Client Advisory

SolarWinds Update – February 2021

As we have learned since the event was first discovered in December, the breach of SolarWinds' proprietary network monitoring software, Orion, is unique in both character and deployment. On January 11, 2021, SolarWinds advised that the incident might have begun in September 2019, which is the earliest suspicious activity on their internal systems identified by their forensic teams[1].

It is believed that as many as 18,000 customers have been victimized, including government agencies and private networks. Furthermore, approximately 30% of both the private-sector and government victims linked to the campaign had no direct connection to SolarWinds, according to Brandon Wales, acting director of the Cybersecurity and Infrastructure Security Agency (CISA). The attackers "gained access to their targets in a variety of ways. This adversary has been creative," said Wales. "It is absolutely correct that this campaign should not be thought of as the SolarWinds campaign.[2]"

With each passing day, we are learning more about the ramifications of this supply chain threat, with the government warning of the effects and impact of the four malware strains identified thus far as Sunspot, Sunburst, Teardrop and Raindrop. In addition, it has been reported that malware separate and apart from the supply chain malware has been identified. Those strains are referred to as Supernova and CosmicGale malware. As fast as CISA, the DOJ and many other regulatory and private entities (such as Symantec who found the fourth strain on or about January 18, 2021) try to determine the extent of the hack, it is likely that the full extent will not be known for quite some time.

Notice Consideration

There has been considerable discussion in the insurance world as to whether companies that are, or are not, customers of SolarWinds should notify their insurers even where they have not seen any evidence of breach on their own systems. Here at McGriff, we believe best practice dictates that, after a discussion with your broker, and to the extent the policy provides language to do so, SolarWinds product users may be best served by giving notice to at least, the Cyber Insurer[3]; keeping in mind that on a "Claims Made" policy, providing notice to an insurer is a condition precedent for coverage.

To date, we know of one domestic cyber insurer that has drafted a SolarWinds exclusion and others may soon follow. Keep in mind that all markets are asking their policyholders, current and potential, to provide information about SolarWinds product usage as part of underwriting discussions. As such, placing your insurer on notice, if possible, is important especially if the policyholder is considering changing primary carriers and/or modifying its excess tower.

In addition to working with you to examine your cyber policy and reporting provisions, we think it is important to also consider the potential implications to your business if your vendors and/or suppliers are users of SolarWinds products.

Preliminary questions for your vendors:

- Are you currently running, or have you previously run, a known affected version of a SolarWinds product?
- Have you updated the affected products to the now current, unaffected version? If so, when?
- What actions are you taking to mitigate the risk of the systems being compromised?
- Are you aware of any suspicious activities or compromise of data related to this SolarWinds incident?
- Are you aware of any third parties with whom you share/transmit our data that currently use, or used affected SolarWinds products? If so, what data is shared with them and what mitigating activities are they taking related to this SolarWinds incident?

[1] Form 8-K filed by SolarWinds before the SEC on January 11, 2021.
[2] Wall Street Journal – January 29, 2021. https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601?mod=tech_lead_pos1
[3] Because each policy reads different, every notice letter sent to the Insurers is tailored to comply with the terms and conditions of the policy.

This large scale event will continue to develop and will likely influence the cyber insurance and reinsurance markets for some time. At a minimum, companies should be assessing their disaster recovery and incident response plans, testing them for effectiveness, and making appropriate improvements as part of a comprehensive, enterprise-wide resiliency plan.

To learn more about the potential impacts SolarWinds could have in the insurance industry please contact us:

Natalia Santiago
VP and Claims Manager
nsantiago@mcgriff.com
713.402.1410

Kieran Hughes
SVP, Senior Claims Counsel
Kieran.hughes@mcgriff.com
917.741.1512

Aarti Soni
Cyber Director & Product Innovation Counsel
aarti.soni@mcgriff.com
470.332.8367

Suzanne Gladle, ARM
SVP, Cyber Practice Leader
sgladle@mcgriff.com
315.750.6010

*The information contained in this document is provided for informational purposes only and should not be construed as a legal advice.