BEECHER CARLSON

PART OF THE BROWN & BROWN TEAM

SOLARWINDS HACK:
A PERFECT STORM CYBER HURRICANE OR A WAKE-UP CALL OF WHAT COULD COME?

A non-technical analysis for Risk Managers, Executive Leadership, and Boards

What We Know So Far

While the full details and broader impact of the SolarWinds Orion hack are still unfolding, one thing is known for sure; the impact of this wide-spread and potentially devastating attack by a highly sophisticated adversary could have easily become the worst-case scenario. Without regard to industry, geography, organization size, or any other discernable commonality, other than being customers of SolarWinds, this attack has left thousands of organizations and government agencies struggling to understand exposure, contain the attack, and remediate the vulnerabilities and potential backdoors created by the attackers. But will this cost businesses and cyber insurers billions of dollars in losses? Is it the "Cyber Hurricane" insurers have tried to avoid, or have we dodged the bullet?

The media and industry have and will continue to cover the details of this cyber event as they unfold in the coming days, weeks, and months, but it is clear that software supply chain attacks such as the one we are in the midst of unraveling are here to stay. These attacks represent unparalleled attractiveness to the attacker groups to scale their efforts and maximize their objectives, without consideration for collateral damage. Based on SolarWinds legal filings, more than 33,000 organizations, mostly large companies and government agencies, are users of the SolarWinds Orion platform – the compromised versions of its software have been installed by nearly 18,000 customers.

Historical Precedent and Incident Details

Software supply chain attacks are not a new phenomenon, and when the final financial impact of this current attack is understood, it will likely pale in comparison to the devastating financial impacts of previous attacks utilizing similar initial vectors. Consider the events occurring in June 2017: the NotPetya virus was released in the wild through a malicious backdoor implanted in M.E.Doc, an accounting software package used by almost every company in or doing business in Ukraine. The NotPetya event crippled major companies that are critical to the global economy for weeks as it ultimately tallied up over an estimated $10 billion in direct financial damages.

SolarWinds Orion Attack Timeline Summary

Tuesday | January 5, 2021	» Russia allegedly behind attacks
Thursday | December 31, 2020	» Microsoft acknowledges source code viewed by adversary
Wednesday | December 30, 2020	» Updated CISA guidance
Thursday | December 24, 2020	» Latest SolarWinds statement and patches
Tuesday | December 22, 2020	» U.S. Treasury Department email compromise identified
Thursday | December 17, 2020	» Leading IT service providers among those targeted » U.S. Nuclear Agency targeted
Wednesday | December 16, 2020	» Attack kill switch activated
Tuesday | December 15, 2020	» Initial attack victims identified
Monday | December 14, 2020	» SolarWinds SEC filing
Sunday | December 13, 2020	» CISA emergency directive, SolarWinds security advisory, FireEye disclosure, Microsoft guidance
Friday | December 11, 2020	» FireEye discovers SolarWinds was attacked
Tuesday | December 8, 2020	» FireEye suffers attack
March 2020 – June 2020	» SolarWinds attacked without knowing
November 2019 – March 2020	» Attacker preparation
October 2019	» Earliest identified modification of SolarWinds Orion software code

So, if there has been historical precedent for software supply chain attacks with financial damages and total insurance claims that exceed what is likely expected in this event, why has the SolarWinds attack shaken the security industry to its core? Why are news outlets and industry experts referring to these events as "A Perfect Storm"?

The level of sophistication and patience exhibited by this adversary has been extraordinary, and the extent of their feats will not be fully understood for some time. This was a targeted, methodical, and coordinated cyber espionage campaign utilizing highly advanced capabilities typically only seen by Nation States. Their objectives at this time seem to have been entirely focused on establishing persistence, maintaining stealth, gathering intelligence, and ultimately exfiltrating data. The initial selection of SolarWinds software as their vector for attack indicates that there was extensive reconnaissance done in advance to ensure entry was gained to the highest number of high value targets. Once a foothold was established in an estimated 18,000 organizations' environments, they appear to have been extremely selective in choosing which environments to pursue further action. (Currently, an estimated 50 companies appear to be victims of further action.)

