White Paper

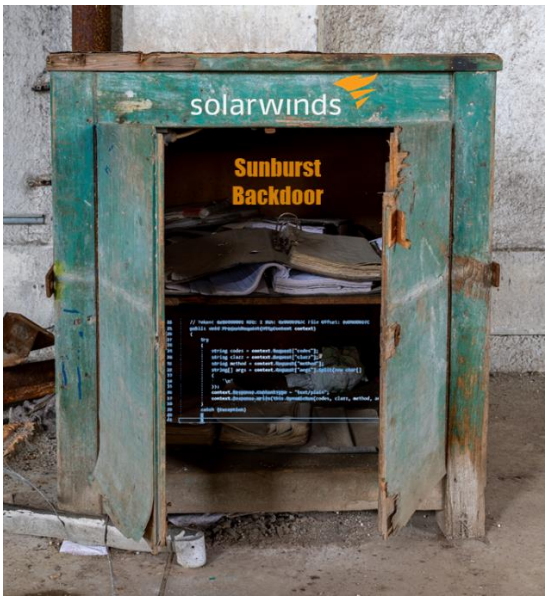
SolarWinds – The comprehensive review

March 2021

In early 2019, hackers secretly broke into Texas-based SolarWind's systems and added malicious code into the company's software system. The system, called "Orion," is widely used by companies to manage critical IT resources. SolarWinds has 33,000 customers that use Orion, according to the SEC documentation. E2Security has investigated the cause of the cause to create a "lessons learned" for their customers and to come up with a quick checklist on "what to consider" in order to apply the findings.

Agenda:

- Opps -this is the first time… …that it happened again.
- Why SolarWinds?
- Why did the hack happen without being noticed?
- How was the SolarWinds hack identified?
- Why did it happen at this particular time?
- How did the Solar Winds (hack) probe technically work?
- Lesson learned: Security hygiene isn't enough
- Lesson learned: Third-party risk assessment



Opps -this is the first time… …that it happened again.

When the SolarWinds hack went public Q03/2020 Security Experts across the globe raised their opinion in various forums stating that “a hack like this did not come as a surprise after the homeland security and NSA had suffered a data breach following a hack where hackers gained access to their own very effective hacking tools and backdoor information.

Looking at the hack, its root cause and impact there are major learning for data security and data privacy.

New investigations shows, that the attackers start the activities in April 2019 with the first injection of test codes and started the first trial runs. In February 2020 the Sunburst where compiled and deployed to the customers environments.

Ten month later (1) Solarwinds where notified of the Sunburst attack.

Why SolarWinds?

In early 2019, hackers secretly broke into Texas-based SolarWind’s systems and added malicious code into the company's software system. The system, called "Orion," is widely used by companies to manage critical IT resources. SolarWinds has 33,000 customers that use Orion, according to the SEC documentation. The hack done enabled the hacker’s access to all SolarWinds Customers internal data – PII, IP the crown jewels of any company.

And not just companies where impacted. Attacked where also US agencies — including parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury.

Aiming at targets like SolarWinds was a very clever approach leading to believe that it was strategically so well planned that only a government related group using time, money, and resources in such a way. Once the homeland security got hacked it did not result in any immediate monetary gain but lead to provide access to information about the core of the IT infrastructure within larger organizations – as for example other government departments. Why would any hacker attack such a target instead of going after Banking, Credit Card or Password -Data?

The installed malware code established a backdoor to customer's information technology systems, which hackers could use to install additional malware on the impacted system to help them spy on companies and organizations. As SolarWinds had a major position in network management market the hack worked like a “super spreader”.

According to FireEye, this attack was the work of sophisticated attackers. This more specifically includes the sophistication of both development and operational teams. The development teams deployed anti-analysis countermeasures. The malware was developed to check file system timestamps to ensure the product has been deployed for 12 to 14 days before it phones home. This effectively prevents the use of malware sandboxes or other instrumented environments to detect it.

