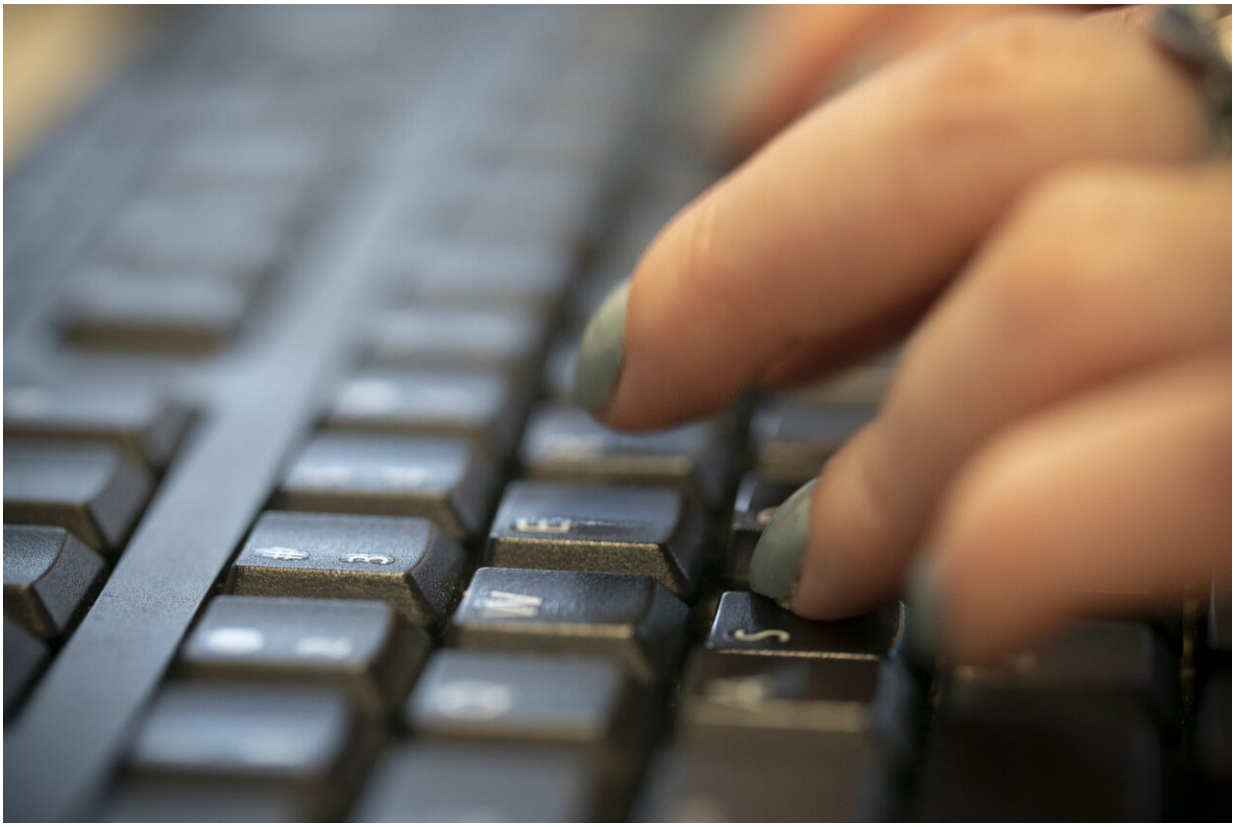
Hack may have exposed deep US secrets; damage yet unknown

December 16 2020, by Frank Bajak



In this Tuesday, Oct. 8, 2019, file photo, a woman types on a keyboard in New York. Following the disclosure of a global cyberespionage campaign that penetrated multiple U.S. government agencies and private organizations, governments and major corporations worldwide are scrambling to see if they, too, were victims. (AP Photo/Jenny Kane, File)

Some of America's most deeply held secrets may have been stolen in a disciplined, monthslong operation being blamed on elite Russian government hackers. The possibilities of what might have been purloined are mind-boggling.

Could hackers have obtained nuclear secrets? COVID-19 vaccine data? Blueprints for next-generation weapons systems?

It will take weeks, maybe years in some cases, for digital sleuths combing through U.S. government and private industry networks to get the answers. These hackers are consummate pros at covering their tracks, experts say. Some theft may never be detected.

What's seems clear is that this campaign—which cybersecurity experts says exhibits the tactics and techniques of Russia's SVR foreign intelligence agency—will rank among the most prolific in the annals of cyberespionage.

