MIDDLE EAST NEWS

Iranian Hacking to Test NSA Nominee Michael Rogers

Infiltration of Navy Computer Network More Extensive Than Previously Thought

By SIOBHAN GORMAN and JULIAN E. BARNES CONNECT

Updated Feb. 18, 2014 11:16 a.m. ET

Vice Adm. Michael Rogers in 2012 *Agence France-Presse/Getty Images*

WASHINGTON—Iran's infiltration of a Navy computer network was far more extensive than previously thought, according to officials, and the officer who led the response will likely face questions about it from senators weighing his nomination as the next head of the embattled National Security Agency.

It took the Navy about four months to finally purge the hackers from its biggest unclassified computer network, according to current and former officials.

Some lawmakers are concerned about how long it took. When Vice Adm. Michael Rogers, President Barack Obama's choice for the new NSA director, faces his confirmation hearing, some senators are expected to ask whether there is a long-term plan to address security gaps exposed by the attack, congressional aides said. The hearing hasn't been scheduled yet, but could be next month.

The Wall Street Journal in September first reported the discovery of the Iranian cyberattack. Officials at the time said the intruders had been removed. However, officials now acknowledge that the attack was more invasive, getting into what one called the "bloodstream" of the Navy and Marine Corps system and managing to stay there until November.

The hackers targeted the Navy Marine Corps Intranet, the unclassified network used by the Department of the Navy to host websites, store nonsensitive information and handle voice, video and data communications. The network has 800,000 users at

An Iranian infiltration of the Navy's biggest unclassified computer network was more extensive and pervasive than previously understood, requiring months of work to finally purge the hackers. Julian Barnes reports on the News Hub. Photo: Getty.

Related

Iran Talks Resume Amid Deep Caution

Popular Now What's This?

ARTICLES

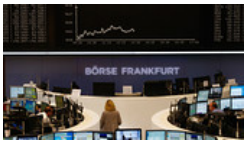
1 Netflix to Pay Comcast to End Traffic Jam

2 Opinion: Niall Ferguson: America's Global Retreat

3 Russia Stung By Ally's Defeat in Ukraine

4 Dave Barry's Manliness Manifesto

5 Stock Investors Like the View in Europe



VIDEO

1 Busted Drug Lord Guzmán on the Perp Walk

2 Ukraine Protesters Topple Lenin Statues

3 The State of Love and Sex in Single America

4 A Look at the Next Winter Games: PyeongChang 2018

5 Afghanistan Experts Stumped By Simple Questions

2,500 locations, according to the Navy.

Officials said there was no evidence the Iranians have been able to break into a network beyond the Navy Marine Corps Intranet and no classified networks were penetrated.

Network repairs continue to close the many security gaps revealed by the intrusion, not just on Navy computers but across the Department of Defense, the officials said.

"It was a real big deal," said the senior U.S. official. "It was a significant penetration that showed a weakness in the system."

Adm. Rogers declined to comment, citing a standard practice of not speaking publicly before a confirmation hearing.

Iranian officials didn't respond to requests to comment, but in the past have said they were victims of cyberattacks by Western powers, including the Stuxnet virus uncovered in 2010.

Details remain classified and murky, but the penetration allowed the Iranians to conduct surveillance on the Navy's and Marine Corps' unclassified networks, said the senior U.S. official. While that official said the intruders were able to compromise communications on the network, a senior defense official said no email accounts were hacked and no data was stolen.

"We were able to eliminate the bad guys from our networks," the senior defense official said.

The military response, an effort known as Operation Rolling Tide, was overseen by Adm. Rogers as the Navy's chief of cybersecurity. But Adm. Rogers, who has also been nominated as chief of the military's Cyber Command, will likely defer most answers at his confirmation hearing to a classified hearing.

While lawmakers have raised questions, senior officials defended Adm. Rogers, saying the Navy response demonstrated leadership and helped buttress the military's overall cyberdefenses.

"It was a big problem, but it was a success," said the senior defense official. "Mike Rogers did a very, very good job handling this."

