SolarWinds hack got emails of top DHS officials

29 March 2021, by Alan Suderman

In this July 21, 2020 file photo, Department of Homeland Security Acting Secretary Chad Wolf, speaks during a news conference in Washington. In December, U.S. officials discovered that federal agencies had fallen victim to a cyberespionage effort pulled off largely through a hack of SolarWinds software .The hackers accessed accounts belonging to then-acting Secretary Chad Wolf and staff at the Cybersecurity and Infrastructure Security Agency who focus on finding cyber threats from nation-state adversaries like Russia, according to current and former senior Homeland Security Department and intelligence officials who were briefed on the extent of the breach. (AP Photo/Manuel Balce Ceneta, File)

Suspected Russian hackers gained access to email accounts belonging to the Trump administration's head of the Department of Homeland Security and members of the department's cybersecurity staff whose jobs included hunting threats from foreign countries, The Associated Press has learned.

The intelligence value of the hacking of then-acting Secretary Chad Wolf and his staff is not publicly known, but the symbolism is stark. Their accounts were accessed as part of what's known as the SolarWinds intrusion, and it throws into question how the U.S. government can protect individuals, companies and institutions across the country if it can't protect itself.

The short answer for many security experts and federal officials is that it can't—at least not without some significant changes.

"The SolarWinds hack was a victory for our foreign adversaries, and a failure for DHS," said Sen. Rob Portman of Ohio, top Republican on the Senate's Homeland Security and Governmental Affairs Committee. "We are talking about DHS's crown jewels."

The Biden administration has tried to keep a tight lid on the scope of the SolarWinds attack as it weighs retaliatory measures against Russia. But an inquiry by the AP found new details about the breach at DHS and other agencies, including the Energy Department, where hackers accessed top officials' schedules.

The AP interviewed more than a dozen current and former U.S. government officials, who spoke on the condition of anonymity because of the confidential nature of the ongoing investigation into the hack.

The vulnerabilities at Homeland Security, in particular, intensify the worries following the SolarWinds attack and an even more widespread hack affecting Microsoft Exchange's email program, especially because in both cases the hackers were detected not by the government but by a private company.

In December, officials discovered what they describe as a sprawling, monthslong cyberespionage effort done largely through a hack of a widely used software from Texas-based SolarWinds Inc. At least nine federal agencies were hacked, along with dozens of private-sector companies.

U.S. authorities have said the breach appeared to be the work of Russian hackers. Gen. Paul Nakasone, who leads the Pentagon's cyber force, said last week that the Biden administration is considering a "range of options" in response. Russia has denied any role in the hack.

Since then, a series of headline-grabbing hacks has further highlighted vulnerabilities in the U.S. public and private sectors. A hacker tried unsuccessfully to poison the water supply of a small town in Florida in February, and this month a new breach was announced involving untold thousands of Microsoft Exchange email servers that the company says was carried out by Chinese state hackers. China has denied involvement in the Microsoft breach.

Sen. Mark Warner, a Virginia Democrat and head of the Senate Intelligence Committee, said the government's initial response to the discovery of the SolarWinds hack was disjointed.

"What struck me was how much we were in the dark for as long as we were in the dark," Warner said at a recent cybersecurity conference.

Wolf and other top Homeland Security officials used new phones that had been wiped clean along with the popular encrypted messaging system Signal to communicate in the days after the hack, current and former officials said.

One former administration official, who confirmed the Federal Aviation Administration was among the agencies affected by the breach, said the agency was hampered in its response by outdated technology and struggled for weeks to identify how many servers it had running SolarWinds software.

The FAA initially told the AP in mid-February that it had not been affected by the SolarWinds hack, only to issue a second statement a few days later that it was continuing to investigate.

At least one other Cabinet member besides Wolf was affected. The hackers were able to obtain the schedules of officials at the Energy Department, including then-Secretary Dan Brouillette, one former high-placed administration official said. The schedules were not confidential and are subject to open records laws.

