The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Hackers Targeted Ukrainian Company at Center of Trump's Impeachment Storm

By Reuters

January 14, 2020

A leak of stolen data could potentially affect the impeachment process and U.S. electoral contest.
Evgenij Razumnyj / Vedomosti / TASS

Russian military hackers tried to steal emails from the Ukrainian energy firm where Hunter Biden, the son of Democratic U.S. presidential contender Joe Biden, had a seat on the board, an American cybersecurity firm said on Monday.

Energy company Burisma Holdings was at the center of attempts by President Donald Trump last July to pressure Ukrainian authorities into announcing an investigation into the Bidens for purported corruption, an effort that has led to the Republican being impeached by the U.S. House of Representatives on charges of abuse of power and obstruction of Congress.

Related article: The Trump-Ukraine Scandal, Explained

Trump denies he did anything wrong by asking Ukrainian officials to investigate Hunter Biden's relationship with Burisma. There has been no evidence of wrongdoing by the Bidens, who reject Trump's allegations of graft.

California-based Area 1 Security identified the hacking of Burisma and linked it to Russia's Main Directorate of Military Intelligence, or GRU. The same hacking group, known as "Fancy Bear" or "APT28" by cybersecurity researchers, breached the Democratic National Committee in 2016 in what U.S. investigators described as part of an operation to disrupt that year's election.

"You can see this attack really is starting to parallel with what we saw in 2016," Oren Falkowitz, Area 1's chief executive, said in an interview.

The Russian Defense Ministry did not immediately respond to a request for comment. Officials at the U.S. National Security Agency and the Department of Homeland Security declined to comment.

Burisma did not immediately respond to a request for comment.

A source close to Burisma told Reuters the company's website had been subject to multiple break-in attempts over the past six months but did not provide further details.

What data the hackers were looking to steal is not clear, Area 1 said. Breaching Burisma could yield communications from, to, or about Hunter Biden, who served as a director between 2014 and 2019. A leak of stolen data could potentially affect the impeachment process and the 2020 U.S. presidential election.

Area 1 said it became aware of the Russian targeting of Burisma after its email security scanning product found suspicious evidence online, including "decoy domains": websites designed to imitate legitimate email services used by Burisma's subsidiaries.

Publicly available domain registration records examined by Reuters show that the hackers created the decoy domains between Nov. 11, the day before U.S. Democrats began their first public impeachment hearings, and Dec. 3, the day before the House Judiciary Committee took up the matter.

The records show that the same people also registered fake domains for a Ukrainian media company, named Kvartal 95, in March and April 2019. Kvartal 95 was founded by Ukrainian President Volodymyr Zelenskiy and multiple employees of the company have since joined his administration.

Kvartal 95 and representatives for Zelenskiy did not immediately respond to requests for comment.

Area 1's report said it discovered the GRU had targeted two subsidiaries of Burisma - KUB Gas LLC and Esko Pivnich - as well as CUB Energy Inc, which was affiliated with the company, using lookalike domains intended to trick employees into providing their email passwords.

Burisma and its subsidiaries share the same email server, Area 1 said, meaning a breach at any of the companies could expose them all.

The report gave a limited indication of how Area 1 determined that the lookalike domains were the work of the GRU, pointing mainly to similarities in how the hackers had previously set their digital traps. Area 1 co-founder Blake Darche said unpublished data gathered by his firm linked the operation to a specific officer in Moscow, whose identity he was unable to establish.

But Darche said "we are 100% certain" that the GRU was behind the hacking.

An outside researcher, Kyle Ehmke of Virginia-based cybersecurity firm ThreatConnect, who reviewed the malicious domains flagged by Area 1, said based on the information he had seen, he believed "with moderate confidence" that the websites were devised by the GRU.

Related article: Seeking Favors, Trump Asked Ukraine President to Investigate Biden

Ehmke said that the hacking operation against Burisma used methods consistent with Russian hackers associated with the GRU, but that a complete picture was lacking.

John Hultquist, director of intelligence analysis with U.S. cybersecurity firm FireEye, told Reuters the domains discovered by Area 1 are "consistent" with other known APT28 activities.

Russian spies have routinely targeted Ukrainian energy firms with cyberattacks since Russia threw its weight behind a separatist takeover in eastern Ukraine in 2014.

U.S. intelligence officials have issued warnings that Russia is working to intervene in the November 2020 election. Trump is seeking re-election and Biden is a leading opponent out of a dozen Democrats seeking their party's nomination.

Andrew Bates, a spokesman for Joe Biden, did not comment directly on the hack but said in an email: "Any American president who had not repeatedly encouraged foreign interventions of this kind would immediately condemn this attack on the sovereignty of our elections."

Original url:
https://www.themoscowtimes.com/2020/01/14/russian-hackers-targeted-ukrainian-company-at-center-of-trumps-impeachment-storm-a68889