SolarWinds Hack: What Businesses Need to Know

By David Breg, Deputy Director, WSJ Pro Research
Last updated: 29 January 2021

Background:

Network management software company SolarWinds Corp. was compromised by an attacker in early September 2019, according to a statement by the company during ongoing investigations into the breach in January 2021.[1] The attacker hid malicious software in updates the company provided to customers from March 2020 onwards. Once the update was installed and the attackers had access to their victim's network, they exploited unpatched vulnerabilities in software from Microsoft Corp. and VMWare Inc. (and possibly other companies) to access and, presumably, steal data.

The tentacles of the attack are ever expanding and the possibility that Microsoft's products could have been used in other attacks was revealed on January 19 when anti-malware software firm Malwarebytes, which doesn't use SolarWinds software, said the same hacking group had apparently breached some of its internal emails by abusing access to Microsoft Office 365 and Azure software.[2]

Further confirmation that victims of the attack likely reach beyond SolarWinds customers came from Brandon Wales, acting director of the Cybersecurity and Infrastructure Security Agency, who said on January 28 that approximately 30% of the private-sector and government victims linked to the campaign did not have a direct connection to SolarWinds.[3]

> ***"It is absolutely correct that this campaign should not be thought of as the SolarWinds campaign."***
>
> **- Brandon Wales, Acting Director, CISA[4]**

U.S. intelligence agencies have attributed the attack to Russian intelligence services,[5] specifically a group known as Cozy Bear which has previously targeted U.S. and European government departments, think tanks, the Democratic National Committee (in 2016), and organizations involved in researching Covid-19 vaccines. Russia has denied any involvement.[6]

---

[1] The Wall Street Journal, 12 January 2021
[2] Malwarebytes Blog, 19 January 2021
[3] The Wall Street Journal, 29 January 2021
[4] Ibid
[5] The Hill, 5 January 202
[6] Reuters, 11 January 2021

The intrusion was discovered in December 2020 by cybersecurity company FireEye Inc., which was itself a victim of the attack. SolarWinds has approximately 300,000 total customers globally, [7] including nearly all Fortune 500 companies and many U.S. government agencies.[8]

According to SolarWinds, only users of the Orion software platform who loaded a March 2020 update may have installed the malicious code. SolarWinds estimates this pertains to roughly 18,000 customers.[9] The exact number of companies compromised by the attack will be difficult to determine, as several observers believe it could take a year or longer for organizations to determine if back-door programs were installed in their networks or if data was stolen.[10] However, a January 2 New York Times report said the attack has affected at least 250 federal agencies and businesses.[11]

The U.S. agencies in charge of intelligence and cybersecurity said on January 5 that the Trump administration had identified fewer than 10 federal agencies whose systems had been penetrated in the hack, with the departments of State, Treasury, Justice, Commerce and Energy among them.[12] Although the information came from different sources, it seems likely that most of the 250 entities cited in the New York Times report are businesses, including Microsoft Corp., Cisco Systems Inc., General Electric Co. and Equifax Inc.

Cybersecurity vendors Mimecast, Palo Alto Networks, Qualys, and Fidelis disclosed they experienced attacks in recent weeks and all had installed trojanized versions of the SolarWinds Orion app.[13] Additionally, cybersecurity firm Kaspersky found that nearly a third of the potential victims were industrial organizations in sectors such as manufacturing and utilities.[14]

"This threat actor is so good, so sophisticated, so disciplined, so patient and so elusive that it's just hard for organizations to really understand what the scope and impact of the intrusions are. But I can assure you there are a lot of victims beyond what has been made public to date."
- Charles Carmakal, FireEye Chief Technology Officer[15]

President Joe Biden's first week in office signalled a change from former President Donald Trump, who hasn't acknowledged the findings from U.S. intelligence and security officials that Russia is suspected to be involved in the SolarWinds attack,[16] as the new President ordered

[7] The Wall Street Journal, 18 December 2020
[8] The New York Times, 14 December 2020
[9] Security Boulevard, 18 December 2020
[10] The Straits Times, 5 January 2021
[11] The New York Times, 2 January 2021
[12] The Wall Street Journal, 6 January 2021
[13] ZDNet, 26 January 2021
[14] Kaspersky, 26 January 2021
[15] Computing, 20 January 2021
[16] Washington Post, 6 January 2021