As a result of that distributed “cover-up” and “countermeasures” the SolarWinds hack remained undetected for a very long time. The threat actors began distributing the backdoor in March 2020, which sat silently in some of the compromised networks for months while harvesting information or performing other malicious activity.

Why did the hack happen without being noticed?

In April 2017 the US homeland security and NSA reported a data breach that impacted vital confidential data as for e.g., spyware and very efficient hacker tools. Some NSA developed hacker tools like Eternal Blue was leaked by the Shadow Brokers hacker group and it was suspected to be used during the SolarWinds hack.

The timing of the SolarWinds hack was perfect while the attack reached back more than a year. Once the outcome of the hack escalated, it appeared at a time when the public was distracted by the political debate resulting out of presidential election campaign.

For the hacker community it was the perfect time to launch a massive spying attack on the US government and globally acting US companies.

As the tools provided by SolarWinds were used by government authorities enforcing the highest standards in IT security one might ask why it took them so long to identify the attack with the number of resources they have at hand?

Among the Solar Winds Customers were not just the Homeland Security and DoD but also the NSA. The NSA is being considered as the “home of cybersecurity intelligence” within the US government an organization that has the most advanced tools and all that cool stuff - and even the cool stuff did not catch the hack?

On top of it is one of the jobs of the NSA to review every code of any software suppliers servicing the DoD – so did they miss out on it? Is that a big red flag for the system established?

Well, the answer is twofold: If neither NSA nor any other big security player detected the Malware it was more a matter of coincidence than incompetence – it is called Murphy’s law and it is still valid.

How was the SolarWinds hack identified?

FireEye being one of the most sophisticated cybersecurity companies and a leader in cybersecurity is a major target for hackers as they have an awesome access to all sorts of customer environments. If you can compromise their security software, you have “the golden key” to all its customers. As a leading security company, FireEye has great defense mechanisms and one of their security measures is a mandatory two-factor authentication for their own employees. It occurred that a notification triggered once a FireEye employee has activated a new device to verify his identity appeared in the network and had been visible to the internal security. Triggered by the event the security expert investigated the case and asked the employee, “if he had a new phone?” and as the answer was negative FireEye began digging….and digging.

Why did it happen at this particular time?

The roots of this attack go back more than a year, and the activity escalated at a perfect time – again the US government agencies were so distracted as the presidential election campaign started. In particular, the US government, and even the security specialists within the US government and Security organizations, were busy worrying about securing the US presidential elections and potential hacking activities – right thing to look at but the wrong place. It just happened to be the "perfect" time to launch a massive spying attack on the government – though the backdoor.

How did the Solar Winds (hack) probe technically work?

Through the SolarWinds attack, the threat actors gained access to the SolarWinds Orion build system and added a backdoor to a legitimate DLL file, including trojanized package containing the Sunburst backdoor. All the detected attacks in this case require meticulous planning and manual interaction.

Current analyses have shown that the implemented Sunburst backdoor, includes several features that overlap with a previously identified backdoor known as Kazuar. Kazuar is a .NET backdoor first reported by Palo Alto in 2017.

Both Sunburst and Kazuar implements a delay between connections to a C2 server, with the goal to make the network activity less obvious. Sunburst uses the same formula known by Kazuar to calculate sleeping time. The only difference between Kazuar and Sunburst is that the code used by Sunburst is less complex.

The backdoor is designed to retrieve and executes commands, called 'Jobs,' after an initial dormant period of up to two weeks it transfers files, executes files, profiles the system, reboots the machine, and disables system services. Furthermore, the backdoor 'masquerades' its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files which allowing it to blend in with legitimate SolarWinds activity making it hard to detect by anti-virus tools and other cybersecurity measures.

On top of it the backdoor also used multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers. The attackers created a 'perfect stealth mode' for the malware running on the system while the malicious source code was delivered via the automated software update mechanism – truly domed for oblivion!

