Proskauer

How to Respond to the SolarWinds "Orion" Supply Chain Attack

New Media and Technology Law Blog on **December 21, 2020**

As reported last week, it appears that a state-sponsored security hack has resulted in a major security compromise in widely-used software offered by a company called SolarWinds. The compromised software, known as Orion, is enterprise network management software that helps organizations manage their networks, servers and networked devices. The software is widely-used by both public and private sector companies.

The exposure, in the form of "spyware" inserted into one or more updates to Orion, is significant. According to an alert issued by the Cybersecurity and Infrastructure Security Agency ("CISA"), it is common for network administrators to configure Orion with pervasive privileges, which would allow it to bypass firewalls and other security measures, thus making it an enviable target for hackers. CISA categorized the SolarWinds attack as presenting a "grave risk" to government agencies and private entities.

The attack had been ongoing and undetected since perhaps March 2020 (or earlier, and certainly planned out for years). SolarWinds's SEC filings last week estimated that about 18,000 of its customers may have downloaded the malware-laden software update for Orion. However, the number of organizations impacted may be even higher. Orion may be part of a larger infrastructure implementation or managed service provided by third party service providers. And as a result, even entities that do not have a direct relationship with SolarWinds may need to investigate potential impacts.

It is important to note, however, that even though a business may have the malicious code integrated into their network, they may not yet have suffered an actual breach or intrusion. "Luckily," this actor seems to have taken great pains to remain concealed, and as a result, it appears that the perpetrators had not yet had an opportunity to invoke their ability to invade every impacted network in all potentially impacted cases.

While we are far from learning all of the various ways in which this backdoor was exploited, early anecdotal evidence suggests that these attackers were very interested in pivoting into other systems, including cloud-based systems, such as Office 365, that may not have any direct connection to a SolarWinds installation. While the disabling of the so-called Orion "Sunburst backdoor" and the confiscation of the original domain name that was receiving communications from the attacker should stop further data loss from the initial entry point, it will not stop further incidents if the attacker has already established persistent access within the network. Thus, it is important to note merely because an affected organization may have closed the initial vulnerability, it should not declare itself as contained too quickly as the hackers may have surreptitiously achieved persistent access beyond the Orion entry point.

There are two sobering consequences from this recognition. First, if an organization determines that it installed the corrupted version of Orion, an organization's investigation may need to be very broad in nature. Second, organizations may need to consider whether previous breaches that were resolved this year might, in fact, have had something to do with this issue that was undiscovered at the time of detection. Accordingly, it may be necessary to revisit prior incidents thought long resolved.

A Response Checklist

How should businesses respond to this development, and how should legal departments direct or support this response? This blog post spells out some of the specific steps that all potentially impacted organizations should consider. Note, these steps are not necessarily appropriate in all cases and for all organizations, and each entity should design its response as appropriate for its particular situation. However, the following thoughts are good starting point considerations for an organization as it plans and executes its incident response effort.

1. It is essential that businesses respond to this threat in an internally coordinated and thoughtful manner. To the extent a business has established processes and procedures for such circumstances, such as an incident response plan, they should be reviewed and possibly invoked. Such plans typically draw together all of the necessary expertise and authority within and external to the organization to evaluate and respond to the situation as it is currently understood and as new

facts are learned, and provide for input as appropriate from governmental resources and external experts. All activity responding to this incident should be coordinated across the various functions of the business (including IT, "business owners" of impacted systems (keeping in mind that if the attack is determined to span multiple systems, there may be different business owners), information security, legal, investor relations, compliance, public relations), all in accordance with the business' response plan. Given the sophistication of this attack, it is likely that an organization that has the compromised software will need to retain experts to assist them in the investigation. Care must be taken to ensure that these experts are properly retained, and, any investigations are properly scoped.

2. CISA issued an emergency directive for Federal agencies to follow. The directive spells out a number of exemplary technical steps to take to mitigate the risk of this incident and provides some specific indicators to look for to determine if data was accessed through the Orion-installed malware. This directive is one possible starting point for the response process, and businesses should evaluate which of the steps set forth therein are practical and applicable for them. Should it ever become necessary to defend the organization's response, reliance on materials such as these could be used by an organization defensively as proof of the reasonableness of its efforts.

