The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Effort to Hack U.S. Conservative Groups Thwarted, Microsoft Says

By Reuters

August 21, 2018



Maxim Shemetov / TASS

Microsoft Corp said on Monday that it had recently thwarted hackers associated with Russian government attempting to steal user information from conservative groups that promote democracy and advocate for cybersecurity.

The company's digital crimes unit (DCU) acted on a court order last week, disrupting and transferring control of a total of six internet domains created by a group known as Strontium, also known as Fancy Bear or APT28, which is associated with the Russian government, the company said in a blog posted late on Monday night.

"We're concerned that these and other attempts pose security threats to a broadening array of groups connected with both American political parties in the run-up to the 2018 elections," Microsoft said. Microsoft's announcement comes amid increasing cyber-tensions between Moscow and Washington and rising concerns regarding security ahead of the 2018 mid-term

elections in the United States.

The Kremlin said on Tuesday it did not understand allegations from Microsoft that hackers linked to Russia's government had tried to target the websites of two right-wing U.S. think-tanks.

The software giant said it had thwarted the Russia-linked attempts last week, which it suggested showed Moscow was broadening its attacks in the build-up to November mid-term elections.

"We don't know what hackers they are talking about," Kremlin spokesman Dmitry Peskov told reporters on a conference call when asked about Microsoft's accusations.

"... Who exactly are they talking about? We don't understand what the proof and the basis is for them drawing these kind of conclusions. Such information (proof) is lacking."

Related article: Trump Says 'No Reason to Believe' Russia Hacked U.S. Election

A federal grand jury in the U.S. indicted 12 Russian intelligence officers earlier in July on charges of hacking the computer networks of 2016 Democratic presidential candidate Hillary Clinton and the Democratic Party.

Special Counsel Robert Mueller is investigating Russia's role in the 2016 election and whether the campaign of Republican candidate Donald Trump colluded with Moscow. Russia denies meddling in the elections while President Trump has denied any collusion.

The attackers created websites to mimic three U.S. Senate websites along with the Microsoft's Office 365 website and the sites of International Republican Institute and the Hudson Institute.

The International Republican Institute promotes democratic principals around the globe and has a board of directors that includes six Republican senators and a senatorial candidate.

The Hudson Institute, another conservative group, has hosted discussions on topics including cybersecurity, according to Microsoft. It has also examined the rise of kleptocracy, especially in Russia and has been critical of the Russian government, the New York Times reported.

"They are pursuing attacks that they perceive in their own national self-interest," said Eric Rosenbach, the director of the Defending Digital Democracy project at Harvard University, on Monday to the New York Times. "It's about disrupting and diminishing any group that challenges how Putin's Russia is operating at home and around the world."

The attackers created websites and URLs that closely resembled the sites that their victims would expect to receive email from or visit, Microsoft said. The type of attack is known as "spear fishing," in which the hackers trick victims to enter their user name and password into the fake site in order to steal their credentials.

"To be clear, we currently have no evidence these domains were used in any successful attacks before the DCU transferred control of them, nor do we have evidence to indicate the identity of

the ultimate targets of any planned attack involving these domains," Microsoft said on the blog.

Original url:
https://www.themoscowtimes.com/2018/08/21/russian-effort-to-hack-us-conservative-groups-thwarted-microsoft-says-a62590