SolarWinds IS Security Threat Analysis and Plan

Zoiab Mustafa

Department of Business, Auckland University of Technology

BSYS702/01: Cyber-Security and Risk Management 2022 S1

Dr. Harminder Singh

27th May 2022

SolarWinds IS Security Threat Analysis and Plan

SolarWinds Corporation is a highly significant software company based in the United States of America. The corporation formulates and develops information technology management software such as network and infrastructure monitoring, virtualisation, database management and configuration (Bloomberg, 2022). What was perceived to be a top-tier software provider, turned into something sinister as this corporation was compromised by alleged Russian threat actors (Hernandez, 2021). The substantial list of victims included telecom, government and technology firms based in North America, Asia, Middle East, and Europe (Novinson, 2020).

Incident Summary

The software and asset which got attacked was the Orion Platform. The Orion Platform is a management and infrastructure monitoring platform which was designed to help businesses manage and optimise their on-premises IT administration, software as a service and hybrid environments in a single window (SolarWinds, n.d.). Orion was used by 18,000 major companies and was placed in the centre of their infrastructure. This exposed the companies' firewalls, credentials, switches, and entire information technology infrastructure (Cimpanu, 2020).

According to SolarWinds (2021a) the main vulnerability was the injection of the SUNBURST malware which was created and executed by the threat actors. This type of malware is known to be a remote access trojan. This method can also be known as a supply chain attack. Instead of attacking each network individually, the threat actors targeted a third party (Orion) that has access to another organisation's systems. It is believed that the threat actors accessed SolarWinds five months prior to SUNBURST being compiled and deployed, and this unauthorised access went virtually unnoticed (SolarWinds, 2021a). The second key vulnerability was SolarWinds' code repository and credentials becoming publicised and

exposed. A security researcher had warned SolarWinds about this as he himself uploaded a file to their update server using the pathetic password ‘solarwinds123’, he added that it is possible for a hacker to use the weak credentials and upload a malicious executable and connect it to an update for SolarWinds. (Claburn, 2020).

According to Oladimeji & Kerner (2021) this is exactly what happened as the threat actors deployed a software update (SUNBURST) to all of Orion's customers. This update was also digitally signed by SolarWinds and there was no reason to believe it was suspicious. Once installed, the threat actors gained backdoor access to the client’s information technology infrastructure. They were able to impersonate users and accounts within the affected firms. The malware was immaculately designed as it was able to access system files and disguise the activity to be genuine activity from SolarWinds, this also prevented antivirus software from detecting these activities. Thousands of federal, local, and state agencies had the Orion software implemented. The attack compromised the systems, data, and networks of the victims when the update was installed.

However, it was not only the customers of SolarWinds that got affected. Since the threat actors were able to access a firm's own network, they had direct access to information about their stakeholders and customers. Although a definitive motive is not clear with this attack, an assumption could be cyber espionage. The threat actors knew government agencies were using the Orion platform and this may have motivated them to use Orion as a target to spy on these agencies (Oladimeji & Kerner, 2021).

A Detailed Timeline

The Initial Incident

According to SolarWinds (2021b), initially, the threat actors gained access to SolarWinds’ servers on the 4th of September 2019. On the 12th of September, threat actors then injected the test code to commence a trial run. The threat actors used a very complex

injection source to implement the SUNBURST malware into the Orion platform software. Multiple servers were used based in the United States, to circumvent threat detection from SolarWinds. This trial concluded on the 4th of November 2019. On the 20th of February 2020, SUNBURST was compiled and deployed. This was the software update for the Orion Software which included the Malware. On the 26th of March 2020, a hotfix became available to customers. On the 4th of June 2020, the threat actors removed malware from SolarWinds' systems (SolarWinds, 2021b).

Movement of the Threat Actors

According to InfoSecAdemy (2021), threat actors first breached and compromised the Orion software updates. They then used their malware SUNSPOT to insert their backdoor malware SUNBURST into software builds of Orion. This allowed them to remain undetected. When the compromised update version is installed, it starts with executables which then turn into compromised DLLs. Defence evasion techniques included mirroring official API calls and making the malwares traffic hidden under Orion Improvement Protocol. The malware could also impersonate trusted network entities and evade specified endpoint security measures. Information is gathered laterally and stored in the official SolarWinds configuration directory. The backdoor then establishes a connection to its command-and-control server. Then the attacking server receives gathered information from the backdoor. With the access of a backdoor, threat actors were able to do hands on keyboard attacks. This opened doors to lateral movement, identity theft and gaining unauthorised access. Various commands were made beforehand to assist in efficient hacking. Commands included KillTask, RunTask & UploadSystemDescription (InfoSecAdemy, 2021).

