As Understanding of Russian Hacking Grows, So Does Alarm

nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

David E. Sanger, Nicole Perlroth, Julian E. Barnes January 2, 2021

Continue reading the main story

On Election Day, General Paul M. Nakasone, the nation's top cyberwarrior, reported that the battle against Russian interference in the presidential campaign had posted major successes and exposed the other side's online weapons, tools and tradecraft.

"We've broadened our operations and feel very good where we're at right now," he told journalists.

Eight weeks later, General Nakasone and other American officials responsible for cybersecurity are now consumed by what they missed for at least nine months: a hacking, now believed to have affected upward of 250 federal agencies and businesses, that Russia aimed not at the election system but at the rest of the United States government and many large American corporations.

Three weeks after the intrusion came to light, American officials are still trying to understand whether what the Russians pulled off was simply an espionage operation inside the systems of the American bureaucracy or something more sinister, inserting "backdoor" access into government agencies, major corporations, the electric grid and laboratories developing and transporting new generations of nuclear weapons.

At a minimum it has set off alarms about the vulnerability of government and private sector networks in the United States to attack and raised questions about how and why the nation's cyberdefenses failed so spectacularly.

Those questions have taken on particular urgency given that the breach was not detected by any of the government agencies that share responsibility for cyberdefense — the military's Cyber Command and the National Security Agency, both of which are run by General Nakasone, and the Department of Homeland Security — but by a private cybersecurity company, FireEye.

"This is looking much, much worse than I first feared," said Senator Mark Warner, Democrat of Virginia and the ranking member of the Senate Intelligence Committee. "The size of it keeps expanding. It's clear the United States government missed it."

"And if FireEye had not come forward," he added, "I'm not sure we would be fully aware of it to this day."

Interviews with key players investigating what intelligence agencies believe to be an operation by Russia's S.V.R. intelligence service revealed these points:

- The breach is far broader than first believed. Initial estimates were that Russia sent its probes only into a few dozen of the 18,000 government and private networks they gained access to when they inserted code into network management software made by a Texas company named SolarWinds. But as businesses like Amazon and Microsoft that provide cloud services dig deeper for evidence, it now appears Russia exploited multiple layers of the supply chain to gain access to as many as 250 networks.

- The hackers managed their intrusion from servers inside the United States, exploiting legal prohibitions on the National Security Agency from engaging in domestic surveillance and eluding cyberdefenses deployed by the Department of Homeland Security.

- "Early warning" sensors placed by Cyber Command and the National Security Agency deep inside foreign networks to detect brewing attacks clearly failed. There is also no indication yet that any human intelligence alerted the United States to the hacking.

- The government's emphasis on election defense, while critical in 2020, may have diverted resources and attention from long-brewing problems like protecting the "supply chain" of software. In the private sector, too, companies that were focused on election security, like FireEye and Microsoft, are now revealing that they were breached as part of the larger supply chain attack.

- SolarWinds, the company that the hackers used as a conduit for their attacks, had a history of lackluster security for its products, making it an easy target, according to current and former employees and government investigators. Its chief executive, Kevin B. Thompson, who is leaving his job after 11 years, has sidestepped the question of whether his company should have detected the intrusion.

- Some of the compromised SolarWinds software was engineered in Eastern Europe, and American investigators are now examining whether the incursion originated there, where Russian intelligence operatives are deeply rooted.

The intentions behind the attack remain shrouded. But with a new administration taking office in three weeks, some analysts say the Russians may be trying to shake Washington's confidence in the security of its communications and demonstrate their cyberarsenal to gain leverage against President-elect Joseph R. Biden Jr. before nuclear arms talks.

"We still don't know what Russia's strategic objectives were," said Suzanne Spaulding, who was the senior cyberofficial at the Homeland Security Department during the Obama administration. "But we should be concerned that part of this may go beyond reconnaissance. Their goal may be to put themselves in a position to have leverage over the new administration, like holding a gun to our head to deter us from acting to counter Putin."

Image
The Commerce Department, the Treasury Department, the State Department, the Energy Department and parts of the Pentagon were targets of the breach.Credit...Alyssa Schukar for The New York Times

Growing Hit List

The U.S. government was clearly the main focus of the attack, with the Treasury Department, the State Department, the Commerce Department, the Energy Department and parts of the Pentagon among the agencies confirmed to have been infiltrated. (The Defense Department insists the attacks on its systems were unsuccessful, though it has offered no evidence.)

