New Report Highlights Cyber Threat to US Electric Industry

As evidence that cyberattacks continue to threaten electric infrastructure in the United States, a report issued in December by cybersecurity firm FireEye indicates that critical infrastructure industrial control systems (ICS) could be susceptible to a new type of malware, reports Morgan Lewis in its **Power & Pipes** blog.

According to the report, a piece of malware called “TRITON” triggered the emergency shutdown capability of an industrial process within a critical infrastructure ICS.

“In 2013, hackers believed to be operating on behalf of a state-actor managed to take partial control of the Bowman Avenue Dam near Rye Brook, New York. More recently, reports emerged this past summer that hackers gained access to the operational grid controls of US-based energy firms,” write **J. Daniel Skees** and **Arjun Prasad Ramadevanahalli**.

Read the article.