SolarWinds Data Breach Action Plan

Overview

Recently reported state-sponsored cyberattack (actors UNC2452) targeting U.S. interests in a widespread cyberespionage campaign has compromised SolarWinds' Orion Network Management Products and poses risks to the security of federal and commercial networks. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an emergency directive to federal and civilian agencies to review their networks for suspicious activity and to disconnect or power down SolarWinds Orion product immediately.

SolarWinds' networking and security products are used by more than 300,000 customers worldwide, including Fortune 500 companies, government agencies and education institutions. It services major U.S. telecommunications companies, all five branches of the U.S. military, and other prominent government organizations, including the Pentagon, State Department, NASA, National Security Agency (NSA), Postal Service, NOAA, Department of Justice, and the Office of the President of the United States.

SolarWinds Orion IT monitoring and management software SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third part servers. Set up as a supply chain attack, the event took advantage of trojanized SolarWinds Orion business software updates to distribute a backdoor called SUNBURST. A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain. Cybercriminals tamper with the manufacturing process of a product by installing a rootkit or hardware-based spying component.

FireEye also recently announced its own investigation into a breach of its network to allow for the widespread distribution of SUNBURST by again hiding it in legitimate updates of SolarWinds' Orion network management technology. FireEye is a cybersecurity company that provides hardware, software, and services to investigate cybersecurity attacks, protect against malicious software, and analyze IT security risks.

The Event

Thought to have been months in the making, beginning in as early as Spring 2020, this campaign is still currently ongoing. Post compromise activity following this supply chain compromise is proving to include lateral movement and data theft. What makes this even more of an embedded risk is that a malicious software class was included among otherwise legitimate classes and then signed into a legitimate certificate. This infected version of SolarWinds Orion plug-in pretends to be the Orion Improvement Program (OIP) protocol and store reconnaissance results within legitimate plugin configuration files allowing it to blend in with the legitimate SolarWinds activity. The trojan, after an initial dormant period of up to two weeks, begins to retrieve and execute commands, called "Jobs" that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. OIP is primarily used to collect performance and usage statistics data from SolarWinds users for product improvement purposes.

SUNBURST is a first stage trojan so that attackers can manipulate to drop additional payloads for escalating privileges, lateral movement, and data theft on infected networks. The trojanized update file appears to be your standard Windows

Installer Patch file that includes compressed resources associated with the update, including the trojanized SolarWinds.Orion.Core.BusinessLayer.dll component. Once this update is installed, the malicious DLL is loaded by the legitimate SolarWinds.BusinessLayerHost.exe or SolarWinds.BusinessLayerHostx64.exe (depending on the system configuration). A list of known malicious infrastructure is available on FireEye's GitHub page.

FireEye also recently disclosed that they have fallen victim to the cyberattack that has compromised its software tools used to test the defenses of its customers. The stolen Red Team tools, totaling in as many as 60 in number, are a mix of publicly available tools (43%), modified version of publicly available tools (17%), and those that were developed in-house (40%).

Since the breach was disclosed, Microsoft and numerous other vendors of malware detection tools have also added signatures for the malicious DLL that FireEye observed was being used to distribute SUNBURST.

Government Response

The White House National Security Council (NSC) announced that a Unified Coordination Group (UCG) has been established to ensure a coordinated federal agency response to the threat. The Presidential Policy Directive—41 (PPD-41) process is to facilitate continuous and comprehensive coordination for whole-of-government efforts to identify, mitigate, remediate and respond to this event.

Additionally, the DHS's CISA issued its emergency directive AA20-352A ordering all federal civilian agencies to immediately power off and disconnect instances of SolarWinds Orion. It also provides new mitigation guidance and revises the indicators of compromise table. Lastly, it includes a downloadable STIX file of the IOCs. In addition, CISA released supplemental guidance to Emergency Directive (ED) 21-01, providing new information on affected versions, new guidance for agencies using third-party service providers, and additional clarify on required actions.

CISA is encouraging users and administrators to review the following resources for additional information on the SolarWinds Orion compromise:

- CISA Emergency Directive 21-01 - Supplemental Guidance v.1
- CISA Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise
- CISA Activity Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

SolarWinds Releases Security Advisory

In its security advisory, SolarWinds states that the attack targets versions 2019.4 through 2020.2.1 of the SolarWinds Orion Platform software released between March and June 2020. It calls for users to immediately upgrade to Orion Platform release 2020.2.1 HF 1 immediately.

