The New York Times | https://nyti.ms/2GzIRrG

EUROPE

In a First, U.S. Blames Russia for Cyber Attacks on Energy Grid

By REUTERS MARCH 16, 2018, 8:24 P.M. E.D.T.

WASHINGTON — The Trump administration on Thursday blamed the Russian government for a campaign of cyber attacks stretching back at least two years that targeted the U.S. power grid, marking the first time the United States has publicly accused Moscow of hacking into American energy infrastructure.

Beginning in March 2016, or possibly earlier, Russian government hackers sought to penetrate multiple U.S. critical infrastructure sectors, including energy, nuclear, commercial facilities, water, aviation and manufacturing, according to a U.S. security alert published Thursday.

The Department of Homeland Security and FBI said in the alert that a "multi-stage intrusion campaign by Russian government cyber actors" had targeted the networks of small commercial facilities "where they staged malware, conducted spear phishing, and gained remote access into energy sector networks." The alert did not name facilities or companies targeted.

The direct condemnation of Moscow represented an escalation in the Trump administration's attempts to deter Russia's aggression in cyberspace, after senior U.S. intelligence officials said in recent weeks the Kremlin believes it can launch hacking operations against the West with impunity.

It coincided with a decision Thursday by the U.S. Treasury Department to impose sanctions on 19 Russian people and five groups, including Moscow's intelligence services, for meddling in the 2016 U.S. presidential election and other malicious cyber attacks.

Russia in the past has denied it has tried to hack into other countries' infrastructure, and vowed on Thursday to retaliate for the new sanctions.

'UNPRECEDENTED AND EXTRAORDINARY'

U.S. security officials have long warned that the United States may be vulnerable to debilitating cyber attacks from hostile adversaries. It was not clear what impact the attacks had on the firms that were targeted.

But Thursday's alert provided a link to an analysis by the U.S. cyber security firm Symantec last fall that said a group it had dubbed Dragonfly had targeted energy companies in the United States and Europe and in some cases broke into the core systems that control the companies' operations.

Malicious email campaigns dating back to late 2015 were used to gain entry into organizations in the United States, Turkey and Switzerland, and likely other countries, Symantec said at the time, though it did not name Russia as the culprit.

The decision by the United States to publicly attribute hacking attempts of American critical infrastructure was "unprecedented and extraordinary," said Amit Yoran, a former U.S. official who founded DHS's Computer Emergency Response Team.

"I have never seen anything like this," said Yoran, now chief executive of the cyber firm Tenable, said.

A White House National Security Council spokesman did not respond when asked what specifically prompted the public blaming of Russia. U.S. officials have historically been reluctant to call out such activity in part because the United States also spies on infrastructure in other parts of the world.

News of the hacking campaign targeting U.S. power companies first surfaced in June in a confidential alert to industry that described attacks on industrial firms, including nuclear plants, but did not attribute blame.

"People sort of suspected Russia was behind it, but today's statement from the U.S. government carries a lot of weight," said Ben Read, manager for cyber espionage analysis with cyber security company FireEye Inc.

ENGINEERS TARGETED

The campaign targeted engineers and technical staff with access to industrial controls, suggesting the hackers were interested in disrupting operations, though FireEye has seen no evidence that they actually took that step, Read said.

A former senior DHS official familiar with the government response to the campaign said that Russia's targeting of infrastructure networks dropped off after the publication in the fall of Symantec's research and an October government alert, which detailed technical forensics about the hacking attempts but did not name Russia.

The official declined to say whether the campaign was still ongoing or provide specifics on which targets were breached, or how close hackers may have gotten to operational control systems.

"We did not see them cross into the control networks," DHS cyber security official Rick Driggers told reporters at a dinner on Thursday evening.

Driggers said he was unaware of any cases of control networks being compromised in the United States and that the breaches were limited to business networks. But, he added, "We know that there is intent there."

It was not clear what Russia's motive was. Many cyber security experts and former U.S. officials say such behaviour is generally espionage-oriented with the potential, if needed, for sabotage.

Russia has shown a willingness to leverage access into energy networks for damaging effect in the past. Kremlin-linked hackers were widely blamed for two

attacks on the Ukrainian energy grid in 2015 and 2016, that caused temporary blackouts for hundreds of thousands of customers and were considered first-of-their-kind assaults.

Senator Maria Cantwell, the top Democrat on the Senate Energy and Natural Resources Committee, asked the Trump administration earlier this month to provide a threat assessment gauging Russian capabilities to breach the U.S. electric grid.

It was the third time Cantwell and other senators had asked for such a review. The administration has not yet responded, a spokesman for Cantwell's office said on Thursday.

Last July, there were news reports that the Wolf Creek Nuclear Operating Corp, which operates a nuclear plant in Kansas, had been targeted by hackers from an unknown origin.

Spokeswoman Jenny Hageman declined to say at the time if the plant had been hacked but said that there had been no operational impact to the plant because operational computer systems were separate from the corporate network. Hageman on Thursday said the company does not comment on security matters.

John Keeley, a spokesman for the industry group the Nuclear Energy Institute, said: "There has been no successful cyber attack against any U.S. nuclear facility, including Wolf Creek."

(Reporting by Dustin Volz and Timothy Gardner, additional reporting by Jim Finkle; Editing by Tom Brown, Alistair Bell and Cynthia Osterman)
