

Power plants vulnerable to hackers: security firm

May 20 2011



Photo illustration of a nuclear power plant in Pottstown, Pennsylvania. US computer security research firm NSS Labs warned that it uncovered new ways that hackers could sabotage power plants, oil refineries or manufacturing operations.

US computer security research firm NSS Labs warned that it uncovered new ways that hackers could sabotage power plants, oil refineries or manufacturing operations.

"This is a global problem," NSS chief executive Rick Moy told AFP.

"There are no fixes to this right now," he continued. "Bad guys would be able to cause real environmental and physical problems and possibly loss of life."

NSS said that it shared its findings with the US Computer Emergency Readiness Team and was briefing legitimate industrial facilities that are at risk but was revealing little publicly for the sake of safety.

NSS researcher Dillon Beresford reported finding "multiple vulnerabilities" in Siemens programmable logic controllers (PLCs) used in plants worldwide to automatically regulate temperatures, pressures, turbine speeds, [robot arms](#) and more.

Those are the same devices targeted by a Stuxnet virus evidently crafted to disable an Iranian [nuclear facility](#).

While the Stuxnet virus struck at PLCs through a plant's [operating system software](#), Beresford discovered ways to reprogram the devices directly if they can be reached on a network, according to Moy.

"The security of these systems is not what it should be," Moy said.

"Comments were made that it took a nation state millions of dollars and teams of people to create Stuxnet," he continued. "We don't believe that to be true; it was not that hard to create these problems."

Beresford came up with the attacks in less than three months with a budget of \$2,000 to \$3,000 dollars, according to NSS.

NSS has shared its findings with the US [Department of Homeland Security](#) and Germany-based Siemens, which downplayed concerns that an attack could be pulled off outside the lab and said it was working to address the vulnerabilities.

(c) 2011 AFP

Citation: Power plants vulnerable to hackers: security firm (2011, May 20) retrieved 25 April

2024 from <https://phys.org/news/2011-05-power-vulnerable-hackers-firm.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.