Energy Department spokesman Kevin Liao said it "has found no evidence the network that maintains senior officials' schedules was compromised."

In this Aug. 18, 2020, file photo acting-Secretary of Homeland Security Chad Wolf, center, arrives to join President Donald Trump at Andrews Air Force Base in Md. In December, U.S. officials discovered that federal agencies had fallen victim to a cyberespionage effort pulled off largely through a hack of SolarWinds software .The hackers accessed accounts belonging to then-acting Secretary Chad Wolf and staff at the Cybersecurity and Infrastructure Security Agency who focus on finding cyber threats from nation-state adversaries like Russia, according to current and former senior Homeland Security Department and intelligence officials who were briefed on the extent of the breach. (AP Photo/J. Scott Applewhite, File)

The new disclosures provide a fuller picture of what kind of data was taken in the SolarWinds hack. Several congressional hearings have been held on the subject, but they have been notably short on details.

Rep. Pat Fallon, R-Texas, indicated at one of the hearings that a DHS secretary's email had been hacked but did not provide additional detail. The AP was able to identify Wolf, who declined to comment other than to say he had multiple email accounts as secretary.

DHS spokesperson Sarah Peck said that "a small number of employees' accounts were targeted in the breach" and that the agency "no longer sees indicators of compromise on our networks."

The Biden administration has pledged to issue an executive order soon to address "significant gaps in modernization and in technology of cybersecurity across the federal government." But the list of obstacles facing the federal government is long: highly capable foreign hackers backed by governments that aren't afraid of U.S. reprisals, outdated technology, a shortage of trained cybersecurity professionals and a complex leadership and oversight structure.

The recently approved stimulus package includes $650 million in new money for the Cybersecurity and Infrastructure Security Agency to harden the country's cyber defenses. Federal officials said that amount is only a down payment on much bigger planned spending to improve threat detection.

"We must raise our game," Brandon Wales, who leads the cybersecurity agency, said at a recent House committee hearing.

The agency operates a threat-detection system known as Einstein. Its failure to detect the SolarWinds breach before it was discovered by a private security company alarmed officials. Eric Goldstein, the agency's executive assistant director for cybersecurity, told Congress that Einstein's technology was designed a decade ago and has "grown somewhat stale."

Anthony Ferrante, a former director for cyber incident response at the U.S. National Security Council and current senior managing director at FTI Consulting, said part of the problem, both in government and in the private sector, is the lack of a skilled workforce.

The Microsoft Exchange hack, which to date has not affected any federal government agencies, was also discovered by a private firm.

One issue that's flummoxed policymakers is that foreign state hackers are increasingly using U.S.-based virtual private networks, or VPNs, to evade detection by U.S. intelligence agencies, which are legally constrained from monitoring domestic infrastructure. The hosting services of Amazon Web Services and GoDaddy were used by the SolarWinds hackers to evade detection, officials said recently.

The Biden administration is not planning to step up government surveillance of the U.S. internet in response and instead wants to focus on tighter partnerships and improved information-sharing with the private-sector companies that already have broad visibility into the domestic internet.

Responsibility for responding to breaches, preventing new ones and providing oversight of those efforts is still unsettled, and last month leaders of the Senate Intelligence Committee initially criticized the Biden administration for a "disorganized response" to the SolarWinds hack before the White House issued a statement clarifying its leadership structure.

The Biden administration tapped Anne Neuberger, the deputy national security adviser for cyber and emergency technology, to respond to the SolarWinds and Microsoft breaches. It hasn't appointed a national cyber director, a new position, frustrating some members of Congress.

"We're trying to fight a multifront war without anybody in charge," said Sen. Angus King, an independent from Maine.

The Biden administration says it's reviewing how best to set up the new position. "Cybersecurity is a top priority," said White House spokesperson Emily Horne.

© 2021 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

APA citation: SolarWinds hack got emails of top DHS officials (2021, March 29) retrieved 30 November 2021 from https://techxplore.com/news/2021-03-solarwinds-hack-emails-dhs.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.