[SolarWinds Breach Analysis Report]

[Chris Miele]

Contents

SolarWinds Company Overview

SolarWinds is a company located in [1] Austin, Texas, United States. The company specializes in Information Technology products. Some of these products include IT Service Management, IT Security, Application Management, Network Management, etc. SolarWinds offers IT Services to a list of clients this includes [2]US Government and its different sectors, [3]Microsoft, Ford, AT&T, Best Western, Cisco, Harvard, Fire Eye, etc. SolarWinds is always trying to innovate in the Information Technology growing landscape. [4] SolarWinds also offers training on its many products that they currently have and are expanding. SolarWinds offers training to clients virtually, and in-person training.

Orion Platform

SolarWinds Orion Platform is a centralized management platform that allows modules to work in conjunction with one another. [5] These modules include Network Performance Monitor, NetFlow Traffic Analyzer, Network Configuration Manager, Ip Address Manager, VoIP &Network Quality Manager, User Device Traffic, Server & Application Monitor, Server Configuration Monitor, Storage Resource Monitor, Virtualization Manager, Web Performance Monitor, Log Analyzer. Also, Orion Platform is expanding to other modules presently and in the future.

Intro

SolarWinds was breached by state-sponsored hackers. The Adversaries used a well thought out sophisticated plan to break into SolarWinds. The target software that the Adversaries manipulated was SolarWinds Orion Platform. How the Adversaries broke into the platform on September 4th,2019 is not known but the [6] proposed way was based on information obtained from Vinoth Kumar Reporter in 2017 an intern that use to work at SolarWinds had a poor password for logging in. The password was solarwinds123.

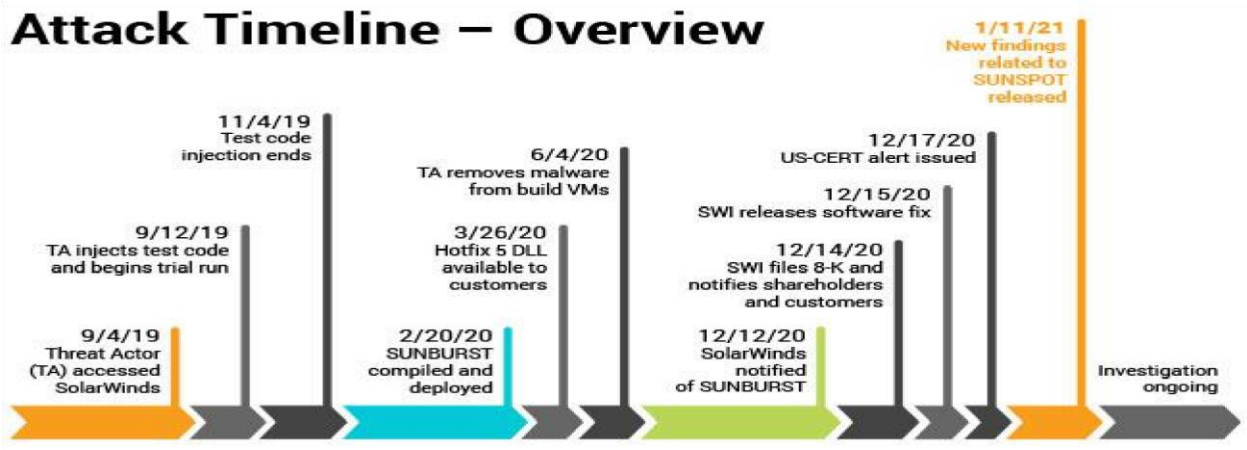
The Adversaries broke into SolarWinds on this was deemed by Network Forensics on SolarWinds Corporate Network and Orion Platform. [7] Adversaries started the attack on September 4th, 2019, and gradually increased their presence on SolarWinds Corporate Network and Orion Platform in September. The month from September 2019 to November 2019 was deemed as the Trial Period. SUNBURST malicious code was sent and deployed to the Orion Platform in February 2020. The Malware was removed from Virtual machines in June 2020. SolarWinds was notified about SUNBURST Malware by FireEye in December 2020. SolarWinds Pushed out Patches notified Stakeholders. The Resolution is software patches were deployed on the Orion Platform. Also, because of how well thought out and sophisticated the attack was more information is coming out of possibly more malware being used in the SolarWinds Attack. [8] Currently, the pieces of malware that affected this breach are SUNBURST, SUPERNOVA. The fallout of this attack is ongoing investigations by US Government, SolarWinds Clients, Hearings, New Cyber Security Hires at SolarWinds. Sanctions are being put on State-Sponsored Adversaries. In this case, it was deemed by network forensics the network forensics software was most likely SolarWinds Software the built environment had to be isolated on the Corporate Network it was said that Russia was behind the attack. The number of customers affected by this is concerning [9] 18,000 from different sectors, companies, and more.

