Fast Growth 100
Lead Generator
Marketing Support Services
Partner Programs Guide
Products of the Year
Promo Finder
Site Map
Solution Provider Locator
State of Technology
State of the Market '09
Top 25 Executives
VARBusiness 500
Vendor Content Community
White Paper Library

Cyberspies Launch Malware On U.S. Electrical Grid: Report

By Stefanie Hoffman, ChannelWeb
5:25 PM EDT Wed. Apr. 08, 2009
Cyberspies from China, Russia and other countries have hacked into the U.S. electrical grid and installed malicious software that could be used to stop power or disrupt the system, according to *The Wall Street Journal*.

Officials believe that the cyberspies intended to navigate and take control of the U.S. electrical grid. While so far no damage has been found to the grid or other national infrastructure, the *Journal* reported that the hack seems to be "pervasive," and experts say that there is a distinct possibility the software left behind by the attackers could be used for malicious purposes in times of war, according to the report.

While the cyberespionage didn't seem to target any specific company or region, some experts worry that cyberattackers could use their acquired access to take control of electricity and other systems, such as a nuclear power plant, remotely via the Web.

So far, authorities have detected software tools that could be used to destroy components of the electrical infrastructure. Meanwhile, cyberspies could also target other systems, such as water, sewage and others, with the intention of causing a major infrastructure disruption or collapse.

However, steps are being taken to remediate the problem. The strength and security of the U.S. cybersystems, which control components of the electrical grid, are now undergoing extensive scrutiny under a comprehensive cybersecurity review, ordered by President Barack Obama, scheduled for completion next week.

Congress is also weighing in on a cybersecurity bill that proposes widespread changes to the governing policies that oversee and protect the U.S. computer network infrastructure, including the appointment of a cybersecurity czar. Among other things, the legislation, developed by Senate Commerce Committee Chairman John Rockefeller IV, D-W. Va. and Sen. Olympia Snowe, R-Maine, cultivates the relationship between government and the private sector in regards to cybersecurity, and gives the federal government the authority to disconnect federal or critical infrastructure from the Internet if it was believed to be susceptible to a cyberattack.

Previously, the Bush administration had approved $17 billion in secret funds to protect government networks, according to the *Journal*.

Security experts say that the reported cyberespionage incident on the U.S. electrical grid underscores the inherent vulnerabilities and the copious security problems created when systems are linked to the Internet.

Paul Ferguson, senior threat researcher for security company Trend Micro, said that any kind of attack on infrastructure would be "pretty damn bad."

"If you're going to connect sensitive networks to the Internet, you're going to expose yourself to security problems," he said. "That same type of spyware and malware now can also ensnare any other systems linked to the Internet as well."

"I would hate to think a machine that was used to manage infrastructure could be accessed by persons

unknown in a foreign or hostile country," he added.

The recent attack on the U.S. electrical grid is not the first time that hackers have leveraged infrastructure in cyberattacks. Last year, CIA analyst Tom Donahue told attendees at a power-industry conference that cyberattacks have occurred on "multiple regions outside the United States," according to Reuters.

Meanwhile, Trend Micro's Ferguson said that he and other IT security professionals have consistently warned authorities and officials for years about the myriad potential threats created when infrastructure is controlled remotely over the Internet, but said that warnings often went unheeded in an effort to cut costs.

"What we've got here is people making business decisions in the name of cost efficiency, and adding additional risk at the security level," Ferguson said. "Those bad business decisions based on costs may come back to haunt them."

In addition, the North American Electric Reliability Corp. (NERC) issued a letter Tuesday warning the public of inherent and inevitable problems that occur when infrastructure can be operated through cyberspace.

"But as we consider cybersecurity, a host of new considerations arise," said Michael Assante, chief security operator for NERC, in the letter. "One of the more significant elements of a cyberthreat, contributing to the uniqueness of cyber-risk, is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyberattacker to impact multiple assets at once, and from a distance."

In his letter, Assante called for a "fresh, comprehensive" look at new and innovative risk-based approaches that consider the potential consequences of an attack resulting in "potential misuse" of "the entire interconnected system."

"Taking this one step further, we as an industry, must also consider the effect that the loss of that [electrical] substation, or an attack resulting in the concurrent loss of multiple facilities, or its malicious operation, could have on the generation connected to it," he said.

IT security channel partners also contend that an infrastructural attack that destroys the power grid or contaminates the water supply is a very real threat.

"Just to penetrate a network is not rocket science any more. We need rocket scientists to prevent [attackers] from doing destructive things," said Tim Carney, CEO of Fremont, Calif.-based NetworkGuys. "The good news is, we have people who realize that."

Discuss This Page

More Security | Email this article | Print this article | Bookmark this article | Digg this article | Submit to Slashdot | Reprint this article

Add Your Comment:

Login To Discuss This Page