

Analysis of Solarwinds Breach, 2020

In my university class, CS4673 – Cyber Operations, I was tasked with analyzing the Solarwinds breach that occurred in 2020–2021. As I conducted research on this incident, I felt compelled to write my first blog post over this security incident.

The Prompt: Provide an overview of the attack and its phases, referring to course models and/or the MITRE ATT&CK framework.



A Background of Solarwinds

In 2020, Solarwinds, a major software company founded in Tulsa, Oklahoma and resides in Austin, Texas who provides system management tools for network and infrastructure monitoring, along with other technical services (TechTarget, What is SolarWinds?), was the victim of a software breach. Solarwinds provided services to thousands of organizations around the world ranging from U.S agencies, to fortune 500 companies, state cities, and other large companies/organizations. Solarwinds was affected by a malware, known as SUNBURST.

It should be noted that it is not known at this time how Solarwinds systems were breached.

The Unrealized Breach of Solarwinds Orion Software

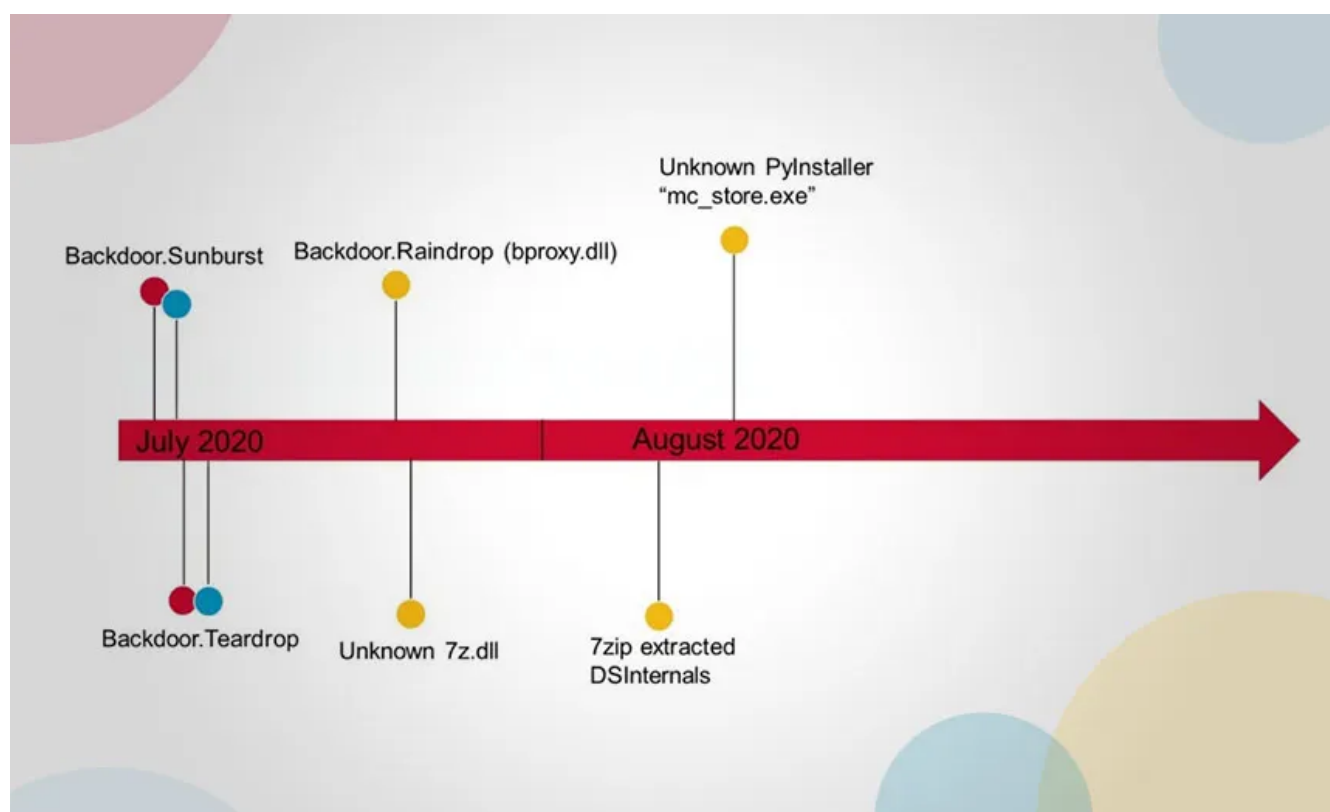
The threat actor, APT29 or formally known as Cozy Bear (MITRE ATT&CK), conducted reconnaissance on Solarwinds. APT29 was able to gain unauthorized source code access to Solarwinds Orion platform, which is used as a networking performance and monitoring tool that helped simplify IT administration (SolarWinds). APT29 took advantage of the the weakest component of the software supply chain, in Solarwinds case being the sourcing stage. APT29's injection method was rather clever, during the compilation process of Orion's new updated source code, it went through an audit process of code review, ensuring that none of the source code (high-level source code) had been tampered with in any way (The TWS Channel), after compilation of the source code to machine code has finished, a Visual Studio process named **MSBUILD.EXE** executes stating that the compilation has finished, at this point SUNSPOT swaps the developers code with the malicious code. (MITRE ATT&CK ID T1195, Supply Chain Compromise). Orion's update is then pushed out to 30,000 customers, 18,000 of which installed this update onto their network.



