0-The Washington Post-Chinese hack US

Local

Chinese hack U.S. weather systems, satellite network

An National Oceanic and Atmospheric Administration satellite image taken Nov. 11 shows a strong area of low pressure over the northern Great Lakes. The NOAA confirmed recently that hackers breached its weather system. (AP)

Email Bio Follow

November 12, 2014

Hackers from China breached the federal weather network recently, forcing cybersecurity teams to seal off data vital to disaster planning, aviation, shipping and scores of other crucial uses, officials said.

The intrusion occurred in late September but officials gave no indication that they had a problem until Oct. 20, said three people familiar with the hack and the subsequent reaction by the National Oceanic and Atmospheric Administration, which includes the National Weather Service. Even then, NOAA did not say its systems were compromised.

[Deny]

Officials also said that the agency did not notify the proper authorities when it learned of the attack.

[Deny, Disappointment]

NOAA officials declined to discuss the suspected source of the attack, whether it affected classified data and the delay in notification *[Deny]*.

NOAA said publicly last month that it was doing “unscheduled maintenance” on its network, without saying a computer hack had made that necessary *[Diminish]*.

In a statement released Wednesday, NOAA spokesman Scott Smullen acknowledged the hacks and said “incident response began immediately *[Reinforce]*.” He said all systems were working again and that forecasts were accurately delivered to the public. *[Reinforce]* Smullen declined to answer questions beyond his statement, citing an investigation into the attack. *[Reinforce]*

NOAA’s satellites provide the bulk of the information for generating weather models, advisories and warnings to the nation and world. Maintaining the operations and data acquisition from these satellites is a 24/7 process. This video was filmed at the NOAA Satellite Operations Facility in Suitland, Md., where command, control and data distribution systems are located. (NOAA/YouTube)

Determining the origin of cyberattacks is difficult, experts said, and Chinese officials have denied repeated accusations that they intrude in U.S. government computer systems for espionage or other purposes.

Geng Shuang of the Chinese Embassy said the consulate was not aware of the case and had not been contacted by the U.S. government about the attacks.

“Cyberattack is quite common in today’s cyberspace,” he said. “Jumping to conclusions on its origin without hard evidence is not responsible at all.” The embassy also urged “relevant U.S. parties to stop this kind of unfounded accusation.”

But NOAA confirmed to Rep. Frank R. Wolf (R-Va.) that China was behind the attack, the congressman said *[Reinforce]*. Wolf has a long-standing interest in cybersecurity and asked NOAA about the incident after an inquiry from The Washington Post.

“NOAA told me it was a hack and it was China *[Diminish]*,” said Wolf, who also scolded the agency for not disclosing the attack *[Anger]* “and

deliberately misleading the American public in its replies *[Deny, Anger]*."

"They had an obligation to tell the truth," Wolf said. "They covered it up."

[Deny, Anger]

Commerce Department Inspector General Todd Zinser said his office was not notified of the breach until Nov. 4, well after he believes the hack occurred. *[Disappointment]* He said that is a violation of agency policy requiring any security incident to be reported to his office within two days of discovering the problem.

[Deny]

"We're in the process of looking into the matter, including why NOAA did not comply with the requirements to notify law enforcement about the incident *[Deny]*," Zinser said.

Wolf said he did not know if the breach involved classified material or what information was accessed.

Confirmation of the NOAA hack followed an admission Monday by the U.S. Postal Service that a suspected Chinese attack — also in September — compromised data on 800,000 employees, including letter carriers on up through the postmaster general.

NOAA officials also would not say whether the attack removed material or inserted malicious software in its system, which is used by civilian and military forecasters in the United States and also feeds weather models at the main centers for Europe and Canada.

NOAA's National Ice Center Web site also was down for a week in late October. The center is a partnership with the Navy and Coast Guard to monitor conditions for navigation.

The two-day outage skewed the accuracy of National Weather Service long-range forecasts slightly, according to NOAA.

The attack in September hit a Web server that connects to many NOAA computers, said one person familiar with the incursion. The server had security protections, but the person compared the security to leaving a house protected by “just a screen door.”

Smullen’s statement said that four sites were hit by the breach.

Weather satellites orbit hundreds to thousands of miles above Earth and offer continuous views of weather systems, such as hurricanes, thunderstorms and cold fronts, while also measuring temperature and moisture at different altitudes — all crucial bits that feed prediction models. To get that information to the public, NOAA makes satellite data and imagery publicly available through the Web, as well as file-transfer networks for downloads.

NOAA has characterized its decision to cut off satellite images as causing minimal disruption. But it has previously touted those same systems as intrinsic to the nation’s “environmental intelligence.”

[Diminish]

NOAA satellites “provide critical data for forecasts and warnings that are vital to every citizen and to our economy as a whole,” NOAA Administrator Kathryn D. Sullivan said a year ago.

Wolf said a hack could steal technical insights or cull isolated information “that may not look significant until they’re put with something else and then they become valuable.”

“The Chinese are stealing us blind,” Wolf said.

[Worry]

The attack on NOAA joins a spate of cyber-espionage on federal systems revealed recently, including an attack suspected from Russia that breached unclassified White House computer networks .

The October satellite data outage meant that the National Weather Service and centers around the world did not receive large amounts of information.

“All the operational data sent via NOAA, which is normally an excellent service, was lost,” said Stephen English, head of the satellite section at the European Centre for Medium-Range Weather Forecasts in Reading, England. The center is renowned for running a highly advanced global weather prediction model that during Hurricane Sandy in 2012, for example, aided evacuations and preparations in the United States when it signaled that the superstorm would hit land rather than hook out to sea.

The Rutgers University Global Snow Lab, which provides daily snow cover updates for researchers and forecasters using a data feed from the Ice Center, posted a notice on its Web site that its reports were incomplete throughout the outage.

A July report on NOAA by the Inspector General for the Commerce Department — where NOAA sits — criticized an array of “high-risk vulnerabilities” in the security of NOAA’s satellite information and weather service systems.

[Disappointment, Legal Action]

The report echoed the views of a 2009 audit from the IG that said the primary system that processes satellite data from two environmental and meteorological systems had “significant” security weaknesses, and that “a security breach could have severe or catastrophic adverse effects.”

[Disappointment]

The watchdog’s previously unreleased report, obtained by The Post under a Freedom of Information Act request, called for “immediate management attention” and said NOAA’s security planning was so poor that the agency had little idea how vulnerable its system was.

[Disappointment]

We are a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a means for us to earn fees by linking to Amazon.com and affiliated sites.

Mary Pat Flaherty Mary Pat Flaherty works on investigative and long-range stories. Her work has won numerous national awards, including the Pulitzer Prize. Follow

Jason Samenow Jason Samenow is The Washington Post's weather editor and Capital Weather Gang's chief meteorologist. He earned a master's degree in atmospheric science and spent 10 years as a climate change science analyst for the U.S. government. He holds the Digital Seal of Approval from the National Weather Association. Follow

Lisa Rein Lisa Rein covers federal agencies and the management of government in the Biden administration. At The Washington Post, she has written about the federal workforce; state politics and government in Annapolis, and in Richmond; local government in Fairfax County, Va.; and the redevelopment of Washington and its neighborhoods. Follow