After hack, officials draw attention to supply chain threats

April 1 2021, by Eric Tucker

In this Feb. 23, 2021, file photo, SolarWinds CEO Sudhakar Ramakrishna speaks during a Senate Intelligence Committee hearing on Capitol Hill in Washington. The U.S. government is working to draw attention to supply chain vulnerabilities. It's an issue that received particular attention late last year after suspected Russian hackers gained access to federal agencies and private corporations by sneaking malicious code into widely used software. (Demetrius Freeman/The Washington Post via AP, Pool)

The U.S. government is working to draw attention to supply chain vulnerabilities, an issue that received particular attention late last year after suspected Russian hackers gained access to federal agencies and private corporations by sneaking malicious code into widely used software.

The National Counterintelligence and Security Center warned Thursday that foreign hackers are increasingly targeting vendors and suppliers that work with the government to compromise their products in an effort to steal intellectual property and carry out espionage. The NCSC said it is working with other agencies, including the Cybersecurity and Infrastructure Security Agency, to raise awareness of the supply chain issue.

April marks what the government is describing as the fourth annual National Supply Chain Integrity Month. This year's event comes as federal officials deal with the aftermath of the SolarWinds intrusion, in which hackers compromised the software supply chain through malware. At least nine federal agencies were hacked, along with dozens of private-sector companies.

The NCSC said it plans to issue guidance throughout the month about how specific sectors, like health care and energy, can protect themselves.

"If the Covid-19 pandemic and resulting product shortages were not a sufficient wake-up call, the recent software supply chain attacks on U.S. industry and government should serve as a resounding call to action," NCSC acting director Michael Orlando said in a statement. "We must enhance the resilience, diversity, and security of our supply chains. The vitality of our nation depends on it."

Orlando and officials from the United Kingdom, Canada and Australia are participating next week in a Harvard University discussion about

protecting the international supply chain.

The sheer number of steps in a product's supply chain process gives a hacker looking to infiltrate businesses, agencies and infrastructure numerous points of entry and can mean no company or executive bears sole responsibility for protecting an entire industry supply chain. That's why officials recommend that supply chains be diversified, that essential assets be identified and protected and that specific senior executives be assigned to deal with the concern.

Perhaps the best-known supply chain intrusion before SolarWinds is the NotPetya attack, in which malicious code found to have been planted by Russian military hackers was unleashed through an automatic update of Ukrainian tax preparation software, called MeDoc.