Devolutions

SolarWinds & Solorigate: What Happened, Why it Matters & What Happens Next

THERE ARE SO MANY DATA BREACHES THESE DAYS

There are so many data breaches these days, that they all seem to morph together into an endless cycle of cyber destruction. Indeed, we have gone from being shocked at stories about hacks (remember Target and Sony?), to seeing them as kind of predictable — like another scorching day in the middle of a heatwave, or a frigid day in the middle of an extreme cold spell.

But then, every once in a while, there is a cyberattack that captures global attention due to its sheer scope, severity, size, and singularity. **Of course, the hack that checks all of these boxes is Solorigate.**

About the Attack

SolarWinds is a U.S.-based company that develops software for large enterprises and government departments, in order to help them manage their networks, systems, and IT infrastructure. One of the company's products is called the SolarWinds Orion Platform, which is a scalable infrastructure monitoring and management platform. The good news is that many organizations use this product to simplify their IT administration for on-premises, hybrid, and SaaS environments. The bad news is that hackers identified and exploited a weakness — and put in motion what is now being hailed as the most sophisticated hack ever.

In September 2019, hackers infiltrated SolarWinds' corporate servers, and inserted malicious code into "SolarWinds.Orion.Core.BusinessLayer.dll", which was a code library belonging to the Orion platform. In March 2020, as part of a software update, this compromised DLL was distributed (via an automatic platform) to around 18,000 of SolarWinds' supply chain customers around the world. This effectively created a backdoor that Microsoft security researchers dubbed "Solorigate" (note that the backdoor is also referred to as "SUNBURST", which is the name given by FireEye security researchers who discovered it in December 2020).

Once the backdoor was established, hackers began stealing credentials and moving laterally to hunt for high-value assets and accounts. The attack persisted for more than half a year, when it was discovered by FireEye researchers in December 2020.

The game changer with Solorigate was that hackers used SolarWinds' supply chain to infiltrate some very high-profile victims, which (so far) includes:

- The Pentagon
- The Department of Homeland Security
- The State Department
- The Department of Energy
- The National Nuclear Security Administration
- The U.S. Treasury
- Microsoft
- Cisco
- Intel
- Deloitte
- The California Department of State Hospitals
- Kent State University

- FireEye
- Palo Alto Networks
- Mimecast (this was just announced in late January 2021, and allegedly has impacted 10% of Mimecast's 36,000 customers — learn more here).

Who's to Blame?

There is speculation that the Russian government is behind Solorigate. And in January 2021, Kaspersky released an analysis suggesting a similarity between Solorigate and another backdoor called Kazur, which has been linked to the Russia-based Turla Advanced Persistent Threat (APT) group. These allegations have yet to be proven, and naturally it is necessary to get the facts before drawing any conclusions. However, we can see that the goal of Solorigate was to generate intelligence over a long period of time. This surveillance-type of cyberattack is typically sponsored by governments.

It is also important to note that, at this time, there is no proof that the attack was related to negligence at SolarWinds — though the investigation is ongoing, and more details will certainly be revealed in the coming months.

What Organizations Need to Do

There is no way that organizations can suddenly stop using third-party cloud-based software, products and apps, since these kinds of solutions are embedded in the organization's infrastructure — and not just among high-profile enterprises and government agencies. SMBs rely heavily, and in some cases exclusively, on third-party SaaS offerings. And so, the only practical response is to mitigate the risk. **To that end, we recommend adopting the following strategies:**

1. Conduct Rigorous Vendor Evaluation

When evaluating vendors, companies obviously focus on things like offerings, technical support, implementation, pricing, and so on. But there is another critical aspect that must be part of the process: compliance.

