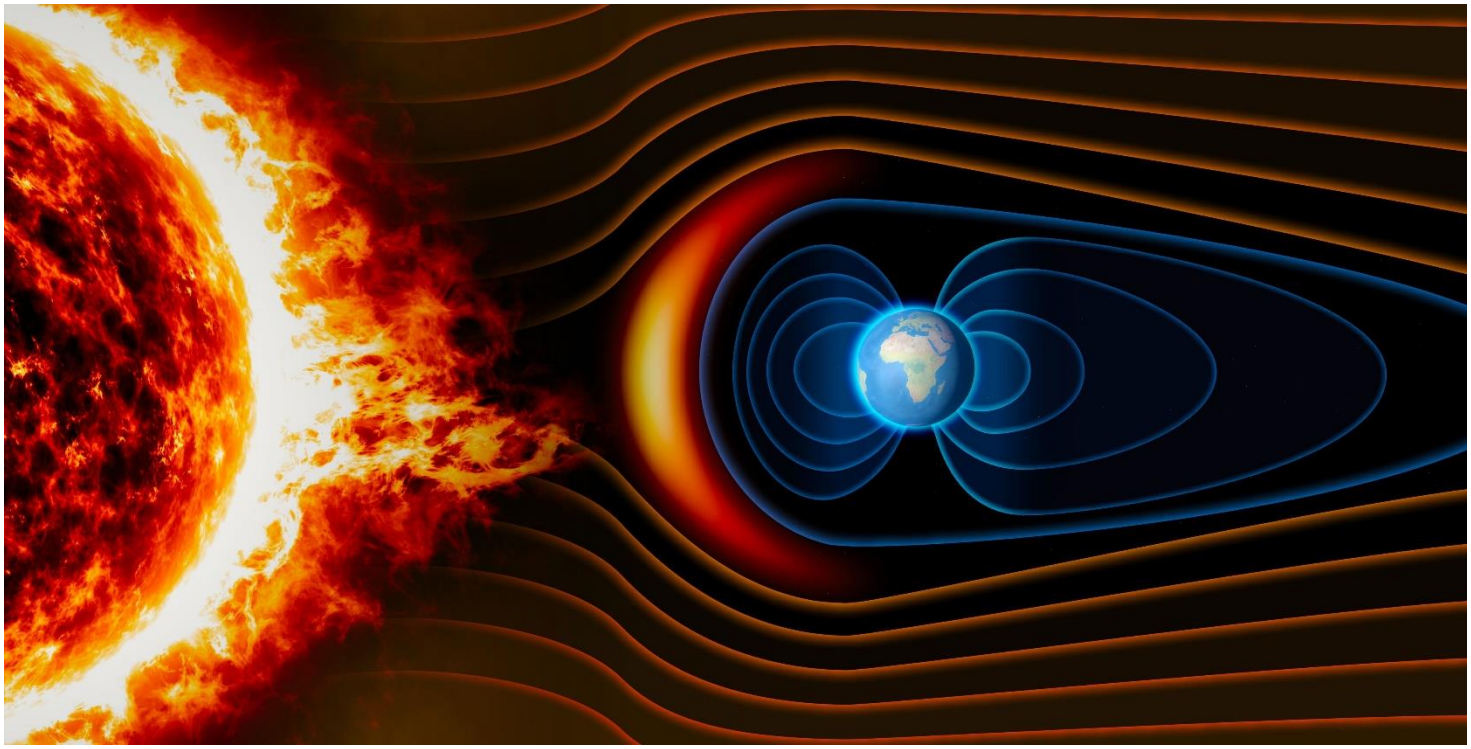
The Solar Winds Breach – How It Happened

By: Ravi Das



Introduction

Every day there always seems to be a hacking story that takes place. Some make the news headlines, and some don't. Probably some of the biggest ones that took place pre-COVID19 were the Sony, British Airways website, and the Marriott Group hacks.

During the pandemic, of course the threat vectors exploded like nothing ever seen before, but there is one hack that totally gripped the world – which is the Solar Winds security breach.

The reason why this hack gained so much attention was the magnitude of it, and especially the entities that were involved and those that were affected.

For example, you have the Russians that were primarily blamed for it, and then on the other side of this, you have Microsoft and some of the largest Federal Government agencies, such as the Department of Defense (DoD) that were gravely impacted by it.

In this whitepaper, we take a closer look as to what could be deemed as one of the largest security breaches of all time, focusing upon the following:

- What Actually Happened;
- The Timeline Of The Attack;
- The Victims Of The Attack;
- The Lessons Learned From The Attack.