The whole process designed lead to happens when the code is being compiled at the last minute and contains the digital signature of SolwarWinds. Code signing and digital certificates are a good thing if – and only if the code was really authorized by the vendor. But in the SolarWinds attack, the attacker also stole the digital signature. The hackers did that at SolarWinds itself during the compilation process with the effect that the distributed software packages looked like it was approved by SolarWinds.

Using "on the shelf security stuff" and commodity tools, it was almost impossible to find, but once they were in, anybody who downloaded at least two relatively recent updates of the Orion software in 2020 downloaded the backdoor.

Once installed, the malware 'looked around' to see where it was, "phoned home" to a command-and-control network run by the hacking group, which enabled them to enter the network and take further action. Connected with the original attackers they could decide whether to deploy additional code to exploit the target further.

```
long random_multiplication(Random random_0, long long_0) {
    return (long)(random_0.NextDouble() * (double)long_0);
  }

TimeSpan get_randomized_sleeping_time(Random random_0,
        TimeSpan timeSpan_0, TimeSpan timeSpan_1)
  {
    if (timeSpan_0 > timeSpan_1)
    {
      TimeSpan timeSpan = timeSpan_0;
      timeSpan_0 = timeSpan_1;
      timeSpan_1 = timeSpan;
    }
    long num = random_multiplication(random_0,
                timeSpan_1.Ticks - timeSpan_0.Ticks);
    return new TimeSpan(timeSpan_0.Ticks + num);
  }
void wait_between_connections() {
    for (;;) {
      ...
      if (timeSpan2 >= timeSpan) {
        break;
      }
 TimeSpan timeout = get_remaining_time(timeSpan - timeSpan2,
                                       this.timespan);
    Thread.Sleep(timeout);
    }
  }
```

The operational teams appear to have used specific infrastructure for each victim, reducing the use of network-based Indicators of Compromise, which companies like FireEye use in part to detect malicious activities. Using these techniques, the attackers were able to evade even best-in-class detection technologies.

The impacted update packages - now effectively malware, were then distributed to SolarWinds customers via an automatic update platform used to push out automated software patches.

The attackers even managed to modify an Orion platform plug-in called **SolarWinds.Orion.Core.BusinessLayer.dll** which is distributed as part of Orion platform updates.

The trojanized software builds for Orion versions 2019.4 HF 5 through 2020.2.1 were released between March 2020 and June 2020. The trojanized component was digitally signed and contained the implemented backdoor communicating with third-party servers being controlled by the attackers.

Lesson learned: Security hygiene isn't enough

SolarWinds is neither the first incident of that kind nor will it be the last. The hack made visible that third-party vulnerabilities can-and-will harm your company. Whenever a third party is involved Metcalf's law applies: The potential attack vectors for an attacker increase proportionally to the square of the number of possible connections while the cost to attack proportionally to the number of participants. Metcalfe's law explains some of the network effects of communication technologies in the field of the Internet.

A single sub-contractor added to your system (connection) is a threat but with every additional sub-contractor and their interaction on top of it the increase in possible attack vectors result out of this communication increases.

The data security and data privacy mechanism used by your supplier might look good on paper, but its effectiveness is beyond your control – and even worse, if your supplier is using a sub-contractor the privacy measures are 'out of your control'.

Your supplier may use best-in-class security mechanisms and guarantee that he will not be exposed to the limitations of security hygiene as the 'Key to avoid any data breaches' but the remaining question will always be 'how should large organizations' manage information security landscape end-2-end to protect their "key assets" if suppliers are involved?

Here are some learnings:

Cheap Labor = Cheap Security !?

It seems that SolarWinds certainly have underspent on security. One example is that its software engineering was outsourced to cheaper software developers overseas, even though that typically increases the risk of security vulnerabilities. Reducing cost up to a point that all you get is cheap labor but 'no intelligence' results in sloppiness.