Specifically, companies should conduct a vendor risk assessment that takes a much deeper dive into cyber supply chain security. In an article for TechRepublic.com, Nick Fuchs, the senior director of infrastructure, security, support, and controls at Springfield Clinic, advises organizations to ask the following questions:

- Does the vendor regularly test the strength of their cybersecurity resilience, and provide evidence of latest source code scan and/or application penetration?
- Does the vendor have application firewalls or network segmentation in place to restrict access to application programs or object source code?
- Does the vendor comply with relevant policies and/or regulations (e.g., SOC 2, GDPR, CCPA, NIST, COBIT, ISO-27001/2), and can they provide evidence of up-to-date certification?
- Does the vendor have an employee security awareness program? The answers to these critical questions will significantly reduce risk exposure by identifying vendors (and their associated software, products, apps, etc.) that should be avoided.

However, it must also be acknowledged that even with rigorous vendor assessment, supply chain attacks (like Solorigate) are typically discreet, and quietly gather data for long periods of time. As pointed out by TechTarget: "Often, security teams won't identify these needles in the haystack until the attackers begin taking next steps. That is why, when it comes to supply chain risk, proactive threat hunting is really the art of exploring everything in your network that you don't completely trust."

2. Implement Zero Trust Security

Zero Trust architecture leverages network micro-segmentation to move the perimeter in as close as possible to privileged apps and protected surface areas. As such, even if hackers breach a device, they will not "hit the jackpot" and move laterally across the network. Best practices for implementing Zero Trust include:

- Add prioritized cloud technologies to replace unauthenticated legacy services and systems.
- Design Zero Trust architecture based on how data moves across the network, and how users and apps access sensitive information.
- Verify trust upon access to any network resource using MFA in real-time.
- Organize users by group/role to support device policies.
- Use automatic de-provisioning, along with the capacity to wipe, lock, and un-enroll stolen or lost devices.
- Regularly update end user rights based on changes to roles/jobs, as well as changes to prevailing security policies and compliance requirements.
- Educate and coach end users to be part of the solution in the new Zero Trust environment (this is part of the "employee security awareness program" that Nick Fuchs advised above).

In addition, Martin Kuppinger, the Founder and Principle Analyst of KuppingerCole Analysts, is warning organizations in the aftermath of Solorigate that they must extend zero-trust beyond networks and security systems, and apply it to all types of software. To do this, Mr. Kuppinger advises five measures to continuously enforcing software security:

- Implement secure design and coding practices, including modern software testing principles.
- Fully track and analyze re-used code such as open-source libraries, in order to determine where it is used, which version is in use, if there are any known vulnerabilities and patches, and what coding practices are being used by those who supply the code.
- Conduct static and dynamic code analysis, in order to detect security issues within code. This analysis should also be extended to areas like API design.
- Integrate all organizational controls into a comprehensive Information Security Management System (ISMS), which is characterized by clearly defined and enforced controls.
- Expand operational analytics to include security telemetry and forensics, as this can help spot anomalies in software.

As Mr. Kuppinger prudently advises: "Zero Trust must be extended and cover software security, for software in any form (embedded, COTS, as-a-service) and regardless of whether it's home-grown or externally procured. Don't trust. Verify' – this is as essential for software as for identity, devices, or networks."

3. Enforce the Principle of Least Privilege (POLP)

A recent ESG survey revealed that overly permissive privileges are the most common attack vector against cloud applications. To mitigate this risk, all organizations should implement POLP. This is a policy in which end users are given only the amount of access they need to carry out their jobs — nothing more.

4. Audit and Monitor Privileged Accounts

Privileged accounts represent one of the biggest attack surfaces, and as such organizations need to mitigate threats and risks in two integrated ways.

First, organizations must audit all accounts and determine which ones legitimately require privileged access, and which ones don't. Research has found that 88% of organizations with more than one million folders lack appropriate access limitations, and 58% of companies have more than 100,000 folders accessible to all employees.

Second, organizations must monitor all privileged sessions, in order to proactively identify suspicious behavior and analyze patterns that may suggest credential theft. As Solorigate demonstrated, hackers who target supply chains go to extreme lengths to hide their traces and avoid detection. Monitoring privileged sessions can reveal subtle clues that lead to a major crime.

