‘Russian hackers’ penetrate US power grid with ‘outdated Ukrainian malware’

Published time: 31 Dec, 2016 10:19Edited time: 31 Dec, 2016 14:30

© Brian Snyder / Reuters

A Vermont utility sounded the alarm after finding malware code on a laptop that the FBI and DHS had touted as associated with Russian hackers. However, cybersecurity specialists say the code came from an outdated Ukrainian hacking tool. On Thursday, the FBI and DHS released a joint report on a hacking operation they called ‘Grizzly Steppe’. They claimed the operation was linked to the Russian government, alleging that it had targeted “US persons and institutions, including from US political organizations.”

Along with the report, the US security agencies released a sample of the malware code allegedly used in the Grizzly Steppe operation to compromise US computer networks. The code was also shared with executives from 16 industries around the nation, including the financial, utility, and transportation sectors, according to a Washington Post report.

On Friday, Burlington Electric, a Vermont-based power company, released a statement saying that the malware code had been detected during a scan of a single company laptop that was not connected to the grid. “We took immediate action to isolate the laptop and alerted federal officials of this finding. Our team is working with federal officials to trace this malware and prevent any other attempts to infiltrate utility systems. We have briefed state officials and will support the investigation fully,” the statement said.

The US media reported the incident as if Russian hackers had penetrated America’s electric grids, prompting some officials to call on the federal government to protect Americans from Russian President Vladimir Putin. “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,” Vermont Governor Peter 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,” he said.

German govt says it has no proof Russia trying to hack upcoming elections

Meanwhile, a number of IT specialists that have analyzed the code and other evidence published by the US government are questioning whether it really proves a Russian connection, let alone a connection to the Russian government. Wordfence, a cybersecurity firm that specializes in protecting websites running WordPress, a PHP-based platform, published a report on the issue on Friday.

Wordfence said they had traced the malware code to a tool available online, which is apparently funded by donations, called P.A.S. that claims to be “made in Ukraine.” The version tested by the FBI/DHS report is 3.1.7, while the most current version available on the tool’s website is 4.1.1b. “One might reasonably expect Russian intelligence operatives to develop their own tools or at least use current malicious tools from outside sources,” the report says.

The second part of the analysis deals with the list of IP addresses provided by the US agencies. The report says they “don’t appear to provide any association with Russia” and “are probably used by a wide range of other malicious actors.”

This week, the Obama administration accused the Russian government of hacking US computer networks in order to influence the presidential to justify imposing some of the toughest sanctions on Russia yet, including the expulsion of 35 Russian diplomats and blocking access to two leisure compounds used by Russian Foreign Ministry personnel and their visitors.

Russia chose to ignore the punitive measures, calling their imposition a clear provocation, while saying that Moscow will build its relations with the US based on the policies of the next administration under President-elect Donald Trump, not President Barack Obama’s parting shots. In October, Putin ridiculed the idea that Russia could influence the US presidential election, saying that America was not “a banana republic.”