New threat: Hackers look to take over power plants

By LOLITA C. BALDOR (AP) – August 3, 2010

WASHINGTON — Computer hackers have begun targeting power plants and other critical operations around the world in bold new efforts to seize control of them, setting off a scramble to shore up aging, vulnerable systems.

Cyber criminals have long tried, at times successfully, to break into vital networks and power systems. But last month, experts for the first time discovered a malicious computer code — called a worm — specifically created to take over systems that control the inner workings of industrial plants.

In response to the growing threat, the Department of Homeland Security has begun building specialized teams that can respond quickly to cyber emergencies at industrial facilities across the country.

As much as 85 percent of the nation's critical infrastructure is owned and operated by private companies, ranging from nuclear and electric power plants to transportation and manufacturing systems. Many of the new attacks have occurred overseas, but the latest episode magnified worries about the security of plants in the U.S.

"This type of malicious code and others we've seen recently are actually attacking the physical components, the devices that open doors, close doors, build cars and open gates," said Sean McGurk, director of control systems security for Homeland Security. "They're not just going after the ones and zeros (of a computer code), they're going after the devices that actually produce or conduct physical processes."

Officials have yet to point to any operating system that has been compromised by the latest computer worm. But cyber experts are concerned that attacks on industrial systems are evolving.

In the past, it was not unusual to see hackers infiltrate corporate networks, breaking in through gaps and stealing or manipulating data. The intrusions, at times, could trigger plant shutdowns. The threat began to escalate last year, with cyber criminals exploiting weaknesses in systems that control what the industries do.

The latest computer worm, dubbed Stuxnet, was an even more alarming progression. Now hackers are creating codes to actually take over the critical systems.

In many cases, operating systems at power plants and other critical infrastructure are decades old. Sometimes they are not completely separated from other computer networks used by companies to run administrative systems or even access the Internet.

Those links between the administrative networks and the control systems provide gateways for hackers to insert malicious codes, viruses or worms into the programs that operate the plants.

Sitting in his office not far from Homeland Security's new state-of-the-art cyber operations center, McGurk recently held out a small blue computer flash drive containing the destructive Stuxnet worm.

Experts in Germany discovered the worm, which has since shown up in a number of attacks — primarily in Iran, Indonesia, India, and the U.S., according to Microsoft. Stuxnet had tried to infect as many as 6,000 computers, as of July 15, according to Microsoft data.

German officials transmitted the malware to the U.S. through a secure network, and experts at the Energy Department's Idaho National Laboratory began to analyze it.

In plain terms, the worm was able to burrow into some operating systems that included software designed by Siemens AG, by exploiting a vulnerability in several versions of Microsoft Windows.

On Monday, Microsoft released another update to address the problem, and Siemens has taken similar steps.

Annual reports issued by Homeland Security and the Department of Energy have detailed weaknesses in the industrial computer systems, and have repeatedly pressed companies to improve security practices. Reports as recently as this May urged companies to routinely download patches to update software, change and improve passwords, carefully restrict access to critical systems and use firewalls to separate commonly used networks from those that control key systems.

A successful attack against a critical control systems, the Energy Department warned in its May report, "may result in catastrophic physical or property damage and loss."

Over the past year, Homeland Security has quietly been deploying teams of experts around the country to assess weaknesses in industrial control systems. The agency has created four teams and — with a budget scheduled to increase from $10 million this year to $15 million next year — has plans to grow to 10 teams in 2011.

The teams are armed with a $5,000 kit: a black, suitcase-sized bag crammed with cables, converters, data storage and high-tech computer forensic tools. With that equipment, they can download the problem malware, analyze it and work with the companies to correct or clean their systems.

So far, said McGurk, the teams have done 50 assessments and have been dispatched 13 times to investigate and help correct cyber incidents and attacks. Nine of those cases involved some type of deliberate cyber intrusion, while the other four were the unintended result of an operator's action.

In one of the nine intrusion cases, a company representative had gone to a conference and had the presentation documents downloaded onto a computer flash drive.

One of the files was infected with the Mariposa botnet, a malicious software code that has infected 12 million computers worldwide, including hundreds of companies and at least 40 major banks in 190 countries since appearing in December 2008.

When the man returned to his office and connected his laptop to the company's network, the botnet spread, eventually affecting nearly 100 computers.

A Homeland Security team was called in and helped the company evaluate the problem and begin to clear up the system.

___

Online:

U.S. Computer Emergency Readiness Team: http://www.us-cert.gov/control_systems/csfaq.html

Copyright © 2010 The Associated Press. All rights reserved.