Exclusive: 'Dumb mistake' exposed Iranian hand behind fake Proud Boys U.S. election emails - sources

reuters.com/article/us-usa-election-cyber-iran-exclusive/exclusive-dumb-mistake-exposed-iranian-hand-behind-fake-proud-boy-u-s-election-emails-sources-idUSKBN2772YL

Christopher Bing, Jack Stubbs

Media Industry
Updated

By Christopher Bing, Jack Stubbs

6 Min Read

WASHINGTON (Reuters) - Government analysts and private sector investigators were able to rapidly attribute to Iranian hackers a wave of thousands of threatening emails aimed at U.S. voters because of mistakes made in a video attached to some of the messages, according to four people familiar with the matter.

A staff member removes the Iranian flag from the stage after a group picture during the Iran nuclear talks in Vienna, Austria July 2015. REUTERS/Carlos Barria

Those failures provided a rare opportunity for the U.S. government to identify and publicly announce blame for a malicious cyber operation in a matter of days, something that usually requires months of technical analysis and supporting intelligence.

“Either they made a dumb mistake or wanted to get caught,” said a senior U.S. government official, who asked not to be identified. “We are not concerned about this activity being some kind of false flag due to other supporting evidence. This was Iran.”

Attribution to Iranian hackers does not necessarily mean a group is working at the behest of the government there. Iranian officials denied the U.S. allegations.

“These accusations are nothing more than another scenario to undermine voter confidence in the security of the U.S. election, and are absurd,” said Alireza Miryousefi, spokesman for Iran’s mission to the United Nations in New York.

On Wednesday, U.S. Director of National Intelligence John Ratcliffe said Russia and Iran have both tried to interfere in the campaign for the Nov. 3 election. U.S. intelligence agencies are still analyzing exactly who in Iran commanded the operation and its intent, three of the sources said.

Within hours of the video being circulated this week, which purported to come from a American far-right group known as The Proud Boys, intelligence officials and major email platform providers, such as Alphabet Inc's GOOGL.O Google and Microsoft Corp MSFT.O, began closely analyzing computer code that appeared in the hackers' video.

While the emails, which demanded that voters change their party affiliation to the Republican Party and vote for President Donald Trump or “we will come after you,” appeared to come from an official-looking Proud Boys email address, the address was inauthentic, security analysts said. The Proud Boys denied they were behind the messages.

How security analysts used intelligence from the video to attribute the email scheme has not been previously reported.

A Microsoft spokesperson declined to comment on the company’s collaboration with law enforcement. A Google statement on Wednesday night said the activity was “linked to Iran.” A Google spokesperson said on Thursday the company was in contact with the FBI.

ATTEMPTS TO BLUR

Despite attempts to blur aspects of the video to hide their identity, the hackers were unable to obfuscate all of the incriminating information, the sources said.

The video showed the hackers’ computer screen as they typed in commands and pretended to hack a voter registration system. Investigators noticed snippets of revealing computer code, including file paths, file names and an internet protocol (IP) address.

Security analysts found that the IP address, hosted through an online service called Worldstream, traced back to previous Iranian hacking activity, the sources said.

Analysts then cross-referenced those clues left in the video with data from other intelligence streams, including communications interceptions, the government official said.

“This public disclosure of attribution to Iran by the government has been done with breakneck speed, compared to the usual process that takes months and often years,” said Dmitri Alperovitch, a co-founder and former CTO of cybersecurity company CrowdStrike.

Two cybersecurity experts, who spoke on condition of anonymity because they were not authorized to talk to the press, independently said they had seen Iranian hackers use infrastructure from Dutch-based Worldstream to launch cyberattacks in recent months.

Worldstream’s chief legal operations officer Wouter van Zwieten said in a statement that the account associated with the IP in question was suspended after Reuters got in touch and that the Dutch National Cyber Security Center was looking into the matter.

“They’ve just informed us that the particular IP address is now officially registered by them and ready for investigation under Dutch Law,” van Zwieten said. The National Cyber Security Center confirmed that Worldstream had been in touch and that it had logged the case but declined further comment.

Van Zwieten said the server used by the hackers was only commissioned on Oct. 6 and had not drawn any complaints until now. The company said it had no access to the content on its servers.

In addition to sending thousands of emails to voters in states including Florida, the hackers also attempted to share links to the video via fake accounts on Facebook and Twitter.

Social media analytics firm Graphika said two Twitter accounts began posting links to the video on Tuesday evening and attempted to get the attention of some media and political organizations.

One account described itself as “Trump’s Soldier” and shared a link to the video with the comment “It seems they hacked voting system.”

A Twitter spokeswoman said: “We acted quickly to proactively and permanently suspend a small number of accounts and limit the sharing of media specific to this coordinated campaign.”

Facebook said: “We disrupted an attempt by a single fake account to seed information related to what appears to be an influence operation primarily focused on spreading false claims via email.”

Reporting by Christopher Bing and Jack Stubbs; Additional reporting by Raphael Satter in WASHINGTON, Joseph Menn in SAN FRANCISCO and Michelle Nichols in NEW YORK; editing by Grant McCool, Cynthia Osterman and Rosalba O’Brien

Our Standards: The Thomson Reuters Trust Principles.