Testimony

Brandon Wales

Acting Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective"

BEFORE THE UNITED STATES SENATE

Committee on Homeland Security & Governmental Affairs

March 18, 2021

Washington, D.C.

Chairman Peters, Ranking Member Portman, and members of the Committee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding the federal response to the SolarWinds cyber supply chain compromise.

While the stated purpose of this hearing is to discuss the SolarWinds supply chain compromise, I would be remiss if I did not mention that just two weeks ago, the Federal Government became aware of the recent widespread exploitation of Microsoft Exchange vulnerabilities. This should further serve as a call for increased focus on modernizing our cybersecurity and network infrastructure in order to truly defend today and secure tomorrow.

CISA leads the Nation's efforts to advance the cybersecurity, physical security, and resilience of our critical infrastructure. CISA serves as a focal point to share information among and enable operational collaboration between the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities.

Regarding the security of civilian executive federal networks, CISA's mission is to provide tools, services, and direction that enable timely identification of, protection against, and response to cybersecurity risks. We *Defend Today* through collective defense against threats and vulnerabilities and *Secure Tomorrow* by ensuring effective long-term risk management. CISA's vision is a secure and resilient cyber enterprise that enables the Federal Government to provide critical services to the American people under all conditions.

To address urgent, operational risks like nation-state threat activity and critical vulnerabilities, CISA works to detect, contain, and remediate cyber threats before they can negatively impact agency operations or result in unauthorized access to sensitive information. CISA seeks to achieve operational visibility of threats and vulnerabilities through a variety of means including sensors, on-site incident response teams, remote scanning, and information sharing. CISA maintains the unique capability to integrate information received from federal civilian networks with data from private sector, state, local, tribal, and territorial, and other government partners. By analyzing information from myriad sources and prioritizing the top operational risks to federal agencies, CISA is able to take focused action to address identified risks. These actions range from information sharing, including alerts and guidance, to mandatory direction Binding Operational Directive and Emergency Directives and ongoing coordination with agency network operators. Where necessary, CISA also provides technical assistance by deploying teams to harden systems, hunt for threats, and respond to incidents.

At the same time, CISA is focused on addressing longer-term gaps in federal cybersecurity, such as outdated systems or inadequate focus on system maintenance. In order to raise the baseline of federal cybersecurity, CISA additionally provides shared services and cybersecurity tools through the Quality Service Management Office and the Continuous Diagnostics and Mitigation program. CISA further leads capacity building efforts to reasonably ensure that civilian agencies implement strong governance programs and effectively manage

their technology environments, in close coordination with the Office of Management and Budget (OMB).

We know that cyber threats are one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Federal networks face large and diverse cyber threats ranging from unsophisticated hackers to nation-state intruders using state-of-the-art techniques. Both recent cyber campaigns targeted Federal networks and private sector entities using advanced cyber capabilities that had the potential to undermine critical infrastructure, target our intellectual property, steal our national security secrets, and threaten our democratic institutions.

Solar Winds Cyber Supply Chain Compromise

In early December, 2020, the Federal government became aware of a cyber intrusion campaign that included compromises of U.S. government agencies, critical infrastructure entities, and private sector organizations beginning in at least September 2019. This was a highly sophisticated operation, using novel techniques, and exquisite tradecraft to remain hidden for an extended period.

The best-known infection vector was through a supply chain compromise of the SolarWinds Orion network management system. Malicious code was inserted into software updates, which were then made available to customers as trusted software patches. Once these updates were applied, the actor was able to gain direct access to customer networks by installing a back door into their environment.

According to SolarWinds, nearly 18,000 entities received a malicious version of the software. We refer to these entities as exposed. The threat actor targeted a much smaller number of these entities by accessing the back door and moving laterally into customer networks. We refer to these entities as compromised.

For many of the confirmed victims of this campaign, the primary objective appears to be gaining access to sensitive but unclassified communications. The actor was able to use their privileged access gained by compromising organizations' on-premise networks to then abuse authentication and authorization mechanisms allowing them to access email and other data through the Microsoft Office 365 cloud.

While the software supply chain compromise has been a primary focus of this activity, the U.S. government is aware of additional victims with related Microsoft Office 365 compromises that pre-date the delivery of the SolarWinds back door. The initial intrusion vector for these earlier victims is currently unknown. This campaign should be thought of as a sustained cyber intrusion campaign and not simply a SolarWinds compromise.

On December 13, 2020, the National Security Council staff stood up the Cyber Unified Coordination Group (UCG). Composed of the CISA, the FBI, and ODNI, with support from NSA, the UCG coordinates both the investigation and remediation efforts for the federal

government. As the lead for asset response in the federal civilian space, CISA provides technical assistance to affected entities who request it as they identify and mitigate potential compromises.

CISA's work in response of this campaign falls under four primary lines of effort: scoping the campaign, sharing information and detection, short term remediation, long term rebuilding

Scoping the Campaign

Under the first line of effort, CISA has worked closely with private sector, government, and international partners to understand the full extent of this campaign. To date, we have confirmed that nine federal agencies have been compromised, along with a number of private sector entities, the majority in the IT sector.

Sharing Information and Detections

CISA began to develop detection techniques and share information immediately upon learning of the intrusion campaign. On December 13, 2020, we issued Emergency Directive 21-01 requiring federal civilian executive branch agencies to power down affected versions of SolarWinds Orion devices. We released our directive publicly to drive immediate mitigation steps and help both public and private sector entities identify if their networks were exposed to the adversary. Within 72 hours of the directive's release, 100% of federal civilian executive branch agencies that reported using an affected version of SolarWinds Orion had taken them off-line.

