SOLARWINDS REPORT

The 2020 breach of SolarWinds exposed several vulnerabilities

BLAKE WESTBROOK & TIMOTHY WICKEY

2107-csu-rm-cyb-pt

Fullstack Academy

Professor Bryan Durrance

1/9/2022

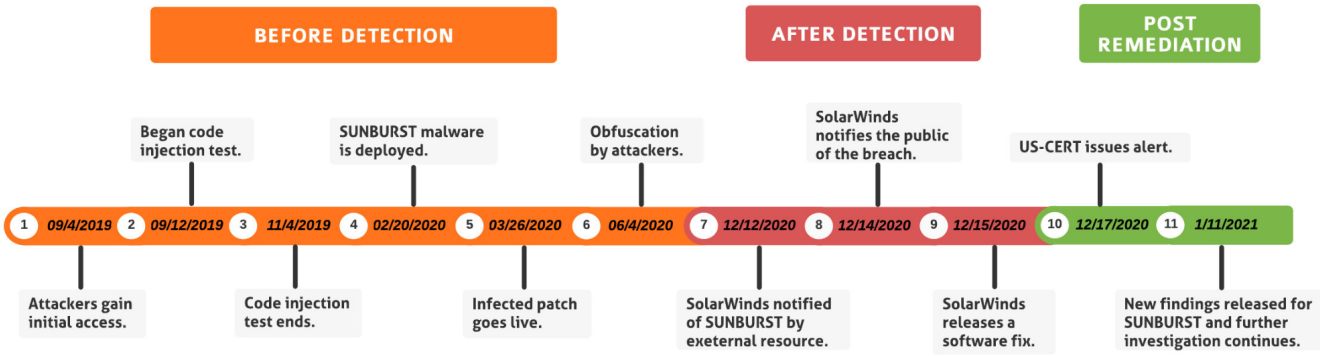
Summary

In March of 2020 one of the largest cybersecurity attacks to date was enacted against SolarWinds, an IT management company. Threat actors were able to gain access to the company's development resources, then used back door access to put malicious software into an update which was then released to customers. This supply chain attack compromised multiple civilian and government agencies for almost a year. It exposed vulnerabilities in the shared services model. It also caught many security firms and government agencies flat footed. With new tools and techniques, potential victims can mount stronger efforts to mitigate against such threats in the future.

Timeline

The SolarWinds data breach occurred over a substantial range of time. The initial compromise occurred back on September 4, 2019 when the threat actors began probing SolarWinds. This was followed up around September 12th with code injection tests to see if it was possible to include malware within compiled code. By February 20, 2020 the compiled trojan, known as SUNBURST, was completed and inserted into a patch that went live on March 26, 2020. The attackers were within SolarWinds' systems for approximately 9 months performing malicious activities. SolarWinds was notified by FireEye on December 12, 2020. The public and shareholders were notified of the breach on December 14th and a fix to the malicious code was created and released on December 15th. Further investigation and remediation continues to this day.

SolarWinds Breach Timeline



Root Cause

The SolarWinds attack was primarily the result of a trojan being inserted into the compiled code of a scheduled update. This supply chain attack allowed threat actors to create backdoors to multiple victims. Once the update was installed and the device connected to the internet, the attacker was able to establish a method of entry and was able to examine and exfiltrate data.

Affected Devices

The primary target of this attack was the Orion Platform provided by SolarWinds. The Orion Platform contains many aspects of centralized IT management including:

- Network Performance Monitoring
- Network Traffic Analyzer
- Network Configuration Manager

- IP Address Manager
- VOIP
- User Device Tracking
- Server and Application Monitor
- Storage Monitor
- Virtualization Manager
- Web Performance Monitor
- Log Analyzer