SolarWinds also released an additional hotfix, 2020.2.1 HF 2 on December 15th to replace the compromise component as well as several extra security enhancements.

FireEye Killswitch

FireEye's analysis of SUNBURST has shown that the malware can be prevented from operating under specific conditions. The killswitch is effective against new and previous SUNBURST deployments that might still be "beaconing out" to avsvmcloud dot com, the location of the malware's command and control server.

SolarWinds Orion Cyberattack and Financial Institutions

As of now, according to the Financial Services Information Sharing and Analysis Center, a network of financial firms sharing information about cyber threats, there has not been significant focus on the financial sector, nor have there been reports indicative of negative impacts amongst the financial services industry. FS-ISAC has been continuously monitoring and providing strategic and tactical reports detailing the attack vectors and offering best practices to mitigate risk. But this is not a guarantee and banks need to remain vigilant in monitoring the supply chain attack on the SolarWinds Orion Platform and subsequent customer breaches.

The Treasury Department is seeking feedback from financial institutions that have run the compromised SolarWinds Orion systems at OCCIP-Coord@treasury.gov or anonymously through FS-ISAC at sharingops@fsisac.com.

Action Plan

The below Action Plan is advisory in nature and is not intended to be legal advice. Financial institutions need to be assessing their own unique vulnerabilities and response plans. Consult with legal counsel, Vendor Management and an IT/IS professional as well as competent third-party vendors on any additional next steps.

ACTION PLAN

1. Determine by working with your Information Security and Technology Operations departments, whether your institution has been compromised because of the SolarWinds Orion cyberattacks. This includes immediately reviewing if and where SolarWinds was used within your organization and if the version installed is at risk. As referenced above SolarWinds has recommended the infected systems be taken offline.
    a. Review the bank's asset management procedures while performing this verification process. Weaknesses could have allowed for undocumented SolarWinds installations.
    b. Inform the Board of Directors immediately upon detection of SolarWinds installations within your organizations and if those versions are vulnerable.
2. Determine by working with your Vendor Management, Information Security and Technology Operations departments and your current third-party service provider or competent vendor and contract management services company to determine whether any of your vendors were affected by the cyberattack.
    a. Have all vendors complete C/A's Third-Party Vendor SolarWinds Orion Platform Questionnaire.
    b. Examine your supply chain and consider what other software has pervasive access like SolarWinds Orion platform. Report to the Board critical supply chain risks and propose appropriate risk mitigation measures.
3. Determine what systems/networks have been impacted by the SolarWinds Orion platform attack, including virtual private networks, staff home routers, and device management tools. Remediate, as necessary.
4. Develop an Action Plan for ongoing testing, monitoring and identification of vulnerabilities because of the SolarWinds Orion platform cyberattacks.
    a. It is recommended that all applications facing the internet be consistently receiving all required critical patches.
    b. Document and report to Senior Management and the Board that your patching process is effective and being executed rigorously.
5. Review and audit the bank's and any third party's cyber incident response plan and prepare and update defenses, as necessary.
    a. It is important to note that once a vulnerability is disclosed, the threat actors can develop and exploit within 48-hours.
6. Review SolarWinds' listed customers [*currently removed from website*], which include the Federal Reserve Bank, MasterCard, NCR, CitiFinancial, and Credit Suisse and determine whether your financial institution has vendor relationships with these and other SolarWinds customers (fourth-party risk).
7. Review monitoring and actionable alerts from your third-party vendors, the appropriate federal agencies and SolarWinds' Orion and FireEye for latest guidance and patches to determine vendor expectations related to the breach.
8. Have Legal, in conjunction with Vendor Management or similar department within your institution, review any third-party agreements for required next steps when a cyber incident like this occurs and notification of breach provisions, for whether both parties are living up to contractual obligations, and to determine whether your financial institution needs to negotiate stronger protections in future contracts.
9. Audit and determine what vendors have completed a Statement on Standards for Attestation Engagements (SSAE) 18 audit to ensure adherence to industry standards for security, compliance, and operational controls.
10. Begin discussions on whether cyber insurance is a viable option for your financial institution and have third-party vendors begin discussions with their insurers on whether they can make a claim against their policies if their organizations are compromised.
11. Contact Compliance Alliance with any additional questions.