To achieve both these objectives — i.e., auditing and monitoring privileged accounts — organizations should use a robust PAM solution, which isolates the use of privileged accounts and reduces the risk of misuse. In this way, every system has its own account. If any particular system is breached, then hackers will not be able to leverage or gain access elsewhere. PAM also supports built-in two-factor authentication, role-based access control, logging, and reporting, and account brokering (so end users never need to see passwords).

5. Take a Defense-in-Depth Approach

Defense in Depth adds multiple diverse controls in an environment that creates layers of security. Just like an onion, an attacker would have to peel its way to the heart. It is a means of slowing down attackers as much as possible using a variety of intricate defenses between networks and systems.

6. Implement Segregation of Duties

Segregation of Duties (SoD) is a policy that forbids a single individual from being responsible for carrying out conflicting duties. The essential purpose, as highlighted in the ISO/IEC 27001 framework, is to reduce opportunities for either the unauthorized or unintentional manipulation or misuse of organizational assets. Basically, when multiple people are involved in a sensitive workflow, there is a smaller chance that anyone will try to break the rules, or for mistakes to go undetected.

SoD has been used for many decades in accounting, risk management, and financial administration. However, in recent years the concept has moved into the cybersecurity space to:

- Prevent conflicts of interest (real or apparent), wrongful acts, fraud, abuse, and the building of secretive "silos" around activities.
- Detect control failures, such as security breaches, information theft, and circumvention of security controls.
- Prevent errors from taking place due to employees wearing "too many hats".

From the Desk of our CSO Martin Lemay:

If there is a lesson to be learned with the SolarWind's incident, it is that no matter who the partner is in their supply chain, your organization must consider the risk of compromise. This concern should be as strong as availability considerations.

Assuming a breach while assessing risks for the use of a new product or service is mandatory, in order to ensure that the security deployed around those offers is proportional to risk exposure. And while a good vendor management process might prevent probable risks from a less security-mature provider, it is definitely not bulletproof and can be compromised by sophisticated (and even non-sophisticated) actors.

In fact, even after implementing all of the above strategies — which should be seen as musts and not options — your organization still might be exposed to some residual risks, and not have the 100% assurance that you want. Does this mean that the game already over and the hackers have won? No, and here is why:

I often hear people argue that if Microsoft and the US government cannot prevent a threat like Solorigate, then what hope do smaller organizations have? Is it worthless to invest money and time on controls that even the biggest and wealthiest organizations out there cannot prove are 100% effective? To those people, I ask: "Do you leave your car unlocked just because a burglar might break a window?"

My point is that some efforts to reduce probability or impact are certainly worth the trouble, given the potential consequences around responding and recovering from an incident. The problem is not necessarily to lose the car, but everything else that is associated with that loss. This statement does not apply solely to supply chain risks, but for any risk. Perhaps ransomware is more important than supply chain for your organization, and that is perfectly fine. But asking for transparency to a vendor or a service IS FREE — just like locking up a car after a drive.

After considering the supply chain risks that exist, your organization might be surprised to discover how some controls are not THAT costly and time-consuming to implement and maintain.

Conclusion

While there are still many unanswered questions, one thing is certain: there will be many more supply chain attacks in 2021 and the years ahead. Hackers are notorious for doing things over and over again until they stop working. And unfortunately, the Solorigate attack was a massive success. It not only compromised some of the world's biggest organizations, but it persisted for seven months before being detected — and even then, the

discovery was made by a private cybersecurity firm (FireEye) and not the U.S. Cyber Command, which admits that it was "blindsided" by the attack.

Will implementing the above strategies eliminate the threat of a supply chain attack? No, because that is not possible. But they will significantly mitigate the risk, and may also limit the duration and severity of a breach. All organizations are therefore urged to make fortifying their cybersecurity — not just for supply chain attacks, but all threats — their number one priority. As the old saying goes, "An ounce of prevention is worth a pound of cure!"