June 19, 2017

CRASHOVERRIDE, The Latest Malware Menacing the Electric Grid

Sophisticated offensive cyber capabilities can be directed against major critical infrastructure, and very recently just such a potential "cyber weapon" has been discovered. Malware developed over years has been uncovered; it has the potential for catastrophic disruption of a variety of infrastructure, most immediately, the electric grid. Those many businesses relying on the internet for their operations would do well to ensure they understand and work to defend against this malware.

Last week, the Maryland-based cybersecurity firm Dragos (a leading firm created by former Department of Defense cyber experts) issued a report titled *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations.* The report details Dragos' finding of a new, tailored malware. Although related to the malware employed in the 2016 Ukraine electric cyber attack, this new malware is of particular concern, according to Dragos, because "there is no simple fix to the capability…. It cannot just be patched or architected away." The malware, which Dragos calls CRASHOVERRIDE, appears to be the "first ever malware framework designed and deployed to attack electric grids."

A copy of the full Dragos report, which is currently being reported on by the media, is available on the Dragos website or by clicking here.

Although the report is somewhat technical, the basics are clear. Infrastructural elements, such as the electric grid, are managed through a digital network, often called the Industrial Internet of Things (IIoT). The IIoT, like its cousin the Internet of Things, is based on networked communications, which allow various physical devices to talk to each other, respond to data from sensors and obey human commands. Many people are familiar with home items such as digitally networked thermostats that can respond to temperature sensors, electric load and user preferences, or refrigerators that can tell when the milk spoils. The IIoT is that, but on a national scale, and instead of your home heater or fridge, the network controls huge switching stations and key parts of power generator stations. Bad things can happen if the Internet of Things is hacked or damaged (your milk may spoil, or your identity may be stolen), but potentially catastrophic results could flow from disruption of the IIoT: We may lose power for hours or days, oil rigs may shut down, and generating plants could be shut down or, worse, damaged beyond repair. The Dragos report, although still preliminary, indicates the significance of these risks.

Day Pitney's Cybersecurity and Data Protection practice group has been particularly focused on the IIoT and will continue to monitor this matter. If you need help understanding or navigating the evolving risks associated with the IIoT, please contact Steven Cash or Daniel Wenner.

Authors



David T. Doot
Of Counsel

Hartford, CT | (860) 275-0102

dtdoot@daypitney.com



Evan C. Reese III
Partner

Washington, D.C. | (202) 218-3917

ereese@daypitney.com



Patrick M. Gerity
Counsel

Hartford, CT | (860) 275-0533

pmgerity@daypitney.com