But the hacking also breached large numbers of corporations, many of which have yet to step forward. SolarWinds is believed to be one of several supply chain vendors Russia used in the hacking. Microsoft, which had tallied 40 victims as of Dec. 17, initially said that it had not been breached, only to discover this week that it had been — and that resellers of its software had been, too. A previously unreported assessment by Amazon's intelligence team found the number of victims may have been five times greater, though officials warn some of those may be double counted.

Publicly, officials have said they do not believe the hackers from Russia's S.V.R. pierced classified systems containing sensitive communications and plans. But privately, officials say they still do not have a clear picture of what might have been stolen.

They said they worried about delicate but unclassified data the hackers might have taken from victims like the Federal Energy Regulatory Commission, including Black Start, the detailed technical blueprints for how the United States plans to restore power in the event of a cataclysmic blackout.

The plans would give Russia a hit list of systems to target to keep power from being restored in an attack like the one it pulled off in Ukraine in 2015, shutting off power for six hours in the dead of winter. Moscow long ago implanted malware in the American electric grid, and the United States has done the same to Russia as a deterrent.

A Supply Chain Compromised

One main focus of the investigation so far has been SolarWinds, the company based in Austin whose software updates the hackers compromised.

But the cybersecurity arm of the Department of Homeland Security concluded the hackers worked through other channels, too. And last week, CrowdStrike, another security company, revealed that it was also targeted, unsuccessfully, by the same hackers, but through a company that resells Microsoft software.

Because resellers are often entrusted to set up clients' software, they — like SolarWinds — have broad access to Microsoft customers' networks. As a result, they can be an ideal Trojan horse for Russia's hackers. Intelligence officials have expressed anger that Microsoft did not detect the attack earlier; the company, which said Thursday that the hackers viewed its source code, has not disclosed which of its products were affected or for how long hackers were inside its network.

"They targeted the weakest points in the supply chain and through our most trusted relationships," said Glenn Chisholm, a founder of Obsidian Security.

Image
SolarWinds, the company most directly exploited by the hackers, had a history of lackluster security for its own products, making it an easy target, according to its employees.Credit...Sergio Flores/Reuters
Interviews with current and former employees of SolarWinds suggest it was slow to make security a priority, even as its software was adopted by America's premier cybersecurity company and federal agencies.

Employees say that under Mr. Thompson, an accountant by training and a former chief financial officer, every part of the business was examined for cost savings and common security practices were eschewed because of their expense. His approach helped almost

triple SolarWinds' annual profit margins to more than $453 million in 2019 from $152 million in 2010.

But some of those measures may have put the company and its customers at greater risk for attack. SolarWinds moved much of its engineering to satellite offices in the Czech Republic, Poland and Belarus, where engineers had broad access to the Orion network management software that Russia's agents compromised.

The company has said only that the manipulation of its software was the work of human hackers rather than of a computer program. It has not publicly addressed the possibility of an insider being involved in the breach.

None of the SolarWinds customers contacted by The New York Times in recent weeks were aware they were reliant on software that was maintained in Eastern Europe. Many said they did not even know they were using SolarWinds software until recently.

Even with its software installed throughout federal networks, employees said SolarWinds tacked on security only in 2017, under threat of penalty from a new European privacy law. Only then, employees say, did SolarWinds hire its first chief information officer and install a vice president of "security architecture."

Ian Thornton-Trump, a former cybersecurity adviser at SolarWinds, said he warned management that year that unless it took a more proactive approach to its internal security, a cybersecurity episode would be "catastrophic." After his basic recommendations were ignored, Mr. Thornton-Trump left the company.

SolarWinds declined to address questions about the adequacy of its security. In a statement, it said it was a "victim of a highly-sophisticated, complex and targeted cyberattack" and was collaborating closely with law enforcement, intelligence agencies and security experts to investigate.

But security experts note that it took days after the Russian attack was discovered before SolarWinds' websites stopped offering clients compromised code.

Offense Over Defense

Billions of dollars in cybersecurity budgets have flowed in recent years to offensive espionage and pre-emptive action programs, what General Nakasone calls the need to "defend forward" by hacking into adversaries' networks to get an early look at their operations and to counteract them inside their own networks, before they can attack, if required.