Detection of Attacker, Response & Public Relations on Activities:

According to Miller (2021), on December 8th, 2020, a cybersecurity intelligence and threat provider called FireEye reported that hackers gained access to their networks and exfiltrated with their Red Team penetration testing and assessment tools. FireEye warned that the hackers would use the classified information and tools to attack other companies. Three days later, while investigating on the attack, FireEye found out that SolarWinds had been victims to an attack and had their systems compromised. They later found out that this was a supply chain attack where the software updates for Orion were malicious. A day after this finding, FireEye releases a statement and informs SolarWinds that their Orion platform had been a victim to a cyber-attack and their systems compromised.

Upon hearing this news, SolarWinds asked all clients to update to a new software immediately to address a security vulnerability. SolarWinds also filed a SEC Form 8-K report, which stated that part of its company has been compromised via a cyber-attack which inserted a vulnerability into its Orion platform. Two hotfixes were released after this vulnerability. The National Security Council commenced an emergency meeting at the White House to discuss the attack on multiple government agencies. The Cybersecurity and Infrastructure Security Agency commanded federal agencies to kill the Orion Platform immediately. SolarWinds addresses the attack further and provides defensive measures to be done. Reuters released the first media coverage on this attack. Microsoft outlines guidance, explanations, and preventative measures on cyberattacks. Microsoft also reported that their software or products were not affected by the threat actors. U.S. intelligence agencies accused Russia of being the sole perpetrator of the attack on SolarWinds, however, Russia denied this act. President Joe Biden hired cybersecurity experts (Miller, 2021).

Public Reactions

Microsoft president, Brad Smith, revealed that its researchers believe at least 1,000 highly skilled and capable engineers were behind this attack. The attack was also the most sophisticated and significant attack that Smith has ever seen (Paul, 2021). The attack took the media by storm and hundreds of content creators on social media gave their explanations, thoughts, and recommendations on the SolarWinds attack. Trolls on the internet also took a humorous stance on this matter and created memes against SolarWinds. Multiple news sources published articles and interviews with cybersecurity experts to make sense of this matter. Cybersecurity and attacks became very popularised and led other experts and organisations to heavily investigate this issue and mitigate the potential risk of them being attacked too. A survey consisting of 1,000 CIOs found out that 82% of CIOs believed that their organisations have vulnerabilities and could be a target for supply chain attacks. CIOs have become more aware and concerned about the integrity of their information technology infrastructure (Zurier, 2022). In another stance, CNBC SurveyMonkey Small Business Survey keeps up to date with over 2,000 small businesses to better understand their view on business trajectory and performance. The survey revealed that only 5% of the business owners considered cybersecurity as their biggest threat currently (Wronski & Cohen, 2022).

Government Investigations & Sanctions

According to GAO (2022) while the investigation on SolarWinds cyberattack was still ongoing, in March 2021, Microsoft reported exploitations and successful access to various versions of Microsoft Exchange Server. Several procedures and steps were taken by federal agencies to attend to the SolarWinds and Microsoft attacks. This included forming two cyber unified coordination groups. One group for each attack. Both groups consisted of the Federal Bureau of Investigation, the National Security Agency, Cybersecurity and Infrastructure Security Agency and the Office of the Director of National Intelligence. The Cybersecurity

and Infrastructure Security Agency disseminated emergency protocols to federal agencies of the potential weak points or vulnerabilities and what actions must be taken in responses to those altercations. Congress held many hearings to collect and disclose information on the specific timeline of incidents in relation to the SolarWinds Hack. The hearing also included conversations regarding information technology supply chain security, future federal actions, improvements, threat actor capability and motivation.

GAO also ensures that the cybersecurity of their nation has been on their high-risk list since 1997. Harwell & Macmillan (2020), reports that top shareholders in SolarWinds sold millions of dollars of shares just before the cyberattack announcement was made. This raises the speculation of insider trading due to the timing of the shareholders shorting their positions. A former official of the U.S. The Securities and Exchange Commission suggested that the trades will likely create an investigation to figure out if insider trading was legitimately committed. An example of this would be Thoma Bravo, an equity firm who sold $128 million of its shares in SolarWinds just a few days before the cyberattack announcement. Another example would be Silver Lake who sold $158 million in shares of SolarWinds on the same day as Thoma Bravo. Both companies share 70% of SolarWinds between them and own multiple board seats, which allows them to receive vital information expeditiously (Harwell & MacMillan, 2020).

