Russian Hackers Attacking U.S. Power Grid and Aviation, FBI Warns

By **Jennifer A Dlouhy** and **Michael Riley**
March 15, 2018, 2:14 PM CDT *Updated on* March 15, 2018, 7:12 PM CDT

- U.S. officials warn of attacks, including on nuclear plants
- Cyber-attacks underway since at least March 2016, U.S. says

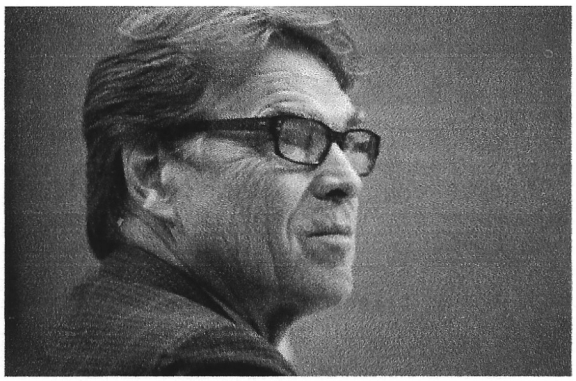
Russian hackers are conducting a broad assault on the U.S. electric grid, water processing plants, air transportation facilities and other targets in rolling attacks on some of the country's most sensitive infrastructure, U.S. government officials said Thursday.

The announcement was the first official confirmation that Russian hackers have taken aim at facilities on which hundreds of millions of Americans depend for basic services. Bloomberg News reported in July <https://www.bloomberg.com/politics/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site> that Russian hackers had breached more than a dozen power plants in seven states, an aggressive campaign that has since expanded to dozens of states, according to a person familiar with the investigation.

"Since at least March 2016, Russian government cyber actors" have targeted "government entities and multiple U.S. critical infrastructure sectors," including those of energy, nuclear, water and aviation, according to an alert <https://www.us-cert.gov/ncas/alerts/TA18-074A> issued Thursday by the Department of Homeland Security and Federal Bureau of Investigation.

Critical manufacturing sectors and commercial facilities also have been

targeted by the ongoing "multi-stage intrusion campaign by Russian government cyber actors."



Rick Perry during a House Appropriations Subcommittee hearing in Washington on March 15. Photographer: Andrew Harrer/Bloomberg

Cyber-attacks are "literally happening hundreds of thousands of times a day," Energy Secretary Rick Perry told lawmakers during a hearing Thursday. "The warfare that goes on in the cyberspace is real, it's serious, and we must lead the world."

Separately Thursday, the U.S. sanctioned a St. Petersburg-based "troll farm," two Russian intelligence services, a close ally of Russian President Vladimir Putin and other Russian citizens and businesses indicted by Special Counsel Robert Mueller on charges of meddling with the 2016 U.S. presidential election.

A joint analysis by the FBI and the Department of Homeland Security described the hackers as extremely sophisticated, in some cases first breaching suppliers and third-party vendors before hopping from those networks to their ultimate target. The government's report did not say how successful the attacks were.

Read More: Russia Is Said to Be Suspect in Hacks of U.S. Power Plants <https://www.bloomberg.com/politics/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site>

The Russian hackers "targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks," according to the Homeland Security alert.

An industry-government partnership provided potential indicators of compromise for electric companies following Thursday's announcement, said Scott Aaronson, vice president of security and preparedness at the utility trade group Edison Electric Institute. The federal government alerted grid operators to a threat targeting the energy and manufacturing sectors last summer, but the incident didn't affect operations, he said.

The hackers deliberately selected targets and methodically went after initial victims as a way to reach their ultimate prizes, including industrial control

systems used by power plants and other infrastructure. Their tactics included sending spear-phishing emails and embedding malicious content on informational websites to obtain security credentials they could then leverage for more information and access.

And once they obtained access, the attackers "conducted network reconnaissance," and moved within the systems to collect information on industrial control systems.

The government's alert on Russian cyber-attacks does not cover suspected meddling by the country in the 2016 election.

An October report by researchers at Symantec Corp., cited by the U.S. government Thursday, linked the attacks to a group of hackers it had code-named Dragonfly, and said it found evidence critical infrastructure facilities in Turkey and Switzerland also had been breached.

The Symantec researchers said an earlier wave of attacks by the same group starting in 2011 was used to gather intelligence on companies and their operational systems. The hackers then used that information for a more advanced wave of attacks targeting industrial control systems that, if disabled, leave millions without power or water.

The disclosure comes amid mounting calls from lawmakers to step up protection of the nation's electric grid. Senator Maria Cantwell, the top Democrat on the Energy and Natural Resources Committee, pushed for a cyberthreat assessment of the grid last year, to better defend the infrastructure against potential attacks.

"I hope today's belated response is the first step in a robust and aggressive strategy to protect our critical infrastructure," Cantwell, a Democrat from Washington state, said in an emailed statement.

U.S. intelligence officials have long been concerned about the security of the country's electrical grid. The recent attacks, striking almost simultaneously at multiple locations, are testing the government's ability to coordinate an effective response among several private utilities, state and local officials, and industry regulators.

Many of the targeted power plants are conventional, but the attacks included at least one nuclear power plant in Kansas, Bloomberg News reported in July. While the core of a nuclear generator is heavily protected, a sudden shutdown of the turbine can trigger safety systems. These safety

devices are designed to disperse excess heat while the nuclear reaction is halted, but the safety systems themselves may be vulnerable to attack.

The operating systems at nuclear plants also tend to be legacy controls built decades ago and don't have digital control systems that can be exploited by hackers.

— With assistance by Toluse Olorunnipa, Ari Natter, Nafeesa Syeed, and Mark Chediak

---