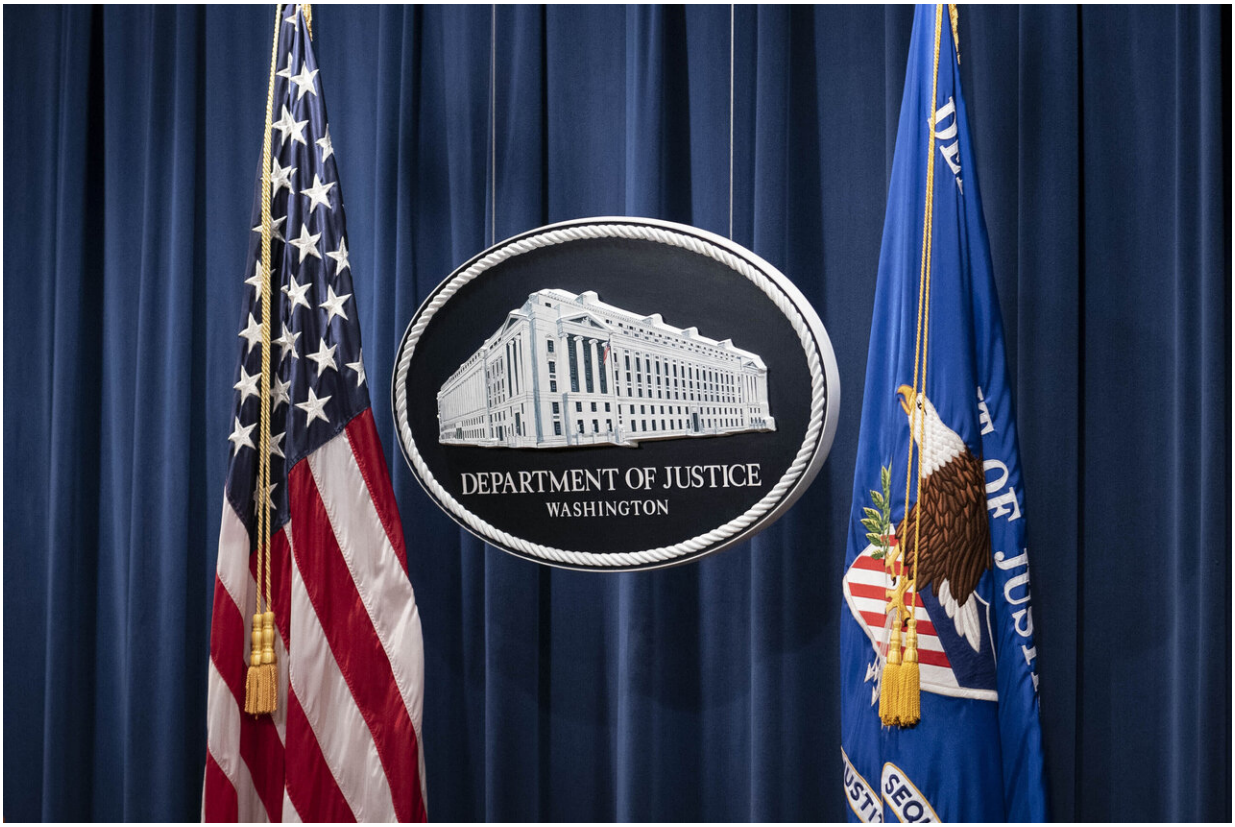
Russian hack of US agencies exposed supply chain weaknesses

January 25 2021, by Eric Tucker



This Jan. 12, 2021, file photo shows a sign for the Department of Justice ahead of a news conference in Washington. The elite Russian hackers who gained access to computer systems of federal agencies last year didn't bother trying to break one-by-one into the networks of each department. Instead, they got inside by sneaking malicious code into a software update pushed out to thousands of government agencies and private companies. (Sarah Silbiger/Pool via AP, File)