What Actually Happened

First, Solar Winds is a rather large software company that creates and deploys network monitoring tools. These are primarily used by larger companies in Corporate America, especially by Managed Service Providers (MSPs) that keep an eye on the IT and Network Infrastructures for their clients.

Through this, any sort or type of anomalies can be detected in the network flow of traffic, and any corrective actions can be taken immediately, which is often done remotely. One of these tools that is manufactured by Solar Winds is known as “Orion”.

It is important to note at this point that this kind of hack is different than the others that we are accustomed to hearing about. Specifically, this is known as a “Supply Chain Attack”. This simply means that rather than breaking into digital assets of Solar Winds, other third parties were targeted that made use of the Orion software package.

With this kind of approach, the Cyberattacker was thus able to breach into the lines of defense of many other private and public entities.

For example, in this situation, over 30,000 entities were impacted on a global basis. Now the question is, what was the main point of entry by which all of this havoc was created? Well, back in December 2020, many of Solar Winds’ customers that made use of Orion already had deployed two major software updates to it.

But what were thought to be system patches were actually pieces of nefarious malware, disguised to look like legitimate and safe downloads.

Even more bewildering is the fact that the Cyberattackers already had gained access to the software development platforms that created these updates going back as far as October 2019. They were able to access them through the gaps and vulnerabilities that were present in the many Microsoft Office 365 that the employees of Solar Winds made use of on a daily basis.

So, once the Cyberattackers were in and were able to stay to that way without going unnoticed, they then examined some of the best ways in which they could cause the maximum amount of damage that was possible. They determined that inserting Trojan Horses into these platforms would be the best way to accomplish this goal.

So, in March 2020, the insertion of these malicious payloads started to take place, which would become known as “SUNBURST”. But apart from this, the Cyberattackers also created various backdoors in these payloads that would communicate with third party servers over which they had control over.

From here, any Personal Identifiable Information (PII) datasets of both employees and customers could be covertly hijacked, and either be sold on the Dark Web for a rather nice profit or be used to launch subsequent Identity Theft attacks.

But what was even worst is that these malicious payloads, backdoors, and Trojan Horses, actually appeared to be legitimate modifications to the software patches and upgrades that were ultimately downloaded by the many business and government entities that made use of the Orion system.

Now, the next question is how could this level of believability actually be established, and why did it take so long to discover?

Well, the various types of malicious payloads were inserted into the "SolarWinds.Orion.Core.BusinessLayer.dll". These are the Dynamic Link Libraries (DLLs) which were created for the software patches and upgrades exclusively for Orion. In order to get through, these DLLs were signed by Digital Certificates that verified their authenticity but were also covertly tampered with.

To make matters even worse, these DLLs were designed to be dormant for a period of 14 days, so that any confidential information could be easily transmitted back to the third-party servers.

The Timeline Of The Attack

It is important to note that the Solar Winds security breach did not happen just all at once. Rather, there was a lot of thought and planning put forth by the Cyberattackers, as the following timeline demonstrates.

From The Standpoint of the Cyberattackers

September 4th 2019:

The Cyberattackers gain the first known foothold into the Solar Winds IT and Network Infrastructures.

September 12th, 2019:

The Cyberattacker group deploys the first malicious payload into the Orion Software platform. This deemed to be just a test run, as the hackers used numerous servers located in various parts of the US in order to cover their network tracks.

February 20th, 2019:

The Cyberattackers do a second test run of the malicious payload in order to make sure that it will cause the damage that it was created to do.

June 4th, 2019:

The test code is removed again so that it cannot be detected. After this second trial run, it appears all is working properly.

From The Standpoint of Solar Winds

December 8th, 2020:

Fire Eye, one of the world's leading Cybersecurity firms, made it known to the public that its IT and Network Infrastructures were hacked into, and that the Cyberattackers even did away with its Red Teaming Penetration Tools.

December 11th, 2020:

Fire Eye also makes the discovery that Solar Winds had also been compromised, to a great degree. The realization that this was actually a Supply Chain style attack came when Fire Eye further discovered that Orion Platform, which was used to deploy the software updates, was also hacked into between the timeframe of March 2020 and June 2020.

December 12th, 2020:

Fire Eye formally notifies Solar Winds that their Orion Platform has been the vehicle for deploying the malware, through the software upgrades and patches. At this time also, the National Security Council of the US Federal Government also intervenes in order to ascertain if any agencies had been impacted by this Cyberattack.

From The Standpoint of The American Public

December 13th, 2020:

A number of key events occurred on this date, which are as follows:

- The Cybersecurity and Infrastructure Security Agency (aka "CISA") requires that all US Federal Government agencies to discontinue use of the Orion Platform immediately.

