The FBI, CISA and ODNI formed a group to address the most significant cyber breach of the U.S. government in years.

Melissa Harris
Fri, 12/18/2020 - 15:52

The Cyber Unified Coordination Group, an effort between the U.S. intelligence community and the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA), is in the midst of coordinating its response to the recent discovery of a major hacking incident across various agencies last week.
Officials suspect Russian actors are responsible for a cybersecurity breach conducted through a "backdoor" supply-chain attack that impacted the Treasury and Commerce departments. The new group comprises the following response roles:

- The FBI will investigate and gather intelligence to attribute, pursue and disrupt the responsible threat actors by engaging with known and suspected victims
- CISA will relay technical assistance and guidance to federal, private-sector and international partners to communicate each party’s potential exposure and how to identify and mitigate any compromises
- The Office of the Director of National Intelligence will marshal all intelligence community resources that are relevant to share information across the government.

The group's formation comes after the “SUNBURST” attack first came to light Dec. 8, when private cybersecurity firm FireEye found that hackers broke into its network. The attackers gained access through a SolarWinds’ Orion network-monitoring software update earlier this year, according to the two companies. FireEye claimed that the hackers got “backdoor” access through this supply-chain form of attack to steal cyber tools it uses to test its clients’ cybersecurity and that the attackers were likely acting on behalf of a nation state.

The hack is what Atlantic Council Cyber Statecraft Initiative Director Trey Herr calls “potentially the greatest cyber crisis the federal government has had in the cloud era.”

Though software supply chain attacks are nothing new, Herr noted that the post-attack activity, which enabled the hackers to go undetected for months after the attack, was the most unique aspect of this attack.

“The differentiating factor here, and what’s made this so compelling, is that the entity behind that espionage operation was able to maintain access to those networks and remained hidden for such a long period of time, based on what was reported,” Herr said.

Although it’s been over half a year since the breach initially occurred, FireEye said that it is working closely with the FBI and SolarWinds to uncover details behind the attack. As of Dec. 13, FireEye’s analysis found the attackers:
used malicious code in legitimate software updates for SolarWinds' Orion software that allowed an attacker remote access into the victim’s environment

- used limited malware to accomplish the mission while avoiding detection
- went significant lengths to observe and blend into normal network activity
- conducted reconnaissance, consistently covered their tracks and used difficult-to-attribute tools.

CISA has so far issued an emergency directive for civilian agencies that have the SolarWinds software to disconnect or power down the products immediately.


The directive will only stop new breaches and will mitigate access enabled through earlier software updates. However, Herr said that such moves are proper initial actions, adding agencies should also start examining network logs and have their CISOs and security leadership share a list of vendors’ products that are in the most sensitive places in their networks.

“Administrative tools, security tools, management tools that you use to keep your architecture up and running — you share that list of what you think are the most vulnerable targets, are the most valuable targets for attackers, who makes all of that gear, and you share it with these other organizations, and you compare notes to see who shares the same vendors,” Herr said. “Prioritize that list, and you work with those other agencies to go out to those vendors and work with them proactively to hunt for exactly this kind of issue in their code and code they depend on in the open-source community, to see if there’s something else like this on the market.”

As the new response group continues its investigation into the supply-chain-based breach, a Government Accountability Office report this week said more than half of 23 civilian agencies it examined did not implement the National Institute of Standards and Technology’s key guidelines for information and communications technology supply chain risk management (ICT SCRM).
One of the key guidelines is in ensuring that agencies develop organizational ICT SCRM requirements for suppliers — a step that could reduce backdoor incidents caused by acquired software like SolarWinds’.

“Without organizational ICT supply chain security requirements for inclusion in contracts, agencies lack an essential mechanism to ensure that suppliers (and their suppliers) are adequately addressing risks associated with ICT products and services,” GAO said.

Herr reiterated that agencies need to be more mindful and strategic about supply chain security moving forward, especially given the great dependency the federal government has on its vendor community.

“From the federal government standpoint, understanding the dependency of federal agencies and organization on vendors like SolarWinds — which is to say, knowing where those organizations have sensitive gear that’s given tremendous access and knowing organization buy that gear from, what has been a useful list to prioritize aggressive [outreach] for security evaluation, for sharing a threat intelligence or potentially for proactive investigations — has to be part of that trusted supply chain by government security,” Herr said.

Herr added that from the vendor perspective, it is important for organizations like SolarWinds to be mindful that one attack on their product can impact thousands of customers, such as with the SUNBURST malware. Approaching their development process and platform in a more secure way would help prevent attackers from accessing the build platform and source code.

Amid recent discoveries and ongoing investigations over the breach, leadership from the House Committee on Homeland Security wrote a letter to FBI Director Christopher Wray, DHS Acting Secretary Chad Wolf and ODNI Director John Ratcliffe calling on them to share the latest information on the breach.
“As the Committees of jurisdiction for U.S. cybersecurity preparedness and the defense of federal information technology systems, it is imperative that our Committees receive the latest information on the number of federal departments, agencies, and other entities affected by the breach, the extent to which sensitive information and data — including classified information — may have been compromised or exposed, the threat actor or actors responsible, and the Administration’s ongoing efforts to prevent further damage, secure its computer networks, and hold those responsible accountable,” the committee leadership wrote.

The committee requested a classified, interagency briefing on the breach on Friday with the intelligence and homeland security leaders.