Hack against US is 'grave' threat, cybersecurity agency says

18 December 2020, by Ben Fox

This Tuesday, Aug. 4, 2009, file photo shows the United States Chamber of Commerce building in Washington. Elite cyber spies have spent months secretly exploiting SolarWinds software to peer into computer networks, putting many of the company's highest-profile customers in national governments, including the U.S. Treasury and Commerce departments, and Fortune 500 companies on high alert. (AP Photo/Manuel Balce Ceneta, File)

Federal authorities expressed increased alarm Thursday about a long-undetected intrusion into U.S. and other computer systems around the globe that officials suspect was carried out by Russian hackers. The nation's cybersecurity agency warned of a "grave" risk to government and private networks.

The hack compromised federal agencies and "critical infrastructure" in a sophisticated attack that was hard to detect and will be difficult to undo, the Cybersecurity and Infrastructure Security Agency said in an unusual warning message. The Department of Energy acknowledged it was among those that had been hacked.

The attack, if authorities can prove it was carried out by Russia as experts believe, creates a fresh foreign policy problem for President Donald Trump in his final days in office.

Trump, whose administration has been criticized for eliminating a White House cybersecurity adviser and downplaying Russian interference in the 2016 presidential election, has made no public statements about the breach.

President-elect Joe Biden, who inherits a thorny U.S.-Russia relationship, spoke forcefully about the hack, declaring that he and Vice President-elect Kamala Harris "will make dealing with this breach a top priority from the moment we take office."

"We need to disrupt and deter our adversaries from undertaking significant cyberattacks in the first place," he said. "We will do that by, among other things, imposing substantial costs on those responsible for such malicious attacks, including in coordination with our allies and partners."

"There's a lot we don't yet know, but what we do know is a matter of great concern," Biden said.

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)

CISA officials did not respond to questions and so it was unclear what the agency meant by a "grave threat" or by "critical infrastructure" possibly targeted in the attack that the agency says appeared to have begun last March. Homeland Security, the agency's parent department, defines such infrastructure as any "vital" assets to the U.S. or its economy, a broad category that could include power plants and financial institutions.

The agency previously said the perpetrators had used network management software from Texas-based SolarWinds t o infiltrate computer networks. Its new alert said the attackers may have used other methods, as well.

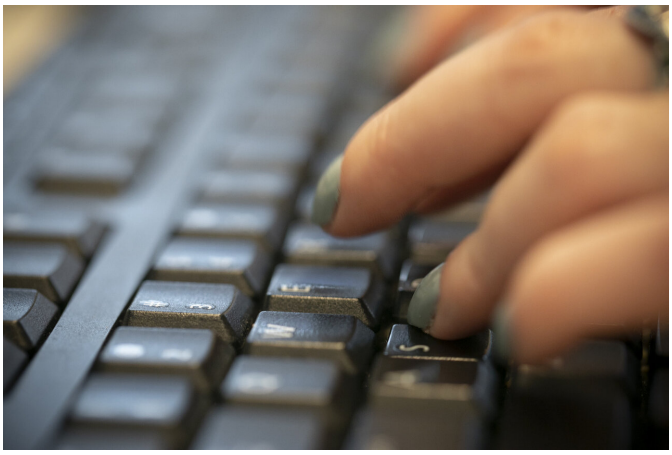
Tech giant Microsoft, which has helped respond to the breach, the hack was severe and extremely damaging although the administration was not yet ready to publicly blame anyone for it.

"This is looking like it's the worst hacking case in the history of America," the official said. "They got into everything."

At the Department of Energy, the initial investigation revealed that malware injected into its networks via a SolarWinds update has been found only on its business networks and has not affected national security operations, including the agency that manages the nation's nuclear weapons stockpile, according to its statement. It said vulnerable software was disconnected from the DOE network to reduce any risk.

The intentions of the perpetrators appear to be espionage and gathering information rather than destruction, according to security experts and former government officials. If so, they are now remarkably well situated.

Thomas Bossert, a former Trump Homeland Security adviser, said in an opinion article in The New York Times that the U.S. should now act as if the Russian government had gained control of the networks it has penetrated. "The actual and perceived control of so many important networks could easily be used to undermine public and consumer trust in data, written communications and services," he wrote.



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)

Members of Congress said they feared that taxpayers' personal information could have been exposed because the IRS is part of Treasury, which used SolarWinds software. Experts involved in the hack response say the intruders are not likely interested in such data because they are intelligence agents narrowly focused on sensitive national security data—and trying to steal taxpayer info would likely set off alarms.

Tom Kellermann, cybersecurity strategy chief of the software company VMware, said the hackers are now "omniscient to the operations" of federal agencies they've infiltrated "and there is viable concern that they might leverage destructive attacks within these agencies" now that they've been discovered.

Among the business sectors scrambling to protect

their systems and assess potential theft of information are defense contractors, technology companies and providers of telecommunications and the electric grid.

A group led by CEOs in the electric power industry said it held a "situational awareness call" earlier this week to help electric companies and public power utilities identify whether the compromise posed a threat to their networks.

And dozens of smaller institutions that seemed to have little data of interest to foreign spies were nonetheless forced to respond to the hack.

The Helix Water District, which provides drinking water to the suburbs of San Diego, California, said it provided a patch to its SolarWinds software after it got an advisory the IT company sent out about the hack to about 33,000 customers Sunday.

"While we do utilize SolarWinds, we are not aware of any district impacts from the security breach," said Michelle Curtis, a spokesperson for the water district.