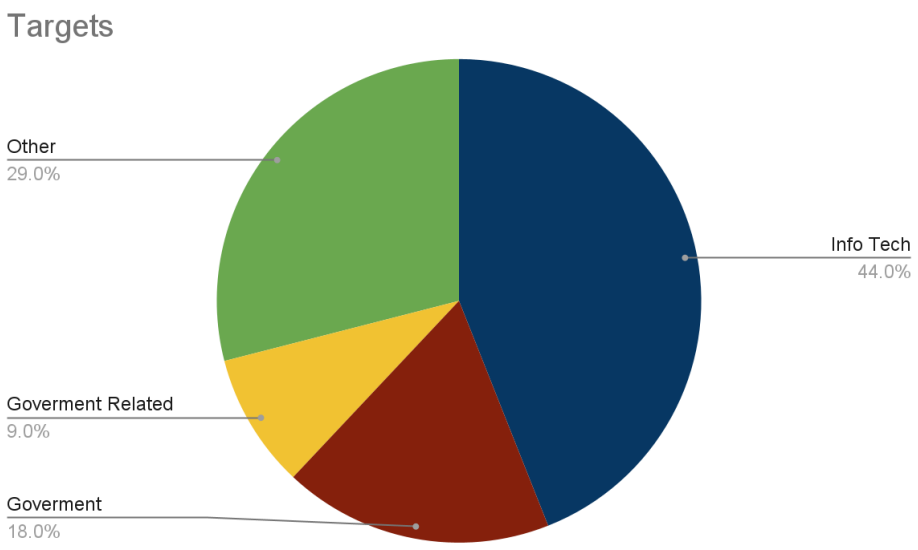
The primary purpose of the Orion Platform is centralized IT management. Many organizations rely on these types of services to simplify their IT operations. This consolidation makes a very attractive target for attackers as an entry point into multiple networks and related systems for further attacks.

Damages

Many systems were damaged in this attack including email accounts, network monitoring tools, compromised networks and FireEye's proprietary hacking tools. The attack also compromised confidentiality and integrity for customer data that was accessed by the attackers. The attack highlighted issues with detection in both the private and public sector. The Department of Homeland Security noted that they failed to catch the attack due to it being in an update which was not scanned (NPR, 2021). Undetected, this attack method could be used on future updates as well as allow potential jumps from corporate networks to system controls.

