Microsoft claims win over 'Russian political hackers'

bbc.co.uk/news/technology-45257081

BBC News

Published
21 August 2018

Image source, Getty Images

Image caption,
A Russian hacking group known as Fancy Bear is accused of trying to disrupt the US midterm elections

Russian attempts to launch cyber-attacks against US conservative groups have been thwarted, Microsoft says.

The software company said Russian hackers had tried to steal data from political organisations, including the International Republican Institute and the Hudson Institute think tanks.

But they had been thwarted when its security staff had won control of six net domains mimicking their websites.

Microsoft said the Fancy Bear hacking group had been behind the attacks.

Domain control

"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 in its blog detailing its work.

The thwarted attack was likely the start of a "spear phishing" campaign, said Microsoft. This would involve tricking people into visiting the mimicked domains allowing the Fancy Bear group to see and steal login information that people use.

As well as the two think-tanks, the domains seized were associated with several Senate offices and services. One domain sought to mimic Microsoft's Office 365 online service.

- Hunt wants 'malign' Russia to face action
- Trump relaxes rules around cyber-attacks
- US accuses Russia of 'pervasive' meddling

Russia has denied Microsoft's allegations that it targeted the right-wing think-tanks.

President Vladimir Putin's spokesman Dmitry Peskov said Moscow was "unaware" of any attempted interference by Russia-linked hackers in the US mid-term elections.

"[Our] reaction is traditional," he told the Interfax news agency. "We are unaware what kind of hackers they refer to, we do not know what this interference entails."

BBC Monitoring reported him as adding: "We do not understand whom exactly it concerns, what the evidence is and what such conclusions are based on. We have no such information."

He said: "We hear confirmation from America that there was no meddling in the election."

Spying charges

The New York Times suggested that the two think tanks were targeted because they were former supporters of President Trump but were now foes who had called for more sanctions to be imposed on Russia.

The International Republican Institute's directors include Senator John McCain and General HR McMaster who was replaced earlier this year as the White House national security adviser.

IRI president Daniel Twining told the Times that the attacks were consistent with the "campaign of meddling" the Kremlin is known to have indulged in.

Image source, Crowdstrike

Image caption,
Some of Fancy Bear's activities had previously been identified by the cyber-security company Crowdstrike

In its blog, Microsoft president Brad Smith said it had grabbed dodgy domains 12 times in two years to shut down 84 websites associated with Fancy Bear.

It said that, so far, it had no evidence that the domains had been used in any attacks. The domains could have been set up to help a future planned assault.

Microsoft added that the attack activity seen around the domains "mirrors" what it saw in 2016 in the US and during the 2017 election in France.

Microsoft's action comes soon after the US charged 12 Russian intelligence officers with hacking computer networks used by Hillary Clinton and the Democratic Party.