U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY JOINT HEARING

HEARING CHARTER

SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains

Tuesday, May 25, 2021
2:00 p.m. EDT – 4:00 p.m. EDT
Zoom

PURPOSE

The purpose of this hearing is to examine the causes and impacts of recent supply chain attacks on Federal agencies, explore how Federal agencies currently mitigate their software supply chain risks, and consider how best to improve software supply chain security. The Subcommittees will examine the challenges of Federal agency compliance with standards and best practices, and hear recommendations on next steps to secure the software supply chain for Federal agencies, especially through improvements to the efficacy of guidance provided by the National Institute of Standards and Technology (NIST). The Subcommittees will further explore how the Federal Government can help facilitate the adoption of supply chain standards and best practices within the private sector.

WITNESSES

- **Mr. Matthew Scholl,** Chief, Computer Security Division of the Information Technology Laboratory, National Institute of Standards and Technology (NIST)
- **Dr. Trey Herr**, Director, Cyber Statecraft Initiative, Atlantic Council
- **Ms. Katie Moussouris,** Founder and CEO, Luta Security
- **Mr. Vijay D'Souza,** Director, Information Technology and Cybersecurity, Government Accountability Office (GAO)

OVERARCHING QUESTIONS

- Including SolarWinds, what are the recent trends regarding supply chain attacks on Federal Government systems or industry networks?
- What challenges limit the capacity of both the private and public sector to respond to these attacks and remediate their vulnerabilities?
- How are Federal agencies meeting existing software supply chain risk management standards and best practices?
- What guidance, tools, and technical assistance does NIST offer public and private sector entities to improve their software supply chain risk management?
- What policy changes can improve the adoption and efficacy of NIST standards and guidance by Federal agencies?

What is a Supply Chain Attack?

Modern computer networks are comprised of hundreds or thousands of pieces of hardware and software from different sources with different levels of access, update timelines, and functions. A cyber supply chain attack occurs when a bad actor infiltrates a network through hardware or software component that has been granted access or incorporated into that network. Similar to other forms of malware, this can result in stolen data or damage to systems. What sets supply chain attacks apart is that the vulnerability enters the network through a trusted source, such as a third-party provider or contractor—no clicking on a bad link or downloading an infected file is required. Supply chain attacks are often harder to detect, prevent, and remediate than traditional malware. System owners and operators may depend on the detection and response capabilities of the third-party source of the infected component. Since it is not feasible for organizations to avoid third-party software entirely, users must have supply chain risk management best practices in place to mitigate the damage supply chain attacks can cause.

SolarWinds

SolarWinds is a software company that gained notoriety when its Orion platform was used in a massive supply chain attack which garnered nationwide press. The SolarWinds attack – also referred to as *Solorigate*, *Sunburst*, and *SolarStorm* – was committed by the Russian intelligence service and occurred in several stages. The attackers initiated reconnaissance on SolarWinds as early as January 2019[1]. By the fall of 2019, they had compromised the SolarWinds network to access the company process for updating their software, inserting a backdoor to allow later access. The attacker then hid its presence and remained dormant while the company spread an infected software update to its customers. The update was distributed to customers in spring of 2020, several months after the initial infection.

The infected Orion software update was downloaded by an estimated 18,000 organizations. However, 18,000 organizations did not suffer impacts. Not all of them installed the update, and of those that did, not all were chosen for further compromise by the attacker. The Orion compromise sent information on the host network back to a server owned by the attacker, allowing them to pick and choose among targets for introducing additional malware. In a sense, the Orion compromise let the hacker make tiny cracks in the walls of houses to peek through and select the ones they wanted to come back and burgle. Of the additional pieces of malware, *Teardrop* served as a second backdoor to help hide how the attacker got into the software, and *Cobalt Strike* allowed the attackers to steal data. The attacker also exploited other vulnerabilities, including those within Microsoft Office 365 and Microsoft Azure, to steal data from many of these systems.

