CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 6 | March 9, 2021

Table of Contents

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

President Biden orders multiple U.S. Supply Chain Reviews

On February 24, 2021, President Biden signed Executive Order 14017 that initiates multiple reviews of major U.S. supply chains. *EO 14017*, available here. Focusing on national security and economic growth, the Executive Order designates the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy to coordinate the 100-Day Supply Chain Review and the one-year Sectoral Supply Chain Assessments.

Summary of the Executive Order

The 100-Day Supply Chain Review directs the following federal agencies to evaluate the following supply chains:

- The Department of Commerce to review supply chains for semiconductor manufacturing and advanced packaging.
- The Department of Energy to review supply chain for high-capacity batteries, including those used in electric vehicles.
- The Department of Defense to review supply chain for critical minerals and other identified strategic materials (as determined by the Secretary of Defense), including rare earth elements.
- The Department of Health and Human Services to review supply chain for pharmaceuticals and active pharmaceutical ingredients.

The Executive Order also calls for the one-year Sectoral Supply Chain Assessments to direct the following federal agencies to evaluate the following supply chains.

- The Department of Defense to review supply chains for the defense industrial base.
- The Department of Health and Human Services to review supply chains for the public health and biological preparedness industrial base.
- The Department of Commerce and the Department of Homeland Security to review supply chains for critical sectors and subsectors of the information and communication technology industrial base.
- The Department of Energy to review supply chains for the energy sector industrial base.
- The Department of Transportation to review supply chains for the transportation industrial base.
- The Department of Agriculture to review supply chains for the production of agricultural commodities and food products.

The one-year review will also evaluate current domestic education and manufacturing workforce skills for the relevant sectors to determine the best strategies to meet the future workforce needs.

The SolarWinds hack: SUNSPOT, SUNBURST, and a compromised Office 365 account

Background

On December 12, 2020, SolarWinds, a U.S. company specializing in producing IT management software, was advised by the cybersecurity company FireEye that a security vulnerability manifested in its product platform as a result of a cyberattack. *SolarWinds Update on Security Vulnerability*, available here. SolarWinds Orion is an infrastructure monitoring and management software platform that is used by several federal agencies in addition to many commercial customers. As part of its services, SolarWinds sends relevant software updates through its platform. After confirming the cyber attack, SolarWinds immediately released hotfix updates (i.e., software updates) to all potentially impacted customers.

One day later, the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security declared Emergency Directive 21-01, directing federal agencies immediately to mitigate the cyber attack originating from SolarWinds Orion software. *Emergency Directive 21-01*, available here. CISA's Directive identified specific versions of the SolarWinds Orion software exploited by the threat actor (TA), where TA used embedded malware within the software to gain backdoor access to network traffic management systems of several government networks.

As an emergency stopgap measure, the Directive initially mandated all federal agencies to disconnect affected devices, regardless of whether SolarWinds provided hotfix updates to close the backdoor vulnerability. On January 6, 2021, CISA issued supplemental guidance that allowed federal agencies to reconnect devices with patched SolarWinds Orion software after undergoing specified security procedures. *Supplemental Guidance v3*, available here.

SolarWinds investigators have identified multiple key events leading up to the cyber attack discovery. *New Findings From Our Investigation of SUNBURST*, available here.

- On September 4, 2019, TA accessed SolarWinds networks, potentially through a compromised Office 365 account.
- Between September 12 and November 4, 2019, TA initiated a trial run of injecting test malicious code into SolarWinds products.
- On February 20, 2020, TA compiled and deployed malware, designated as SUNBURST, into SolarWinds products.
- On December 12, 2020, SolarWinds was notified of the SUNBURST malware attack.
- On December 13, 2020, CISA issued Emergency Directive 21-01 to mitigate the effect of the SUNBURST malware attack within U.S. government networks.
- On December 14, 2020, SolarWinds notified customers and shareholders (through an 8-K filing).

