



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Addressing Vulnerabilities in Critical Infrastructure

July 21, 2016

TLP: WHITE | *The NJCCIC assesses with high confidence the greatest threats to US critical infrastructure are unpatched vulnerabilities, customized malware with no known signatures, and the compromise of user credentials to facilitate remote exploitation of network tools such as Remote Desktop Protocol.* Therefore, standard antivirus solutions and passive defense mechanisms are not sufficient to defend against the most serious threats facing Industrial Control Systems and Supervisory Control and Data Acquisition (ICS/SCADA) networks, which could result in serious consequences to utilities, communications, and transportation.

- Although attacks on critical infrastructure and key resources (CIKR) have not occurred at nearly the same frequency as cybercrimes against government and commercial entities, consequential attacks against CIKR are on the rise. On December 23, 2015, an [attack against three energy utilities in Ukraine](#) resulted in six hours of power outages impacting over 225,000 customers. In a separate incident, hackers compromised ICS/SCADA infrastructure at an [undisclosed water treatment plant](#) and were able to manipulate the level of chemicals released into the public water supply.
- Last week, cybersecurity researchers at [Kaspersky](#) released reports on the state of industrial cybersecurity. Most notably, they were able to discover 220,668 ICS components in 170 different countries via the publicly accessible Shodan search engine, 30.5 percent of which were in the United States. The use of hard-coded credentials, weak authentication, and insecure protocols increases the vulnerability and exposure of these components.
- Security researchers discovered 189 vulnerabilities in ICS components in 2015, compared to just 19 published in 2010. Only 85 percent of the vulnerabilities in 2015 were fully patched by the vendor, and there are known exploits against 26, according to [Kaspersky](#). The number of devices that were actually updated with these patches is likely much smaller, as it can prove to be exceptionally difficult, operationally and logistically, to update operational ICS components.

Further increasing the risk to CIKR networks is the availability of malware designed to exploit ICS/SCADA systems. [SentinelOne](#) researchers recently disclosed a hacking tool on a dark web forum that has targeted at least one European energy company. The malware, Furtim, reportedly has the ability to conduct reconnaissance on systems commonly integrated within the energy sector. Due to its sophistication and functionality, SentinelOne suspects the hacking tool could have been created by government-sponsored hackers.

- Furtim is a ‘dropper tool’ used for the initial compromise of a system, creating the opportunity for additional exploitation. The malware was discovered in May and targets Windows operating systems. Furtim attempts to evade detection by antivirus, sandboxes, and virtual machines and attempts to remove any antivirus software installed on the targeted system before dropping its final payload. [Furtim](#) is distributed by multiple methods including drive-by downloads, malvertising, and spam messages.

Critical infrastructure owners and operators must adopt a proactive, multi-layered cybersecurity strategy to more effectively counter the threats posed by state and non-state actors, including implementing the [ICS-CERT](#) seven strategies to defend ICS: implement application whitelisting, ensure proper configuration/patch management, reduce your attack surface area, build a defensible environment, manage authentication, implement secure remote access, and monitor and respond. More information on these strategies is found [here](#).

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