TimeLine of Attack

The timeline of the SolarWinds Breach that affected [10] 18,000 Clients is ever-changing new information is coming out every day about the SolarWinds Breach. The Clients that were affected because of the breach are different US Government Sectors, Microsoft, Cisco, Intel, Deloitte, FireEye, etc. How the attack started is different depending on the company that got compromised. Majority of the breach timeline from other companies that were affected still mention the correct dates based on the SolarWinds Breach Timeline. The Timeline below is based on a lengthy process of network forensics being used. The following image below is the breach timeline for SolarWinds.

The Breakdown of each event is the following:

1) September 4th, 2019 Adversaries Presumably accessed a SolarWinds account by utilizing a poor password. How I believe they accessed the account was using wordlist attacks, brute-forcing attacks on the employee account to access the account. The account most likely had access to a specific portion of the Orion Platform
2) September 12th, 2019 Adversaries injected test code in the Orion Platform. I believe the adversaries slowly injected the code to not cause suspicious behavior on the build server and the corporate network.



3) November 4th, 2019 Adversaries injected test code ends in the Orion Platform. There was a 2month gap in between to make it seem like the software developers that were working on Orion Platform were pushing and deploying updates.
4) February 20th, 2020 Adversaries deploy an update on the Orion Platform. This update affected 18,000 clients. [11] The affected Orion Platform versions were 2019.4 HF 5, 2020.2, 2020.2 HF1. The following Modules were affected by this Application Centric Monitor, Database Performance Analyzer, Enterprise Operations Console, High Availability, IP Address Manager, Log Analyzer, Network Automation Manager, Network Configuration Manager, Network Operations Manager, User Device Tracker, Network Performance Monitor, NetFlow Traffic Analyzer, Server & Application Monitor, Server Configuration Monitor, Storage Resource Monitor, Virtualization Manager, VoIP & Network Quality Manager, and Web Performance Monitor.
5) March 26th, 2020 Hotfix 2019.4F and 2020.2 HF 1 is pushed to the affected clients that did install the update and were affected by the update.
6) June 4th, 2020 The Adversaries removed the malware from the build virtual machines.
7) [12] December 12th, 2020 SolarWinds is notified by Fire eye executive based on network forensics from fire eye on their internal corporate workstations it was determined that FireEye was affected by the breach and, SolarWinds target was Orion Platform.
8) December 14th, 2020 SolarWinds contacts stakeholders, Corporate and notifies them of a breach that occurred on SolarWinds Orion Platform. Files for 8-k.
9) December 15th, 2020 SolarWinds releases software fix on the Orion Platform that affected the Modules.
10) December 17th, 2020 US-Cert issued to SolarWinds.
11) January 11th, 2021 New Findings of sunspot was released to the public.

Incident Response Details

The incident response by SolarWinds was poor SolarWinds were notified by FireEye about SUNBURST malware. FireEye found out about the malware by using network forensics on its internal network. What SolarWinds did was perform internal network forensics on the Corporate Network and Orion Platform to determine how the Adversaries pushed updates on the Orion Platform. Once the Network Forensics was completed, they could make a timeline on how the attack occurred, when did it start, why was it undetected for so long, etc. The software patches were pushed on the Orion Platform they were version 2019.4 HF 5, 2020.2 HF 1, 2020.2. The affected modules were patched by the clients. [13] New Malware strains are still being talked about now to this date and introduced they are Nobelium. The goal of the sunburst malware is highly sophisticated what the malware does is blocks anti-virus/anti-malware software. Also, after 2 weeks of the backdoor in your system, the malware can do malicious things like reboot the system, disable services, transfer, execute files, basically obtaining root privileges on the workstation. Each incident was responded to differently by the companies involved. Fire Eye a well-known information threat detection technology company that was also breached because of the SolarWinds incident recommended