The length of the intrusion varied by victim, but in some cases lasted for months. The supply chain attack was finally detected in December of 2020 by the cybersecurity company FireEye and quickly attributed to Russia, though public confirmation from the White House confirmation took months.[2][3] FireEye realized

[1] https://www.rsaconference.com/Library/presentation/USA/2021/solarwinds-what-really-happened
[2] https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html
[3] https://www.reuters.com/business/white-house-blames-russian-spy-agency-svr-solarwinds-hack-statement-2021-04-15/

their own network had been accessed and later tracked the original intrusion back to the infected Orion update.

Information on the reach of this attack has been slow to emerge. Of the 100 companies impacted relatively few were publicly identified. In May of 2021 was it revealed that 37 of the companies were part of the defense industrial base[4]. Nine Federal agencies had data stolen from their systems, and several more were vulnerable but not targeted with secondary malware by the attacker. Per the latest briefings received by the Science Committee, Federal agencies have completed immediate remediation, but a full analysis of the attack is still ongoing.

Recent Trends in Supply Chain Attacks

The SolarWinds attack is uncommon in scope, but the avenue of attack is not rare. The Atlantic Council's *Breaking Trust* project grappled with the landscape of software supply chain intrusions and assembled a dataset of supply chain attacks stretching back to 2010.[5] This dataset is not comprehensive, as it relies on public disclosure of the supply chain attack in English language news sources, but it does illustrate the growing frequency of supply chain attacks.

Over eight months in 2019-2020, 23 supply chain attacks were added to the *Breaking Trust* dataset, increasing the total count from 115 to 138. In addition, most of the attacks occurred in the latter half of the decade. The report suggests that the quantity of supply chain attacks is likely increasing.

The damage caused by supply chain attacks can also be extensive. The 2017 *NotPetya* malware that shut down computers across the world and caused billions in damage was spread through a supply chain attack on a Ukrainian tax accounting application.[6] Other attacks, such as the 2017 compromise of CCleaner or the 2016 *Kingslayer* attack on a Windows IT admin application, had millions of victims, including networks at high value targets such as Federal agencies, banks, and telecoms[7]. Both *NotPetya* and *Kingslayer* were attributed to nation-state actors, Russia and China respectively. In fact, 30 of the attacks in the Atlantic Council dataset were linked to nation-state actors. This is likely because supply chain attacks are highly effective as espionage tools or for the theft of high-value data. They are also relatively cheap on the scale of nations. The President of Microsoft, Brad Smith, estimated that the SolarWinds attack required on the order of 1000 engineers to carry out, a quantity easily within the reach of Russia or China[8].

Federal Information Security Management Act (FISMA)

The *Federal Information Security Management Act of 2002 (FISMA)* established a framework for protecting federal information systems. FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program for information security systems supported or

[4] https://www.fedscoop.com/solarwinds-defense-industrial-base-hack-dod/
[5] https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/
[6] https://www.wired.com/story/white-house-russia-notpetya-attribution/
[7] https://www.dni.gov/files/NCSC/documents/supplychain/20190327-Software-Supply-Chain-Attacks02.pdf
[8] https://www.csis.org/events/lessons-learned-cyberattack-conversation-solarwinds-part-1-2

managed by the agency. Under FISMA, there is no centralized enforcement authority. Rather, each agency is responsible for its own FISMA compliance. The *Federal Information Security Modernization Act of 2014* updated FISMA to streamline reporting, update breach notification policies, and clarify the roles of different agencies. However, the appropriate roles of different agencies in responding to cyber-attacks remain on ongoing topic of debate.