- Solar Winds releases temporary fixes that the impacted entities could use in order to mitigate the risk of further damage taking place.

- Fire Eye makes this Cyberattack officially a Supply Chain hack, because other third parties were also impacted, namely some of the largest companies in the Fortune 500.

- Microsoft also intervenes and explains to the public how its customer base could be impacted by this Cyberattack.

- The hack makes the news wires for the first time, with finger pointing and blame being at nation state threat actors.

From The Standpoint of Risk Mitigation

December 15th, 2020:

Key events also transpired on this date, which include the following:

- Solar winds releases the first software fixes to further mitigate the damage that has already been done.

- The first victims have been identified.

- The CISA and the FBI launch joint efforts into determining how the Solar Winds breach occurred in the first place, and to further investigate the damage that has been done to US Federal Government agencies.

The Victims Of The Attack

Recent reports peg the total number at about 18,000 individual victims, which were primarily employees. Over 40 business entities were impacted, and according to Microsoft, 44% of these were technology related companies. Here is a listing of which companies were hit by this:

- US Department of Commerce;
- Department of Defense;
- Department of Energy;
- Department of Homeland Security;
- Department of State;
- Department of the Treasury;
- Department of Health;
- Microsoft;
- Intel;
- Cisco;
- Nvidia;
- VMware;
- Belkin;
- FireEye;
- Cisco;
- Deloitte;
- Mount Sinai Hospital;
- Ciena;
- NCR;
- SAP;
- Intel;
- Digital Sense;
- Stratus Networks;
- City of Page;
- Christie Clinic Telehealth;
- Res Group;
- City of Barrie;
- TE Connectivity;
- The Fisher Barton Group;
- South Davis Community Hospital;
- College of Law and Business, Israel;
- Magnolia Independent School District;
- Fidelity Communications;
- Stingray;
- Keyano College;
- NSW Health;
- City of Kingston, Ontario, Canada;
- Ironform;
- Digital Sense;
- Signature Bank;
- PQ Corporation;
- BancCentral Financial Services Corporation;
- Kansas City Power and Light Company;
- SM Group;

- CYS Group;
- William Osler Health System;
- W. R. Berkley Insurance Australia;
- Dufferin County, Ontario, Canada;
- City of Farmington;
- Newton Public Schools;
- Stearns Bank;
- Ville de Terrebonne;
- Hamilton Company
- Cosgroves;
- City of Moncton;
- Mediatek;
- Capilano University;
- City of Prince George;
- Community Options for Families & Youth;
- IES Communications;
- Saskatoon Public Schools;
- Regina Public Schools;
- Public Hospitals Authority, Caribbean;
- INSEAD Business School
- DenizBank;
- Bisco International;
- IDSolutions;
- Arizona Arthritis & Rheumatology Associates;
- Optimizely;
- Aerion Corporation;
- Pima County, Arizona;
- City of Sacramento;
- Clinica Sierra Vista;
- Sana Biotechnology;
- Ecobank;
- Helix Water District;
- Lukoil;
- Mutual of Omaha Bank;
- NeoPhotonics Corporation;
- Samuel Merritt University;
- College of the Siskiyous;
- Vantage Data Centers;
- Vocera Communications.

The Lessons Learned From The Attack

Given the large scope of this breach, there are many key takeaways an IT Security can apply, but the following are some of the big ones:

1) <u>Always know where your source code is coming from</u>:

As it was reviewed in our last article, the malicious payload was inserted into the various Dynamic Link Libraries (DDLs), and then masqueraded as a legitimate software software/upgrade to the Orion Platform. In this instance, it is unlikely that any kind of tests were conducted in the source code of the software to make sure that there was no malware in them before they were deployed onto the customer's IT/Network Infrastructure. Had this been done, it is quite probable that this kind of attack could have been stopped in its tracks, or at the very least, the damage that it created could have been contained. Therefore, it is crucial that CISOs take a proactive approach in testing all forms of source code (for example, whether it is used in creating a Web app or software patch) to remediate any gaps and vulnerabilities before they are released out to the production environment.