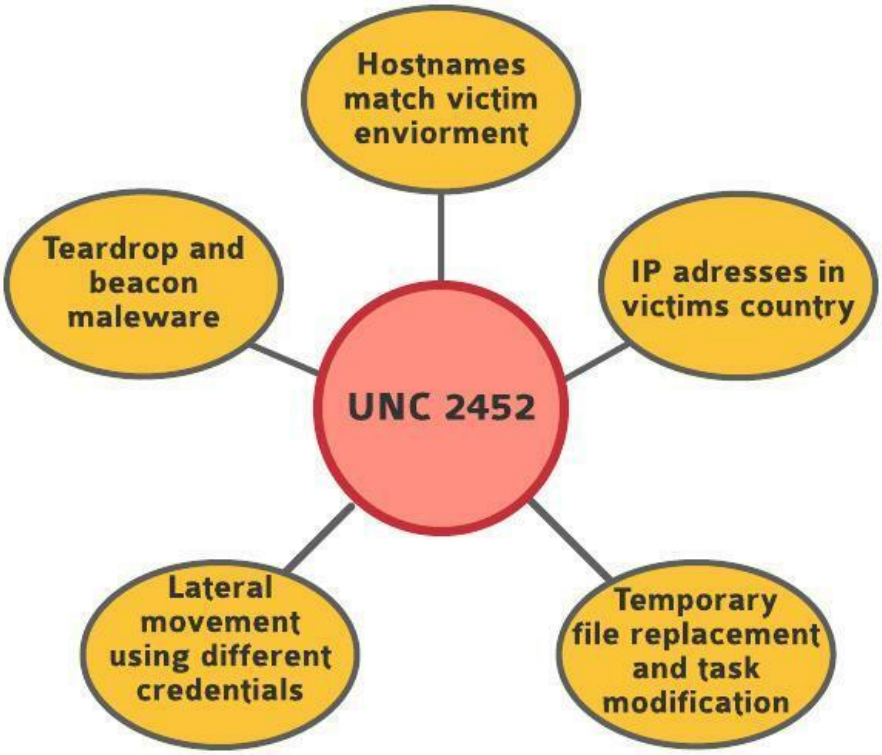
Threat actors

The threat actors involved in this breach are believed to be associated with Russia's SVR (Foreign Intelligence Service). The name of this particular threat actor is UNC2452. UNC in this case refers to a cluster of related activities. UNC2452 is a threat actor that targets a wide range of interests. Here is a breakdown of common targets:



UNC2452 routinely steals internal documents, email, and intellectual property with an emphasis on security documents and items related to IT security staff. They are not after personal Identities or financial data and generally avoid destructive or disruptive actions. UNC2452 uses sophisticated tactics, techniques and procedures to manipulate existing access and maintain robust persistence in compromised networks.

UNC2452 works to accomplish their goals with the following general approach:



Exploit

The primary vector for this attack was the Orion Platform. The two main components of this attack were a trojanized update and the internet. By infecting a planned update with malware, the attacker was able to gain access to systems connected to the platform. This created a backdoor trojan. The backdoor allowed access to any device connected to the internet. It had a base CVE score of 9.8 due to the fact that it had low complexity requirements and could be done over the network.

Methods

The attack against SolarWinds was rather complex. The attack began when UNC2452 inserted a small line of code into SolarWinds systems to check the running processor type of the device (32 bit or 64 bit). This code would then return a 1 or 0 in binary. This was essentially a proof of concept that it is possible to insert code into the system. The second step was malicious code to check when a digital repository was used, specifying the start of the build process for updates. Next a temporary update file was created to house the malicious code. This file was then swapped with the legitimate code when the update was in the compiling process. This happened at the last possible second as the source code was transitioned into binary. When the update was released to the public the threat actors got their access.

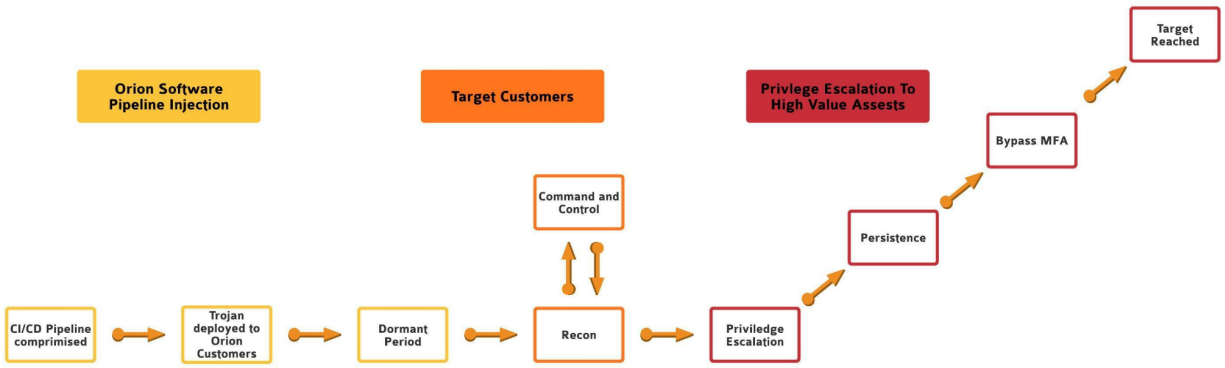
The next step of the process was lateral movement. From the initial SUNBURST backdoor, the threat actor then deployed TEARDROP, a loader that decrypts and executes embedded payloads on target systems. The attackers further used the Cobalt Strike Beacon Implant v4. This malware provides remote operation and command-and-control capabilities over target systems through an encrypted network tunnel. This malware also included data exfiltration, screen capture, and keylogger capabilities as well as the ability to deploy additional payloads. The attacker also deployed MimiKatz for credential harvesting. All types of malware served to expand access and exfiltrate data.

