New York State
Department of Financial Services

Report on the SolarWinds Cyber Espionage Attack and Institutions' Response

April 2021

I. Introduction

The next great financial crisis could come from a cyber attack. With each passing day our world gets more interconnected. This brings many advantages, but it also makes us far more vulnerable to cyber attacks. Our growing vulnerability was made clear on December 13, 2020, when the world learned that a sophisticated adversary used the SolarWinds Orion Platform ("Orion") to plant stealthy backdoors in the networks of thousands of companies and government agencies ("the SolarWinds Attack"). The SolarWinds Attack shows how terrifyingly easy it is to compromise thousands of organizations in one stroke – even sophisticated government agencies and technology firms.

The SolarWinds Attack was one part of a widespread, sophisticated cyber espionage campaign by Russian Foreign Intelligence Service actors known as "APT 29" and/or "Cozy Bear," which focused on stealth and stealing sensitive information.[1] Although most Orion customers were not targeted for a follow-on intrusion, at least nine federal agencies and approximately 100 companies were compromised.[2]

The New York State Department of Financial Services ("the Department" or "DFS") responded to this extraordinary cyber attack by publishing a Supply Chain Compromise Alert ("the Alert") that instructed its regulated companies to notify DFS, pursuant to its Cybersecurity Regulation,[3] if they used the infected versions of Orion.[4] The Department followed up with almost 100 companies, and appreciates the many financial services companies that assisted and promptly answered questions.

---

[1] *See* Nat'l Security Agency, Cybersecurity & Infrastructure Security Agency, and Federal Bureau of Investigation, Cybersecurity Advisory: Russian SVR Targets U.S. and Allied Networks (April 15, 2021), available here.
[2] White House, Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger (Feb. 17, 2021), available here.
[3] 23 NYCRR Part 500.
[4] DFS, Supply Chain Compromise Alert (Dec. 18, 2020), available here.

Some key findings from the Department's investigation are:

- To date, no DFS-regulated company has reported that the hackers behind the SolarWinds Attack actively exploited their company's network. This is consistent with other reporting that financial services companies were not actively targeted for exploitation.
- Overall, DFS-regulated companies responded to the SolarWinds Attack swiftly and appropriately. For example, 94% of impacted companies removed the vulnerability announced by SolarWinds on December 13 from their networks within 3 days by disconnecting vulnerable systems from their networks and/or patching them.
- Our review of Orion installations and patch implementations revealed that several DFS-regulated companies' patch management programs are immature and lack the proper "patching cadence"[5] needed to ensure timely remediation of high-risk cyber vulnerabilities.

The SolarWinds Attack is, to date, the most visible, widespread, and intrusive information technology ("IT") software supply chain attack – *i.e.*, a cyber attack that corrupts IT software and uses that software as an attack vector. Supply chain attacks are dangerous because the malware is embedded inside a legitimate product, and because supply chain attacks can allow an attacker to access the networks of many organizations in a single stroke.

This attack confirms the importance of vigorous third party risk management, which starts with a thorough assessment of an organization's third party risk. DFS found that some regulated companies using Orion were not classifying SolarWinds as a critical vendor, even though Orion had privileged access to the company's network. Third party risk management is a key part of DFS's Cybersecurity Regulation, and the Department is exploring ways to further address this critical component of cybersecurity.

[5] "Patching cadence" refers to how often an organization reviews systems, networks, and applications for updates that remediate security vulnerabilities.

This attack also exposed the lack of transparency and effective information sharing regarding cybersecurity breaches. Several organizations apparently detected some aspect of this cyber espionage campaign before December 13, 2020. Some have publicly revealed that they blocked an intrusion,[6] but some have not. This Report is part of DFS's ongoing effort to improve information sharing and transparency.

This Report summarizes the facts surrounding the SolarWinds Attack, the remediation efforts by DFS-regulated companies that reported using an infected version of Orion, and the Department's recommendations for organizations to strengthen cybersecurity practices to protect against future attacks. Part II of this Report provides background information on SolarWinds and the Department. Part III sets forth a timeline of the SolarWinds Attack and DFS's response to it. Part IV provides information about DFS-regulated companies that reported or were identified as downloading one of the versions of the compromised Orion software and describes their remediation efforts after the SolarWinds Attack. Part V identifies key cybersecurity steps to address the weaknesses exposed by the SolarWinds Attack.