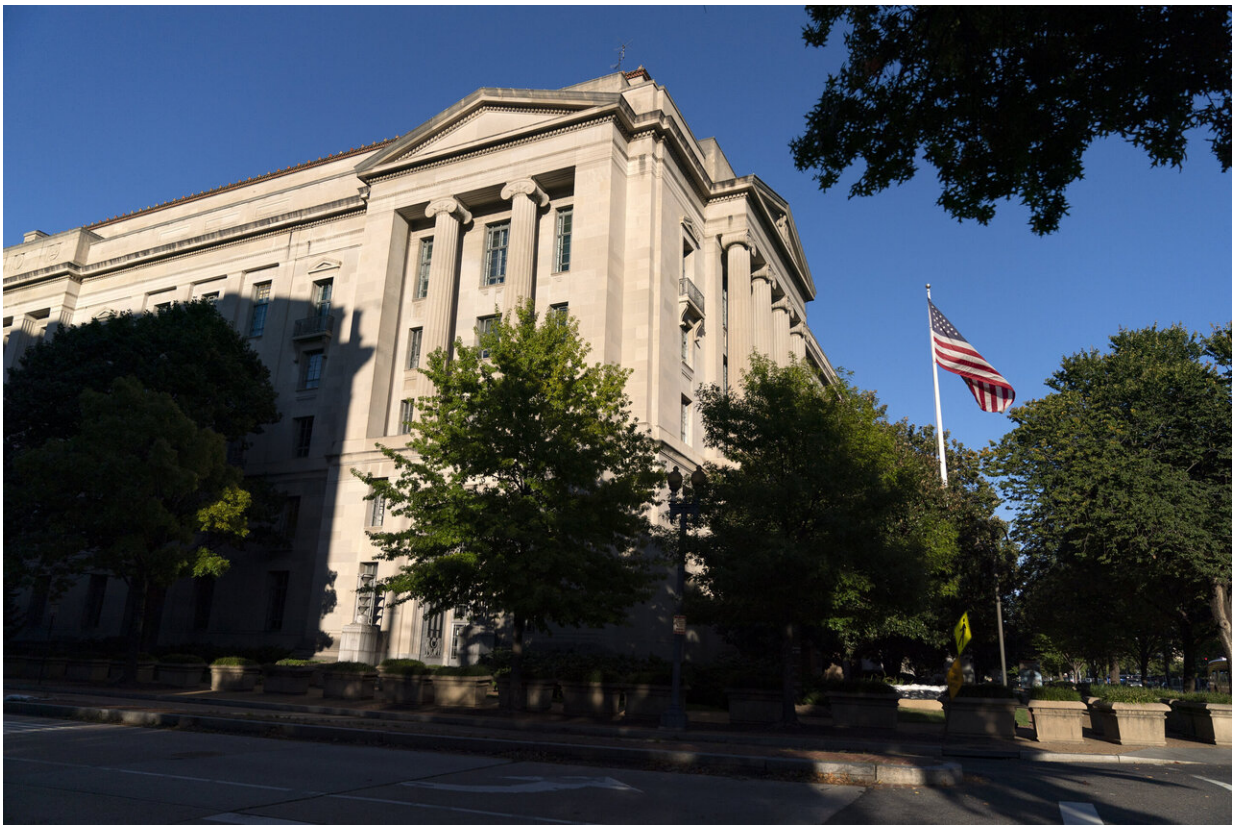
The elite Russian hackers who gained access to computer systems of federal agencies last year didn't need to painstakingly break one-by-one into the networks of each department in order to do damage.

Instead, they got inside by sneaking malicious code into a software update pushed out to thousands of government agencies and private companies.

That hackers were able to exploit vulnerabilities in the supply chain to launch a massive intelligence gathering operation wasn't especially surprising. U.S. officials and cybersecurity experts have sounded the alarm for years about a problem that has caused havoc, including billions of dollars in financial losses, while also defying easy solutions from the government and private sector.

"We're going to have to wrap our arms around the supply-chain threat and find the solution, not only for us here in America as the leading economy in the world, but for the planet," William Evanina, who resigned last week as the U.S. government's chief counterintelligence official, said in an interview. "We're going to have to find a way to make sure that we in the future can have a zero-risk posture, and trust our suppliers."

In general terms, a supply chain refers to the network of people and companies involved in the development of a particular product, not dissimilar to a home construction project that relies on a contractor and a web of subcontractors. The sheer number of steps in that process, from design to manufacture to distribution, and the different entities involved give a hacker looking to infiltrate businesses, agencies and infrastructure numerous points of entry.



In this Oct. 8, 2020, file photo an American flag flies outside of the Justice Department building in Washington. The elite Russian hackers who gained access to computer systems of federal agencies last year didn't bother trying to break one-by-one into the networks of each department. Instead, they got inside by sneaking malicious code into a software update pushed out to thousands of government agencies and private companies. (AP Photo/Jacquelyn Martin, FIle)

That can mean no single company or executive bears sole responsibility for protecting an entire industry supply chain. And even if most vendors in the chain are secure, a single point of vulnerability can be all that foreign government hackers need. In practical terms, homeowners who construct a fortress-like mansion can nonetheless find themselves victimized by an alarm system that was compromised before it was installed.

The most recent case targeting federal agencies involved Russian government hackers who are believed to have inserted malicious code into popular software that monitors computer networks of businesses and governments. That product is made by a Texas-based company called SolarWinds that has thousands of customers in the federal government and private sector.

The malware gave hackers remote access to the networks of multiple agencies. Among those known to have been affected are the departments of Commerce, Treasury and Justice.

For hackers, the business model of directly targeting a supply chain is sensible.

"If you want to breach 30 companies on Wall Street, why breach 30 companies on Wall Street (individually) when you can go to the server—the warehouse, the cloud—where all those companies hold their data? It's just smarter, more effective, more efficient to do that," Evanina said.

Though President Donald Trump showed little personal interest in cybersecurity, even firing the head of the Department of Homeland Security's cybersecurity agency just weeks before the Russian hack was revealed, President Joe Biden has said he will make it a priority and will impose costs on adversaries who carry out attacks.

Supply chain protection will presumably be a key part of those efforts, and there is clearly work to be done. A five Chinese hackers who it said had compromised software providers and then modified source code to allow for further hacks of the providers' customers. In 2018, the department announced a similar case against two Chinese hackers accused of breaking into cloud service providers and injecting malicious software.

"Anyone surprised by SolarWinds hasn't been paying attention," said Rep. Jim Langevin, a Rhode Island Democrat and member of the Cyberspace Solarium Commission, a bipartisan group that issued a white paper calling for the protection of the supply chain through better intelligence and information sharing.

Part of the appeal of a supply chain attack for hackers is that it's "low-hanging fruit," with the U.S. often not appreciating or understanding how dispersed its networks actually are, said Brandon Valeriano, a cybersecurity expert at the Marine Corps University and a senior adviser to the solarium commission.

"The problem is we basically don't know what we're eating." Valeriano said. "And sometimes it comes out later that we choke on something."