Indication: In 2019, before this hack happened it was already known to the hacker-community that the password of the update server's for SolarWinds's network management software was reported and published to be "solarwinds123." – no comment needed.

Sloppy Software leading to "on premise" risks

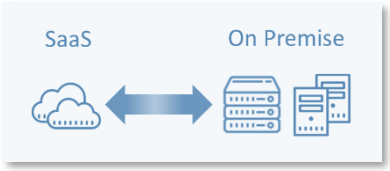
If companies are cutting costs and outsource their software development to 'cheaper countries' its customers won't notice – until they are being hacked. In case customer are being hacked it happens after the fact they will have already paid for their license to oblivion – in other words, the risk of a cyberattack is being transferred to the customer.

Software Supply Chain and On-Premise – state of the art?

It's important to know that SolarWinds Orion is an on-premises product. On-Premises products require local resources to install and keep it current. Dedicated resources will have to be trained to be kept current.

On-premises products carry a whole lot of potential security risks that need to be constantly observed and taken care of by IT operations and IT leadership.

What's the option?



If companies choose a SaaS solution they decide what data is to be send to the SaaS provider. The customer does not need to install complex software on local servers and keep it current. With a SaaS solution there is no risk of a local server or network being hacked with potential access to other systems acting as a super spreader within a corporate network.

The usage of on-premises tools was a contributing factor for the SolarWinds "supply chain" hack. The attackers were able to use the compromised patch to infiltrate other systems and used these systems to infiltrate more systems.

Most SaaS providers use a modern security architecture that compartmentalizes the data, security, and identity as well as access management by placing them into different cloud accounts. The access to critical systems is restricted to high authorized admins and is being granted based on the "least privileges" and user access requires multifactor authentication.

Within the SaaS solution, data at-rest is generally encrypted by default. Encryption keys are secured in a Key Management System (KMS) where keys are also encrypted. This helps secure customer data in the event of a rogue application gaining access to the SaaS solution.

If attackers gain access to on-premises solutions into the customers network environment, the attacker can potentially read any of the data flowing within that network.

Once they have access the attacker often move laterally from one device, host, application or service, to another and extract everything they can. By design, that's just not possible with SaaS-based tools.

Lesson learned: Third-party risk assessment

The SolarWinds attack makes the necessity of a thoroughly supplier management and supplier risk assessment very visible. It's a known fact of the "analog world" that suppliers can make -or break companies. If not following a stringent control, quality management and regular audits the risks resulting out of poor quality are far greater than the effort invested into managing the supplier thoroughly.

Supplier Management is a known problem. One might remember the security breach impacting Target breach resulting out of a weakness in supplier management. A maintenance company with system access was exploited in order to distribute malware that compromised the Target point-of-sale system. Recent forms of supplier attacks included the hijacking of Ruby Gem and npm repositories that could potentially compromise the distribution of software libraries used by thousands of developers worldwide.

Each time after such an incident the security community is alerted that third-party risk management is a requirement to handle security threats. However, despite the best efforts of organizations to install security protocols for their vendors the remaining risk of a compromise results out of the increasing sophistication of the attack vectors explored by hackers. They are heavily attacking suppliers as they seem to be an easier target than a multi-million-dollar enterprise with a solid security systems.

Any investment into information security needs to reduce the risk of cyber loss

As much as the SolarWinds attack teaches us a lesson in managing cybersecurity risks and improving governing capability to avoid data breaches it also exposes the limits of good security hygiene alone to stop them. In other words, organizations must be increasingly prepared to deal with breach events and focus on mitigating the risk of a resulting loss.

Risk of loss, in the legal sense, means which party bears the burden to pay the cost of a breach and the gets the blame resulting out of a loss of reputation. Would you still buy SolarWinds products today?

The risk of loss and a resulting liability may shift depending on applicable laws, while the contractual obligations in place may add another dimension to the numbers – international liability claims.

To adequately protect virtual assets, organizations must increase their investment in mechanisms to mitigate the risk of loss in the event of a failing security mechanism.

