering, increase internal efficiencies and effectiveness and, ultimately, build a mature cybersecurity posture.

Whether shoring up an existing security strategy or serving as the primary line of defense, ActZero enables business growth by empowering customers to cover more ground.

ActZero | ActZeroAI | ActZero.ai

---

www.ActZero.ai/contact

TORONTO
207 Queens Quay, Suite 820
Toronto, Ontario M5J 1A7

MENLO PARK
2882 Sand Hill Road, Suite 115
Menlo Park, California 94025

SEATTLE
925 4th Ave., 20th Floor
Seattle, Washington 98104

This content was commissioned by ActZero and produced by TechTarget Inc.