Potent malware targets electricity systems

June 12 2017

New malware can take control of electricity substation switches and circuit breakers by accessing their decades-old communication protocols

Hackers have developed powerful malware that can shut down electricity distribution systems and possibly other critical infrastructure, two cyber security firms announced Monday, with one report linking it to Russia.

Slovakia-based ESET said the malware is the most powerful threat to appear since Stuxnet, the hacking tool used to sabotage Iran's nuclear program believed developed by US and Israeli intelligence.

ESET said the malware, which it dubbed Industroyer, may be behind the one-hour shutdown of power to the Ukraine capital Kiev last December.

The company said Industroyer's potent threat is that it works using the communication protocols designed decades ago and built into energy, transportation, water and gas systems around the world.

Making use of these poorly-secured protocols, Industroyer can take direct control of electricity substation switches and circuit breakers, giving hackers the ability to shut down power distribution and damage equipment.

The malware is the "biggest threat to industrial control systems since Stuxnet," ESET said, without indicating who was behind it.

But in a separate report on the same malware Monday, a second cyber security company, Dragos, tied it to a Russian hacker group called Sandworm which has been linked to the Russian government.

Dragos gave its own name to the malware, "CrashOverride," and said it is only the second-ever malware deployed for disrupting physical industrial processes, after Stuxnet.

"CrashOverride is not unique to any particular vendor or configuration, and instead leverages knowledge of grid operations and network communications to cause impact," Dragos said.

"In that way, it can be immediately re-purposed in Europe and portions of the Middle East and Asia."

In addition, it said, the malware could be adapted "with a small amount of tailoring" to render it potent against the North American power grid.

It said that the malware can be applied to work at several electricity substations at the same time, giving it the power to create a widespread power shutdown that could last for hours and potentially days.

Dragos said it had "high confidence" the malware was behind the power outage in Kiev on December 17.