1-The Washington Post-U.S. suspects Russia in hack

U.S. suspects Russia in hack of Pentagon computer network

Joint Chiefs Chairman Gen. Martin Dempsey. (Susan Walsh/AP)

Email Bio Follow

August 6, 2015

U.S. military officials said Thursday that they suspect Russian hackers infiltrated an unclassified Pentagon e-mail system used by employees of the Joint Chiefs of Staff, the latest in a series of state-sponsored attacks on sensitive U.S. government computer networks.

The electronic intrusion was detected about July 25, officials said. The Pentagon immediately disabled the e-mail system, which is used by about 4,000 military and civilian personnel, in an attempt to contain the damage. *[Rebuild]* The network remains offline, although officials said they hoped to restart it in the coming days.

The Defense Department disclosed the attack shortly after it occurred, but only in recent days have investigators traced it to Russia. Officials said the complexity and advanced nature of the hack strongly suggested that a foreign government was responsible.

“This attack was fairly sophisticated and has the indications . . . of having come from a state actor such as Russia,” said a U.S. official who spoke on the condition of anonymity to discuss details of the investigation.

The cyberattack on the Joint Staff, which coordinates operations among the branches of the armed forces, is similar to one last fall that successfully penetrated unclassified e-mail systems at the White House and the State

Department. In that case , U.S. officials said the trail also led to hackers thought to be working for the Russian government.

Even so, officials cautioned that it is difficult to pinpoint the origin or perpetrator of such hacks. “Attribution in this business is near impossible. Rarely are you ever able to say with 100 percent certainty” who was behind a particular incident, the official said.

The incident follows several other, more destructive cyberattacks on U.S. government networks, including devastating breaches of databases maintained by the Office of Personnel Management. U.S. officials believe hackers working for the Chinese government were responsible for those, which exposed sensitive information about more than 22 million people .

Responding to the spate of attacks, officials in Washington have said they were working to bolster the security of computer systems across the federal government. The disclosure of a successful breach of a Pentagon e-mail network, however, is likely to generate new scrutiny from Congress on the reliability of Washington’s cyberdefenses.

U.S. officials said the hackers penetrated the Joint Staff network with an old-fashioned technique known as “spear-phishing,” which relies on unsuspecting e-mail users clicking on links infected with malware.

Russia’s intelligence agencies are also suspected of masterminding a successful attack on U.S. military classified networks that was discovered in 2008 and took months to contain.

The Obama administration has been reluctant to formally blame the Russian or Chinese governments for the recent cyberattacks or offer hard evidence of their involvement, reasoning that to do so could inadvertently reveal details about U.S. cyberdefenses.

Moreover, the U.S. government operates its own cyberespionage campaigns against other countries, so publicly pointing the finger at other countries could be seen as hypocritical.

In the recent attack on the Pentagon, officials said that only unclassified e-mails were exposed and that the damage did not appear to be significant. They said the Joint Staff's classified networks were unaffected and are operating normally. *[Diminish]*

"We continue to identify and mitigate cybersecurity risks across our network, and we continue to investigate this incident, and our top priority is to restore services when we can," said Navy Capt. Jeff Davis, a Pentagon spokesman. *[Rebuild]*

There was no immediate reaction from Moscow. In the past, Russian officials have responded to such reports with sarcastic denials.

In April, Kremlin spokesman Dmitry Peskov dismissed reports that the Russian government was to blame for last year's attack on the White House e-mail network. "It has become a kind of sport to blame everything on Russia," he said at the time.

Washington's allies in NATO have reported similar attacks, however, and have traced some intrusions back to shadowy groups with suspected ties to Russian intelligence services.

In May, for instance, a computer network for Germany's lower house of Parliament was penetrated in a major hack. German news outlets reported that investigators thought that a Russian cyber-gang known as APT28, or Advanced Persistent Threat 28, was responsible.

FireEye, a U.S. cybersecurity firm, has scrutinized APT28 and suggested it has targeted government computers in Poland, Hungary, Ukraine and Georgia.

Julia Smirnova contributed to this report.

Craig Whitlock Craig Whitlock is an investigative reporter who specializes in national security issues. He has covered the Pentagon, served as the Berlin bureau chief and reported from more than 60 countries. He joined The Washington Post in 1998. Follow

Missy Ryan Missy Ryan writes about diplomacy, national security and the State Department for The Washington Post. She joined The Post in 2014 to write about the Pentagon and military issues. She has reported from Iraq, Egypt, Libya, Lebanon, Yemen, Afghanistan, Pakistan, Mexico, Peru, Argentina and Chile. Follow