isolation of SolarWinds technologies, software, etc. [14] Microsoft one of the companies affected by the SolarWinds Attack stated to use 365 defender and Microsoft defender to mitigate the malware.

Fallout

The fallout from the attack is extraordinary 18,000 customers were affected by the SUNBURST Malware that was deployed on the Orion Platform. [15] Once SolarWinds announced the breach to the public their stock fell $20. Multiple investigations were done to determine the root cause of SolarWinds Attack the investigations were done by [16] the FBI, [17] Sec, Whitehouse(Affected by Breach US Government), [18] SolarWinds CEO Kevin Thompson leaves the company is now consulting the new CEO of the company is Sudhakar Ramakrishna. [19] US Intelligence blames Russia for the SolarWinds Attack that affected 18,000 clients. [20] SolarWinds hires CISA leader Chris Krebs(former director CISA), and Alex Stamos(Former chief security officer Facebook) to boost their cybersecurity team. [21] New hires to help with cybersecurity state-sponsored attacks occurred when Biden took over as president of the united states. [22] The New CEO discloses to the public SolarWinds ways on how they are improving their cybersecurity infrastructure. [23] The Senate is investigating the SolarWinds Breach to determine what the root cause and the steps moving forward to mitigate state-sponsored hackers from happening in the future to IT Information Technology Companies. [24] Sanctions are being put on Russia for its involvement in the SolarWinds Cyber Attack this was determined by network forensics. [25] Lawsuits will be filed because of the SolarWinds incident.

Improvements

Based on the SolarWinds attack what could have been done better to mitigate the risk of the breach is:

1) Change the Default password on SolarWinds Accounts. I believe this was the root cause of the entire breach occurring poor password policy and lack of luster password. Make sure the password is 16 characters minimum and multifactor authentication is enabled on accounts.
2) Make sure to check the logs daily for suspicious activity on the Orion Platform.
3) Practice secure coding to mitigate the risk of potential code being exploited on the Orion Platform.
4) If there is suspicious activity on any account, make sure it is reported to the correct managers so they can determine the root cause of the account that is being affected.

Conclusion

In conclusion, the changes I have suggested moving forward would prevent the SolarWinds Breach. Password policy 16 Character password can help prevent brute force attacks, wordlist attacks. The longer the character of passwords the longer Adversaries would take to breach into the account. Multifactor Authentication can be used on the accounts to prevent brute force attacks. Logs should be checked daily to check for suspicious activity on the Orion Platform and also on the corporate network. By checking the logs daily, it would lead to Adversaries being found out sooner rather than later. Secure coding would help with this because sunburst malware was exploiting a vulnerability in the Orion Platform. If employee accounts are found to contain suspicious activity they should be reported to

managers in the IT Department and their department. The accounts should be disabled and removed from the system if the employees are not working at SolarWinds anymore. Disabling and removing accounts will prevent Adversaries from using that specific employee account to gain access to the corporate network and Orion Platform. Also, SolarWinds if a breach does occur should notify the required parties sooner rather than later.

References

[1] SolarWinds Wikipedia SolarWinds - Wikipedia

[2] Government Reseller and Systems Integrator Partners, SolarWinds SolarWinds Government Partner

[3] These big firms and Us Agencies all use software from the company breached in a massive hack being blamed on Russia, Mia Jankowicz and Charles Davis List of Companies, Agencies at Risk After SolarWinds Hack (businessinsider.com)

[4] SolarWinds ACADEMY, SolarWinds https://support.solarwinds.com/solarwinds-academy

[5] Orion Platform, SolarWinds https://www.solarwinds.com/orion-

platform#:~:text=The%20SolarWinds%C2%AE%20Orion%C2%AE%20Platform%20is%20a%20powerful%2C%20scalable,a%20single%20pane%20of%20glass.

