



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Energy: Cyber Attack Implicated in Ukraine Power Outage

January 7, 2016

TLP: WHITE | *Intelligence agencies and cybersecurity researchers are investigating a power outage that occurred in Western Ukraine on December 23, specifically whether or not malware discovered on the targeted utility's network played a direct role in impacting the electric grid.* If malware is confirmed to have caused the outage, as opposed to human error or equipment failure, this would mark the first documented power disruption resulting from a cyber attack. While attribution, motive, and technical details of this incident remain unclear, Ukraine's intelligence service was quick to publicly blame the Kremlin, and ongoing tensions with Russia further speculation of state-sponsorship. International media sources have identified the malware as BlackEnergy, a trojan previously discovered on critical infrastructure systems throughout the United States and linked to an advanced persistent threat (APT) group known as Sandworm, widely reported as a Moscow-backed actor. Though this incident was likely targeted, posing no direct threat to US infrastructure, it underscores the susceptibility of industrial control systems (ICS) that distribute critical resources such as energy, water, transportation, and communications. Moreover, it demonstrates the willingness of sophisticated threat actors, whether state-sponsored or inspired, to conduct attacks which can impose significant consequences on civilian populations, as well as governments.

- The malware recovered from the Ukrainian power company's network was [identified as KillDisk](#) and reported to be a component of BlackEnergy designed to overwrite data and render systems unbootable. [Reports](#) indicate similar malware was also identified on the networks of at least two other Ukrainian utilities, as well as an indication that a spear-phishing email was used to deliver the malware, including an attached [Microsoft Excel spreadsheet containing malicious macros](#). It is unclear as to what infection vectors were used in this incident, and while spear-phishing is a common and likely vector, others such as [watering-holes](#), [exploit kits](#), or physical introduction to the network via removable media are possible.
- In November 2015, multiple [Ukrainian media organizations were reportedly attacked](#) with BlackEnergy malware—specifically the destructive KillDisk component—during the country's local elections in October, leading to the loss of video content and other data. Analysis of the latest version of KillDisk revealed [new functionality](#), including a set time delay for when to initiate, anti-forensic capabilities to delete Windows Event Logs, and the ability to terminate and overwrite specific processes, potentially designed to sabotage targeted industrial systems.
- Multiple iterations of BlackEnergy have been in [circulation since 2007](#), exchanged on dark web forums and black market sites attributed to [Russian cyber actors](#). In 2014, the Department of Homeland Security's ICS Computer Emergency Response Team (ICS-CERT) reported that, since 2011, BlackEnergy infected numerous US critical infrastructure sectors by exploiting at least three Human Machine Interface devices: [GE Cimplicity](#), [Advantech/Broadwin WebAccess](#), and [Siemens WinCC](#)

The NJCCIC advises all critical infrastructure owners and operators to implement defense-in-depth strategies as outlined by ICS-CERT, which provides detailed best practices for securing ICS networks, including, but not limited to: [Seven Steps to Effectively Defend ICS](#), [Improving ICS Cybersecurity, Guide for Firewall Deployment](#), [Patch Management for Control Systems](#), and [Developing an Incident Response Capability](#).

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