On December 17, CISA released a detailed alert describing the tactics of this actor and providing initial guidance and indicators to entities with suspected compromises. We have updated both our Emergency Directive and Alert several times and we will continue to do so if we uncover new information. We followed the release of our directive and alert with broad stakeholder calls, engaging with thousands of public and private sector entities, providing information to help guide their own detection and response efforts. On Christmas Eve, our threat hunting team released a tool to help detect possible compromised accounts and applications in the Microsoft Office 365 cloud environment, which was widely targeted by the adversary as part of this campaign.

To the extent that we uncover new adversary techniques during our response efforts, we will continue to develop new detection analytics with the intent to share broadly with our stakeholders so they can search for this activity in their networks, remediate as necessary and put protections in place for the future.

Short Term Remediation

Under the third line of effort, CISA provided incident response support to federal agencies that have been compromised as part of the campaign. To date, CISA has provided assistance to all requesting agencies without delay. We are also working with a small number of

private sector entities that have seen suspected or confirmed activity associated with this campaign.

Beginning last week, CISA has released guidance to support federal departments and agencies in evicting this threat activity from compromised on-premises and cloud environments. This guidance addressed tactics, techniques, and procedures (TTPs) leveraged by the threat actor and provides short- and intermediate-term actions that agencies should take to mitigate this activity and prevent future threat activity. By taking steps to evict this adversary from compromised on-premises and cloud environments, agencies will position themselves for long-term actions to build more secure, resilient networks.

Long-term Rebuilding Secure Networks

Under the fourth line of effort, rebuilding secure networks across the federal civilian branch and the broader community is just beginning. In the coming weeks, as affected entities begin to plan for their long-term rebuilds, CISA will work hand-in-hand with our partners to ensure standardization and consistency. This is a patient and focused adversary that has sustained its presence on victim networks, in some cases, for many months. As such, the recovery and rebuilding process will be time and resource intensive.

Mitigating Future Attacks

We expect that impact of the recent cyber compromises will be far reaching and reflect an urgent need to strengthen our nation's cyber defenses, invest in new capabilities, and begin to change how we think about cybersecurity. For example, due to the global pandemic, the risk landscape has shifted dramatically over the past year. Between the ongoing cyber intrusions and the seismic shift in how we work, legislate, educate and support our daily lives, we need to take decisive action today to be ready to defend our National security tomorrow. To this end, CISA is focused on urgent improvements across four areas of strategic growth.

First, we must increase CISA's visibility into cybersecurity risks across the federal civilian executive branch and, where feasible, across non-federal entities. Second, we must expand CISA's incident response capacity. Third, we must improve our ability to analyze large volumes of cybersecurity information in order to rapidly identify emerging risks and direct timely mitigation, and fourth, we must drive adoption of defensible network architectures, including by progressing toward zero-trust environments.

Operational Visibility. We must increase and improve our visibility into agency cloud environments and end-points. Due to COVID-19, many Federal agencies have accelerated cloud migration to support a remote workforce, a trend that we expect will continue. Recent compromises of federal agencies show that cloud resources are an attractive target to our most sophisticated adversaries. Across different cloud environments, security standards differ based on contracting decisions, vendor-specific offerings, and risk decisions. This compromise has highlighted that a common baseline of security controls, particularly focused on logging and retention, may be necessary across cloud environments. Additionally, we need to gain better

visibility into end-points within agency networks and support improvements to risk management practice and software assurance across agencies' ICT supply chains.

Incident Response Capacity. We need to continue to build the capacity to hunt for threats on agency networks and respond to incidents. While we are effectively responding today, this most recent attack should serve as a warning that federal government incident response resources must be fortified now to ensure that we will not be overwhelmed in the future, resulting in delayed incident response and recovery. Going forward, we must shift to a model of persistent threat hunting, enabled by authorities provided by Congress in the Fiscal Year 2021 National Defense Authorization Act, to more rapidly identify potential intrusions into federal civilian networks.

Defensible Network Architectures. Agencies must adopt network architectures that are more defensible. We are exploring additional capabilities to support defensible architectures, including through offering secure cloud environments to agencies, expanding identity management efforts and cloud security efforts under the Continuous Diagnostics and Monitoring (CDM) program, and implement principles of zero-trust architecture.

Analysis and Coordination. We are maturing our capabilities to analyze risk in order to more effectively identify cybersecurity risks within individual agencies and across the federal civilian executive branch, which require new analytical capabilities that can rapidly adapt to our operators' needs, automate as much as possible, and provide a common operating picture.

Conclusion

More than ever, Federal agencies and key service providers are under attack from nation-state adversaries and criminals seeking to make a profit. Both the Microsoft Exchange vulnerabilities and the SolarWinds campaign highlight the lengths to which sophisticated adversaries will go to compromise our networks. They will use never-seen-before techniques, exquisite tradecraft and zero-day vulnerabilities, to defeat our current cybersecurity architecture.

CISA's charge is clear: protect and defend the Federal enterprise through collaborative risk management. This is a complicated mission space with evolving technology and risks, but we know that the Federal Enterprise can be made safe and secure. By enhancing our visibility, implementing persistent hunt capabilities, increasing provision of shared services, and moving toward a zero-trust model, we can most effectively ensure that the Federal Government can provide critical services to the American people under all conditions.

Thank you again for the opportunity to be to appear before the committee. We stand ready to answer your questions.