Testimony

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

Eric Goldstein
Executive Assistant Director
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"MODERNIZING THE FEDERAL CIVILIAN APPROACH TO CYBERSECURITY"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
Committee on Appropriations- Homeland Security Subcommittee

March 10, 2021

Washington, DC

Chairwoman Roybal-Allard, Ranking Member Fleischmann, and members of the Committee, thank you for the opportunity to testify today regarding the Cybersecurity and Infrastructure Security Agency's (CISA) perspectives and recommendations on modernizing the federal civilian approach to cybersecurity following the recent cyber intrusion campaign that targeted many of our government and private sector organizations. 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, territorial, and other government partners. By analyzing information from numerous 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 activities, including issuing alerts and guidance, to mandatory direction through directives known as Binding Operational Directive and Emergency Directives, and ongoing coordination with agency network operators. Where necessary, CISA also provides technical assistance by deploying teams to hunt for threats, respond to incidents, and provide recommendations to harden systems.

In addition, CISA focuses on addressing longer-term gaps in federal cybersecurity, such as outdated systems or inadequate organizational focus on system maintenance. In order to raise the baseline of federal cybersecurity, CISA 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.

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 individual hackers to nation-state intruders using state-of-the-art techniques. The recent widespread cyber intrusion campaign targeted federal networks 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. We must act now and decisively to truly defend today and secure tomorrow.

Cyber Supply Chain Compromise

In early December 2020, the Federal Government became aware of a cyber intrusion campaign that included compromises of some U.S. government departments and agencies, critical infrastructure entities, and private sector organizations dating back to at least September 2019. This operation was highly sophisticated using novel techniques and advanced tradecraft to remain undetected 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, who regularly install and trust such updates to patch their software. In this case, once these updates with the malicious code were applied, the threat actor was able to directly access customer networks by installing and accessing a back door into their environment.

There are two important categories: According to SolarWinds, nearly 18,000 entities received a malicious version of the software. We refer to these entities as "exposed." The threat actor then targeted a much smaller number of these exposed 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 threat actor was able to use its privileged access gained by compromising organizations' on-premises 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 attack through SolarWinds has been a primary focus of this activity, the U.S. government is aware of additional victims of related Microsoft Office 365 compromises that pre-date the delivery of the SolarWinds software update that, unbeknownst to the vendor, contained a back door accessible to the threat actor. The initial intrusion vector for these earlier victims is currently unknown.

Considering these different vectors, 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 a Cyber Unified Coordination Group (UCG). Composed of 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 guidance and coordinates with departments and agencies, and provides technical assistance to affected entities upon request.

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

Scoping the Campaign

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

Sharing Information and Detection

CISA began to develop detection techniques and share information immediately upon learning of the malicious cyber campaign. On December 13, 2020, we issued Emergency Directive 21-01 requiring federal civilian executive branch agencies to shut down affected versions of the SolarWinds Orion platform. We decided to release our directive publicly in order to drive immediate mitigation steps and help both public and private sector entities identify whether their networks may have been exposed to the adversary. Within 72 hours after CISA published the directive, 100% of devices running affected versions of SolarWinds Orion had been taken off-line across the federal civilian executive branch.

On December 17, CISA released a detailed alert describing the tactics of the threat actor and providing initial guidance and indicators to entities with suspected compromises. We have updated both our Emergency Directive and Activity Alert several times, and we will issue additional updates as appropriate if we uncover new information. Following the release of our directive and alert, we held stakeholder calls with thousands of public and private sector entities through which we provided detailed 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 has been widely targeted by the adversary as part of this malicious cyber 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. Additionally, we continue engaging with stakeholders daily to understand changes in the scope of the campaign and continuously share information and necessary actions across all stakeholders as the incident response continues.

Short-Term Remediation

Under the third line of effort, short-term remediation, CISA has 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.

This week, CISA released guidance to support federal departments and agencies in evicting this threat actor from compromised on-premises and cloud environments. This guidance addresses 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 immediate 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 of Secure Networks

Under the fourth line of effort, rebuilding secure networks across the federal civilian branch and the broader community over the long term 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. The threat actor responsible for this malicious cybercampaign 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.

COVID-19 Impact and CISA's Growth

While the short-term impact of the malicious cyber campaign and resulting breach of federal networks is already being felt, this kind of exploitation has far-reaching longer-term impacts and consequences. Due to the global pandemic, the risk landscape has shifted dramatically over the past year. Between the ongoing malicious cyber campaign 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 nation tomorrow. CISA has identified several key areas of growth needed to address lessons-learned from the widespread malicious cyber campaign and the broader COVID-19 response.

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 timelines in order to support a remote workforce, a trend that we expect will continue. However, recent compromises of federal agency networks show that cloud resources continue to be an attractive target to our most sophisticated adversaries. Across different cloud environments, security standards differ based on many factors, including contracting decisions, vendor-specific offerings, and risk decisions. This malicious cyber campaign has highlighted that a common baseline of security controls, particularly focused on logging and retention, may be necessary across cloud environments in the Federal Government. We will work jointly with the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board and the National Institute of Standards and Technology (NIST) on tightening these controls. Additionally, we need to gain better visibility into end-points within agency networks and support improvements to risk management practices and software assurance across agencies' information and communication technology (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 immediately deployed CISA and interagency resources to effectively respond to this campaign, the scale and significant time span of this 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 program, and implement principles of more secure and resilient 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. This includes developing new analytical capabilities that can rapidly adapt to our operators' needs and provide a common operating picture, and which are automated to the extent possible.

Conclusion

The Federal Government provides countless services that are vital to the functioning of the country and our economy. More than ever, federal agencies and key service providers are under attack from nation-state adversaries and criminal, profit-driven actors.

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. What's more, today's landscape reflects challenges stemming from decades of under-investment in technology infrastructure; federal network security has been on the Government Accountability Office's High Risk list since 1997.

The federal enterprise can be made more resilient and secure. By enhancing our visibility, implementing persistent hunt capabilities, increasing provision of shared services, and moving toward more robust architecture models, 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.