II. Background

A. The New York State Department of Financial Services

The Department was created in 2011 as the merger of the former Banking and Insurance Departments "[t]o establish a modern system of regulation, rulemaking and adjudication" responsive to the needs of the banking and insurance industries and New York consumers and residents.[7] As part of its mission, the Department has instituted robust cybersecurity standards to protect New York consumers and businesses against cybersecurity threats. In 2017, the

[6] *See, e.g.*, FireEye, "Unauthorized Access of FireEye Red Team Tools," *Threat Research* (Dec. 8, 2020), available here; Sergiu Gatlan, "FireEye reveals that it was hacked by a nation state APT group," *Bleeping Computer* (Dec. 8, 2020), available here.
[7] N.Y. Fin. Servs. L. § 102(b).

Department launched its first-in-the-nation Cybersecurity Regulation that requires all DFS-regulated financial services organizations to implement a risk-based cybersecurity program and to report any attempted or executed unauthorized access to their Information Systems.[8] The regulation has served as a model for other regulators, including the U.S. Federal Trade Commission, multiple states, and the National Association of Insurance Commissioners. Under the leadership of Superintendent Linda A. Lacewell, the Department in 2019 became the first financial regulator in the nation to create a Cybersecurity Division to protect consumers and industries from cyber threats.

B. SolarWinds and the Orion Platform

SolarWinds is a Texas-based software company that develops products for IT infrastructure. As of December 31, 2020, SolarWinds had over 320,000 customers across many sectors, including government, financial services, telecommunications, and others.[9] Orion is a SolarWinds product that monitors and manages the performance of an organization's network, systems, and applications in a single window or application.

III. The SolarWinds Attack and Resulting Supply Chain Compromise

A. Key Events

Phase 1: Hackers Install Malware Into Orion Software

In approximately September 2019, hackers accessed Orion and tested their ability to insert code into the Orion software build process, during which source code was converted into software to be installed on computers and systems.[10] After successfully completing the test run, on February

[8] *See* 23 NYCRR § 500.01(e) (defining Information System).
[9] *See* Solar Winds Annual Report (March 2021), at 7, available here (listing customer statistics); Jason Lemon, "SolarWinds Hides List of Its High-Profile Corporate Clients After Hack," *Newsweek* (Dec. 15, 2020), available here (describing customer base).
[10] *See* Sudhakar Ramakrishna, "New Findings From Our Investigation of SUNBURST," *OrangeMatter* (SolarWinds blog) (Jan. 11, 2021), available here. According to SolarWinds, an October 2019 update to Orion "contained modifications designed to test the perpetrators' ability to insert code into our builds." *Id.*

20, 2020, hackers inserted malware, dubbed Sunburst, into Orion during the Orion software build process.[11]

Between March and June 2020, SolarWinds distributed corrupted updates for Orion to its customers around the globe. Sunburst was installed on the systems of approximately 18,000 Orion customers through these updates.[12] On June 4, 2020, hackers removed Sunburst from the Orion software updates, but Sunburst remained on Orion customers' systems undetected.[13]

Phase 2: Sunburst Discovered and Patches Issued

On December 12, 2020, FireEye, a cybersecurity company, notified SolarWinds about the existence of Sunburst malware in certain versions of Orion.[14] The next day, SolarWinds announced that its customers running three different versions of Orion had the Sunburst vulnerability on their systems (the "Sunburst Announcement"). SolarWinds released patches on December 14 and 15 that removed Sunburst.

Phase 3: Supernova Discovered and Patches Issued

On December 24, 2020, SolarWinds announced that another vulnerability, named Supernova, was found not only in the same versions of Orion that had Sunburst, but also in other versions of Orion that did not have Sunburst (the "Supernova Announcement").[15] The day before the Supernova Announcement, on December 23, SolarWinds had released three patches that addressed Supernova. Further, SolarWinds determined that the patches released on December 14 and 15 to address Sunburst also eliminated Supernova. On January 25, 2021, SolarWinds released two more patches that addressed both Sunburst and Supernova.

---

[11] *See* "New Findings," *supra* note 10.
[12] Brian Krebs, "SolarWinds Hack Could Affect 18K Customers," *Krebs on Security* (Dec. 15, 2020), available here.
[13] *Id.*
[14] *See* SolarWinds, "SolarWinds Update on Security Vulnerability" (Dec. 17, 2020), available here.
[15] *See* SolarWinds Advisory FAQ, Question 25 (updated Jan. 29, 2021), available here.

Both the Sunburst and Supernova vulnerabilities allowed hackers to gain access to an Orion customer's internal network and its Nonpublic Information (NPI).[16] As of the date of this Report, there have been no reports or indications that hackers exploited the vulnerabilities resulting from Sunburst or Supernova in any financial services organization.

