washingtonpost.com

Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce

Ellen Nakashima, Craig Timberg

8-10 minutos

Russian government hackers breached the Treasury and Commerce departments, along with other U.S. government agencies, as part of a global espionage campaign that stretches back months, according to people familiar with the matter.

Officials were scrambling over the weekend to assess the nature and extent of the intrusions and implement effective countermeasures, but initial signs suggested the breach was long-running and significant, the people familiar with the matter said.

The Russian hackers, known by the nicknames APT29 or Cozy Bear, are part of that nation’s foreign intelligence service, the SVR, and they breached email systems in some cases, said the people familiar with the intrusions, who spoke on the condition of anonymity because of the sensitivity of the matter. The same Russian group hacked the State Department and the White House email servers during the Obama administration.

The FBI is investigating the campaign, which may have begun as early as spring, and had no comment Sunday. The victims

have included government, consulting, technology, telecom, and oil and gas companies in North America, Europe, Asia and the Middle East, according to FireEye, a cyber firm that itself was breached.

The Russian Embassy in Washington on Sunday called the reports of Russian hacking “baseless.” In a statement on Facebook it said, “attacks in the information space contradict” Russian foreign policy and national interests. “Russia does not conduct offensive operations” in the cyber domain.

All of the organizations were breached through the update server of a network management system made by the firm SolarWinds, FireEye said in a blog post Sunday.

The federal Cybersecurity and Infrastructure Security Agency issued an alert Sunday warning about an “active exploitation” of the SolarWinds Orion Platform, from versions of the software released in March and June. “CISA encourages affected organizations to read the SolarWinds and FireEye advisories for more information and FireEye’s GitHub page for detection countermeasures,” the alert said.

SolarWinds said Sunday in a statement that monitoring products it released in March and June of this year may have been surreptitiously weaponized in a “highly-sophisticated, targeted . . . attack by a nation state.”

The company filed a document Monday with the Securities and Exchange Commission saying that “fewer than 18,000” of its more than 300,000 customers may have installed a software patch enabling the Russian attack. It was not clear, the filing said, how many systems were actually hacked. The corporate filing also said that Microsoft’s Office 365 email may have been “an attack vector” used by the hackers.

Microsoft said in a blog post Sunday that it had not identified any Microsoft product or cloud service vulnerabilities in its investigation of the matter.

The scale of the Russian espionage operation appears to be large, said several individuals familiar with the matter. “This is looking very, very bad,” said one person. SolarWinds products are used by organizations across the world. They include all five branches of the U.S. military, the Pentagon, State Department, Justice Department, NASA, the Executive Office of the President and the National Security Agency, the world’s top electronic spy agency, according to the firm’s website.

Its clients also include the top 10 U.S. telecommunications companies.

“This is a big deal, and given what we now know about where breaches happened, I’m expecting the scope to grow as more logs are reviewed,” said John Scott-Railton, a senior researcher at Citizen Lab at the University of Toronto’s Munk School of Global Affairs and Public Policy. “When an aggressive group like this gets an open sesame to many desirable systems, they are going to use it widely.”

FireEye reported last week that it was breached and that hacking tools it uses to test clients’ computer defenses were stolen. The Washington Post reported that APT29 was the group behind that hack. FireEye and Microsoft, which were investigating the breach, discovered the hackers were gaining access to victims through updates to SolarWinds’ Orion network monitoring software, FireEye said in its blog post, without publicly naming the Russians.

Reuters first reported the hacks of the Treasury and Commerce departments Sunday, saying they were carried out by a foreign

government-backed group. The SVR link to the broader campaign was previously unreported.

The matter was so serious that it prompted an emergency National Security Council meeting on Saturday, Reuters reported.

“The United States government is aware of these reports, and we are taking all necessary steps to identify and remedy any possible issues related to this situation,” said National Security Council spokesman John Ullyot. He did not comment on the country or group responsible.

At Commerce, the Russians targeted the National Telecommunications and Information Administration, an agency that handles Internet and telecommunications policy, Reuters reported. They have also been linked to attempts to steal coronavirus vaccine research.

In 2014 and 2015, the same group carried out a wide-ranging espionage campaign that targeted thousands of organizations, including government agencies, foreign embassies, energy companies, telecommunications firms and universities.

As part of that operation, it hacked the unclassified email systems of the White House, the Pentagon’s Joint Chiefs of Staff and the State Department.

“That was the first time we saw the Russians become much more aggressive, and instead of simply fading away like ghosts when they were detected, they actually contested access to the networks,” said Michael Daniel, who was White House cybersecurity coordinator at the time.

One of its victims in 2015 was the Democratic National Committee. But unlike a rival Russian spy agency, the GRU,

which also hacked the DNC, it did not leak the stolen material. In 2016, the GRU military spy agency leaked hacked emails to the online anti-secrecy organization WikiLeaks in an operation that disrupted the Democrats' national convention in the midst of the presidential campaign.

The SVR, by contrast, generally steals information for traditional espionage purposes, seeking secrets that might help the Kremlin understand the plans and motives of politicians and policymakers. Its operators also have filched industrial data and hacked foreign ministries.

Because the Obama administration saw the APT29 operation as traditional espionage, it did not consider taking punitive measures, said Daniel, who is now president and chief executive of the Cyber Threat Alliance, an information-sharing group for cybersecurity companies.

"It was information collection, which is what nation states — including the United States — do," he said. "From our perspective, it was more important to focus on shoring up defenses."

But Chris Painter, State Department cyber coordinator in the Obama administration, said even if the Russian campaign is strictly about espionage and there's no norm against spying, if the scope is broad there should be consequences. "We just don't have to sit still for it and say 'good job,' " he said.

Sanctions might be one answer, especially if done in concert with allies who were similarly affected, he said. "The problem is there's not even been condemnation from the top. President Trump hasn't wanted to say anything bad to Russia, which only encourages them to act irresponsibly across a wide range of activities."

At the very least, he said, “you’d want to make clear to [Russian President Vladimir] Putin that this is unacceptable — the scope is unacceptable.”

So far there is no sign that the current campaign is being waged for purposes of leaking information or for disruption of critical infrastructure, such as electric grids.

SolarWinds’ monitoring tool has extremely deep “administrative” access to a network’s core functions, which means that hacking the tool would allow the Russians to freely root around victims’ systems.

APT29 compromised SolarWinds so that any time a customer checked in to request an update, the Russians could hitch a ride on the weaponized update to get into a victim’s system. FireEye dubbed the malware that the hackers used “Sunburst.”

“Monday may be a bad day for lots of security teams,” tweeted Dmitri Alperovitch, a cybersecurity expert and founder of the Silverado Policy Accelerator think tank.

Joseph Marks contributed to this report.