[6] SolarWinds blames intern for weak 'solarwinds123' password, Keumars Afifi-Sabet SolarWinds blames intern for weak 'solarwinds123' password | IT PRO

[7] New Findings From Our Investigation Of SUNBURST, Sudhakar Ramakrishna, SolarFocus https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

[8] SolarWinds Security Advisory, SolarWinds https://www.solarwinds.com/saoverview/securityadvisory

[9] The US is readying sanctions against Russia over the SolarWinds cyberattack. Here's a simple explanation of how the massive hack happened and why it's such a big deal, Isabella Jbilian and Katie Canales. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cybersecurity-2020-12#:~:text=The%20victims&text=Since%20SolarWinds%20has%20many%20high,victims%20targeted%20were%20nongovernment%20organizations

[10] SOLARWINDS CORPORATION, SECURITIES AND EXCHANGE COMMISSION https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf55bd5e34d451.pdf

[11] SolarWinds Security Advisory, SolarWinds https://www.solarwinds.com/saoverview/securityadvisory

[12] Threat Research, FireEye https://www.fireeye.com/blog/threat-research/2020/12/evasive-attackerleverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[13] GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's Layered Persistence, Ramin Nafisi, Andrea Lelli https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzingnobelium-malware/

[14] Ensuring Customers are Protected From Solorigate, Microsoft 365 Defender Threat Intelligence Team https://www.microsoft.com/security/blog/2020/12/15/ensuring-customers-are-protected-fromsolorigate/

[15] SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details, Joe Panettieri https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timelineand-updated-details/

[16] JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY(CISA), AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE(ODNI) https://www.cisa.gov/news/2020/12/16/joint-statement-federal-bureauinvestigation-fbi-cybersecurity-and-infrastructure

[17] UNITED STATES SECURITIES AND EXCHANGE COMMISSION, SOLARWINDS CORPORATION https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

[18] SolarWinds CEO Kevin Thompson Leaves, exchange https://exechange.com/20404/solarwinds-ceokevin-thompson-leaves

[19] US Intel Agencies Blame Russia for Massive SolarWinds Hack, Maggie MILLER, The HILL https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwindshack

[20] SolarWinds Hires Krebs, Stamos as Cybersecurity Consultants After Orion Hack, Joe Panettieri, MSSP Alert https://www.msspalert.com/cybersecurity-talent/solarwinds-hires-krebs-stamos-as-cybersecurityconsultants-after-orion-hack/

[21] U.S. Cyber Security Strategy: President Biden Executive Orders, Legislation, Leaders, and More, Joe Panettieri, MSSP Alert https://www.msspalert.com/cybersecurity-markets/americas/u-s-cybersecuritypresident-biden-plan-policy/

[22] New SolarWinds CEO Discloses Three Security Priorities, Joe Panettieri, ChanneLe2e https://www.channele2e.com/technology/security/new-solarwinds-ceo-discloses-three-securitypriorities/

