Understanding the SolarWinds Supply Chain Attack

When the public became aware of an advanced persistent threat (APT) responsible for compromising the SolarWinds Orion software supply chain in December 2020, experts were quick to warn it would likely be years – maybe decades – before the fallout could be fully accounted for. The more we learn about the attack, however, the more it seems we may never know the full extent of its damages. As speculation continues to abound, witness testimonies delivered in the February 23, 2021 Senate Select Committee on Intelligence provided a few critical insights.

- This was a highly sophisticated identity-based supply chain attack executed via a "backdoor" into a SolarWinds update server, likely aided by password spraying.
- The attackers were able to bypass multi-factor authentication and move laterally within the network, posing as regular users.
- Information stolen from those systems and malware left behind by the hackers will likely be used for follow-on attacks, including account takeover.

Given the targeted, surgical nature of this attack, no single security solution could have prevented it. However, witness testimonies during the Senate hearing highlighted the importance of identity and password security. Using these testimonies, SpyCloud was able to map our solution to the primary attack phases – Compromise, Distribution and Aftermath – to show how and where we could have helped.

Timeline of the Attack

1. Compromise

While the initial entrypoint that attackers used to gain a foothold within SolarWinds' network is still under investigation, media outlets and security experts have speculated that it may have been an exposed server, unpatched software, or **even simple account takeover using password spraying or stolen credentials.** Once inside, the attackers were able to modify the build process and inject malicious code into versions of SolarWinds' Orion software platform released between March and June of 2020.

2. Distribution

Over 18,000 organizations downloaded the malicious update, leading to known compromises of at least 9 federal agencies and over 100 private sector organizations. Attackers used their access **to steal identities and tokens to impersonate real users, sidestep multi-factor authentication**, and extend their foothold within affected networks.

3. Aftermath

Senate testimonies emphasized that more victims and follow-on attacks will emerge over time. Additionally, the mountain of identity data the attackers harvested means it can now be **loaded into additional password spraying and credential stuffing tools to target individuals and services**, such as payroll services and code repositories, in the future.

1 Compromise

> *"We believe the Orion platform was specifically targeted by this nation-state to create a backdoor into the IT environments of [our] select customers. The threat actor did this by adding malicious code, which we call SUNBURST, to versions released between March and June of 2020. So, a three month window was when the malicious SUNBURST code was deployed."*
>
> ***- Sudhakar Ramakrishna, President & CEO, SolarWinds***

> *"This is the largest and most sophisticated sort of operation that we have seen."*
>
> ***- Brad Smith, President, Microsoft***

The Senate Select Committee on Intelligence testimonies made clear that investigators are still working to understand the details of this attack, including how attackers initially compromised SolarWinds. However, both the expert witnesses at the Senate hearing and the Cybersecurity and Infrastructure Security Agency (CISA) have pointed to **weak passwords** as a probable entrypoint.

According to CISA's alert, "Incident response investigations have identified that initial access in some cases was obtained by password guessing, password spraying, and inappropriately secured administrative credentials accessible via external remote access services."

Password spraying is a type of brute force attack where a cybercriminal uses a list of usernames and common passwords like "password1234" to try to gain access to a particular site. Once they get a match, the criminal may test that same username and password combination against as many accounts as possible.

> *"If I were to go back to where I'm from near Green Bay, Wisconsin, and I have 1,000 email addresses from people [there] and I just applied the password 'gopackgo,' I'll bet dollars-to-donuts there's a Green Bay Packers fan using that password."*
>
> ***- Brad Smith, Microsoft***

As Brad Smith's "gopackgo" example suggests, humans tend to be lazy about passwords; not only do we use obvious passwords that can be easy to guess, we also use them across multiple accounts. Attackers commonly exploit users' bad password hygiene to gain illegitimate access to their personal or corporate accounts.

1

In the case of the SolarWinds hack, it was widely reported that attackers successfully accessed a software build server using the password "solarwind123."

Whether or not this is the primary avenue the hackers used remains unclear. But it is a fact that the password had been in use as far back as 2017.

Ultimately, threat actors were able to use their access to introduce malware into SolarWinds' signed CI/CD platform, affecting specific versions of the SolarWinds Orion software platform, a popular suite used to manage networks, endpoints and IT infrastructure.

SpyCloud Can Help

With SpyCloud, you can combat password spraying by preventing users from setting weak or compromised passwords. When a third-party breach exposes your users' credentials, SpyCloud will automatically force your exposed users to change their passwords, before a criminal can take advantage of your employees' exposure.

In 2020 alone, SpyCloud recovered nearly 1.5 billion stolen credentials and operationalized them to protect hundreds of enterprises and over 2 billion consumers from account takeover and online fraud.

How many times has "gopackgo" appeared in SpyCloud's recovered breach data?

9,610 Exact Matches

18,566 Fuzzy Variations

Company names are even more common:

6 out of the **top 10** Aerospace & Defense employee passwords found in third-party breaches include a company name.*

2

Distribution

SolarWinds Orion software updates delivered the SUNBURST trojan to more than 18,000 customers, including major enterprises and government agencies. Immediately, the attackers began to harvest customers' identities and tokens, allowing them to bypass multi-factor authentication and extend their reach within victims' networks.

