US still unraveling 'sophisticated' hack of 9 gov't agencies

17 February 2021, by Ben Fox

White House deputy national security adviser Anne Neuberger speaks during a press briefing, Wednesday, Feb. 17, 2021, in Washington. (AP Photo/Evan Vucci)

U.S. authorities are still working to unravel the full scope of the likely Russian hack that gave the "sophisticated" actor behind the breach complete access to files and email from at least nine government agencies and about 100 private companies, the top White House cybersecurity official said Wednesday.

Anne Neuberger, the newly appointed deputy national security adviser for cyber and emerging technology, also warned that the danger has not passed because the hackers breached networks of technology companies whose products could be used to launch additional intrusions.

A task force is investigating the extent of the damage from the breach, assessing potential responses and trying to confirm the identity of whoever was behind it—a process Neuberger warned will take more time.

"This is a sophisticated actor who did their best to hide their tracks," she told reporters at the White House. "We believe it took them months to plan and execute this compromise. It will take us some time to uncover this layer by layer."

U.S. authorities have said the breach, disclosed in December, appeared to be the work of Russian hackers. Neuberger, a former senior official at the National Security Agency who was appointed by President Joe Biden this month, went no further.

"An advanced, persistent threat actor likely of Russian origin was responsible," she said, without providing any further details and sounding a cryptic note on potential responses.

White House deputy national security adviser Anne Neuberger speaks during a press briefing, Wednesday, Feb. 17, 2021, in Washington. (AP Photo/Evan Vucci)

"This isn't the only case of malicious cyber activity of likely Russian origin, either for us or for our allies and partners," Neuberger added. "So, as we contemplate future response options, we are considering holistically what those activities were."

The Russian government has denied involvement.

Private security company FireEye was first to identify the breach, revealing that hackers hijacked widely used network software from SolarWinds Inc. to install malicious software through a what appeared to be a routine security update.

Intelligence agencies did not detect the breach because they largely have "no visibility into private-sector networks," and it was launched within the U.S., Neuberger said. The Biden administration supports changes to "culture and authorities" that prevented the hack from being detected on the federal civilian systems, she added.

The hack, Neuberger said, highlights the need to modernize the nation's IT infrastructure and its cyber defenses, issues that will be addressed in an upcoming executive order from Biden aimed at addressing security and technology gaps highlighted by the breach.

White House deputy national security adviser Anne Neuberger speaks during a press briefing, Wednesday, Feb. 17, 2021, in Washington. (AP Photo/Evan Vucci)

Several agencies have acknowledged that they were breached, including the Treasury Department and Justice Department, but the full list has not been publicly released. Once inside, the hackers had full access to the victims' data.

"The techniques that were used lead us to believe that any files or emails on a compromised network were likely to be compromised," Neuberger said.

Some members of Congress have criticized the response based on what they have been told so far, all in private. "The briefings we have received convey a disjointed and disorganized response to confronting the breach," Sen. Mark Warner, a Democrat from Virginia, and Sen. Marco Rubio, Republican from Florida, said in a recent letter to the White House.

Neuberger said she intended to return to the Capitol to brief lawmakers in the coming days.