Russian Hackers Launched New Attacks Right After Trump Victory: Targets Were US Think Tanks And NGOs

http://www.techtimes.com/articles/185594/20161112/russian-hackers-launched-new-attacks-right-after-trump-victory-targets-were-us-think-tanks-and-ngos.htm

12 November 2016, 7:48 am EST By Aaron Mamiit Tech Times

Russian hackers launched new attacks less than six hours after Donald Trump was proclaimed as the next president of the United States, according to cybersecurity company Volexity.

The attacks were in the form of targeted phishing campaigns, and the targets were political think tanks and non-government organizations in the United States.

Who Are The Russian Hackers?

In Volexity's blog post covering the incidents, the cybersecurity company calls the hacking group as The Dukes, though they are also known as Cozy Bear and APT29. The group of hackers have been previously tied to the security breaches suffered by the Democratic National Committee and several high-profile organizations in the United States government.

The group is believed to have started targeting NGOs and research organizations in July of last year, and that it had access to the systems of the Democratic National Committee for over a year.

What Kind Of Hacking Attack Was Launched?

According to Volexity, the attacks that The Dukes launched after the

proclamation that Trump had won the United States presidential election were very similar to what the group launched in the past. Making its appearance once again was the PowerDuke malware, a backdoor that was first used by the group in August.

The Dukes sent out phishing emails to its targets, with the emails being very cleverly crafted to entice possible victims to open them. The emails claimed to contain the truth behind election rigging, or promised documents which show the flaws of the United States presidential election. The hackers then launched additional waves of emails that claimed to have come from members of the Clinton Foundation.

The Goal Of The Phishing Attempt

The hackers sent out the phishing emails as they looked to gain long-term access to the systems of their targets, similar to how they were able to infiltrate the systems of the Democratic National Committee. By gaining access to think tanks and NGOs, The Dukes will have more channels from which it could acquire sensitive information regarding the United States government and its policies.

Is The Government Of Russia Behind These Attacks?

Last month, the United States government officially accused Russia of being the mastermind of hacking attacks that have been launched in the country, with Russia said to be looking to interfere with the national elections. The government of the United States might be planning to

retaliate in some way, but engaging in an all-out cyberwar against Russia is not a good idea.

There have also been accusations that Trump is actually supported by Russia, with a recent report said to reveal that the largest private commercial bank of Russia has been communicating with a server of the Trump Organization. Trump's camp, however, has strongly denied the claims.

Russian hackers launched new attacks against political think tanks and non-government organizations in the United States. The attacks happened less than six hours after Donald Trump won the presidential election. (Zach Gibson | Getty Images)

http://www.techtimes.com/articles/185594/20161112/russian-hackers-launched-new-attacks-right-after-trump-victory-targets-were-us-think-tanks-and-ngos.htm

After Trump Win, Russian Hackers Strike US Think Tanks

- BY STEPHANIE MLOT
- NOVEMBER 11, 2016 09:43AM EST
- 10 COMMENTS

American political think tanks and NGOs were targeted by a well-known hacking group called The Dukes

http://www.pcmag.com/news/349492/after-trump-win-russian-hackers-strike-us-think-tanks

Russian hackers wasted no time this week, attacking American political think tanks and non-government organizations (NGOs) on Wednesday.

A round of targeted phishing campaigns (attempts to obtain sensitive information by pretending to be a trustworthy entity) came less than six hours after Donald Trump was named President-elect of the US.

According to cyber incident response firm Volexity, the hackers belong to a Russian gang best known for infiltrating computer networks at the Democratic National Committee and the Democratic Congressional Campaign Committee. The group—often referred to as APT29, Cozy Bear, or The Dukes—began targeting research organizations and NGOs in July 2015.

"This represented a fairly significant shift in the group's previous operations and one that continued in the lead-up to and immediately after the 2016 United States Presidential election," Volexity founder Steven Adair wrote in a blog post.

The Dukes in August launched several waves of highly targeted spear-phishing attacks, sending spoofed email messages to specific individuals at US-based organizations via backdoor malware dubbed PowerDuke. The same malware, which allows the hackers to examine and control a system, was used again in this week's post-election invasions.

Why Trump's Cyber Is the Strongest

As reported by Volexity, two of the attacks purported to be messages forwarded from the Clinton Foundation, two posed as eFax links or documents regarding rigged election results, and the last claimed to be a link to a PDF download on "Why American Elections Are Flawed."

Last month, federal officials said they are "confident"that the Russian government is behind recent attacks of US political organizations, like the DNC. Russian President Vladimir Putin has denied any involvement in said hacks.

"The Dukes continue to launch well-crafted and clever attack campaigns. They have had tremendous success evading anti-virus and anti-malware solutions at both the desktop and mail gateway levels," Adair wrote on Wednesday. "Volexity believes that The Dukes are likely working to gain long-term access into think tanks and NGOs and will continue to launch new attacks for the foreseeable future."

http://www.pcmag.com/news/349492/after-trump-win-russian-hackers-strike-us-think-tanks