Lateral movement within the networks allowed the attacker to gain access to Active Directory servers. This allowed them to modify trusted domains and authenticate to Microsoft Office 365 as any user. The active directory access also allowed for reconnaissance to identify privileged accounts. Cloud resources were also vulnerable. By using GoldenSAML, the actors were able to steal token certificates and database files. They altered Active Directory's DKM thus granting secret keys. This allowed the attackers to bypass Multi Factor Authentication.

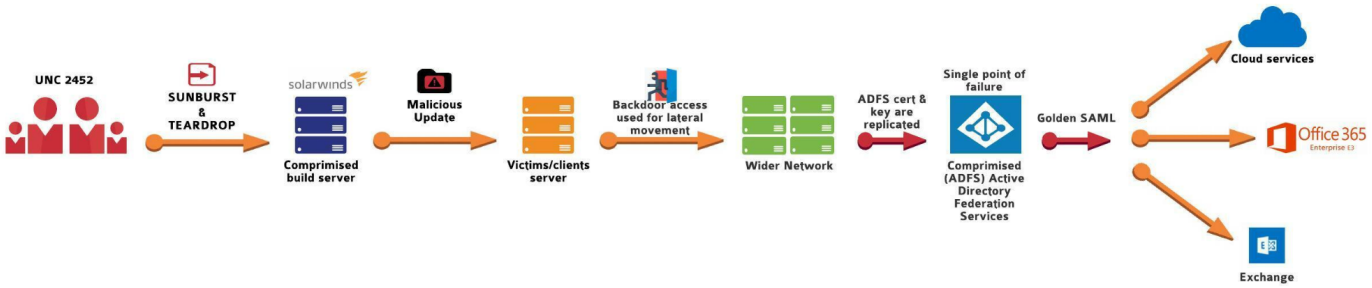
The attacker established persistence by creating multiple points of access to hijacked networks including service and application accounts. This allowed for data exfiltration using passive DNS servers. These servers did not trigger advanced warning as they were rented from US-based companies Amazon Web Services and GoDaddy. Finally the attacker performed anti-forensic remediation to scrub all traces of human interaction with the malware. This made it harder to find the attackers.