The House Committee on Science, Space, and Technology is one of three House committees that agencies, under *FISMA,* are required to notify within seven days of a major cyber incident. Agency compliance with *FISMA* in the case of SolarWinds was mixed. Most agencies offered briefings and followed through on information sharing as the investigation proceeded. However, relatively few provided official *FISMA* notification at any point in the process. When pressed, agencies – including some that had data stolen – claimed that because there was no demonstrable harm the breach did not qualify as a major incident and notification was not required. In some cases, this decision may have been correct. Even with significant levels of access the attacker was not always successful in stealing data, and where they were it was not always sensitive data. However, agencies often underestimate future harms that may result from data stolen during the breach when considering whether to label it a "major incident" and thus properly report it to the committees of jurisdiction. Ambiguity in the definition of "major incident" may have resulted in an uneven agency response to Congressional overseers.

Assessing Federal Agency Supply Chain Cybersecurity

The relative prevalence of supply chain attacks, both in general and as a tool of nation-state actors, highlights the importance of securing Federal Agency systems against this threat where possible, including by employing risk management best practices. To that end, in December 2020 the GAO published a report with the alarming title: *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks.*[9] The report identified several foundational practices for Information Communications Technology (ICT) Supply Chain Risk Management (SCRM) that Federal agencies needed to implement. Of the 23 agencies surveyed, none had yet implemented all foundational practices, none had implemented a process to conduct agency-wide assessments of their supply chains, and 14 of the agencies had implemented none of the practices. To their credit, a large majority of agencies concurred with GAO's recommendations, and expressed their intent to implement the foundational practices. Almost half of the agencies reported they were waiting for additional Federal guidance before enacting some or all of the foundational practices.[10] However, agencies have been required by the Office of Management and Budget (OMB) since 2016 to adopt NIST guidance to mitigate supply chain risks (discussed in detail below).[11] The gap between recommendation and implementation was large, and in some cases the agency timeline for completing the recommendations stretched to 2024.

Federal Activities for Software Supply Chain Risk Management

There are several agencies in charge of producing guidance to prevent and respond to software supply chain vulnerabilities and attacks:

[9] https://www.gao.gov/assets/gao-21-171.pdf

[10] This anticipated guidance is from the Federal Acquisition Security Council (FASC), which will recommend NIST standards.

[11] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

The Cybersecurity and Infrastructure Security Agency

The Department of Homeland Security's CISA helps Federal civilian agencies, critical infrastructure entities, and the private sector share cybersecurity information and respond to emerging incidents. CISA, the Federal Bureau of Investigation and the Office of the Director of National Intelligence led the Federal response to SolarWinds.[12] Throughout the response, CISA remained in regular contact with affected public and private sector entities, publishing guidance and forensics capabilities to help network defenders identity and mitigate the threat.[13] In briefings with Committee staff, all affected agencies spoke highly of the support they received from CISA.

The agency has also conducted several activities to improve the Nation's supply chain security risk management. Launched in 2019, CISA's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force is a public-private partnership created to improve the Nation's collective ability to assess and mitigate threats to the ICT supply chain and improve the security and resilience of those supply chain elements and systems.[14] The task force is made up of industry representatives from the information technology and communications sectors as well as Federal partners like NIST. The task force has released several reports regarding both software and communications technology risk management.[15]

National Institute of Standards and Technology

NIST is the agency primarily in charge of the nation's cybersecurity standards and best practices. In February 2013, President Obama signed an Executive Order on critical infrastructure cybersecurity. In 2014, after convening public and private sector stakeholders, NIST published a voluntary framework for reducing cybersecurity risks to critical infrastructure. NIST has since updated and expanded its guidance to apply to new scenarios, such as supply chain risk management. For example, NIST published SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,*[16] which offers guidance for organizations to manage the increasing risk of cyber supply chain compromise, whether intentional or unintentional. NIST is currently working to revise this publication. By statute, Federal agencies must use NIST's cybersecurity standards and guidelines to protect non-national security Federal information and communications infrastructure. After the development of a standard or framework, NIST works with OMB to publish a final rule, requiring agencies to adopt the standard.

