



# NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

## Critical Infrastructure: Vulnerabilities Increasing, Risks High

July 21, 2015

*Critical infrastructure sites are increasingly vulnerable to cyberattack as the systems that run them become more accessible, interconnected, and reliant on cyberspace. The risks posed to Industrial Control System and Supervisory Control and Data Acquisition (ICS/SCADA) systems will continue to heighten as new and existing vulnerabilities are exploited by both criminal and state-sponsored threat actors.* According to incidents reported to the [Department of Homeland Security](#), the energy sector remains the most heavily targeted, and others such as water, critical manufacturing, and communications sectors are facing increased attacks. Hardware manufacturer [Dell Inc. reported](#) attacks against ICS/SCADA systems doubled in 2014; however, the NJCCIC assesses many attacks against critical infrastructure go undisclosed, or undetected, and therefore the extent of the problem is largely understated.

- [US Intelligence](#) has reported multiple state-sponsored adversaries are regularly conducting reconnaissance and developing access to critical infrastructure that could be exploited for hostile purposes. A Remote Access Trojan (RAT) known as BlackEnergy and the malware HAVEX are two known tools used to exploit vulnerabilities of ICS/SCADA systems in the US. Numerous industry reports and security researchers have attributed these tools to Russian actors, with suspected government support. A Russian information security company, GLEG, sells exploit kits used against ICS/SCADA software and one that specifically targets healthcare industry software.
- Information and tools used to conduct cyberattacks are increasingly available online, lowering the barriers for malicious actors who otherwise would not possess the technical means to penetrate critical infrastructure networks. Technical information pertaining to some ICS/SCADA systems, including schematics and default administrator passwords, is openly available on the internet or otherwise for sale on the criminal underground of the internet known as the 'deep web' or 'darknet'. SHODAN, a publicly available port scanning search engine, allows users to locate internet-connected devices and easily identify vulnerable systems to exploit within a targeted location's network.
- A recent [University of Cambridge study](#) examined the impacts of a cyberattack on the US's Northeastern electrical grid and the interdependencies between sectors, concluding an attack on the energy sector would result in devastating damages to the economy and public health. As one of the most densely populated states, with much of the nation's most critical infrastructure running through or around it, New Jersey has a uniquely high cyber-risk profile. The NJCCIC recommends that all asset owners sever any direct internet connections to control systems, properly segment operational and business networks, and patch all ICS/SCADA systems when new updates or vulnerabilities are disclosed.

### Contact Information

Any agency with comments or questions should contact [njccic@cyber.nj.gov](mailto:njccic@cyber.nj.gov) or visit [www.cyber.nj.gov](http://www.cyber.nj.gov).

Traffic Light Protocol: **WHITE** information may be distributed without restriction.