Although investigations are ongoing, one news report suspects that TA used a compromised Office 365 account used by SolarWinds as a point of entry to access the company's internal

network. *Hackers Lurked in SolarWinds Email System for at Least 9 Months, CEO Says*, available here. Coincidentally, Malwarebytes, a company specializing in anti-malware software, disclosed that its Office 365 accounts were compromised by the same TA, even though the company does not use SolarWinds products. *Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say*, available here.

After infiltrating SolarWinds' internal network, TA used another malware, designated as SUNSPOT, to secretly embed the SUNBURST malware code within the pending firmware update files for SolarWinds Orion products. SolarWinds was not initially aware that the update files were modified maliciously, and the company unintentionally distributed the infected update among its customers. Implicitly trusting SolarWinds' firmware updates, customers unknowingly installed the SUNBURST malware within their SolarWinds Orion products. As a result, TA had a backdoor eavesdropping access to SolarWinds customers' networks, including some federal agencies' networks. According to CISA, fewer than ten federal agencies are known to have been affected by the SolarWinds attack. *Joint Statement by FBI, CISA, ODNI, and NSA*, available here.

Using backdoor network access, TA reportedly monitored internal email traffic at the Department of Treasury and the Department of Commerce. *Suspected Russian hackers spied on U.S. Treasury emails – sources*, available here. The Administrative Office of the U.S. Courts also announced that the Office and the Department of Homeland Security would be auditing the federal court document system to determine whether the SolarWinds attack on the federal Judiciary may have exposed highly sensitive sealed court filings. *Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records*, available here.

It is also being reported that TA was able to create single sign-on tokens that could be used to impersonate any user within the target organization. *U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise*, available here. This would allow TA to gain access to highly privileged accounts and create its own elevated credentials to access highly sensitive resources even further. It is not yet clear what steps have been taken to mitigate this risk. *Important steps for customers to protect themselves from recent nation-state cyberattacks*, available here. The U.S. Department of Justice reported that around 3% of its Office 365 accounts were compromised due to the SolarWinds attack. *Department of Justice Statement on Solarwinds Update*, available here.

The investigations over the SolarWinds attack, including the effects of the SUNBURST malware attack, are ongoing.

Analysis

The SUNBURST malware attack raises the issue of outsourcing critical IT management services to third parties, especially where customers do not have the means to audit the safety mechanisms of third-party services independently. There are two potential failures stemming from the SUNBURST attack. First, the security failure at the supply chain level enabled TA to install backdoor access across various SolarWinds customers' networks. Second, the (mis)configuration of the Office365 credential management system allowed TA to seemingly gain unrestricted access to protected Office365 accounts, which may include access to email and Cloud storage systems.

A supply chain attack focuses on infiltrating the software development process to incorporate surreptitiously malware within published products, including via software updates. *Supply chain attacks*, available here. SolarWinds authenticated the firmware update as being safe even though the update was infected with the SUNBURST malware. SolarWinds customers relied on the company's supply chain security in maintaining their SolarWinds products. SolarWinds customers did not have the practical means to check whether the SolarWinds firmware update contained embedded malware. The SUNBURST attack demonstrates the need for a robust supply chain security among third-party service providers because client organizations implicitly trust the due diligence of these companies. At the same time, client organizations need to re-evaluate the risks of being largely dependent on third party managed services because there is always a potential for these service providers to be compromised by a cyber attack.

As noted above, SolarWinds, Malwarebytes, and the Department of Justice had their Office 365 accounts compromised by TA. As Microsoft transitioned its Microsoft Office product away from software-as-a-product to software-as-a-service, organizations face a different set of security risks associated with Cloud-based services. *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, available here. In the Cloud, user credential management becomes more critical because a compromised account could be used to facilitate further unauthorized access to other Cloud assets. Organizations must maintain robust user credential management systems to secure their assets tied to related Cloud services. It is worth reemphasizing that a compromised SolarWinds Office 365 account may have been the first step towards one of the most devastating cyber attacks against the U.S. government.

Finally, CISA's Emergency Directive 21-01 is notable because the Directive addressed an *ongoing* cyber attack targeting the federal government, which is rare for the agency. The quick response by the agency may have limited the potential damage caused by the SolarWinds attack. CISA will likely take a more active and proactive role in responding to large-scale cyber attacks in the U.S.