3. For example, CISA advises federal agencies to evaluate which of their telecommunications systems use the Orion products at issue, and consider disconnecting from such system or blocking any connecting systems which use the Orion products as an immediate remediation step until longer term actions can be planned. While this is also an action that businesses should consider, alternatively, there may be less disruptive options available, such as restoring older versions of Orion, or installing newer, clean versions as they become available. There may be other ways to reasonably address the risk, and based on the input from qualified experts, an organization should consider which avenue of risk mitigation is right for its specific circumstances. Organizations should also consider whether compensating controls, such as enhanced network monitoring, are prudent to mitigate risk while a more permanent repair is designed and implemented.

4. In certain circumstances, an organization may need to evaluate whether it would be appropriate to invoke its business' disaster recovery plan or use disaster recovery or business continuity systems. Or do those systems also use Orion?

5. In cases where businesses either outsource the management of their telecommunications system to third party, use systems hosted by third parties or SaaS-based services, the business should evaluate whether it is necessary to reach out to their service providers to determine whether such third party uses

Orion and evaluate whether it would have been possible for motivated actors to pivot from such third party systems into the business' systems. Of course, in these circumstances, the contract between those parties should be reviewed by legal. Legal should also be involved in determining the particular details of those communications, including whether these communications should proceed business-to-business or counsel-to-counsel.

Beyond such communications, legal may need to review their agreements with their technology providers that may be, in part, responsible for any Orion infection, and consider what contractual remedies may be available to them. As a more general issue, businesses should implement more rigorous policies and procedures for the implementation of third-party software. These should be part of internal procedures and should be requirements for any third party technology providers. For more details on that, please see a companion post about SolarWinds-related issues on our *Privacy Law* blog.

6. To the extent a business has been impacted by this incident, it should (as may be required by law or contract), to the greatest extent possible, identify any specific data that has been accessed or acquired. Businesses should consider what notices are required to be issued pursuant to applicable law or contract and when those notices must issue.
7. Even to the extent not required by law or contract, businesses should consider how they will communicate to their community (including customers, business partners and employees) on this issue. Businesses should put together a response plan for such inquires based on input from amongst others, governmental resources, internal and external technical experts, public and investor relations experts and counsel. Businesses must keep in mind that the implications of this incident may include claims and assertions against the business by members of the community, notwithstanding the fact that the business itself is a victim of this incident, and thus all internal and external communications must be crafted with that in mind.
8. To the extent this incident or a business' response will interfere with business operations, the business should consider whether this may constitute a force majeure event under relevant contracts.
9. Impacted businesses should consider notifying insurance carriers of the potential claims arising from this event.

Final Thoughts

The forensic investigation into the SolarWinds hack and the mitigation efforts are still ongoing and will continue into 2021. Since the attack was undetected for months, and conducted by a sophisticated actor using advanced techniques designed for operational security and secrecy, affected service providers likely do not yet know the extent of infiltration (and, may never even discover the entirety of the scope). As noted above, given the sophistication of the attack and extent of unauthorized access (particularly given the nature of Orion software which analyzed company networks), the hackers may have had the ability to establish other access mechanisms and backdoors within the affected networks beyond the exposure that has already been detected, patched and disabled. Thus, the evaluation process promises to extend over a significant period of time. Staying abreast of developments, CISA advisories and advisories from other experts, alerts from major technology companies involved in the response and further communications from SolarWinds are important and will define further risk mitigation approaches. This process will continue as the extent of the incident is further clarified.

As part of the evaluation of the impact of this incident on any organization, it is important to remember to conduct the incident response and risk assessments under privilege whenever possible to minimize the generation of potentially harmful discoverable materials. Please see our discussion of that and related issues in a detailed post on the firm's *Privacy Blog*.

To learn more information about the SolarWinds attack and evolving cybersecurity threats, please visit the NSA's Cybersecurity Advisories & Technical Guidance. Additional information about this attack and emerging cybersecurity threats can be found in a recent post by Microsoft calling the cyberattack a "moment of reckoning."

View Original

Related Professionals

- **Jeffrey D. Neuburger**
- **Margaret A. Dale**
  Partner
- **Nolan M. Goldberg**

Partner