The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia's Power Grid Is an Easy Target for U.S. Hacking

The real message U.S. officials are sending to Moscow is that Russia can be attacked without White House authorization.

By Leonid Bershidsky

June 12, 2019

AF.mil

A report in the New York Times that the U.S. Cyber Command has intensified secret efforts to hack the Russian power grid is less interesting for its content than because of U.S. officials' apparent cooperation in publicizing the activity. Like any power grid undergoing a digital transformation, the Russian one is quite hackable — but why would the U.S. want public discussion of the matter?

The New York Times story talks about "implants" — the placement of malware in networks involved in managing the Russian power grid that could be activated in case of a major conflict. It's careful to avoid any detail, but Russians know better than many others how

vulnerable power grids are to attack.

Kaspersky Lab JSC, the cybersecurity firm, has been running grid equipment hacking contests for years. In 2016, a hacking group from Yekaterinburg described in a blog post how it won points in the competition by taking over a substation and causing a short circuit on a power transmission line, without any prior knowledge of the specific industrial system or even much general understanding about how substations work.

Russian researchers have identified numerous vulnerabilities in so-called smart grid equipment, which constantly analyzes consumption data and helps manage systems flexibly and efficiently. Many elements of electrical grids are accessible from the internet. A relatively successful, and likely Russian, attack that shut down 27 substations in Ukraine in 2015 showed that primitive methods like sending spear-phishing emails to employees of regional energy companies are effective in getting hackers into parts of national grids.

Related article: Russia Thwarts U.S. Cyber Attacks on Its Infrastructure — News Agencies

The Russian grid is particularly vulnerable for several reasons. First, it's vast. Russian Grids PJSC runs 2.35 million kilometers of transmission lines and 507,000 substations. Second, it's in the process of an ambitious digital transformation. The state-controlled company's digitization plan, adopted last year, is meant to achieve major cuts in transmission losses and breakdown numbers by 2030. The plan talks about creating a cybersecurity unit, but that's a work in progress. As my colleague David Fickling has pointed out, making a grid "smart" creates new avenues of attack, and big technology rollouts can be messy and increase the risks. In the case of Russia, the problem is exacerbated by the Western origin of three quarters of all the equipment and pretty much all of the software.

If U.S. intelligence puts in the implants before the equipment is supplied or en route, there's no guarantee they can be detected.

In other words, securing the Russian grid is a mammoth task even with Russians' superior expertise when it comes to detecting (and likely exploiting) vulnerabilities. U.S. cyberattacks are certainly possible. How crippling they can be is another matter. The 2015 attack on the Ukrainian regional energy companies left some 225,000 customers without electricity for a few hours; that's not a lot of damage given the wide array of techniques involved (the attackers even flooded an energy company's call center with automated calls to make it impossible for customers to report outages). Unless critical equipment is irreparably damaged, it's usually possible to switch to manual mode, which is what the Ukrainians did.

Related article: Kremlin Says Report on Alleged U.S. Power Grid Incursion Is Worrying

It would be naive, however, to think the Russian government hasn't been worried about U.S. cyber attacks on the country's critical infrastructure. So President Donald Trump's vehement reaction to the New York Times story — he called publishing it "a virtual act of treason" in a tweet — is a little overdone. What's more telling, though, is the newspaper's response: It says the Times "described the article to the government" before publication and got no objections.

This raises the question what purpose the article might serve for the government officials who talked to the newspaper and those who vetted the publication. My theory is that they wanted to send a message to the Kremlin — but not specifically that the Cyber Command has increased its activity in the Russian power grid. The Russian political leadership, intelligence and cybersecurity professionals are already aware of these efforts.

Rather, the message concerns the approval procedure for the offensive efforts. The Times story says they occur under new, obscure legislation passed by Congress last summer that allows the defense secretary to authorize "clandestine military activity" in cyberspace without going to the president for approval. It's one thing for the Russians to know the U.S. is working to infiltrate their country's infrastructure, but quite another to be aware that intrusions and attacks don't require White House approval and can happen routinely and without much ado.

The U.S. officials are effectively telling Russian President Vladimir Putin not to remonstrate with Trump in case of attack — the U.S. president may not even know what's happening, and it'll be perfectly legal.

This article was originally posted by Bloomberg

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2019/06/12/russias-power-grid-is-an-easy-target-for-us-hacking-a66036