In addition to supply chain risk management, NIST has also worked with stakeholders to develop other critical frameworks and guidance for securing software. For example, NIST has produced guidance for vulnerability remediation.[17] The agency has also developed *The Secure Software Development Framework* to help software developers reduce the number of vulnerabilities released in software.[18]

---

[12] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
[13] https://www.cisa.gov/supply-chain-compromise
[14] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf
[15] https://www.cisa.gov/ict-supply-chain-toolkit
[16] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
[17] https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
[18] https://csrc.nist.gov/Projects/ssdf

However, to date relatively little attention has been paid to the lifecycle of software after it has been deployed. As the SolarWinds incident shows, risks remain throughout a piece of software's lifecycle.

National Telecommunications and Information Administration

Modern software products are often an aggregation of multiple software components from different developers, code repositories, and other sources. Suppliers of software components also use different naming schemes for the same software components. As a result, identifying which vulnerabilities compromise which products can be a challenging technical feat. To address this challenge and promote transparency in software supply chains, the NTIA at the Department of Commerce is leading a multi-stakeholder initiative called the Software Bill of Materials (SBOM).[19] The goal of this effort is to create a machine readable inventory that will enable software developers and users to track software components and dependencies and make responding to vulnerabilities in the event of an incident more straightforward.

Federal Acquisition Security Council

In 2017, DHS concluded that software products from the Russian cybersecurity firm, Kaspersky Laboratories, were a security threat to government networks. However, because no government agency had the clear jurisdiction to immediately address this concern, DHS was forced to issue a binding directive to require agencies to remove the software.[20] This authority, granted under FISMA 2014, was not designed to address individual software or companies.

To address this issue, Congress passed the *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act* in 2018.[21] This act created the Federal Acquisition Security Council (FASC), to provide a process by which the Federal government could address threats posed by specific products. The FASC is made up of seven executive branch agencies, including NIST. It is charged with recommending supply-chain risk management standards, developed by NIST, and establishing criteria for sharing information on supply-chain risks between Federal agencies and other entities. In addition, if the FASC believes that a certain product in Federal supply chains is a threat to Federal systems, it can recommend Federal agencies exclude that product from agency procurement or remove it from agency networks. As of May 2021, the FASC is still working to initiate its strategy and processes, and it was not fully operational during the SolarWinds response.

Executive Order 14028: Improving the Nation's Cybersecurity

On May 12, the Biden Administration released an Executive Order, "Improving the Nation's Cybersecurity."[22] The goal of this Executive Order is to address government supply chain security deficiencies in the wake of SolarWinds. The most relevant for this hearing is Section 4, which primarily tasks NIST to work with public and private sector entities to conduct several activities to improve Federal guidance for software supply chain security.[23] Each of these activities has an aggressive timeline.

---

[19] https://www.ntia.gov/SBOM
[20] https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01
[21] https://www.congress.gov/bill/115th-congress/house-bill/7327/text
[22] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[23] Ibid.

- Within 90 days, NIST must identify or develop standards, procedures, or criteria that enhance the security of the software supply chain, including criteria that can be used to evaluate software security and provide SBOMs to all software purchasers.
- Within 45 days, NIST must publish a definition of the term "critical software," which the Executive Order nominally defines as "software that performs functions critical to trust."
- Within 60 days, NIST must publish guidance for critical software security measures.
- Within 60 days, NIST must recommend minimum standards for vendors' testing of their software source code.
- NIST is also tasked with identifying criteria and initiating pilot programs for labeling to promote transparency in the security of consumer products, such as Internet of Things devices and software development.

Notably, the Executive Order also calls for all executive agencies to develop plans to implement Zero Trust Architecture, systems that treat all users as potential threats and prevent access until the users can be properly authenticated and their access authorized. Agencies are required to adopt NIST standards and guidance to accomplish this task. Implementing zero trust architectures is expensive and time consuming, and agencies may not comply without sufficient appropriations or technical assistance from NIST and DHS.