Threat Model/Diagram

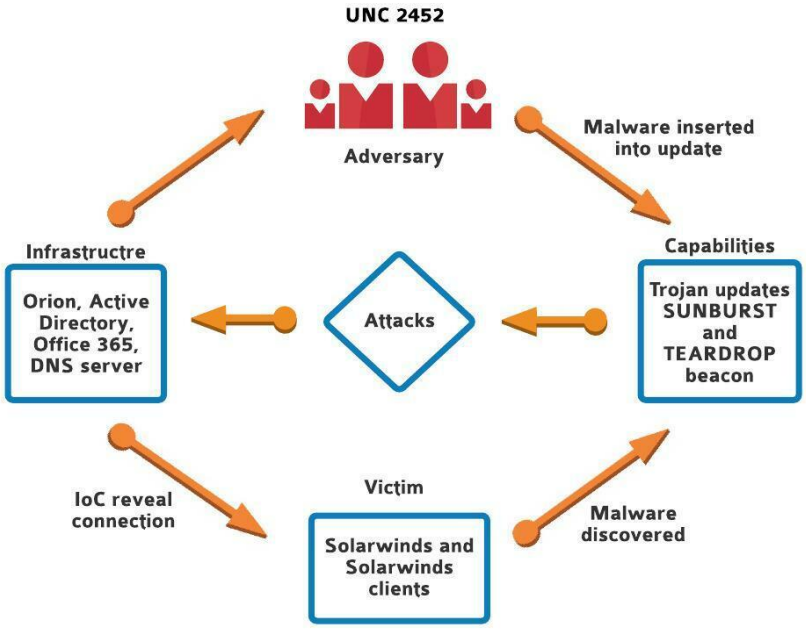
Method



Attack Flow



Diamond Intrusion Analysis



Victims

Victims of the SolarWinds breach range from Fortune 500 companies to branches of the US military and government. Post-discovery, SolarWinds put out a statement that less than 18,000 of its 33,000 customers had downloaded the malicious code (Krebs, 2020). The attack compromised the confidentiality and integrity of large swaths of data and the nature of the breach revealed that it could happen again in future updates both from SolarWinds or other third party vendors. It was one of the

worst supply chain attacks on record.

Mitigation Strategies

There are several known mitigation strategies for this breach.

1. The actual attack was well-publicized and systems should be searched for tell-tale evidence. The update in question is CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp (02af7cec58b9a5da1c542b5a32151ba1). The malware is contained in the file SolarWinds.Orion.Core.BusinessLayer.dll (b91ce2fa41029f6955bff20079468448).
2. Another mitigation strategy is to update blocklists. The attacker used several C2 servers created using a Domain Generation Algorithm to construct subdomains to the domain awsvmcloud. These types of connections and associated IP addresses should be blocked by the firewall.
3. Increase detection for problematic activities including:

    a. The attacker leaked their configured hostname in RDP SSL certificates. Certificates must be checked internet-wide for malicious IP addresses

    b. Most of the IP addresses were from VPS which could also be checked.

    c. The attacker primarily used remote access credentials. Seeing these credentials used by a single system accessing multiple different systems should be considered a red flag.

d. Another method is to look for SMB sessions that show access to legitimate directories and show a pattern of deletion and creation in a short amount of time. This is caused by the attackers removing backdoors as legitimate access was achieved.

e. There are also MITRE ATT&CK Techniques observed including:

- T1012 - Query Registry
- T1027 - Obfuscated Files or Info
- T1057 - Process Discovery
- T1070.004 - File Deletion
- T1071.001 - Web Protocols
- T1071.004 - Application Layer Protocol DNS
- T1083 - File and Directory Discovery
- T1105 - Ingress Tool Transfer
- T1132.001 - Standard Encoding
- T1195.002 - Compromise Software Supply Chain
- T1518 - Software Discovery
- T1518.001 - Security Software Discovery
- T1543.003 - Windows Service
- T1553.002 - Code Signing
- T1568.002 - Domain Generation Algorithms
- T1569.002 - Service Execution
- T1584 - Compromise Infrastructure

4. Use better tools for identification and repair. As a result of the attack, multiple security companies created firewall rules and hashes for indicators of compromise. FireEye specifically has released several to their GitHub to facilitate faster prevention and recovery. Whether using these directly or crafting in-house solutions, it should be possible to respond to such incidents.
5. Other important steps to respond to this incident include:
    a. Update older software and utilize current security patches.
    b. Isolate/contain SolarWinds servers by blocking the internet.
    c. Restrict connectivity to endpoints from SolarWinds Servers.
    d. Restrict admin accounts on SolarWinds Servers.
    e. Block internet access from endpoints with SolarWinds software.
    f. Change account passwords.
    g. Review network device configurations for modifications.

Lessons Learned

There is no denying that the SolarWinds breach is one of the worst supply chain breaches in recent history. The attackers used complex techniques to insert malware into what should have been a safe, secure update. The attackers were able to remain in affected systems for a long period of time, mostly unbeknownst to security experts. Finally it created an untold number of additional compromises as the techniques used here could be used elsewhere for further nefarious purposes.

There are several key takeaways and lessons-learned from this breach.