But that approach, while hailed as a long-overdue strategy to pre-empt attacks, missed the Russian breach.

Image
General Paul M. Nakasone leads both the National Security Agency and the military's Cyber Command.Credit...T.J. Kirkpatrick for The New York Times
By staging their attacks from servers inside the United States, in some cases using computers in the same town or city as their victims, according to FireEye, the Russians took advantage of limits on the National Security Agency's authority. Congress has not given the agency or homeland security any authority to enter or defend private sector networks. It was on these networks that S.V.R. operatives were less careful, leaving clues about their intrusions that FireEye was ultimately able to find.

By inserting themselves into the SolarWinds' Orion update and using custom tools, they also avoided tripping the alarms of the "Einstein" detection system that homeland security deployed across government agencies to catch known malware, and the so-called C.D.M. program that was explicitly devised to alert agencies to suspicious activity.

Some intelligence officials are questioning whether the government was so focused on election interference that it created openings elsewhere.

Intelligence agencies concluded months ago that Russia had determined it could not infiltrate enough election systems to affect the outcome of elections, and instead shifted its attention to deflecting ransomware attacks that could disenfranchise voters, and influence operations aimed at sowing discord, stoking doubt about the system's integrity and changing voters' minds.

Image
The focus on election defense, while critical in 2020, may have diverted both resources and attention from other long-brewing problems.Credit...Lauren Justice for The New York Times
The SolarWinds hacking, which began as early as October 2019, and the intrusion into Microsoft's resellers, gave Russia a chance to attack the most vulnerable, least defended networks across multiple federal agencies.

General Nakasone declined to be interviewed. But a spokesman for the National Security Agency, Charles K. Stadtlander, said: "We don't consider this as an 'either/or' trade-off. The actions, insights and new frameworks constructed during election security efforts have broad positive impacts for the cybersecurity posture of the nation and the U.S. government."

In fact, the United States appears to have succeeded in persuading Russia that an attack aimed at changing votes would prompt a costly retaliation. But as the scale of the intrusion comes into focus, it is clear the American government failed to convince Russia there would be a comparable consequence to executing a broad hacking on federal government and corporate networks.

Getting the Hackers Out

Intelligence officials say it could be months, years even, before they have a full understanding of the hacking.

Since the extraction of a top Kremlin informant in 2017, the C.I.A.'s knowledge of Russian operations has been diminished. And the S.V.R. has remained one of the world's most capable intelligence services by avoiding electronic communications that could expose its secrets to the National Security Agency, intelligence officials say.

The best assessments of the S.V.R. have come from the Dutch. In 2014, hackers working for the Dutch General Intelligence and Security Service pierced the computers used by the group, watching them for at least a year, and at one point catching them on camera.

It was the Dutch who helped alert the White House and State Department to an S.V.R. hacking of their systems in 2014 and 2015, and last month, they caught and expelled from the Netherlands two S.V.R. operatives accused of infiltrating technology companies there. While the group is not known to be destructive, it is notoriously difficult to evict from computer systems it has infiltrated.

Image
President Vladimir V. Putin of Russia outside S.V.R. headquarters in Moscow in December.Credit...Alexey Nikolsky/Sputnik, via Agence France-Presse — Getty Images
When the S.V.R. broke into the unclassified systems at the State Department and White House, Richard Ledgett, then the deputy director of the National Security Agency, said the agency engaged in the digital equivalent of "hand-to-hand combat." At one point, the S.V.R. gained access to the NetWitness Investigator tool that investigators use to uproot Russian back doors, manipulating it in such a way that the hackers continued to evade detection.

Investigators said they would assume they had kicked out the S.V.R., only to discover the group had crawled in through another door.

Some security experts said that ridding so many sprawling federal agencies of the S.V.R. may be futile and that the only way forward may be to shut systems down and start anew. Others said doing so in the middle of a pandemic would be prohibitively expensive and time-consuming, and the new administration would have to work to identify and contain every compromised system before it could calibrate a response.

"The S.V.R. is deliberate, they are sophisticated, and they don't have the same legal restraints as we do here in the West," said Adam Darrah, a former government intelligence analyst who is now director of intelligence at Vigilante, a security firm.

Sanctions, indictments and other measures, he added, have failed to deter the S.V.R., which has shown it can adapt quickly.

"They are watching us very closely right now," Mr. Darrah said. "And they will pivot accordingly."