The White House released Executive Order 14024 which issued sanctions targeting the obscene foreign activities of the Russian Government (GAO, 2022). According to Brandom (2021), the order also included restrictions on Russia's sovereign debt, making it harder for Russia's government to support its currency and to raise money. 32 individuals are also a target in the sanction as they are believed to have been involved in government ploys to influence the 2020 election. Multiple privatised entities of cybersecurity firms in Russia were also sanctioned for their crafts supporting government endeavours (Brandom, 2021).

Changes in Share Price

SolarWinds ticker symbol (SWI) had mediocre performance from the period between its IPO in October 2019 and February 2020 (See Appendix A). It had support levels around the $18 mark and resistance levels around the $20 mark for most of this period. The stock was trading at $19.79 on the 7th of February 2020, however, it became bearish and tanked -32% by the 20th of March 2020 and it traded at $13.43. This was due to the global pandemic COVID-19. The stock recovered well and became extremely bullish from the 20th of March 2020 up until 11th of December. It went from $13.43 in March to $24.83 in December, resulting in an 84.88% increase. After the announcement of the cyberattack, the stock dropped to $14.95, a 39.79% decrease. Since the attack, the stock has been on a downwards trend. As of today, 1st of June 2022, the stock trades at $11.64 a share.

Analysis

What vulnerabilities existed in the technology that was compromised, and could they have been addressed?

The use of a mediocre password resulted in the hackers obtaining access to Orion's update server. This could have been addressed by using a more robust password containing a mixture or lower and uppercase letters, symbols, and numbers. Passwords should also be reviewed and changed fortnightly or monthly. Two factor or biometric authentication could have also been implemented to make the login more secure, especially for privileged accounts. The issue of the weak password was addressed by a cybersecurity pro, however, the response to that issue was not resolved quick enough. There were simply not enough end-point security measures in place, the malware as we know, terminates itself if it encounters an endpoint security measure. Had SolarWinds had enough endpoint security measures, the malware would end up terminating more often which would have allowed SolarWinds more time to identify the breach. The vulnerability of software source code being

leaked and publicised on GitHub shows the lack of monitoring and awareness of SolarWinds Staff. Policies are a guideline but not everyone will follow them. SolarWinds should have had extensive monitoring on all information being shared by staff and implemented more access controls to maintain information integrity.

Another vulnerability would be that SolarWinds had no systems in place that would allow users to block an outbound attempted connection to their servers. This could have been addressed by implementing a firewall that automatically rejects an outbound attempted connection to their server. A lack of cybersecurity knowledge, risk management and negligence during the developmental stages of SolarWinds information technology infrastructure created a huge vulnerability for hackers to exploit. The team responsible should have heavily invested time into formulating the potential threats and their appropriate responses to those threats. This could have been addressed by following the COBIT framework which would have given more stability and protection to their information technology sector and their business.

How did organisational policies or culture contribute to the incident or the lack of detection of the attack?

There was a clear lack of communication once the password issue was addressed. Proving this point is the fact that the password had been in use since 2017 as testified by SolarWinds CEO himself. This contributed to the cyberattack becoming a success. The employee publishing integral source code to an open-source platform such as GitHub shows lack of organisational behaviour. Management needs to make it a priority that staff understand company policies, consequences, and relevant processes that staff should conduct themselves with. SolarWinds should have continuously emphasised the importance of cooperation with company policy to create a strong company culture around information integrity. The lack of detection of the attack explains that there were not enough

cybersecurity testing policies in place and being implemented. The fact that it took another company (FireEye) to tell SolarWinds themselves that their own systems had been compromised proves the aforementioned statement.

The lack of interest in cybersecurity policies in SolarWinds is also factual as former employee Ian Thornton-Trump warned SolarWinds that they were not taking cyberattacks seriously in 2017. He also claimed that there was a lack of security at the product level and miniscule security leadership at upper management (Lemon, 2020).

Individual Note

The intern who published the password to GitHub, violated company policies, carelessly posted it on their private GitHub account and proved to be a liability. Although it could be possible that there were compromised ex or current employees involved in the attack, there is no factual evidence to prove this point.

Lessons for SolarWinds, Good and the Bad & Recommendations

Cybersecurity should be at the top of SolarWinds' priority list. Especially as it is a breeding ground for supply chain attacks, and they are directly connected to thousands of major companies and federal agencies. Cybersecurity policies and practices need to be enforced not only to seniors but the entire company, stakeholders, and their clients as a whole. The lesson SolarWinds learned was that with inadequate policies and not addressing vulnerabilities, it will lead to the destruction of your business and stakeholders. SolarWinds did take the situation well, in terms of addressing the government and public, they did everything calmly and with professionalism.