2) Vetting out of third parties:

The Solar Winds security breach has been technically referred to as a "Supply Chain Attack". This simply means that the Cyberattackers took advantage of the vulnerabilities of third parties that Solar Winds made use of, in order to inflict the maximum damage possible. This underscores the importance of one of the most basic rules: Always vet your suppliers before you hire and onboard one. This means that a CISO, you need to make sure that your IT Security is carefully scrutinizing the security procedures and policies of that particular third party that you are thinking of outsourcing some of your business functions to. It must be on part of what you have in place in your organization, or even better than that. But simply making sure of what your potential supplier has put into place in terms of controls is not a one-time deal. Even after you have hired and have a business relationship with them, you need to make sure that they are strictly enforcing these controls on a regular basis. This can take place by conducting a security audit. In the end, if your supplier becomes a victim of a Cyberattack, and the Personal Identifiable Information (PII) datasets you have entrusted the are breached, ***you will be held legally and financially responsible, not them***.

3) Keep things simple and easy to track:

It is simply human nature to think that investing in a large amount of security tools and technologies means that you will be immune from a security breach. But in reality, this is far from the truth. In fact, taking this proverbial "Safety In Numbers" approach simply expands the attack surface for the hacker, which was experienced in the Solar Winds breach. Instead, it is far wiser to invest in perhaps 5 firewalls versus 10 of them but making sure that they are strategically deployed to where they are needed the most. By using this kind of methodology, not only will your IT Security team be able to filter out for those threats that are real, but you will also be able to pinpoint the entry point of the Cyberattacker in a much quicker fashion, versus the time it took Solar Winds, simply due to the fact of the overload of tools and technologies they had in place. Because of this, and as it was also pointed out in the last article, it took literally months before anybody realized that something was wrong. In this regard, you may even want to make use of both Artificial Intelligence (AI) and Machine Learning (ML) tools. With this kind of automation in place, false positives will be a thing of past, and those alerts and warnings that are legitimate and for real will be triaged and escalated in a much quicker time frame.

4) Make use of segmentation:

In today's environment, many businesses are now seriously considering of adopting what is known as the Zero Trust Framework. This is the kind of methodology where absolutely nobody is trusted in both the internal and external environments. Further, any individual wishing to gain access to a particular shared resource must be authenticated through at least three or more layers of authentication. But apart from this, another critical component of this the creation of what are known as "Subnets". With this, you are breaking up your entire network infrastructure into smaller ones. But what is key here is that each of these Subnets has its own layer of defense, so it becomes almost statistically impossible for a Cyberattacker to break through each and every layer. Solar Winds did not take this approach with their network infrastructure, so as a result, the Cyberattackers were able to get in through the first time around.

5) Update your security technologies:

   With the advent of the Remote Workforce, the traditional security tools such as the Virtual Private Network (VPN) has started to reach their breaking points, and thus their defensive capabilities. Because of this, it is important that you consider upgrading these systems to what is known as the Next Generation Firewall. These kinds of technologies are now becoming much more robust in ascertaining malicious data packets that are both entering and leaving your network infrastructure. Solar Winds did not invest properly in these kinds of upgrades, so therefore, the Cyberattackers were able to penetrate through the weaknesses of the VPNs that they were making use of.

Conclusions

Upon a closer examination of this list of victims, one can see that this truly represents a cross section of industries. For example, public, private, educational, government agencies (on both the federal and local levels), and even nonprofit centers were heavily impacted.

It is important to keep in mind that many of these organizations listed here may not have been hit directly, but rather, they were hit indirectly because of the cascading nature of this security breach.

But none the less, this list clearly demonstrates that the Solar Winds attack has been deemed to be one of the largest in the world, and attacks like these or even worse are likely to occur and occur again until a proactive mindset is completely enforced with CISOs and IT Security teams on a worldwide basis.

The financial damage caused by the Solar Winds breach is now up to $90 Million and is estimated that it could even reach as high as $100 Billion when all is said and done.

In the end, whenever a Cyberattack hits any business entity, no matter how large or small, it is always very important to reconstruct a detailed timeline like this one. The primary advantage of this is that it can aid in the process of attribution, which is determining who the actual perpetrators are.

Also, it can pinpoint those areas in which latent evidence may lie, which is very crucial in carrying out the forensics investigation.

Sources

1) https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention

2) https://www.kiuwan.com/solarwinds-hack-timeline/
3) https://blog.truesec.com/2020/12/17/the-solarwinds-orion-sunburst-supply-chain-attack/
4) https://www.datacenterknowledge.com/security/list-known-solarwinds-breach-victims-grows-do-attack-vectors
5) https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided
6) https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/#:~:text=Cleaning%20up%20SolarWinds%20hack%20may%20cost%20as%20much%20as%20%24100%20billion,-Government%20agencies%2C%20private&text=American%20businesses%20and%20government%20agencies,companies%20and%20U.S.%20government%20departments.
7) https://www.crn.com.au/news/12-lessons-learned-from-solarwinds-breach-rsa-conference-564841