Breached PII Can Help Attackers Bypass MFA

In 2020 alone, SpyCloud collected:

4.6B PII ASSETS, INCLUDING:

1.2B Phone Assets

70M Secret Answers

> *"The attackers came in through the SolarWinds implant and **the first thing they did is they went for your keys, your tokens.** Basically they stole your identity architecture so they could access your networks the same way your people did. That's why this attack was hard to find; these attackers, from day one, had a backdoor, a secret door, to your house, and once inside, all of your keys were laying out there. They grab them and now they can get open any locks you have in your house the same way your people do."*
>
> ***- Kevin Mandia, CEO, FireEye***

The tactics these attackers used to bypass multi-factor authentication were sophisticated. However, criminals have many methods of sidestepping MFA at their disposal, including SIM-swapping, social engineering, answering security questions using exposed PII, and searching other stolen accounts for TOTP seeds.

MFA is a layer of protection – an important first step – but additional layers are required to safeguard the identities of the employees, consumers, and suppliers logging into your systems. If a user logs in with valid credentials (aka account takeover), the organization has no way to determine if the user is a criminal because the login doesn't 'trip a sensor.'

> *"The SolarWinds Orion software update was the principal initial vector for many of these attacks, but it was not the only entry into these houses. In some instances we have seen, the Russian actor used **aggressive password spray attacks** to gain access. A password spray is when an attacker attempts to log in using a variety of common or relatively simple passwords against many targets, knowing that someone in an organization is likely to have one of them as their password."*
>
> ***- Brad Smith, Microsoft***

Senate testimony also revealed that some customers had failed to follow basic cybersecurity measures, making it easy for attackers to extend their reach. In fact,

2

not all victims of this supply chain attack were compromised directly via SolarWinds Orion software. Once again, weak and compromised passwords played a significant role, accounting for the next most prevalent entrypoint into affected companies.

> *"We're doing Stage 2 investigations for our customers, and* ***the number one other way we're seeing these attackers break in is what's called password spraying.*** *[...] We have 3,300 employees at FireEye. I have to believe that some of them used their fireeye.com email to access dozens if not more of the apps on the internet. If any of the vendors get compromised and they use the same passphrase for amazon.com as fireeye.com, we may have a problem."*
>
> ***- Kevin Mandia, FireEye***

SpyCloud Can Help

SpyCloud enables you to detect and reset compromised passwords early in the breach lifecycle – before criminals have a chance to exploit them via password spraying and all the forms of MFA bypass mentioned above – along with automated remediation of those exposed credentials (making it less of a burden for you to keep your users safe). You can monitor not only your employees and consumers, but also third parties whose poor password security might put your enterprise at risk.

3

Aftermath

> *"SUNSPOT poses a grave risk of automated supply chain attacks through many software development companies since the software processes SolarWinds uses are common across the industry."*
>
> ***- Sudhakar Ramakrishna, SolarWinds***

With over 18,000 potentially-affected customers, the scope of the SolarWinds attack is unprecedented. Senate testimonies emphasized that more victims will emerge over time, and we can expect to see follow-on attacks. Other threat actors may exploit the same injector tool, SUNSPOT, to compromise software development processes in the future.

57% of people have reused passwords across more than one account, according to SpyCloud data

Targeted attacks account for 10% of ATO attacks and 80% of the losses

Based on the information captured from victims, the threat actors responsible now have an enormous database of individuals at affected customer organizations who they can target over time, representing a significant threat to these individuals and their employers. An attacker can load this information into password spraying and credential stuffing tools and attempt to compromise thousands of accounts at once.

For individuals with valuable assets, access, or influence, a motivated attacker might invest even more time and creativity in targeted attacks. Bad actors may go after victims' personal accounts, testing whether they've reused their corporate passwords at major banks, cryptocurrency exchanges, and credit card companies. Work-related accounts are also at risk; even if affected companies reset corporate-managed passwords, employees may have reused these credentials to protect third-party accounts used for software development, cloud hosting, human resources, customer relationship management, and more.

SpyCloud Can Help

The risk of targeted attacks is highest in the 18-24 months immediately after a breach occurs, while access to the stolen data is restricted to a tight circle of criminals. Because SpyCloud recovers and operationalizes data early – within days or weeks of the breach occurring – we are able to help enterprises identify stolen information swiftly and protect vulnerable users from targeted account takeover attacks. For high-risk employees, board members, and investors, SpyCloud provides the option to extend enterprise-grade protections to executives' personal accounts.

Conclusion

The full extent of the damage from the SolarWinds supply chain attack will take years to unravel. In the meantime, the incident has highlighted the significant role weak and exposed passwords can play in enterprise security.

Busy executives commonly choose simple passwords or reuse old favorites in order to remember their logins, a practice threat actors are well acquainted with.

In order to trust the identities of their consumers, employees, and third parties, enterprises must build early detection and remediation of exposed credentials into their cybersecurity strategies.

The SpyCloud Difference

SpyCloud is a SOC 2-compliant company that takes every precaution to keep your data secure. Our code goes through internal and third-party security reviews upon every major release, and our data is always encrypted in transit and at rest. Access to sensitive data is tightly controlled using appropriate identity and access management solutions.

SpyCloud's solutions, backed by the world's largest repository of recovered stolen credentials and PII, enable enterprises to stay ahead of account takeover by detecting and automatically resetting compromised passwords early, before criminals have a chance to use them.

Our customers continue to tell us their ability to prevent account takeover hinges both on access to relevant data (including the most plaintext passwords in the industry) and on being able to make that data operationally actionable through automation.

Employee ATO Prevention

Protect your organization from breaches and BEC due to password reuse.

Learn More →

VIP Guardian

Protect your highest-risk executives from targeted account takeover.

Learn More →

Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More →

Third Party Insight

Monitor third party exposures and share data to aid in remediation.

Learn More →

Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized purchases.

Learn More →

See Your Account Takeover Risk →

Discover how many breach records we have associated with your email address and your domain as a whole. Once you know, you can take action.