In contrast to the NotPetya event of 2017, the SolarWinds attack was one that had clear mission objectives and detailed planning that was carefully followed. This attack was not seemingly motivated by financial gain, destruction, or as blast radius fallout of a targeted attack. While the financial impacts of the current event will likely not come close in size to previous events, financial impact is only one approach to future modeling of cyber threats.

"This was not a drive-by shooting on the information highway. This was a sniper round from somebody a mile away from your house," said Kevin Mandia, FireEye CEO, on Dec. 20, 2020 on CBS's "Face the Nation." "This was special operations. And it was going to take special operations to detect this breach." For all these reasons and more, this ongoing event has the security industry viewing this as a perfect storm event.

Ironically, the brazenness and targeted nature of the SolarWinds attack is precisely what led to its detection. By choosing to target FireEye, a leading cybersecurity consultancy and incident response firm, and one of a small group of private companies globally with the capabilities to detect and defend against such a sophisticated attack, the adversary wound up revealing themselves. Once that initial detection took place, FireEye's incident response capabilities were immediately mobilized to understand the nature of the attack and the vectors used. It was only through this investigation that the SolarWinds code compromise was discovered. Immediately, a coordinated investigative and response effort including government agencies, Microsoft, FireEye, SolarWinds, and others began leading to the identification of a kill-switch to the attack that was executed by Microsoft. While the investigation is still ongoing and new attacker techniques are still being identified and addressed, it was through this industry-wide partnership that future damages were hopefully mitigated.

Cyber Insurance Implications

The SolarWinds event has caused insureds to look back at their cyber insurance policies to understand whether they need to report a matter and what actions should be taken, if any. While insureds are assessing whether they utilize SolarWinds, if they ran the version that was compromised, and whether their systems were in fact breached, they are trying to determine the appropriate means of reporting this event to their respective cyber policies – as an incident, notice of circumstance, or none of the above. Meanwhile, insurance companies are looking at possible aggregation across their book considering the significant numbers of insureds providing notification of the event.

Whether or not SolarWinds becomes the "Cyber Hurricane" event that the insurance markets fear, it confirms the fact that such an event is a reality, as was proven by the NotPetya event of 2017. The extent to which cyber insurance policies will provide coverage will depend on the effect of the SolarWinds intrusion on the individual insured organization and the language of the cyber insurance policy.

As a SolarWinds compromise to a third-party service provider can potentially expose its clients if there is network interconnectivity, contingent business interruption and security liability provisions of policies may come to the fore. The appropriate time for a notification of circumstances or a claim will depend on the wording of the cyber insurance policy and the level of certainty companies have on whether the threat actors have breached their network and can cause damage. Understanding the analysis requires expertise in insurance policy interpretation and an understanding of the effect of the malicious code on systems. Beecher Carlson is committed to helping its clients with this combined analysis.

Where Do We Go from Here?

While the SolarWinds attack does not seem to be the financial "Cyber Hurricane" the global economies and cyber insurance industry fear, these events should be treated as a wake-up call for governments and organizations of all sizes across all industries. As displayed by the coordinated and rapid private and public sector response, some degree of parity with our cyber adversaries can only be achieved through ongoing collaboration with the common goal of a more secure global internet. This will require transparency and timely information sharing, joint intelligence gathering, comprehensive risk management throughout the supply chain, and following industry best practices.

Chris Keegan leads the Beecher Carlson Cyber and Technology Practice and places network, privacy, technology, and media E&O insurance for companies in a variety of industries including financial institutions, authentication providers, manufacturers, healthcare, retail, and telecommunications companies. He has also executed cyber information risk assessment projects and worked with regulators on evaluation of E-Business risks. He can be reached via email at ckeegan@beechercarlson.com.

Oren Wortman leads the Cyber Advisory team, helping customers better understand their maturity and risk exposures and enabling them to make quantifiable and fact-based decisions relative to cyber risk treatment. He has specific subject matter expertise in information security, technology and cyber risk management, conducting cyber maturity and regulatory assessments, governance, and overall security program development. He can be reached via email at owortman@beechercarlson.com.