The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia Prime Suspect in Cyber Attack Against U.S. Military — U.S. Officials

By The Moscow Times

August 07, 2015

WASHINGTON — Russia is the leading suspect in a sophisticated cyber attack on the unclassified email network of the U.S. military's Joint Staff that prompted the Pentagon last month to restrict access to portions of that network, U.S. officials said on Thursday.

Early reports firmly linked Russia to the attack, said one U.S. official, who declined to be named since the investigation is still underway.

"It was a spearphishing attack traced to that country," said the official, when asked about Russia's possible involvement. Spearphishing emails purport to be from colleagues.

A second official, who also spoke on condition of anonymity, described Russia as a leading suspect but cautioned that it would take time for investigators to firmly attribute blame.

The Pentagon declined comment on the investigation.

In late April, U.S. Defense Secretary Ash Carter blamed Russian hackers for a cyber intrusion

on an unclassified U.S. military network this year, saying they discovered an old vulnerability that had not been patched.

In that case, Carter said the Pentagon quickly identified the compromise and had incident responders "hunting the intruders within 24 hours."

In this latest case, the U.S. military's Joint Staff, which employs about 2,500 civilian and uniformed personnel, have seen their unclassified email access severely restricted since the last weekend of July. The rest of the Pentagon appeared to be unaffected.

Officials told Reuters the attack bore the hallmarks of the actions of a foreign state, as opposed to a less sophisticated hacker.

Dmitri Alperovitch, chief technology officer and co-founder of CrowdStrike, a cybersecurity firm, said his company had seen a "massive escalation" in cyber attacks tied to the Russian government since sanctions were imposed last year over Moscow's actions in Ukraine.

He said he had no information on the alleged attack on the Joint Chiefs of Staff network, but his firm had detected a large number of attacks against U.S. national security agencies and commercial companies by a hacker group called "Cozy Bear" that had clear ties to the Russian government.

Cozy Bear engaged in a variety of cyber attacks ranging from spearphishing to more sophisticated and complex attacks. The latest set of attacks used hundreds of emails with a zipfile attachment that, if double-clicked, could introduce the malware to an organization's networks, Alperovitch said.

"Once they get a beachhead, their tradecraft is very, very good," he said.

Original url:
https://www.themoscowtimes.com/2015/08/07/russia-prime-suspect-in-cyber-attack-against-us-military-us-officials-a48820