SolarWinds
MICS-204 Report 2, Summer 2024

Karl-Johan Westhoff
email kjwesthoff@berkeley.edu

UC Berkleley School of Information
MICS Course 204 Summer 2024

Summary Of The Breach

December 13, 2020 a vigilant security analyst at the security company FireEye (later Mandiant) reacted to an unauthorized phone registering on their network [1]. It was during the covid pandemic so a lot of employees were adding new 'work from home' equipment, but the analyst decided to investigate and determined that the company had been breached, someone unauthorized was logging in. After a thorough search through systems, the breach was isolated to origin in the company's 'SolarWinds Orion' network monitoring system. The SolarWinds Orion product was(is) a tool for monitoring corporate networks and endpoints [2], meaning it had high system privileges on windows networks.

It turned out that the SolarWinds company had been hacked, and a trojan had been implanted with the Orion software. The trojan had been transplanted into SolarWinds software build pipeline (it was not present in codebase), and pushed to their customers with digitally signed updates.

Sunburst is a sophisticated malware deeply integrated with its SolarWinds host, it has a small footprint[1] and hides in plain sight. Command and control functions communicate via the same ports and protocols as Orion thereby evading detection, another feature of the malware is that it patiently lies dormant for extended time on the host to evade detection through logging. The trojan gathered data on the victims and made it possible for attackers to move laterally on the victims systems and install further exploitation tools[2]. It is assumed that relatively few[3] high value targets were exploited further, the targets were government institutions defense and security companies, hereunder FireEye who discovered the breach.

[1] 3500 lines of code
[2] Cobalt strike Beacon was mentioned[3]
[3] According to SolarWinds CISO Tim Brown in [4] Less than 100

Description Of The Attack

The SolarWinds hack is a "supply chain" attack, this has a number of advantages for the attacker:

- It utilizes the trust companies have in out-sourced resources (management have a tendency to see such things as "a risk that has been mitigated by transferring it to a subcontractor")
- The attack surface and reach is much larger for the same effort (a lot more can be hit with the same hack)
- In this case, the target is an IT security software vendor, putting the attacker in a wolf in shepherds clothing situation. In hindsight security vendors are an obvious target

The SolarWinds company was presumably hacked in September 2019[5], The attackers implanted a trojan malware to be known as "SUNBURST[4]" in the company's build pipeline for the Orion software in February 2020, prior to this the attackers even tested their malicious deployment pipeline with other pieces of code[7].

FireEye (of course) shared their findings with SolarWinds who then managed the breach with legal assistance, CISA and CloudStrike[5]

SolarWinds never found any malware in their source code, the malware was implanted into the build pipeline and thereby evaded code analysis.

SUNBURST

The attackers transplanted the SUNBURST Backdoor malware into the SolarWinds.Orion.Core.BusinessLayer.dll[3]. The dll was digitally signed by SolarWinds and distributed as updates to clients systems.

[4] Microsoft named it "Solorigate" [6]
[5] The handling of the breach has become a model for how to handle devastating breaches, SolarWinds CISO Tm Brown talks about it in [8]

Malware analysis

The SolarWinds.Orion.Core.BusinessLayer.dll has been decompiled and analyzed. FireEye did a thorough analysis in[3] and CISA provided a deatiled analysis in [8] furthermore [9] provided a walkthrough decompiling the code using dnSpy, which the following is inspired by.

Stealth

Data Collection

Exfiltration

Conclusion

Something does not add up wrt. the presumed breach time and the features of the malware code, and the implementation in the build pipeline. The attackers would need to know the codebase with more than a decompilation would reveal and they would also need details on the solar winds build pipeline. This would either require a longer reconnaissance period or insider knowledge..

Description of the attack (What and how vulnerability was exploited? Was malware used?)

Signatures/Attribution

Super patient

No variable names etc.., they had "washed the code" send it through a de-compiler before.. "SolarWinds Hackers[6]"

Impact/Legal Actions

Impact and/or Legal Actions (Was the company subject to fines? How was the company affected?)

Remediation

Remediation steps (What measures were put in place to prevent future breaches?)

[6] Microsoft again had their own name "Nobelium"

References

[1] *FireEye CEO on how the SolarWinds hack was discovered CNN video*. https://www.cnn.com/videos/business/2021/02/24/fireeye-ceo-solarwinds-hack.cnnbusiness. Accessed: 2024-06-13.

[2] *Orion Platform (Web archive)*. https://web.archive.org/web/20201214092129/https://www.solarwinds.com/orion-platform. Accessed: 2024-06-13.

[3] *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor google*. https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor/. Accessed: 2024-06-13.

[4] Tim Brown. *Youtube (SUNBURST From The Inside Tim Brown, CISO of SolarWinds)*. https://youtu.be/6gQ5oAWHMoU?si=mBBETA6P8e44MPs_. Accessed: 2024-06-13.

[5] Sean Michael Kerner Saheed Oladimeji. *TechTarget (SolarWinds hack explained: Everything you need to know)*. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. Accessed: 2024-06-13.

[6] *Microsoft Secutiry (MS Security Page)*. https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop. Accessed: 2024-06-13.

[7] Sudhakar Ramakrishna. *SolarWinds (New Findings From Our Investigation of SUNBURST)*. https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/. Accessed: 2024-06-13.

[8] CISA. *CISA (MAR-10318845-1.v1 - SUNBURST)*. https://www.cisa.gov/news-events/analysis-reports/ar21-039a. Accessed: 2024-06-21.

[9] cybercdh. *Youtube (SUNBURST SolarWinds Malware - Tools, Tactics and Methods to get you started with Reverse Engineering)*. https://youtu.be/JoMwrkijTZ8?feature=shared. Accessed: 2024-06-21.

Appendix A

Test