CYBER ATTACKS ON THE UKRAINIAN GRID: WHAT YOU SHOULD KNOW

INTRODUCTION

In the first publicly documented power outage attributed to a cyber attack, Russian-nexus actors caused blackouts in several regions in Ukraine. The actors used spear phishing to plant BlackEnergy3 malware, which was used to disable control system computers. As a result, the utilities relied on manual efforts to restore power.

Ukrainian power companies are not unique in their control systems technology or vulnerabilityto cyber attack. BlackEnergy3 has also been found within organizations that operate critical infrastructure in the United States and abroad. Power companies around the world should review the security architecture of ICS networks, log and monitor ICS events and traffic, search for indicators of compromise, and prepare incident response plans.

What happened?

On Dec. 23, 2015, three regional Ukrainian electricity distribution companies – Kyivoblenergo, Prykarpattyao-blenergo and Chernivtsioblenergo – suffered power outages due to a cyber attack. Ukrainian sources reported finding the BlackEnergy3 malware within the utilities' systems. Responders also found a wiper module called killdisk that was used to disable both control and non-control systems computers. At the same time, the attackers overwhelmed utility call centers with automated telephone calls, impacting the utilities' ability to receive outage reports from customers and frustrating the response effort.

FireEye

While killdisk does not have the functionality to open breakers – which would cause the outages – it would impede utility visibility of breaker status, and inhibit remote control of the substations. This suggests that the attackers used another method to cause the power outage, perhaps using interactive access via compromised corporate and SCADA accounts to remotely open individual breakers or initiate load shedding, sending simultaneous trip commands to multiple breakers.

Who is behind this attack?

BlackEnergy malware is a tool that first appeared in the Russian underground for use in distributed denial-of-service attacks. A later variant called BlackEnergy2 added credential theft functionality useful for cyber crime. BlackEnergy3 is a distinctive tool only used by the Sandworm team for cyber espionage. Documents recovered from an open command and control server indicate that Russian speakers operate the tool.

BlackEnergy3 is a distinctive tool only used by the Sandworm team for cyber espionage.

A list of Sandworm victims aligns with interests of the Russian state. In October 2014, iSIGHT Partners noted the Sandworm Team targeting NATO and European governments, including Ukraine, while relying on a zero-day vulnerability.

Additional investigations by iSIGHT Partners revealed BlackEnergy modules targeting industrial control systems software from several leading vendors, indicative of preparation for an attack on industrial systems.

In August 2015, iSIGHT Partners reported BlackEnergy3 had been found within Ukrainian utilities as early as the preceding March. In November 2015, iSIGHT warned that given the geopolitical situation between Ukraine and Russia, ICS-related attacks were foreseeable.

How can electric utilities protect themselves?

In December 2014, ICS-CERT indicated that BlackEnergy had been found on control system networks in the United States. As utilities in diverse geographies rely on the same technological approaches that made the Ukrainian firms susceptible to attack, we recommend four fundamental practices:

Review SCADA/ICS security architecture. Experienced and qualified ICS security professionals should regularly review ICS network architecture including VPN configuration, firewall placement and rules, and router access control lists. Utilities in North America should recognize that the Ukrainian attacks affected distribution providers, which are not subject to NERC CIP cyber security regulations.

Enhance network security monitoring capability. Robust log collection and network traffic monitoring are the foundational components of a defensible ICS network. Failure to perform these essential security functions prevents timely detection, pre-emptive response, and accurate incident investigation.

Search for Indicators of Compromise. With network security monitoring capability in place, automated tools can alert security analysts and process operators when anomalous behavior or ICS-oriented malware, such as BlackEnergy3, is identified in your environment.

Review Incident Response Plans. While electric utilities frequently and capably respond to outages caused by weather or equipment failure, they must now construct and test response plans for cyber attack. The plans should cover response protocols for realistic scenarios such as the wiper malware seen the Ukraine attacks.

How can FireEye help?

FireEye combines our deep knowledge of threat actors and experience responding to security incidents with ICS domain expertise to help organization improve their prevention, detection and response capabilities for ICS.

AREA	FIREEYE CAPABILITY
Technology	FireEye solutions such as PX, TAP, and FireEye as a Service provide agentless visibility and monitoring for Industrial Control Systems environments.
Intelligence	iSIGHT Partners offers unparalleled collection and analysis, resulting in accurate forewarning and precise understanding of the evolving threat landscape.
Expertise	Mandiant's specialized Industrial Control Systems Security Consulting team includes engineers, ICS software security specialists, and published experts, who have significant experience shaping ICS cyber security programs across industry verticals.

Contact us if your organization needs immediate assistance for a possible incident or security breach

call: +1 (866) 962-6342

email: investigations@mandiant.com

For more information, visit our ICS Gap Assessment web page.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 / 408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com