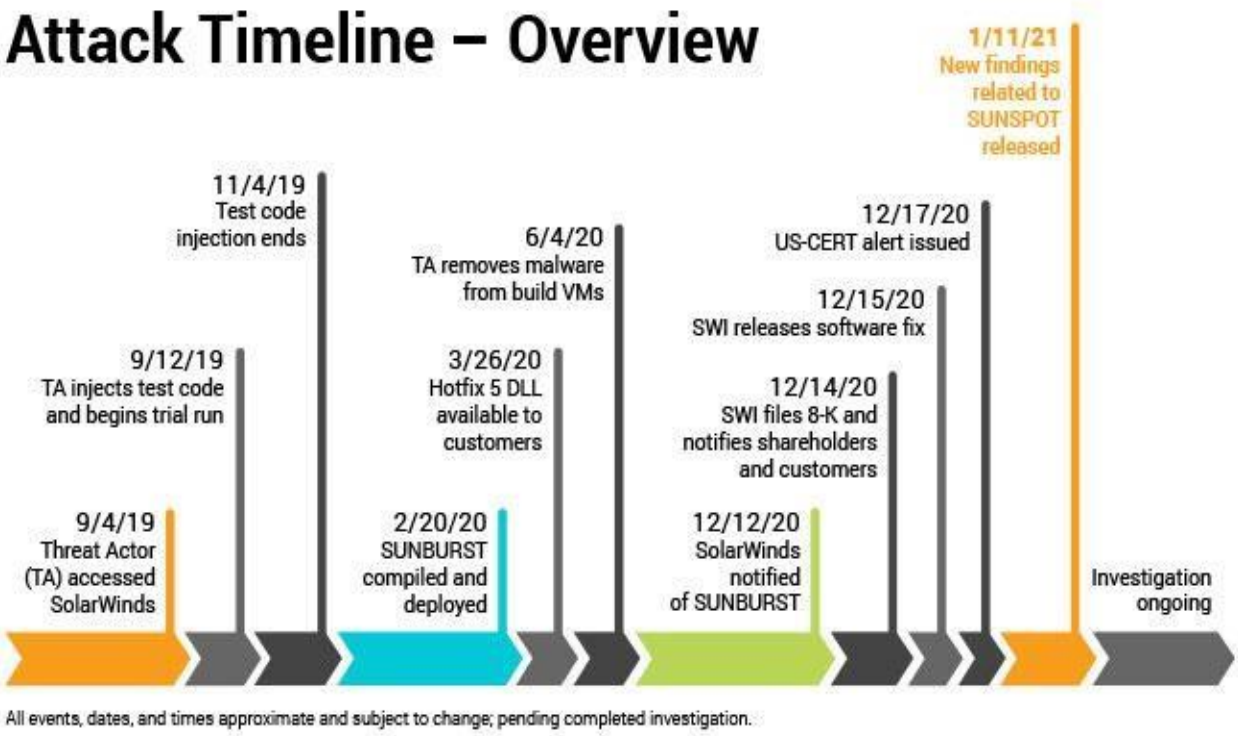
[23] SolarWinds, Microsoft, FireEye, CrowdStrike defend actions in a major hack – U.S. Senate Hearing, Raphael Satter, Joseph Menn Reuters https://www.reuters.com/article/us-cyber-solarwinds/solarwindsmicrosoft-fireeye-crowdstrike-defend-actions-in-major-hack-u-s-senate-hearing-idUSKBN2AN1Q4

[24] Biden administration preparing to sanction Russia for SolarWinds hacks and the poisoning of an opposition leader, Ellen Nakashima, The Washington Post https://www.washingtonpost.com/nationalsecurity/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fae0ccb3660358_story.html?source=content_type%3Areact%7Cfirst_level_url%3Anews%7Csection%3Am ain_content%7Cbutton%3Abody_link

[25] SWI SECURITIES FRAUD LAWSUIT FILED: Hagens Berman Encourages SolarWinds(SWI) Investors with Losses to Contact Firm Now, Hagens Berman Sobol Shapiro LLP, Hagens Berman https://www.globenewswire.com/news-release/2021/01/11/2156623/0/en/SWI-SECURITIES-FRAUDLAWSUIT-FILED-Hagens-Berman-Encourages-SolarWinds-SWI-Investors-with-Losses-to-Contact-FirmNow.html

[26] Emergency Directive 21-01, Mitigate SolarWinds Orion Code Compromise. https://cyber.dhs.gov/ed/21-01/

Appendix


Attack Timeline – Overview
9/4/19
Threat Actor (TA) accessed SolarWinds
9/12/19
TA injects test code and begins trial run
11/4/19
Test code injection ends
2/20/20
SUNBURST compiled and deployed
3/26/20
Hotfix 5 DLL available to customers
6/4/20
TA removes malware from build VMs
12/12/20
SolarWinds notified of SUNBURST
12/14/20
SWI files 8-K and notifies shareholders and customers
12/15/20
SWI releases software fix
12/17/20
US-CERT alert issued
1/11/21
New findings related to SUNSPOT released
Investigation ongoing
All events, dates, and times approximate and subject to change; pending completed investigation.