Client Alert: Urgent Security Advisory – SolarWinds® Orion® Breach

Beginning on Tuesday, December 8th, and continuing into the afternoon of December 14th, news services reported several high-profile cyber security incidents, including those at a cyber security firm and other organizations and institutions such as the Department of Homeland Security, the United States Treasury and the Commerce Department.[1] ***As the news developed, it became clear that all of the incidents appeared to share a common attack vector: the successful supply-chain compromise of a security tool developed and distributed by Austin, Texas-based IT company SolarWinds.***[2]

Overview. While this situation continues to develop, based on government advisories, releases from SolarWinds, and reporting from the threat intelligence community, here is what is known to date:

- The attack on SolarWinds is apparently a targeted supply chain attack attributed to foreign nation state threat actors. The attackers embedded malicious code into SolarWinds' Orion product before its release to clients. Any client that installed an impacted version of Orion was then vulnerable to the exploit of the embedded malicious code.
- The threat actors trojanized SolarWinds' Orion business software updates in order to distribute malware to corporate and other enterprise end-users.
- The impacted software is SolarWinds® Orion® Platform software builds for versions **2019.4 HF 5** and **2020.2 *with no hotfix installed*** or **2020.2 HF 1**. (Source: SolarWinds Security Advisory, updated December 15, 2020, 8:00am CST).
- Companies, non-profits, and other organizations around the world that utilized the impacted SolarWinds software are at risk, as the software would potentially allow the threat actors to access their networks and compromise credentials.
- According to reports, once compromised, the threat actor appears to leverage multiple techniques within an end-user environment to evade detection and obscure their activity.[3] Each attack also appears to have been customized, tailoring malicious hostnames to match naming conventions within the target's environment.
- Further reports indicate that the campaign is widespread, affecting public and private organizations around the world.[4]
- This campaign may have begun as early as Spring 2020 and is currently ongoing.

Are you impacted? Based on the SolarWinds advisory updated as of December 15, 2020, if you had Orion Platform versions **2019.4 HF 5** and **2020.2 *with no hotfix*** or with **2020.2 HF 1** installed in your environment (see the list of "Known affected products" on SolarWinds' website), your network is possibly impacted by the presence of the exploit and may have been subsequently compromised by the threat actors.

Foreign nation state threat actors have been seen using the impacted software to gain an initial foothold into the network. Once the threat actor gains access to the network, they could escalate their access to global administrative user rights. The threat actor could leverage the global administrative user rights to impersonate any user, including administrative users, on the network. Once the threat actor has successfully acquired this level of control and authority on a network, they could move within the company's network, including to cloud infrastructure if the network extends to that space.

What should you do? If you have or had a trojanized version of SolarWinds Orion on your infrastructure, Stroz Friedberg advises that you take a risk-based approach to the situation. Specific steps to act upon and consider should include:

1. Install the SolarWinds update patch. However, while patching SolarWinds is an essential part of the process, it is not the end of the work needed. "Fixing" the initial entry point and not investigating to fully understand the extent of the incident will leave your organization in the dark about impact. Taking a risk-based approach to deal with this situation is advisable given the sophistication of the threat group associated with this complex attack.
2. Work with an incident response team to help you assess your unique situation. There is no single solution for clients across varied industries, with different internal resources available for remediation and investigation, different nation-state threat profiles, and different experience levels dealing with incidents, threats, and risks.
3. Perform a threat hunt and compromise assessment, including, but not limited to, a search for the known specific indicators of compromise (IOCs) associated with this exploit and attack.
4. Perform remediation immediately upon discovery of any indicators of compromise or exploits.
5. Practice diligent security monitoring at all times, but especially until all patches and updates are released (some are still pending), and until a compromise assessment is performed.
6. Continue to monitor the situation for additional developments, including new IOC releases, and new patches from SolarWinds.

Below are several resources to consider:

Microsoft Security Response Center – this resource provides technical details, including the methods leveraged by the actor believed to be involved in recent nation-state cyber-attacks, to enable the broader security community to hunt for activity in their networks and contribute to a shared defense against this sophisticated threat actor.

- **https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/**

Department of Homeland Security – the Department of Homeland Security published Emergency Directive 21-01 in response to this incident.

- **https://cyber.dhs.gov/ed/21-01/**
- Note DHS' requirement to "Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion" impacted versions. This is an important step to ensure preservation of artifacts to support a follow on investigation in furtherance of determining any impact of compromise.

SolarWinds – SolarWinds is advising its customers with any of the products listed as known affected for **Orion Platform v2020.2 *with no hotfix*** or **2020.2 HF 1** to upgrade to Orion Platform version **2020.2.1 HF 1** as soon as possible "to ensure the security of [their] environment." That version is currently available at customerportal.solarwinds.com. SolarWinds is also asking customers with products listed as known affected for **Orion Platform v2019.4 HF 5** to update to **2019.4 HF 6**, which is also available at customerportal.solarwinds.com. The SolarWinds Security Advisory can be found at **https://www.solarwinds.com/securityadvisory**

According to SolarWinds, companies that cannot upgrade immediately should follow the guidelines available for securing their Orion Platform instance on their website at: **https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-secure-configuration.htm**. The primary mitigation steps include having your Orion Platform installed behind firewalls, disabling internet access for the Orion Platform, and limiting the ports and connections to only what is necessary.

This is a developing situation that Aon's Cyber Solutions continues to monitor. We will provide more details as they emerge.

Contacts:

John Ansbach
Vice President
214.377.4566
john.ansbach@strozfriedberg.com

Cheri D. Carr
Managing Director and Cyber Solutions CISO
469.866.2478
cheri.carr@strozfriedberg.com

Heidi Wachs
Vice President
202.464.5813
heidi.wachs@strozfriedberg.com

Jonathan Rajewski
Vice President
802.238.8530
jonathan.rajewski@strozfriedberg.com

Sources

1. Sources: ZDNet, "FireEye, one of the world's largest security firms, discloses security breach." December 8, 2020; Washington Post, "DHS, State and NIH join list of federal agencies – now five – hacked in major Russian cyberespionage campaign," December 14, 2020.
2. Source: Wall Street Journal, "Suspected Russian Cyberattack Began With Ubiquitous Software Company," December 15, 2020.
3. Source: FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," December 13, 2020.
4. Source: Newsweek, "SolarWinds Says Hack Affected 18,000 Customers, Including Two Major Government Agencies," December 14, 2020.

About Cyber Solutions: Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon: Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Empower Results®