U.S. government agencies, including the Treasury and Commerce departments, were among dozens of high-value public- and private-sector targets known to have been infiltrated as far back as March through a commercial software update distributed to thousands of companies and government agencies worldwide. A Pentagon statement Monday indicated it used the software. It said it had "issued guidance and directives to protect" its networks. It would not say—for "operational security reasons"—whether any of its systems may have been hacked.

On Tuesday, acting Defense Secretary Chris Miller told CBS News there was so far no evidence of compromise.

In the months since the update went out, the hackers carefully exfiltrated data, often encrypting it so it wasn't clear what was being taken, and

expertly covering their tracks.

Thomas Rid, a Johns Hopkins cyberconflict expert, said the campaign's likely efficacy can be compared to Russia's three-year 1990s "Moonlight Maze" hacking of U.S. government targets, including NASA and the Pentagon. A U.S. investigation determined the height of the documents stolen—if printed out and piled up—would triple the height of the Washington Monument.

In this case "several Washington Monument piles of documents that they took from different government agencies is probably a realistic estimate," Rid said. "How would they use that? They themselves most likely don't know yet."

The Trump administration has not said which agencies were hacked. And so far no private-sector victims have come forward. Traditionally, defense contractors and telecommunications companies have been popular targets with state-backed cyber spies, Rid said.

Intelligence agents generally seek the latest on weapons technologies and missile defense systems—anything vital to national security. They also develop dossiers on rival government employees, potentially for recruitment as spies.

President Donald Trump's national security adviser, Robert O'Brien, cut short an overseas trip to hold meetings on the hack and was to convene a top-level interagency meeting later this week, the White House said in a statement.

O'Brien had been scheduled to return Saturday and had to scrap plans to visit officials in Italy, Germany, Switzerland and Britain, said an official familiar with his itinerary who was not authorized to discuss it and spoke on condition of anonymity.

The U.S. Treasury Department building viewed from the Washington Monument, Wednesday, Sept. 18, 2019, in Washington. Hackers got into computers at the U.S. Treasury Department and possibly other federal agencies, touching off a government response involving the National Security Council. Security Council spokesperson John Ullyot said Sunday, Dec. 13, 2020 that the government is aware of reports about the hacks. (AP Photo/Patrick Semansky, file)

Earlier, the White House said a coordinating team had been created to respond, including the FBI, the Department of Homeland Security and the Office of the Director of National Intelligence.

At a briefing for congressional staffers Monday, DHS did not say how

many agencies were hacked, a reflection of how little the Trump administration has been sharing with Congress on the case.

Critics have long complained that the Trump administration failed to address snowballing cybersecurity threats—including from ransomware attacks that have hobbled state and local governments, hospitals and even grammar schools.

"It's been a frustrating time, the last four years. I mean, nothing has happened seriously at all in cybersecurity," said Brandon Valeriano, a Marine Corps University scholar and adviser to the Cyber Solarium Commission, which was created by Congress to fortify the nation's cyber defenses. "It's tough to find anything that we moved forward on at all."

Trump eliminated two key government positions: White House cybersecurity coordinator and State Department cybersecurity policy chief.

Valeriano said one of the few bright spots was the work of Chris Krebs, the head of the Cybersecurity and Infrastructure Security Agency, whom Trump fired for defending the integrity of the election in the face of Trump's false claims of widespread fraud.

Hackers infiltrated government agencies by piggybacking malicious code on commercial network management software from SolarWinds, a Texas company, beginning in March.

The campaign was discovered by the cybersecurity company FireEye when it detected it had been hacked—it disclosed the breach Dec. 8—and alerted the FBI and other federal agencies. FireEye executive Charles Carmakal said it was aware of "dozens of incredibly high-value targets" infiltrated by the hackers and was helping "a number of organizations respond to their intrusions." He would not name any, and

said he expected many more to learn in coming days that they, too, were compromised.

Carmakal said the hackers would have activated remote-access back doors only on targets sure to have prized data. It is manual, demanding work, and moving networks around risks detection.

The SolarWinds campaign highlights the lack of mandatory minimum security rules for commercial software used on federal computer networks. Zoom videoconferencing software is another example. It was approved for use on federal computer networks last year, yet security experts discovered various vulnerabilities exploitable by hackers—after federal workers sent home by the pandemic began using it.

Rep. Jim Langevin, a Rhode Island Democrat and Cyberspace Solarium Commission member, said the breach reminded him of the 2015 Chinese hack of the U.S. Office of Personnel Management, in which the records of 22 million federal employees and government job applicants were stolen.

It highlights the need, he said, for a national cyber director at the White House, a position subject to Senate confirmation. Congress approved such a position in a recently passed defense bill.

"In all of the different departments and agencies, cybersecurity is never going to be their primary mission," Langevin said.

Trump has threatened to veto the bill over objections to unrelated provisions.