Prompt Transparency

Two days after being notified of the cyber attack, SolarWinds promptly notified its customers and investors, and the company provided security updates to all impacted customers, regardless of having an active maintenance plan with the company. *SolarWinds Update on Security Vulnerability*, *supra*. Unless previously stipulated by a contract, SolarWinds was under no legal obligation to inform its customers of the attack when it did. It was also not legally obligated to provide security updates to customers who no longer had a maintenance plan with the company.

SolarWinds' proactive engagement provided much-needed transparency within the cybersecurity community to contain effectively the SUNBURST threat on all compromised systems. Although it may not appear to be in the company's best interest, prompt cyber attack notification can help to contain and mitigate the collateral damage arising out of the cyber attack incident.

By way of comparison, while it only took two days for SolarWinds to acknowledge publicly the cyber attack, Equifax took over a month to announce its data breach in 2017. *Equifax Data Breach*, available here

Hacker Attempted to Control Florida Water Treatment Plant

Background

On February 5, 2021, an unknown intruder attempted to sabotage the water treatment system of the city of Oldsmar, Florida, using a remote desktop software. *A Hacker Tried to Poison a Florida City's Water Supply, Officials Say*, available here. City officials announced that the water treatment plant's operator noticed his computer mouse cursor moving out of his control. The operator was not concerned initially because the water treatment plant previously used TeamViewer, a remote desktop software, to allow remote staff to view the computer screen and control the system. The operator specifically mentioned that his boss often used TeamViewer to monitor the facility systems remotely.

Later, the mouse cursor was attempting to adjust the sodium hydroxide levels to a hundred times more than normal levels, which could be hazardous. The operator was able to take control over his mouse and return the chemical treatment level to normal parameters. Fortunately, city officials noted that there was an additional safeguard in place to prevent the poisoned water from being distributed to the city population.

Analysis

TeamViewer is one of the most popular remote desktop software that had security vulnerabilities in the past. *E.g., High-Risk Vulnerability in TeamViewer Could be Exploited to Crack Users' Password*, available here. It is not yet known whether the unidentified intruder used a zero-day vulnerability (a vulnerability in a system, where there is no technical fix available) to take control over the water treatment control computer. However, remote desktop services have been notoriously exploited by hackers. These exploits are so widespread that hackers are selling remote desktop protocol (RDP) access to compromised computers on the dark web. *Dark Web Pricing Skyrockets for Microsoft RDP Servers, Payment-Card Data*, available here; *Organizations Leave Backdoors Open to Cheap Remote Desktop Protocol Attacks*, available here.

Poorly managed RDP systems can potentially allow intruders to take over entire computer systems. As such, it is commonly advised to remove or disable any remote desktop software when the computer is not being used for remote control purposes. *Remote Desktop Can Be Useful, but You Can Easily Disable It*, available here.

If a computer is regularly needed for remote control, then stringent security protocols should be implemented, including regularly changing user credentials with strong passwords. However, if a computer were regularly needed for remote *monitoring*, then using a screen capture streaming software would be ideal. A screen capture streaming software, such as Open Broadcaster Software, can capture a part of the computer screen and send it as a video stream to an authorized third party without handing over computer input controls.

According to the principle of least privilege, "[o]nly the minimum necessary rights should be assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary." *Least Privilege*, available here. Under various use scenarios,

using remote desktop software may introduce unnecessary cyber risks for conducting the simplest of tasks. Although no one was hurt from the Florida hacking incident, it may be possible that another similar hack could lead to devastating consequences on our critical infrastructure.

This incident underscores the vital role of cybersecurity in securing our critical infrastructure to protect the safety of our citizens. As noted earlier, there were additional safeguards in place to prevent the poison water from flowing to city residents. If the water treatment plant's operator had not noticed the hack and additional safeguards were not in place, it is foreseeable that injuries and potentially loss of life would have occurred as a direct result of this cyber attack.