U.S. intelligence agencies to provide him an assessment of the attack and Russia's possible role in it.[17] President Biden also raised his concerns over the attack during his first call with Russian President Vladimir Putin on January 26.[18]

The likely incoming Senate Intelligence Chair Mark Warner (D., Va.), who is planning hearings to address issues brought on by the Russian hacking campaign behind the SolarWinds attack, said that Congress will consider whether to require companies and possibly government agencies to disclose when they have been the victims of a breach.[19]

In what Microsoft described as "one of the most sophisticated and protracted" operations of the decade, the technology company reported on January 20 that the attackers managed to avoid detection for such a prolonged period by separating their most prized hacking tool from other malicious code on their victims' networks and effectively covering their tracks.[20] Microsoft had previously disclosed that the hackers were able to access the company's source code, but the account that had been penetrated didn't have the ability to modify code.[21]

A lawsuit has been filed against SolarWinds in the Western District of Texas on behalf of shareholders who acquired SolarWinds stock between February 24, 2020, and December 15, 2020. The lawsuit notes the value of SolarWinds shares dropped significantly in the days after the disclosure of the attack-- from nearly $24 per share to roughly $14 within a week. An investigation has also been launched to discover if SolarWinds executives had known about the breach before deciding to sell hundreds of millions of dollars worth of stock shortly before the hack was disclosed.[22]

Further Information:

The Cybersecurity and Infrastructure Security Agency released an alert on January 8 on detecting post-compromise threat activity that includes links to several free tools that can help identify indicators of the attack.[23] FireEye also released a free tool on January 19 called the Azure AD Investigator.[24]

SolarWinds issued a security advisory[25] and Frequently Asked Questions[26] on its website and the Department of Homeland Security issued an emergency advisory[27] and supplemental guidance detailing all affected versions[28].

[17] Cyberscoop, 21 January 2021
[18] The Wall Street Journal, 26 January 2021
[19] Washington Post, 15 January 2021
[20] Cyberscoop, 20 January 2021
[21] CNET, 31 December 2020
[22] Security Week, 6 January 2021
[23] CISA Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments, 8 January 2021
[24] ZDNet, 19 January 2021
[25] SolarWinds Security Advisory, 20 December 2020
[26] SolarWinds Security Advisory FAQs, 20 December 2020
[27] DHS Emergency Directive 21-01, 13 December 2020
[28] DHS Supplemental Guidance, 18 December 2020

Customers of SolarWinds should not assume that only the largest organizations or government departments have been targeted. SANS Institute[29] and Talos Intelligence[30], among others, have provided the following recommendations for businesses and organizations that are uncertain if their systems may have been compromised by the SolarWinds intrusion:

- Activate the incident response plan, decommission the software and examine data sources for indications of compromise.
- Be cautious if your business runs SolarWinds software even if it's not Orion and consider mapping your attack surface in case those were also compromised in the supply chain attack.
- Block access from network management software to the internet. If it is explicitly required, limit destinations according to zero-trust networking.
- Consider hiring a threat-hunting company to search for attackers on the network.
- Implement a third-party risk management program that covers any type of vendor access.
- Monitor for intrusions and be diligent about keeping a log. Companies that don't have logs spanning the nine months since the March intrusion are in an uncertain situation.[31]

Developing Situation:

The impact of this attack is not yet fully clear and it is likely the number of victims will grow over the coming days and weeks as affected organizations conduct investigations and incident response operations. Organizations should pay close attention to updates from both SolarWinds and the Cybersecurity and Infrastructure Security Agency[32].

This incident demonstrates the vulnerability of all organizations to sophisticated attacks and highlights the importance of being able to respond swiftly to mitigate damage.

David Breg is Deputy Director at WSJ Pro Research, focused on providing actionable intelligence for readers interested in learning about issues involving cybersecurity through white papers and other research activities. Dave has prior experience managing the research unit at public relations firm Burson-Marsteller and policy knowledge from serving as an analyst at the Congressional Research Service.

Write to Dave at david.breg@wsj.com

[29] SANS Institute, 15 December 2020
[30] Talos Intelligence, 14 December 2020
[31] Business Insider, 18 December 2020
[32] CISA Joint Cybersecurity Advisory, 20 December 2020