

Russia warns of “cyberwar” following report the US attacked its power grid

Enlarge / Zapadnaya in the Moscow region.

reader comments

69 with 46 posters participating

Share this story

The Kremlin on Monday warned that reported US digital incursions into Russia’s electric power grid could trigger a “cyberwar” between the two countries.

The warning came two days after The New York Times reported that the US Cyber Command, the arm of the Pentagon that runs the military’s offensive and defensive operations in the online world, was aggressively stepping up its targeting of Russia’s grid. Saturday’s report said the command had taken steps to place “potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before.” In some cases, the NYT reported, Pentagon and intelligence officials have been hesitant to brief President Trump in detail about the activities out of concern he might countermand the operations or discuss them with foreign officials. Last year, Trump gave the Cyber Command more leeway to conduct offensive online operations, the publication said.

Some analysts have cast doubt on the NYT reporting that the United States has put implants inside Russia’s grid, and the

publication was clear it had no classified information detailing how deep into Russia's power infrastructure the US has bored. The report, however, was enough to get the attention of Kremlin officials, who pushed back in a post published Monday by the TASS news agency, which is owned by the Russian government.

"If one assumes that some government agencies do this without informing the head of state, then of course this may indicate that cyberwar against Russia might be a hypothetical possibility," Russian Presidential Spokesman Dmitry Peskov said. The spokesman went on to say that "vital areas of our economy are under continuous attacks from abroad." Russian agencies have countered the attacks to prevent damage to the country's economy.

Saturday's NYT article came one day after researchers with security firm Dragos said that hackers behind at least two dangerous intrusions on industrial facilities have expanded their activities to probing dozens of power grids in the US and elsewhere. Last year, researchers with security firm FireEye said the hacker group's malware—which actively targets safety systems used to prevent explosions, fires, and other potentially fatal accidents—was developed with the help of the Central Scientific Research Institute of Chemistry and Mechanics in Moscow.

The NYT said the United States' increasingly offensive digital incursions into Russia's electric infrastructure were part of a broader view designed to make Russia and other US adversaries pay a price for engaging in cyberoperations against the US or US interests. Such operations include inroads into US industrial systems by the same Russian hackers who breached regional power authorities in Ukraine in December 2015. Those breaches left hundreds of thousands of people in the Ivano-Frankivsk region of the country without electricity.

Following revelations in 2016 that Russian hackers breached

the Democratic National Committee and focused on the US power grid, the NYT said, then-President Obama decided to be less passive.

“Mr. Obama secretly ordered some kind of message-sending action inside the Russian grid, the specifics of which have never become public,” reporters David Sanger and Nicole Perlroth wrote. “It is unclear whether much was accomplished.”

More recently, Trump advisors have signaled a more aggressive posture. Speaking last Tuesday at a conference organized by The Wall Street Journal, President Trump’s national security advisor John Bolton reportedly said: “We thought the response in cyberspace against electoral meddling was the highest priority last year, and so that’s what we focused on. But we’re now opening the aperture, broadening the areas we’re prepared to act in.”

Sharply reduced shelf life

As noted earlier, at least one analyst has publicly doubted the NYT’s reporting that the US operations included the placing of implants inside the Russian power grid.

“Revealing potent ‘implants’ to the adversary means sending the adversary into intense search mode, so ‘implants’ likely will have a sharply reduced shelf-life,” Johns Hopkins political scientist Thomas Rid wrote on Twitter on Sunday. “Publicity burns capabilities. I find it hard to believe that CYBERCOM would burn top-tier tools like this.”

a—keep them: revealing potent “implants” to the adversary means sending the adversary into intense search mode, so “implants” likely will have a sharply reduced shelf-life. Publicity burns capabilities. I find it hard to believe that CYBERCOM would burn top-tier tools like this.

— Thomas Rid (@RidT) June 16, 2019

On Monday, Prof. Rid posted this update as he was en route to Moscow to speak about hacking: "Don't put too much stock into the core 'implant' claim in the original story (sorry I can't say more)."

*Oh good timing, I'm literally en route to Moscow to give a talk on "attributing cyber attacks" later this week (ICC) ...
<https://t.co/M0uu0L4XBu>*

Also, update: don't put too much stock into the core "implant" claim in the original story (sorry I can't say more)

– Thomas Rid (@RidT) June 17, 2019

While it remains unclear precisely how the new, more aggressive digital incursions into Russia's power grid are manifesting themselves, Saturday's report has clearly gotten the attention of Russian foreign policy commentators. "This is a direct challenge that Moscow cannot leave unanswered," Ruslan Pukhov, an arms expert and head of the Center for Strategies and Technologies, told the Russian business daily Kommersant, according to the NYT. Monday's NYT article also said US efforts to insert malware into Russia's energy system might jeopardize a possible Putin-Trump meeting at the G20 Summit in Japan later this month.

<https://arstechnica.com/?p=1523381>