

# Ukraine's power outage was a cyber attack: Ukrenergo

[reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA](https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA)

Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes



Technology News  
Updated

By Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes

3 Min Read

KIEV/MILAN (Reuters) - A power blackout in Ukraine's capital Kiev last month was caused by a cyber attack and investigators are trying to trace other potentially infected computers and establish the source of the breach, utility Ukrenergo told Reuters on Wednesday.

Dispatchers are seen inside the control room of Ukraine's National power company Ukrenergo in Kiev, Ukraine, October 13, 2016. REUTERS/Valentyn Ogirenko

When the lights went out in northern Kiev on Dec. 17-18, power supplier Ukrenergo suspected a cyber attack and hired investigators to help it determine the cause following a series of breaches across Ukraine.

Preliminary findings indicate that workstations and Supervisory Control and Data Acquisition (SCADA) systems, linked to the 330 kilowatt sub-station “North”, were influenced by external sources outside normal parameters, Ukrenergo said in comments emailed to Reuters.

“The analysis of the impact of symptoms on the initial data of these systems indicates a premeditated and multi-level invasion,” Ukrenergo said.

Law enforcement officials and cyber experts are still working to compile a chronology of events, draw up a list of compromised accounts, and determine the penetration point, while tracing computers potentially infected with malware in sleep mode, it said.

The comments make no mention of which individual, group or country may have been behind the attack.

“It was an intentional cyber incident not meant to be on a large scale... they actually attacked more but couldn’t achieve all their goals,” said Marina Krotofil, lead cyber-security researcher at Honeywell, who assisted in the investigation.

In December 2015, a first-of-its-kind cyber attack cut the lights to 225,000 people in western Ukraine, with hackers also sabotaging power distribution equipment, complicating attempts to restore power.

Ukrainian security services blamed that attack on Russia.

In the latest attack, hackers are thought to have hidden in Ukrenergo’s IT network undetected for six months, acquiring privileges to access systems and figure out their workings, before taking methodical steps to take the power offline, Krotofil said.

“The team involved had quite a few people working in it, with very serious tools and an engineer who understands the power infrastructure,” she said.

The attacks against Ukraine’s power grid are widely seen by experts as the first examples of hackers shutting off critical energy systems supplying heat and light to millions of homes.

Writing by Oleg Vukmanovic; reporting by Pavel Polityuk in Kiev, Oleg Vukmanovic and Stephen Jewkes in Milan; editing by Susan Fenton/Ruth Pitchford

Our Standards: [The Thomson Reuters Trust Principles.](#)

for-phone-onlyfor-tablet-portrait-upfor-tablet-landscape-upfor-desktop-upfor-wide-desktop-up