1. Be protective of on-premises Microsoft Active Directory. This was the primary way that the attackers were able to get from SolarWinds products to other internal resources.
2. Require increased code validation. Knowing where code is coming from and protecting it from tampering is of the utmost importance.
3. Impose limited trust especially with suppliers. This is a good mitigation strategy to protect against further supply chain attacks.
4. Test components used in products.
5. Examine all traffic leaving the network. It is not enough just to filter traffic entering the network but also the traffic leaving to prevent data exfiltration.
6. Understand the location of sensitive data and protect it.
7. Research potential attackers' tools, techniques and procedures.
8. Increase network segmentation.
9. Improve security architecture.
10. Increase security in the development process for updates and other software.
11. Implement defense in depth.

By undertaking these and additional security best practices it should be possible to mitigate damages and help prevent future attacks.

Resources

Summary

BBC (2020, Dec 24), *SolarWinds: Hacked firm issues urgent security fix* (online image), BBC.com, https://www.bbc.com/news/technology-55442732

Jibilian, Isabella and Canales, Katie (2021, Apr 15), Insider, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Oladimeji, S. and Kerner, S.M. (2021, Jun 16), *SolarWinds hack explained: Everything you need to know*, WhatIs.com, TechTarget, https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Timeline

Baker, Pam (2021, Jun 4), *The SolarWinds hack timeline: Who knew what, and when?,* CSO (U.S.), https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html

Krebs, B. (2021, Jan 12), *SolarWinds: What Hit Us Could Hit Others*, KrebsonSecurity, https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

Rouse, Lauren (2021, May 31), *A Timeline of Cyber Attacks from the SolarWinds Hackers*, Gizmodo (AU), https://www.gizmodo.com.au/2021/05/solarwinds-hackers-cyber-attacks-timeline/

Root Cause

Archer, A, et al. (2020, Dec 13), *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*, Mandiant, "https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

Jibilian, Isabella and Canales, Katie (2021, Apr 15), *The US is readying sanctions against Russia over the SolarWinds cyber attack,* Insider, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

SolarWinds, Orion Platform, (2021), https://www.solarwinds.com/orion-platform

Damages

Krebs, B. (2021, Jan 12), *SolarWinds: What Hit Us Could Hit Others*, KrebsonSecurity, https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

Temple-Raston, Dina (2021, Apr 16), *A 'Worst nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*, NPR, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Threat Actors

Read, Ben (2020), *UNC2452: What We Know So Far*, FireEye, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wbnr-unc2452-presentation-slides.pdf

Method

NIST (2020, Dec 29), CVE-2020-10148 Detail, https://nvd.nist.gov/vuln/detail/CVE-2020-10148

Read, Ben (2020), *UNC2452: What We Know So Far*, FireEye, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wbnr-unc2452-presentation-slides.pdf

Temple-Raston, Dina (2021, Apr 16), *A 'Worst nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*, NPR, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (2021, Apr 15), *Malware Analysis Report (AR21-039B),* https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-039b

Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (2021, Apr 15), *Malware Analysis Report (AR21-148a)*, https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-148a

Victims

Krebs, B. (2020, Dec 15), *SolarWinds Hack Could Affect 18K Customers* KrebsonSecurity, https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/

Krebs, B. (2020, Dec 14), *U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise*,. KrebsonSecurity, https://krebsonsecurity.com/2020/12/u-s-treasury-commerce-depts-hacked-through-solarwinds-compromise/

Mitigation

Archer, A, et al. (2020, Dec 13), *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*, Mandiant, "https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

GitHub (2021), *Mandiant/Sunburst_countermeasures*, https://github.com/mandiant/sunburst_countermeasures

SolarWinds (2021, Apr 6), *SolarWindsSecurity Advisory*, https://www.solarwinds.com/sa-overview/securityadvisory

Lessons Learned

Novinson, M. (2021, May 21), *12 lessons learned from SolarWinds breach: RSA Conference*, CRN (AU), https://www.crn.com.au/news/12-lessons-learned-from-solarwinds-breach-rsa-conference-564841