B. The Department's Response

On December 18, 2020, the Department issued its Alert about the SolarWinds Attack, which advised regulated companies to assess the risk to their systems and customers from the SolarWinds Attack and to act immediately to address vulnerabilities and minimize consumer impact.[17] The Alert also identified authoritative guidance from the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"), SolarWinds, and other sources, and instructed its regulated companies to notify DFS, pursuant to its Cybersecurity Regulation, if they were using, or had used, any of the corrupted Orion products. Subsequently, the Department interviewed companies that reported or were identified as being impacted by the SolarWinds Attack to assess the impact of the incident and the cybersecurity maturity of DFS-regulated companies.

IV. Remediation Efforts

Of the 88 companies DFS interviewed that were using a corrupted version of Orion on December 13, 2020, 36 had versions of Orion that included the Sunburst malware (and were therefore vulnerable to Supernova as well), and 52 had versions of Orion that were only vulnerable to Supernova. DFS-regulated companies indicated that they relied on vendor and governmental guidance, including from SolarWinds, FireEye, CISA, and DFS, to assess their cyber risk and

[16] *See* 23 NYCRR § 500.01(g) (defining Nonpublic Information); *see also* SolarWinds Annual Report (March 2021) at 2, available here (describing Sunburst attack).
[17] DFS, Supply Chain Compromise Alert (Dec. 18, 2020), available here.

shape their responses to the SolarWinds Attack. The companies the Department contacted that were vulnerable to Sunburst or Supernova (88 in total) took the following steps to mitigate the associated risks:

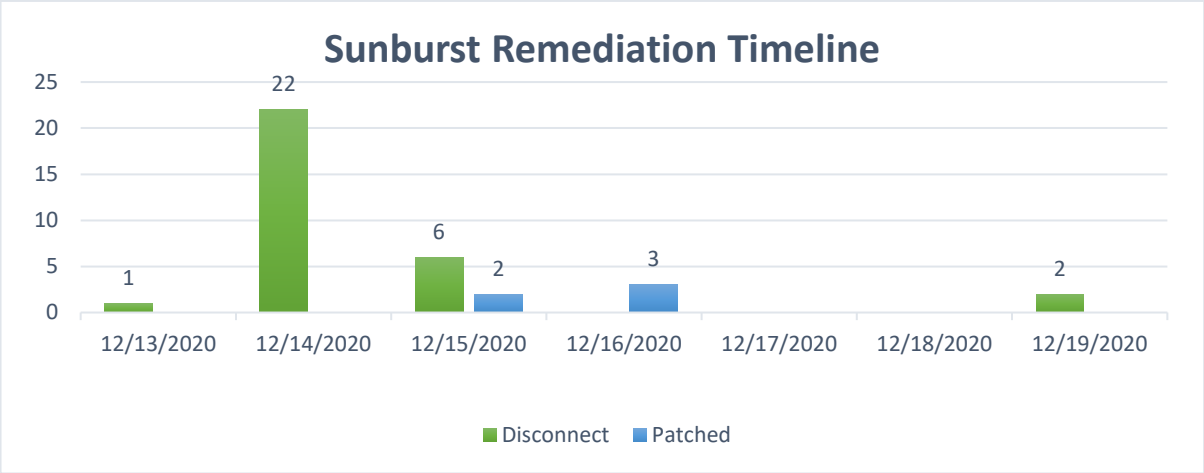
- Checked system integrity and audit logs for indicators of compromise (88 of 88);
- Disconnected affected systems from their networks (66 of 88);
- Applied security patches to affected systems (64 of 88);
- Isolated affected systems by blocking access to the internet (21 of 88);
- Isolated affected systems by blocking specific external DNS domains, as listed by CISA[18] (21 of 88);
- Decommissioned Orion and replaced it with another monitoring product (14 of 88); and
- Applied mitigation scripts[19] to affected systems (2 of 88).

Most companies performed these actions within a few days of the Sunburst and Supernova Announcements, and the majority applied security patches so they could continue using Orion.[20]

[18] CISA, Alert (AA20-352A), "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations" (Dec. 17, 2020, updated Apr. 15, 2021), available here.
[19] SolarWinds provided a mitigation script for those companies unable to upgrade immediately, which it said could be installed to temporarily protect their environment. *See* SolarWinds Advisory FAQ, Question 8 (Jan. 29, 2021, updated Apr. 6, 2021), available here.
[20] *See* SolarWinds Security Advisory (Jan. 29, 2021, updated Apr. 6, 2021), available here.

A. Sunburst

All of the 36 companies with Sunburst removed the vulnerability from their Information Systems within six days of the Sunburst Announcement (*i.e.*, by December 19, 2020) by disconnecting Orion or applying a patch. Most removed Sunburst within three days.[21] Most of the companies that disconnected eventually patched and reconnected Orion. However, 10 companies decided to decommission Orion.