Actions Taken Against Compromised Systems

Over the next 14 days, the SUNBURST backdoor waited to do anything malicious to stay undetected as new updates are generally monitored heavily to ensure business continuity is not affected (The TWS Channel). After

successfully staying undetected in client systems, SUNBURST disabled all anti-virus software and forensic tools that were capable of detecting the malware. From here, the malware utilized a C2 server (Command & Control Server) to send information such as the IP address, the operating system, and usernames allowing APT29 to detect who the compromised system(s) belong to. Depending on the IP address, the malware decides whether it wants to act passively, actively, or disable itself. In the case of the malware acting actively, it assigns a unique C2 server to the victim, allowing the attackers (APT29) to intervene with the systems. It should be noted that the C2 server was U.S based to avoid red flags for detection (MITRE ATT&CK, TA011). In May, this C2 server was utilized in hands-on keyboard attacks that consisted of privilege escalation, and stealing high value assets & user credentials. (MITRE ATT&CK, TA004, TA006). In June, TEARDROP and RAINDROP were introduced onto systems with the primary function to place a cobalt strike beacon, a popular pentesting tool to detect further vulnerabilities (The TWS Channel).



Indicator Of Compromise

The first IOC (Indicator of Compromise) occurred on December 8th of 2020, when a member of the FireEye cybersecurity team notices a new device has been added to a FireEye employee in order to perform 2FA actions, the member of the FireEye security team called the employee asking if they added any devices, and the employee responded with "It wasn't me" (The TWS Channel, MITRE ATT&CK, T1649, T1111). FireEye then became aware that an outside actor had been watching over their systems secretly looking over systems and stealing, FireEye discovered that red team tools such as penetration testing & assessment tools had been stolen,

these tools replicated some of the most “sophisticated hacking tools in the world” (The TWS Channel). On Friday, December the 11th the attack was traced back to the source, Solarwinds Orion networking and performance monitoring tool containing nearly 4000 lines of malicious code.



Killswitch & Origin of Attack

After 3–4 days of the update being public, FireEye, Microsoft, and GoDaddy cooperated to introduce a kill switch to the malware. GoDaddy uncovered that if the victim IP responded with a IP falling under Microsoft’s range, it would switch the malwares state to disabled as previously mentioned the malware would decide its state based on the IP address, and other information. GoDaddy implemented the kill switch that ultimately manipulated the DNS to always respond with an IP from Microsoft’s IP range (The TWS Channel). As mentioned before, APT29 utilized U.S based C2 servers to avoid detection, as well as a zero-day SAML exploit that allowed the attackers to impersonate any user, with any privilege bypassing multi-factor authentication by forging a response from the authentication server making it seem that the identity was verified. It is still unknown how Solarwinds internal systems were breached, allowing for the tampered source code used for Orion’s update that was installed across 18,000 client systems. In January of 2021, the CISA (Cybersecurity & Infrastructure Security Agency), NSA, FBI, and the ODNI stated that the attack was likely Russian in origin, further backed up by a statement released by The White House officially attributing the attack to the Russian Foreign Intelligence Service (SVR), also known as APT29, Cozy Bear, and The Dukes. However, the Director of Russian Foreign Intelligence Services denied these claims stating that they were a “bad detective novel” and that SVR would be “flattered” if they were involved in the attack due to its sophistication (The TWS Channel). The United States stood by its claims of it being Russian

in origin, strongly believing that the hack has matched many years of Russian foreign intelligence activity (The TWS Channel).



References

The TWS Channel. (2021). The SolarWinds Hack: The Largest Cyber Espionage Attack in the United States. In *YouTube*. <https://www.youtube.com/watch?v=Kf7Motm36Go>

Oladimeji, S., & Kerner, S. M. (2023, November 3). *SolarWinds hack explained: Everything you need to know*. Techtarget; TechTarget. <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>

Davis, M. J., Charles. (2020, December 15). *These big firms and US agencies all use software from the company breached in a massive hack being blamed on Russia*. Business Insider. <https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12>

FireEye. (2020, December 13). *SolarWinds Supply Chain Attack Uses SUNBURST Backdoor*. Google Cloud Blog. <https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor>

CrowdStrike Intelligence Team. "SUNSPOT Malware: A Technical Analysis | CrowdStrike." *Crowdstrike.com*, 2024, www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/.

MITRE ATT&CK. "Group: APT29, YTTTRIUM, the Dukes, Cozy Bear, CozyDuke | MITRE ATT&CKTM." *Mitre.org*, 31 May 2017, attack.mitre.org/groups/G0016/

SolarWinds. "Orion Platform | SolarWinds." [Www.solarwinds.com](http://www.solarwinds.com), www.solarwinds.com/orion-platform.⁸

(2023). Itsasap.com. <https://www.itsasap.com/hs-fs/hubfs/computer%20networks%20with%20different%20users.png?width=778&height=260&name=computer%20networks%20with%20different%20users.png>

(2025). Rackcdn.com. https://130e178e8f8ba617604b-8aedd782b7d22cfe0d1146da69a52436.ssl.cf1.rackcdn.com/raindrop-latest-malware-tied-to-solarwinds-hack-showcase_image-2-a-15800.jpg

(2025b). Cybersecurityventures.com. <https://cybersecurityventures.com/wp-content/uploads/2021/03/system-hacked.jpg>

MITRE. (2024). *MITRE ATT&CKTM*. Mitre.org. <https://attack.mitre.org/>

(2025c). Educause.edu. https://er.educause.edu/-/media/images/blogs/2019/3/er19_1113_706x394_blog.jpg

USA.gov. (2018). *Official Guide to Government Information and Services | USAGov*. Usa.gov. <https://www.usa.gov/>



hunts.dev

Originally published on hunts.dev

<https://hunts.dev/blog/solarwinds/>