The Washington Post

National Security

Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say

Editor's Note: *An earlier version of this story incorrectly said that Russian hackers had penetrated the U.S. electric grid. Authorities say there is no indication of that so far. The computer at Burlington Electric that was hacked was not attached to the grid.*

By Juliet Eilperin and Adam Entous December 31 at 11:50 AM

A code associated with the Russian hacking operation dubbed Grizzly Steppe by the Obama administration has been detected within the system of a Vermont utility, according to U.S. officials.

While the Russians did not actively use the code to disrupt operations, according to officials who spoke on the condition of anonymity to discuss a security matter, the discovery underscores the vulnerabilities of the nation's electrical grid. And it raises fears in the U.S. government that Russian government hackers are actively trying to penetrate the grid to carry out potential attacks.

Officials in government and the utility industry regularly monitor the grid because it is highly computerized and any disruptions can have disastrous implications for the country's medical and emergency services.

Burlington Electric said in a statement that the company detected a malware code used in the Grizzly Steppe operation in a laptop that was not connected to the organization's grid systems. The firm said it took immediate action to isolate the laptop and alert federal authorities.

Friday night, Vermont Gov. Peter Shumlin (D) called on federal officials "to conduct a full and complete investigation of this incident and undertake remedies to ensure that this never happens again."

"Vermonters and all Americans should be both alarmed and outraged that one of the world's leading thugs, Vladimir Putin, has been attempting to hack our electric grid, which we rely upon to support our quality-of-life, economy, health, and safety,"

Shumlin said in a statement. “This episode should highlight the urgent need for our federal government to vigorously pursue and put an end to this sort of Russian meddling.”

Sen. Patrick J. Leahy (D-Vt.) said he was briefed on the attempts to penetrate the electric grid by Vermont State Police on Friday evening. “This is beyond hackers having electronic joy rides — this is now about trying to access utilities to potentially manipulate the grid and shut it down in the middle of winter,” Leahy said in a statement. “That is a direct threat to Vermont and we do not take it lightly.”

Rep. Peter Welch (D-Vt.) said the attack shows how rampant Russian hacking is. “It’s systemic, relentless, predatory,” Welch said . “They will hack everywhere, even Vermont, in pursuit of opportunities to disrupt our country. We must remain vigilant, which is why I support President Obama’s sanctions against Russia and its attacks on our country and what it stands for.”

American officials, including one senior administration official, said they are not yet sure what the intentions of the Russians might have been. The incursion may have been designed to disrupt the utility’s operations or as a test to see whether they could penetrate a portion of the grid.

Officials said that it is unclear when the code entered the Vermont utility’s computer, and that an investigation will attempt to determine the timing and nature of the intrusion, as well as whether other utilities were similarly targeted.

“The question remains: Are they in other systems and what was the intent?” a U.S. official said.

This week, officials from the Department of Homeland Security, FBI and the Office of the Director of National Intelligence shared the Grizzly Steppe malware code with executives from 16 sectors nationwide, including the financial, utility and transportation industries, a senior administration official said. Vermont utility officials identified the code within their operations and reported it to federal officials Friday, the official said.

The DHS and FBI also publicly posted information about the malware Thursday as part of a joint analysis report, saying that the Russian military and civilian services’ activity “is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens.”

Another senior administration official, who also spoke on the condition of anonymity to discuss security matters, said in an email that “by exposing Russian malware” in the joint analysis report, “the administration sought to alert all network defenders in the United States and abroad to this malicious activity to better secure their networks and defend against Russian malicious cyber activity.”

According to the report by the FBI and DHS, the hackers involved in the Russian operation used fraudulent emails that tricked their recipients into revealing passwords.

Russian hackers, U.S. intelligence agencies say, earlier obtained a raft of internal emails from the Democratic National Committee, which were later released by WikiLeaks during this year’s presidential campaign.

President-elect Donald Trump has repeatedly questioned the veracity of U.S. intelligence pointing to Russia's responsibility for hacks in the run-up to the Nov. 8 election. He also has spoken highly of Russian President Vladimir Putin, despite President Obama's suggestion that the approval for hacking came from the highest levels of the Kremlin.

Trump spokesman Sean Spicer said it would be "highly inappropriate to comment" on the incident given the fact that Spicer has not been briefed by federal authorities at this point.

Obama has been criticized by lawmakers from both parties for not retaliating against Russia before the election. But officials said the president was concerned that U.S. countermeasures could prompt a wider effort by Moscow to disrupt the counting of votes on Election Day, potentially leading to a wider conflict.

Officials said Obama also was concerned that taking retaliatory action before the election would be perceived as an effort to help the campaign of Democratic presidential nominee Hillary Clinton.

On Thursday, when Obama announced new economic measures against Russia and the expulsion of 35 Russian officials from the United States in retaliation for what he said was a deliberate attempt to interfere with the election, Trump told reporters, "It's time for our country to move on to bigger and better things."

Trump has agreed to meet with U.S. intelligence officials next week to discuss allegations surrounding Russia's online activity.

Russia has been accused in the past of launching a cyberattack on Ukraine's electrical grid, something it has denied. Cybersecurity experts say a hack in December 2015 destabilized Kiev's power grid, causing a blackout in part of the Ukrainian capital. On Thursday, Ukrainian President Petro Poroshenko accused Russia of waging a hacking war on his country that has entailed 6,500 attacks against Ukrainian state institutions over the past two months.

Since at least 2009, U.S. authorities have tracked efforts by China, Russia and other countries to implant malicious software inside computers used by U.S. utilities. It is unclear if the code used in those earlier attacks was similar to what was found in the Vermont case. In November 2014, for example, federal authorities reported that a Russian malware known as BlackEnergy had been detected in the software controlling electric turbines in the United States.

The Russian Embassy did not immediately respond to a request for comment. Representatives for the Energy Department and DHS declined to comment Friday.

Alice Crites, Carol Morello and Ellen Nakashima contributed to this report.

Juliet Eilperin is The Washington Post's White House bureau chief, covering domestic and foreign policy as well as the culture of 1600 Pennsylvania Avenue. She is the author of two books—one on sharks, and another on Congress, not to be confused with each other—and has worked for the Post since 1998. Follow @eilperin

Adam Entous writes about national security, foreign policy and intelligence for The Post. He joined the newspaper in 2016 after more than 20 years with The Wall Street Journal and Reuters, where he covered the Pentagon, the CIA, the White House and Congress. He covered President George W. Bush for five years after the September 11, 2001, attacks.