April 29, 2021

New York State Department of Financial Services Releases Report on SolarWinds Cyber Espionage Attack

Report Characterizes Attack as a "Wake-up" Call, Recommends Cybersecurity Measures for Financial Services Industry

SUMMARY

On April 27, 2021, the New York Department of Financial Services ("DFS") released a "Report on the SolarWinds Cyber Espionage Attack and Institution's Response" (the "Report").[1] As set forth in the Report, the SolarWinds attack was part of a widespread, sophisticated cyber espionage campaign by actors reported to be affiliated with Russia's intelligence services that compromised sensitive information of at least nine federal agencies and approximately 100 companies. The Report describes the SolarWinds attack and the weaknesses it exposed, and considers the remediation efforts of DFS-regulated institutions impacted by it. The Report concludes that although none of the networks of DFS-regulated companies were actively exploited, the SolarWinds attack highlights the financial services industry's vulnerability to "supply chain" attacks. The Report recommends several steps to reduce supply chain risk, including fully assessing and addressing third-party risk, adopting a "zero trust" approach and multiple layers of security, addressing vulnerabilities in a timely manner through patch deployment, testing, and validation, and addressing supply chain compromise in incident response plans.

BACKGROUND

SolarWinds is a Texas-based company that provides software and information technology infrastructure services to customers around the globe. One of its software products, Orion, monitors and manages the performance of an organization's network, systems, and applications. As described in the Report, on February 20, 2020, hackers affiliated with Russian intelligence services accessed the Orion platform and

inserted code containing a malware called "Sunburst" into the Orion software build process. Between March and June 2020, SolarWinds distributed corrupted updates for Orion containing the Sunburst malware to approximately 18,000 customers. On December 12, 2020, a cybersecurity company notified SolarWinds of the existence of the malware, and SolarWinds informed its customers the following day of the vulnerability. On December 24, 2020, SolarWinds announced that another form of malware, "Supernova," had also been identified in various versions of Orion. The Report found that the Sunburst and Supernova malware allowed hackers to gain access to the internal networks and non-public information ("NPI") of Orion customers, but the Report found no indications that hackers exploited these vulnerabilities in any financial services organization. SolarWinds released patches addressing both forms of the malware shortly after they were identified. The Report characterizes the SolarWinds attack as the most visible, widespread, and intrusive example to date of a supply chain attack.

As noted in the Report, in 2017 DFS instituted a cybersecurity regulation, 23 NYCRR 500 (the "Cybersecurity Regulation"), which requires all DFS-regulated organizations to implement a risk-based cybersecurity program and to timely report certain cybersecurity events. On December 18, 2020, DFS issued an Alert advising regulated entities to assess risks, address vulnerabilities, and minimize consumer impact from the SolarWinds attack. Subsequently, to assess the impact from the incident, DFS interviewed 88 companies that reported or were identified as being impacted by the SolarWinds attack and outlined its findings in the Report.

DFS FINDINGS AND RECOMMENDATIONS

The Report notes that, overall, DFS-regulated companies responded to the SolarWinds attack "swiftly and appropriately." The Report does, however, identify areas in which certain of the companies that were the subject of the review could strengthen their cybersecurity measures. In particular, the Report notes, several companies' patch management programs did not ensure timely remediation of high-risk cyber vulnerabilities. Other companies had not classified SolarWinds as a critical vendor, even though the affected Orion software had privileged access to the company's network. The Report also observes that the attack exposed a lack of public transparency and effective information-sharing regarding cybersecurity breaches noting that certain companies had detected some aspect of the attack prior to SolarWinds' announcement on December 13, 2020.

The Report observes supply chain attacks are particularly dangerous because they can allow an attacker to access the networks of many organizations at once. The Report recommends that companies reduce supply chain risk by adopting the following cybersecurity measures:

First, third-party service provider and vendor risk management policies and procedures should include processes for due diligence and contractual protections that ensure the company can monitor the

cybersecurity practices and overall cyber hygiene of critical vendors including, for critical vendors, provisions requiring immediate notification when a cyber event occurs that potentially impacts the company's information systems or NPI.

Second, companies should adopt a "zero trust" mindset that assumes any software installation or third-party service provider could be used as an attack vector. Companies should only provide access to the extent needed, monitor systems for anomalous or malicious activity, and employ layers of security for sensitive information such that if one layer is compromised, other controls can detect and prevent intrusion.

Third, companies should have a vulnerability management program that prioritizes patch testing, validation processes, and deployment. The 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.

Fourth, companies should have incident response plans which include, at a minimum, procedures to: isolate affected systems; reset account credentials for users of all affected assets and users of assets controlled by compromised software; rebuild from backups created before the compromise; archive audit and system logs for forensic purposes; and update response plans based on lessons learned. Incident response plans should also be aligned with the organization's overall business continuity plan, and should include plans to respond to unauthorized changes in the versions and configuration of the assets residing in the company's environment. The Report also recommends engaging in "table-top" exercises after revising an incident response plan to increase organizational preparedness.

IMPLICATIONS

DFS-regulated institutions should assess and update, as needed, their cybersecurity program and controls in light of the Report and its findings. In addition to the Report's recommendations, DFS's emphasis on other areas of the cybersecurity program that require enhancement, including information-sharing and transparency regarding cyber breaches, may be an indication that DFS intends to focus more on these areas going forward.

* * *

ENDNOTES

[1] The full Report is available at https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.