DHS: Energy Targeted by Cyber Attacks

Written by Yaron Vorona
Thursday, 24 January 2013 00:00

The Department of Homeland Security reports that in 2012, ICS-CERT responded to a steady stream of cyber incidents, coordinated ICS vulnerabilities with vendors, and produced alerts and advisories to notify the ICS community of emerging cyber risks.

For fiscal year 2012, the largest single target for cyber security incidents was the Energy sector, accounting for 41% of attacks, followed by water (15%) and internet-facing (11%).

In fiscal year 2012, ICS-CERT received and responded to 198 cyber incidents as reported by asset owners and industry partners. Attacks against the energy sector represented 41 % of the total number of incidents. Notably, ICS-CERT assisted 23 ONG sector organizations with incident response and recovery efforts following a targeted spear-phishing campaign. Analysis of the targeted systems indicated that information pertaining to the ICS/SCADA environment, including data that could facilitate remote unauthorized operations, was exfiltrated. ICS-CERT worked closely with many of the involved organizations and during the course of this response effort, analyzed over 50 malware samples and malicious files, 20 emails, and 38 hard drive images to determine the extent of the compromise and identify the techniques and tactics used the threat actors. ICS-CERT also deployed onsite incident response teams to assist 2 organizations that were compromised as a result of this campaign. Source [pdf]