The issue isn't expected to derail Adm. Rogers' nomination, but it coincides with scrutiny of the NSA over complaints world-wide about the way it conducts electronic surveillance.

The intrusion into the Navy's system was the most recent in a series of Iranian cyberoffensives that have taken U.S. military and intelligence officials by surprise.

In early 2012, top intelligence officials held the view that Iran wanted to execute a cyberattack but had little capability. Not long after, Iranian hackers began a series of major "denial-of-service" attacks on a growing number of U.S. bank websites, and they launched a virus on a Saudi oil company that immobilized 30,000 computers.

The senior defense official said the cost to repair the Navy network after the attack was approximately $10 million. But other officials said the ultimate price tag is likely to be higher. The attack and other cyberthreats prompted a broader review of Navy and DoD network security and upgrades to military cyberdefenses were needed. The added defenses are expected to cost several hundred million dollars, officials said.

Current and former officials differ on whether the time it took to push the Iranians out of the system and clean up the intrusion—approximately four months—was excessive. In part, the response took a long time because hackers were able to infiltrate deep into the system.

"The thing got into the bloodstream, and it wasn't just in the main arteries, it was in all the little capillaries," the senior U.S. official said.

The senior defense official said within three weeks of the intrusion, officials understood the full scope of the attack and put in place a plan to try and push the intruders out. As part of the response, the unclassified network was taken down twice for upgrades and to clean out the intruders, the senior defense official said.

As part of the response, a former official said the Navy ordered a surge of so-called

cyberwarriors and contractors to work on the response to the attack. They are working with a list of roughly 60 actions to be taken to fix the network, the former U.S. official said.

One official said part of the reason the response has taken so long is that Adm. Rogers has sought to employ a comprehensive strategy that fixes broader network security problems rather than solely cleaning up after the incident. Cybersecurity experts said the roughly four-month-long penetration created security risks.

"That's a long time," said James Lewis, a cybersecurity specialist at the Center for Strategic and International Studies. "Generally, not being able to get people off your network is a significant risk for any military operation."

Defense officials were surprised at the skills of the Iranian hackers. Previously, their tactics had been far cruder, usually involving so-called denial of service attacks that disrupt network operations but usually don't involve a penetration of network security. They then established what is known as a beacon, which communicated back to the hackers and allowed them to execute their surveillance remotely.

The intruders were able to enter the network through a security gap in one of the Navy's many public-facing websites, and investigators have discovered that poor internal network security allowed them to migrate deep inside that network, according to current and former officials.

Officials said the vulnerabilities that allowed the Iranians to get into the network were closed by early October, but it took several more weeks to eliminate hidden spyware lurking throughout the system.

By early November, the senior U.S. official said, the Navy was finally confident it had rid its networks of the hackers and had ensured they could no longer remotely access Navy systems. Officials said the Iranians probably obtained account credentials used to log into the network.

"It was a real eye-opener in terms of the capabilities of Iran to get into a Defense Department system and stay in there for months," said a former U.S. official. "That's worrisome."

Corrections & Amplifications
The hackers targeted the Navy Marine Corps Intranet. An earlier version of this article incorrectly said it was the Navy Marine Corps Internet.

Write to Siobhan Gorman at siobhan.gorman@wsj.com and Julian E. Barnes at julian.barnes@wsj.com

Customer Service

Customer Center
Contact Us
WSJ Weekend
Contact Directory
Corrections

Policy

Privacy Policy
Cookie Policy
Data Policy
Copyright Policy
Updated : Subscriber Agreement & Terms of Use
Your Ad Choices

Ads

Advertise
Place a Classified Ad
Sell Your Home
Sell Your Business
Commercial Real Estate Ads
Recruitment & Career Ads
Franchising
Advertise Locally

Tools & Features

Apps
Emails & Alerts
Graphics & Photos
Columns
Topics
Guides
Portfolio
Old Portfolio

More

Register for Free
Reprints
Content Partnerships
Conferences
SafeHouse
Mobile Site
News Archive

Jobs at WSJ