PIXEL_DREAMS - FOTOLIA

White House considers proportional response to Russian hackers

by
Michael Heller
Senior Reporter

Published: 12 Oct 2016

U.S. intelligence agencies officially attributed potential election-tampering activity to government-led Russian hackers, and the White House said it is considering a proportional response.

THIS ARTICLE COVERS
Government IT security

+ Show More

The Russian government has long been suspected of various cyberattacks targeting political organizations. And, now, U.S. intelligence agencies officially blamed Russian hackers for potential election-tampering activity.

In a joint statement, the U.S. Department of Homeland Security (DHS) and the Office of the Director of National Intelligence on Election Security attributed government-led Russian hackers with stealing and publishing emails from political organizations, such as the

Democratic National Committee, and said "only Russia's senior-most officials could have authorized these activities."

"The U.S. Intelligence Community (USIC) is confident that the Russian government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations," the statement read. "The recent disclosures of alleged hacked emails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the U.S. election process. Such activity is not new to Moscow -- the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there."

DHS refused to comment on whether this last sentence indicated international cooperation in the attribution investigation.

While the statement officially blamed government-led Russian hackers for these email hacks, the USIC would not officially attribute recent attacks on voter-database systems to the Russian government, but said the attacks "originated from servers operated by a Russian company." Despite these attacks, USIC and DHS again asserted that election systems are secure.

"The USIC and the Department of Homeland Security assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyberattack or intrusion," the statement read. "States ensure that voting machines are not connected to the internet, and there are numerous checks and balances, as well as extensive oversight at multiple levels, built into our election process."

John Bambenek, threat systems manager at Fidelis Cybersecurity, based in Bethesda, Md., was skeptical of the impact to expect on an election.

"The emails -- and other information gleaned from the breach -- will continue to be used to drive the media cycle and create controversy. The scanning and probing likely would have nominal impact. Voting records, while useful, probably cannot be effectively used this close to an election," Bambenek said. "My examination of the data indicated that activity is commodity

scanning used against every site on the internet. Most election jurisdictions have little public internet exposure of their voting technology as well."

In response to the USIC statement, Sen. Cory Gardner (R-Colo.) said he would push legislation to impose cybersanctions on Russia.

"I plan to introduce legislation that builds upon my North Korea Sanctions and Policy Enhancement Act by mandating the Administration sanction Russia's bad actors who are responsible for malicious cyber activities," Gardner wrote. "Russia's interference with American democracy is a direct threat to our political process, and it may only be the tip of the iceberg. It is imperative that Russia's behavior is met with strength in the form of aggressive sanctions to show the world that its cybercrimes will not be tolerated."

President Barack Obama also made it clear that cyberattacks by Russian hackers would not be tolerated, as White House spokesman Josh Earnest told reporters on Air Force One: "There are a range of responses that are available to the president, and he will consider a response that is proportional. It is certainly possible that the president can choose response options that we never announce."

Bambenek said he would expect Obama to back sanctions against Russian hackers.

"What we can expect is that the response will intend to inflict a similar, if not greater, level of pain on Russia as has been inflicted on us both as a response to the threats of electoral manipulation and as a deterrent to other nation states who may wish to plan such operations in the future," Bambenek told SearchSecurity. "This is a line in the sand and a harbinger to cyberwarfare."

Michael Heller asks:

Do you think attributing election tampering to Russian hackers is justified? Why or why not?

0 Responses

Join the Discussion

Next Steps

Learn more about fears of voting machine hacks during the general election.

Find out how voter database hacks trigger election concerns.

Dig Deeper on Government IT Security Management

ALL NEWS GET STARTED EVALUATE MANAGE PROBLEM SOLVE

Yahoo implicated in secret surveillance program, but questions remain

Q&A: Looking at cyberweapons and other issues with Nathaniel Gleicher

Cyber attribution: Whodunit takes on new meaning in November

FBI confirms more state voter databases targeted by attackers

Load More

0 comments

Oldest

Share your comment

Send me notifications when other members comment.

Register or Login

E-Mail

email@techtarget.com

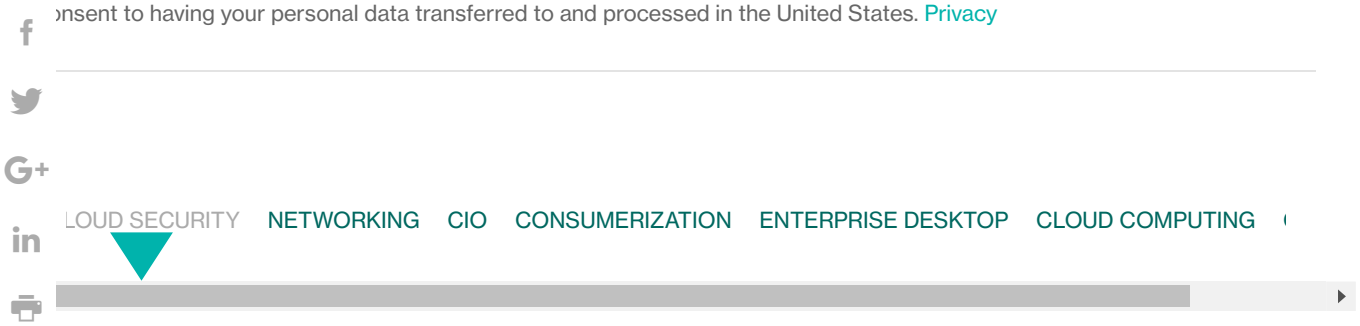
Username / Password

Username

Password

Comment

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and processed in the United States. Privacy



SearchCloudSecurity

PaaS security: Four rules for lowering enterprise risks

Securing a platform as a service can sometimes get overlooked within enterprises. Expert Char Sample offers four simple rules for...

How to handle cloud-based big data strategies according to the CSA

Assembling big data strategies is a nuanced process, but the Cloud Security Alliance offers guidance on some best practices. ...