For SolarWinds to prepare for future threats, I recommend them to do regular penetration testing on their security systems. This will uncover potential areas that could be prone to an attack and existing malware. Results should be stored in encrypted and private files with numerous access requirements. The results can also be shared to other

cybersecurity firms for further analysis and iterations. Just like the malware, it will need more than 1,000 people to work together and create preventative measures to beat unethical hackers. Honeytokens should be used to divert attackers away from legitimate files. It can also isolate hackers in a specific place and keep them distracted until they trip an alarm.

Company culture needs to heavily involve information integrity, this can be done by presentations and workshops. Monitoring for potential insider threats will be useful, but it's more important to make sure all staff are happy and not confused about anything. Surveys can be introduced to check employee satisfaction and direct support should be encouraged for staff. Sensitive data must be protected with counter measures and limited access. Implement zero trust in IT architecture. Always require verification and credentials at each site necessary.

References

Bloomberg. (2022). *SolarWinds Corp*. https://www.bloomberg.com/profile/company/SWI:US

Brandom, R. (2021). *US institutes new Russia sanctions in response to SolarWinds hack*. The Verge. https://www.theverge.com/2021/4/15/22385371/russia-sanctions-solarwinds-biden-white-house-putin-hack

Cimpanu, C. (2020). *SEC filings: SolarWinds says 18,000 customers were impacted by recent hack*. ZDNet. https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/

Claburn, T. (2020). *We're not saying this is how SolarWinds was backdoored, but its FTP password 'leaked on GitHub in plaintext'*. The Register: Enterprise Technology News and Analysis. https://www.theregister.com/2020/12/16/solarwinds_github_password/

GAO. (2022). *SolarWinds cyberattack demands significant federal and private-sector response (infographic)*. U.S. Government Accountability Office (U.S. GAO). https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

HARWELL, D., & MacMillan, D. (2020). *Investors in breached software firm SolarWinds traded $280 million in stock days before hack was revealed*. The Washington Post.

https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/

Hernandez, J. (2021). *The Russian hacker group behind the SolarWinds attack is at it again, Microsoft says*. NPR.org. https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft

InfoSecAdemy. (2021, March 2). *SolarWinds hack and supply-chain attack demystified*. Learn InfoSec | Cyber Security Made Easy | InfoSecAdemy. https://www.infosecademy.com/solarwinds-hack/

Lemon, J. (2020). *Ex-solarwinds adviser warned company of security issues in 2017: "Incredibly easy target to hack"*. Newsweek. https://www.newsweek.com/ex-solarwinds-adviser-warned-company-security-issues-2017-incredibly-easy-target-hack-1556453

Miller, J. (2021). *SolarWinds cybersecurity breach: What happened, who it affects, and what to do next | BitLyft cybersecurity*. BitLyft Cybersecurity: Threat Detection and Automated Remediation. https://www.bitlyft.com/resources/solarwinds-cybersecurity-breach-what-happened-who-it-affects-and-what-to-do-next

Novinson, M. (2020). *Here are 24 reported victims of the SolarWinds hack (So far)*. CRN. https://www.crn.com/slide-shows/security/here-are-24-reported-victims-of-the-solarwinds-hack-so-far-

Oladimeji, S., & Kerner, S. M. (2021). *SolarWinds hack explained: Everything you need to know*. WhatIs.com. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know#:~:text=How%20did%20the%20SolarWinds%20hack,to%20hack%20the%20networks%20directly

Paul, K. (2021). *SolarWinds hack was work of 'at least 1,000 engineers', tech executives tell Senate*. the Guardian. https://www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft

SolarWinds. (n.d.). *Orion platform*. IT Management Software and Observability 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

SolarWinds. (2021a). *Security advisory*. IT Management Software & Remote Monitoring Tools | SolarWinds. https://www.solarwinds.com/sa-overview/securityadvisory

SolarWinds. (2021b). *New findings from our investigation of sunburst*. Orange Matter. https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Wronski, L., & Cohen, J. (2022). *America's small businesses aren't ready for a cyberattack*. CNBC. https://www.cnbc.com/2022/05/21/americas-small-businesses-arent-ready-for-a-cyberattack.html

Zurier, S. (2022). *Most CIOs say their organizations are vulnerable to software supply chain attacks*. SC Mediapage. https://www.scmagazine.com/news/third-party-risk/most-cios-say-their-organizations-are-vulnerable-to-software-supply-chain-attacks

Appendix A

Market Summary > SolarWinds Corp

11.64 USD

-4.21 (-26.56%) ↓ past 5 years

NYSE: SWI

+ Follow

Closed: 31 May, 4:40 pm GMT-4 • Disclaimer

Pre-market 12.12 +0.48 (4.12%)

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max

Open	12.20	Mkt cap	1.87B	52-wk high	23.00
High	12.31	P/E ratio	-	52-wk low	10.40
Low	11.57	Div yield	-		