Of the 36 companies with Sunburst, 86% (31 of 36) disconnected or patched their systems by December 15, 2020.[22] The other 14% (5 of 36) disconnected affected systems from their network and rebuilt servers with a new installation of Orion that did not contain Sunburst or Supernova.

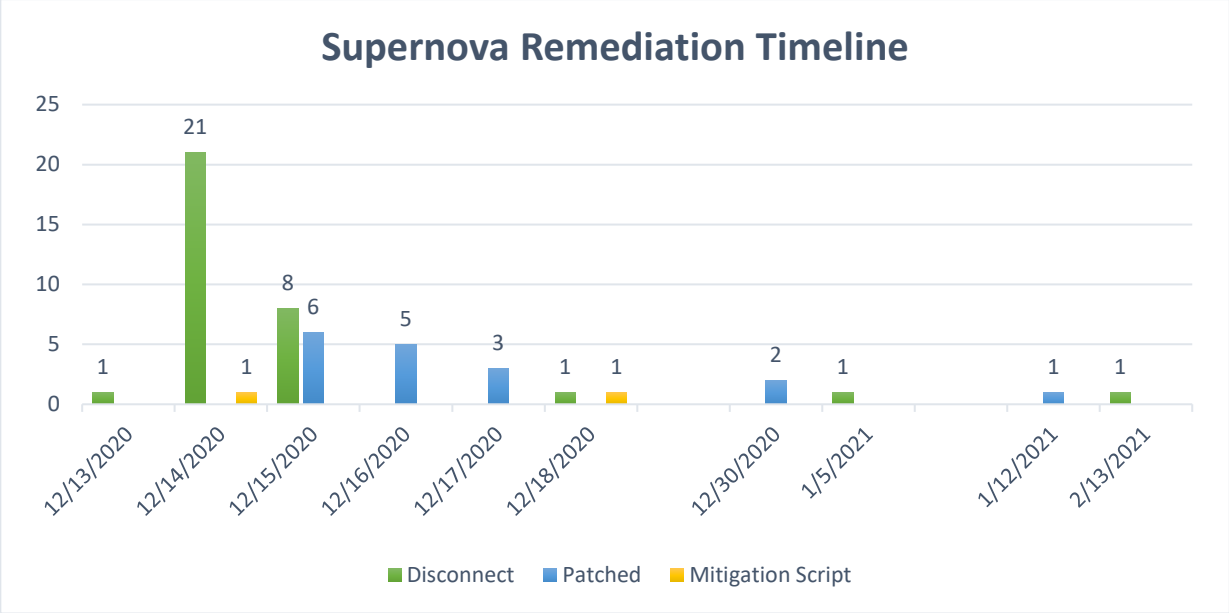
Notably, the companies that were vulnerable to Sunburst on December 13, 2020, had not applied two patches released by SolarWinds in August and October 2020. Those patches, if implemented, would have eliminated Sunburst.

[21] Two companies did not remove the vulnerable version of Orion until December 19, 2020. One of the companies had been running Orion in a test environment isolated from the organization's network and had never used it for business purposes, so they disconnected altogether on December 19, 2020. The other had patched on December 15, 2020, but used a still-vulnerable patch released in October 2020 instead of either of the patches SolarWinds released in mid-December; the correct patch was applied on December 19, 2020.

[22] All the companies that disconnected Orion and later reconnected patched it before reconnecting.

B. Supernova

Most DFS-regulated companies also addressed the Supernova vulnerability quickly. Given the serious nature of the media reports and uncertainty regarding Orion after the Sunburst Announcement, many companies that used Orion – including those without versions corrupted by the Sunburst malware – disconnected, patched, or applied a mitigation script. In fact, of the 52 DFS-regulated companies with Supernova only, 90% (47 of 52) remediated by December 20 – four days before the Supernova Announcement. Most companies removed the vulnerability by disconnecting Orion or applying a patch, although two companies with versions of Orion from 2017 instead applied a mitigation script provided by SolarWinds. After the December 24 Supernova Announcement, the remaining five companies that had not yet remediated Supernova patched or disconnected Orion.



Notably, 31% (16 of 52) of the companies with only Supernova had not patched their Orion Platform since 2019. Of those 16, one company had not patched since 2018 and two companies

had not patched since 2017. While this poor patching cadence may have resulted in avoiding Sunburst, it left these companies with other unpatched vulnerabilities.

V. Reducing Supply Chain Risk

While there is no silver bullet that will stop all supply chain attacks, there are steps companies should take to reduce supply chain risk. Some key cybersecurity measures are highlighted below.