Increased focus on data privacy risk mitigation

Mechanisms to mitigate the risk of cyber loss include the ability of an organization to evaluate and minimize the risk materialization of an organization caused by a potential incident, as well as to withstand that incident with a minimum impact - technically and financially,

The following mechanisms can assist with these objectives.

Topic	Description
End-2-End Risk Management	Evaluating and minimizing security and data privacy risks is done through risk assurance mechanisms. While managing third-party risk through security evaluations alone will not help reduce the likelihood of breaches. The suppliers must be rated according to their potential harm and access to the infrastructure and based on a criticality auditing measures have to be put in place. Even though the risk is never zero. Tools like data protection impact assessments should be used to identify the level of scrutiny that the third party warrants and the resulting data protection requirements needed shall be translated into contractual obligations – otherwise there is no lever. According to local law such as the EU General Data Protection Regulation or California Consumer Privacy Act, organizations not only have the duty to ensure reasonable security safeguards to protect personal data, but are being held liable any data breach, even if caused by their third party vendor. Therefore, they should mitigate the risk of loss by making sure that contractual commitments commensurate with the risk exposure are put in place with the third parties.
Security Incident Management	Incident Management and Security Incident Management on top of it using a tested response method mitigates technical and financial impact to an organization in case of a data breach. A Security Incident response plan must be defined, implemented, trained and tested in order to become effective. Once done it will speed up recovery and remediation, notification and will save valuable time when time is money. It will add to your reputation and can mitigate financial and legal consequences. Local law may enforce immediate notifications to the appropriate parties including regulatory authorities in case of a breach event. Failure to comply lead to stiff penalties and can lead to additional liabilities if deemed in violation of an organization's legal obligation.

Topic	Description
Cyber Risk Insurance	Insurance companies started offering cyber insurance to cover the cost of performing breach management protocol, incident responses and potential liabilities. A cyber risk insurance policy typically only covers associated investigation and restoration cost such as forensics teams to investigate the incident and establish a root cause. When it comes to related liability or public relations handling as well as reimburse affected parties or regulatory penalties the waiver kicks in. The latter is seen as a consequence of misbehavior or even benevolent neglect and is typically carved out. Important to say that any good cyber risk policy including liability insurance will shield the company from potential liability claims resulting out of cyber loss. It must be explicitly and specifically explained in the contract – if it's not there it will not be covered and can't be transferred. However, organizations should not solely rely on risk transfer but may combine it with • solid risk management and • security incident mechanisms. • negotiate the contractual commitments of third parties and • cover the delta with the liability protection cap in its cyber risk insurance. This will prevent any push backs of security claims caused by the organization's inability to respond quickly to a security incident or any lack of a well-designed security incident response mechanism.
Review Access for on-premise Software	Review any access for on-premises software on a regular basis Any permission and any privileged user accounts bear a risk: While SaaS-based software does not have a need for complex third-party software your on-prem network surely does. With on-prem software one must grant elevated permissions or highly privileged accounts for the software to be configured to run. Funny enough the SolarWinds customers highly exposed were the ones that were diligent about installing Orion patches in a timely manner. Anyone running a back-leveled version of Orion was not impacted by this hack. Sadly, this is an example of IT shops choosing an on-prem solution "doing everything right" in regards to patches found out that those actions actively put them in greater danger.

Autor:

Kay Wolf

Kay Wolf, CEO and Founder of **e2 Security GmbH**, is an innovative and highly experienced Senior IT Management Consultant in the areas of IT strategy, IT Security, IT Governance, IT operations processes, Business Technology and IT migrations - with over 20 years of experience across multiple industries including Manufacturing, Communications, Defense & Governance, Finance & Insurance, Energy and Consumer & Transportation.

EADPP member of Committee Events & Communication

https://www.eadpp.eu/organisation/

https://www.linkedin.com/in/kaywolf/