Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

A Strategy to Get Started with an Information Security Program

What Does the SolarWinds Data Breach Mean for Your Business?

Patrick Rost prost@dopkins.com

Published March 5, 2021 – There has been extensive reporting recently about the wide-sweeping impact of the data breach at SolarWinds, a global supplier of IT infrastructure management software. In this post, we will examine the implications the breach and what this incident may mean for organizations of all sizes and industries. For more about the cost of a data breach, read our February 2021 post.

Key Takeaways: Four Actions You Should Take Now

1. **Maintain an accurate software inventory.**
   Retaining precise records will allow you to quickly determine if you could be directly impacted by the recent SolarWinds breach.
2. **Verify if the vendors you outsource to are properly securing themselves.**
   All vendors, including cloud solutions, should be held to the same security standard as your own company.
3. **Implement and rely on your own risk assessment.**
   An updated risk assessment will help you determine the risk your organization faces in a more relevant manner than relying on news coverage of a high-profile breach.
4. **Apply critical security patches and updates.**
   Software vendors, like SolarWinds, release security updates after finding vulnerabilities in their products. Be sure to apply these updates as soon as possible.

SolarWinds History and Scope

We must know who the company SolarWinds is before we can fully understand the wide-reaching impact of this breach. In their own words, SolarWinds[1] is "a leading provider of powerful and affordable IT infrastructure management software." Headquartered in Austin, Texas, the company has over 3,200 employees worldwide, serving over 320,000 customers in 190 countries, including 499 companies from the Fortune 500 list. In addition, SolarWinds serves over 22,000 MSPs (Managed Service Providers) who in turn serve over 450,000 organizations.

Overview of the Breach

For a 15-month time period (September 2019 through December 2020), SolarWinds was unaware that their network was compromised. In addition, their client's networks were compromised because of their software for up to 10 months.

Current estimates are that 18,000 SolarWinds clients were affected by this software vulnerability, including at least 100 private sector businesses, nine (9) federal agencies, and six (6) cabinet level departments were specifically targeted. Government networks impacted by the breach included the

Commerce, Energy and Treasury departments, the Department of Justice and the Administrative Office of the U.S. Courts.

Let's get technical. Here's a breakdown of the 15-month timeline:

- Approximately 9/4/2019, a Threat Actor (TA) accessed the SolarWinds network.
- On 9/12/2019 the TA used malware named SUNSPOT to begin injecting the malicious code known as SUNBURST onto the Orion Platform, a product line offered by SolarWinds:
    - SUNBURST provides a backdoor into the system it is deployed on.
    - SUNBURST was injected during the build process so that when the Orion Platform product was compiled by SolarWinds it would be included in their signed update.
    - This would allow it to remain hidden to those who apply the update.
    - Using this backdoor the SUPERNOVA malware could be deployed on affected systems.
- On 2/2/2020 SUNBURST was compiled into the Orion Platform and began being deployed to customers.
- On 6/4/2020, the TA removed traces of malware in an effort to hide its tracks.
- This threat remained undetected, or at least not publicly disclosed, until 12/8/2020 when Kevin Mandia, CEO and Board Director at FireEye, a Cybersecurity firm, posted a blog[2] announcing that they had been the target of an attack.
- On 12/12/2020 FireEye notified SolarWinds that the attack came from their software using the SUNBURST vulnerability.
- SolarWinds made their first public announcement[3] about the breach on 12/17/2020.

Extent of the attack.

An attack of this size is unprecedented. In SolarWinds's January 11, 2021 update[4], company President and CEO Sudhakar Ramakrishna stated, "As we and industry experts have noted previously, the SUNBURST attack appears to be one of the most complex and sophisticated cyberattacks in history." In addition, according to a ZDNet article[5], Microsoft president Brad Smith called this attack "the largest and most sophisticated attack the world has ever seen." He goes on to explain that Microsoft itself was breached and that they tasked 500 engineers to look into the breach internally. He estimates that over 1,000 engineers would have been needed to conduct the attack. This led to a widely-held belief that this attack was carried out by a nation-state cyber operation, with many experts suggesting Russia as the origin. In SolarWinds' February 3, 2021 update[6], Sudhakar acknowledges the attack origin was a nation-state without naming a specific country.

Big Picture: How does this impact YOU?

In the course of running your business, the most important issue is how this incident may affect your company. Here are critical considerations you should think about immediately:

1. **Does your company use the affected products?**
   SolarWinds released a security advisory[7] with their affected products listed. If you use SolarWinds products and have not checked the advisory yet, you should do so immediately.
   Best Practice: Maintaining an accurate software inventory will allow you to quickly compare your software in use to the software listed in the advisory.

2. **Does your company do business with another company that has been affected?**
   Even if you don't use SolarWinds products, a vendor or other business associate may. It is important to require trusted business associates maintain proper security practices.
3. **Keep in mind, 30% of attacks had no direct connection to SolarWinds.**
   According to Brandon Wales, the acting director of the Cybersecurity and Infrastructure Security Agency (CISA), in an article by the Wall Street Journal[8], "Approximately 30% of both the private-sector and government victims linked to the campaign had **no direct connection to SolarWinds**." This means that companies other than SolarWinds must have been compromised in a similar way, indicating another reason that not using SolarWinds products doesn't guarantee you are safe from this threat.
4. **This attack was targeted, but you are NOT immune from being attacked by the common cyber-criminal.**
   A nation-state threat actor was actively attempting to compromise government and high-profile companies with a specific agenda. Is your company in a market and of a large enough size to warrant that attention? The biggest global threats may not always affect you, but you should not just take your cues from what is in the news.
   Why?
   If you don't believe you are a target for a nation-state, you are likely the ideal target for hackers who send out phishing emails and other attacks in an attempt to gain financially. These attackers target small-medium businesses indiscriminately hoping someone will fall for their tricks.
5. **Rely on your own risk assessment**
   To understand the risk you face you need to perform regular risk assessments. This will identify the actual risks to your company. You can then begin to make steps to manage the risks.
6. **Always apply critical security updates**
   SolarWinds released an update to fix this vulnerability after just three days. Software vendors regularly release security updates to help keep their product secure. Be sure to apply these updates as soon as possible.

In Closing: What's Next?

The extent of this shocking cyberattack will continue to be revealed for years, and may not ever be fully realized. A proactive approach to your organization's information security is more critical than ever to thwart these risks.

If you would like to have a conversation and discuss ways to mitigate the risk of a breach contact Patrick Rost (prost@dopkins.com). Check out our STARTegy page for more information about our Strategy for Getting Started with Information Security.

Read our other recent issues covering:

- **Cost of a Data Breach (February 2021)**
- **Working from Home (December/January 2021)**
- **Cybersecurity Awareness Training (November 2020)**
- **Data Backups (October 2020)**

[1] https://www.solarwinds.com/company/home

[2] https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

[3] https://orangematter.solarwinds.com/2020/12/17/solarwinds-update-on-security-vulnerability/

[4] https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

[5] https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create/

[6] https://orangematter.solarwinds.com/2021/02/03/findings-from-our-ongoing-investigations/

[7] https://www.solarwinds.com/sa-overview/securityadvisory

[8] https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601