A. Fully Assess and Address Third Party Risk

Third Party Service Provider[23] and other vendor risk management policies and procedures should include processes for due diligence and contractual protections that will ensure the company can monitor the cybersecurity practices and overall cyber hygiene of critical vendors.[24] Furthermore, contracts with critical vendors should include provisions requiring immediate notification (ideally to at least two persons in different roles at an organization) when a cyber event occurs that impacts – or potentially impacts – an organization's Information Systems or any NPI that is maintained, processed, or accessed by the vendor.

B. Adopt a "Zero Trust" Approach and Implement Multiple Layers of Security

Organizations should anticipate and prepare for breaches in the supply chain by incorporating supply chain risk analysis into their requisite Risk Assessments[25] and risk management programs. To do this most effectively, organizations should adopt a "zero trust" mindset and assume that (1) any software installation and (2) any Third Party Service Provider could be compromised and used as an attack vector. Access should be limited "to only what is

[23] *See* 23 NYCRR § 500.01(n) (defining Third Party Service Provider(s) as those vendors who provide services to a regulated entity and maintain, process or otherwise are permitted "access to Nonpublic Information through its provision of services").
[24] *See* 23 NYCRR § 500.11 (describing requirements for Third Party Service Provider security policies).
[25] DFS's Cybersecurity Regulation requires Risk Assessments to be "sufficient to inform the design" of an organization's cybersecurity program and internal controls to be updated as needed "to respond to technological developments and evolving threats." *See* 23 NYCRR § 500.09.

needed" and systems should be monitored "for anomalous or malicious activity."[26] Organizations should have layers of security and extra protection for sensitive information so that if one layer is compromised, other controls can detect or prevent an intrusion.

C. Timely Address Vulnerabilities Through Patch Deployment, Testing, and Validation

Organizations should have a vulnerability management program that prioritizes the organization's patch testing, validation processes, and deployment – including which systems to patch and in what order they should be patched.[27] Furthermore, an organization's patch management strategy should include performing tests of all patches to the internal system environment with defined rollback procedures if the patch creates or exposes additional vulnerabilities.[28]

If your company uses Orion, ensure your organization is running a recent version that has eliminated the Sunburst and Supernova vulnerabilities.

D. Address Supply Chain Compromise in Incident Response Plans

An effective and tested incident response plan with detailed procedures and playbooks is crucial.[29] Incident response plans should include the following, at a minimum, to address supply chain compromises or attacks:

- Procedures to isolate affected systems;
- Procedures to reset account credentials for users of all affected assets and users of assets controlled by compromised software;

---

[26] *See* Nat'l Security Agency, "NSA Issues Guidance on Zero Trust Security Model" (Feb. 25, 2021), available here.
[27] *See* Murugiah Souppaya & Karen Scarfone, "Guide to Enterprise Patch Management Technologies," Natl. Inst. Stand. Technol. Spec. Publ. 800-40 Rev. 3 (July 2013), available here (providing an in-depth look at patch management, including verifying the integrity of software updates).
[28] *See* 23 NYCRR § 500.03(g).
[29] *See* 23 NYCRR §§ 500.03(n) and 500.16.

- Procedures to rebuild from backups created before the compromise;
- Procedures to archive audit and system logs[30] for forensic purposes; and
- Procedures to update response plans based on lessons learned.

Engaging in "table top" exercises after revising an incident response plan will help increase awareness, evaluate preparedness, clarify roles, and validate an organization's incident response plan and training. An incident response plan should also be aligned with the organization's overall business continuity plan to address enterprise-wide changes to key processes and to plan for operating with reduced capacity or replacing them altogether.

Finally, cybersecurity fundamentals, such as knowing your environment, can often mitigate damage and assist with remediation. Companies should understand what assets reside in the environment – including their versions and configurations – and enable timely notifications when changes occur. The incident response playbook should include plans to respond to unauthorized changes.

VI. Conclusion

The SolarWinds Attack should serve as a wake-up call. Through a single vector, Russian hackers opened back doors into thousands of organizations, including almost 100 companies in New York's financial services industry. Although none of the networks of the DFS-regulated companies were actively exploited, the SolarWinds Attack highlights the financial services industry's vulnerability to supply chain attacks.

The SolarWinds attack confirms that cyber risks are a threat not just to consumers and individual companies, but also to the stability and soundness of our entire financial services industry. This is an existential threat and we urge the industry to treat it as such.

[30] *See* 23 NYCRR § 500.06(a)(2) (requiring Covered Entities to "maintain systems that . . . include audit trails designed to detect and respond to Cybersecurity Events").