Russians Hacked Ukrainian Gas Company at Center of Impeachment

nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

Nicole Perlroth January 13, 2020

With President Trump facing an impeachment trial over his efforts to pressure Ukraine to investigate former Vice President Joseph R. Biden Jr. and his son Hunter Biden, Russian military hackers have been boring into the Ukrainian gas company at the center of the affair, according to security experts.

The hacking attempts against Burisma, the Ukrainian gas company on whose board Hunter Biden served, began in early November, as talk of the Bidens, Ukraine and impeachment was dominating the news in the United States.

It is not yet clear what the hackers found, or precisely what they were searching for. But the experts say the timing and scale of the attacks suggest that the Russians could be searching for potentially embarrassing material on the Bidens — the same kind of information that Mr. Trump wanted from Ukraine when he pressed for an investigation of the Bidens and Burisma, setting off a chain of events that led to his impeachment.

The Russian tactics are strikingly similar to what American intelligence agencies say was Russia's hacking of emails from Hillary Clinton's campaign chairman and the Democratic National Committee during the 2016 presidential campaign. In that case, once they had the emails, the Russians used trolls to spread and spin the material, and built an echo chamber to widen its effect.

Then, as now, the Russian hackers from a military intelligence unit known formerly as the G.R.U., and to private researchers by the alias “Fancy Bear,” used so-called phishing emails that appear designed to steal usernames and passwords, according to Area 1, the Silicon Valley security firm that detected the hacking. In this instance, the hackers set up fake websites that mimicked sign-in pages of Burisma subsidiaries, and have been blasting Burisma employees with emails meant to look like they are coming from inside the company.

The hackers fooled some of them into handing over their login credentials, and managed to get inside one of Burisma’s servers, Area 1 said.

“The attacks were successful,” said Oren Falkowitz, a co-founder of Area 1, who previously served at the National Security Agency. Mr. Falkowitz’s firm maintains a network of sensors on web servers around the globe — many known to be used by state-sponsored hackers — which gives the firm a front-row seat to phishing attacks, and allows them to block attacks on their customers.

“The timing of the Russian campaign mirrors the G.R.U. hacks we saw in 2016 against the D.N.C. and John Podesta,” the Clinton campaign chairman, Mr. Falkowitz said. “Once again, they are stealing email credentials, in what we can only assume is a repeat of Russian interference in the last election.”

The Justice Department indicted seven officers from the same military intelligence unit in 2018.

The Russian attacks on Burisma appear to be running parallel to an effort by Russian spies in Ukraine to dig up information in the analog world that could embarrass the Bidens, according to an American security official, who spoke on the condition of anonymity to discuss sensitive intelligence. The spies, the official said, are trying to penetrate Burisma and working sources in the Ukrainian government in search of emails, financial records and legal documents.

Neither the Russian government nor Burisma responded to requests for comment.

American officials are warning that the Russians have grown stealthier since 2016, and are again seeking to steal and spread damaging information and target vulnerable election systems ahead of the 2020 election.

[Read: Even as American election defenses have improved, Russian hackers and trolls have become more sophisticated.]

In the same vein, Russia has been working since the early days of Mr. Trump’s presidency to turn the focus away from its own election interference in 2016 by seeding conspiracy theories about Ukrainian meddling and Democratic complicity.

The result has been a muddy brew of conspiracy theories that mix facts, like the handful of Ukrainians who openly criticized Mr. Trump’s candidacy, with discredited claims that the D.N.C.’s email server is in Ukraine and that Mr. Biden, as vice president, had corrupt dealings with Ukrainian

officials to protect his son. Spread by bots and trolls on social media, and by Russian intelligence officers, the claims resonated with Mr. Trump, who views talk of Russian interference as an attack on his legitimacy.

With Mr. Biden's emergence as a front-runner for the Democratic nomination last spring, the president latched on to the corruption allegations, and asked that Ukraine investigate the Bidens on his July 25 call with President Volodymyr Zelensky of Ukraine. The call became central to Mr. Trump's impeachment last month.

The Biden campaign sought to cast the Russian effort to hack Burisma as an indication of Mr. Biden's political strength, and to highlight Mr. Trump's apparent willingness to let foreign powers boost his political fortunes.

"Donald Trump tried to coerce Ukraine into lying about Joe Biden and a major bipartisan, international anti-corruption victory because he recognized that he can't beat the vice president," said Andrew Bates, a spokesman for the Biden campaign.

"Now we know that Vladimir Putin also sees Joe Biden as a threat," Mr. Bates added. "Any American president who had not repeatedly encouraged foreign interventions of this kind would immediately condemn this attack on the sovereignty of our elections."

The corruption allegations hinge on Hunter Biden's work on the Burisma board. The company hired Mr. Biden while his father was vice president and leading the Obama administration's Ukraine policy, including a successful push to have Ukraine's top prosecutor fired for corruption. The effort was backed by European allies.

The story has since been recast by Mr. Trump and some of his staunchest defenders, who say Mr. Biden pushed out the prosecutor because Burisma was under investigation and his son could be implicated. Rudolph W. Giuliani, acting in what he says was his capacity as Mr. Trump's personal lawyer, has personally taken up investigating the Bidens and Burisma, and now regularly claims to have uncovered clear-cut evidence of wrongdoing.

The evidence, though, has yet to emerge, and now the Russians appear to have joined the hunt.

Area 1 researchers discovered a G.R.U. phishing campaign on Ukrainian companies on New Year's Eve. A week later, Area 1 determined what the Ukrainian targets had in common: They were all subsidiaries of Burisma Holdings, the company at the center of Mr. Trump's impeachment. Among the Burisma subsidiaries phished were KUB-Gas, Aldea, Esko-Pivnich, Nadragas, Tehnocom-Service and Pari. The targets also included Kvartal 95, a Ukrainian television production company founded by Mr. Zelensky. The phishing attack on Kvartal 95 appears to have been aimed at digging up email correspondence for the company's chief, Ivan Bakanov, whom Mr. Zelensky appointed as the head of Ukraine's Security Service last June.

To steal employees' credentials, the G.R.U. hackers directed Burisma to their fake login pages. Area 1 was able to trace the look-alike sites through a combination of internet service providers frequently used by G.R.U.'s hackers, rare web traffic patterns, and techniques that have been used in previous

attacks against a slew of other victims, including the 2016 hack of the D.N.C. and a more recent Russian hack of the World Anti-Doping Agency.

“The Burisma hack is a cookie-cutter G.R.U. campaign,” Mr. Falkowitz said. “Russian hackers, as sophisticated as they are, also tend to be lazy. They use what works. And in this, they were successful.”