The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Firm Blames Russian 'Sandworm' Hackers for Ukraine Power Outage

By The Moscow Times

January 08, 2016

U.S. cyber intelligence firm iSight Partners said on Thursday it has determined that a Russian hacking group known as Sandworm caused last month's unprecedented power outage in Ukraine.

"We believe that Sandworm was responsible," iSight's director of espionage analysis, John Hultquist, said in an interview.

The conclusion was based on analysis of malicious software known as Black Energy 3 and KillDisk, which were used in the attack, and intelligence from "sensitive sources," he said.

The Dec. 23 outage at Western Ukraine's Prykarpattya Oblenergo cut power to 80,000 customers for about six hours, according to a report from a U.S. energy industry security group.

Ukraine's SBU state security service has blamed Russia, but the nation's Energy Ministry said it would hold off on attribution until after it finishes a formal probe.

Other firms have linked that malware to the attack. But iSight is the first firm to so confidently assert that Sandworm was responsible.

ISight said it is not clear whether Sandworm is working directly for Moscow. The group is named Sandworm because references to the "Dune" science-fiction series are embedded in its malware.

"It is a Russian actor operating with alignment to the interest of the state," Hultquist said. "Whether or not it's freelance, we don't know."

To date, it has primarily engaged in espionage, including a string of attacks in the United States using Black Energy that prompted a December 2014 alert from the Department of Homeland Security, according to iSight.

That alert said a sophisticated malware campaign had compromised some U.S. industrial control systems. A DHS spokesman declined to comment Thursday on iSight's findings.

While no outages or physical destruction was reported in conjunction with those attacks in the United States, some experts said that may be simply because the attackers did not want to go that far.

"It's not a major stretch to conclude the difference in the outcomes of the attacks in the Ukraine versus those in the United States were an issue of intent not capability," said Eric Cornelius, managing director of cyber security firm Cylance Inc and former DHS official responsible for securing critical infrastructure.

"It would be naive to say the same attackers couldn't successfully execute in the United States," said Chris Blask, executive director of the Industrial Control System Information Sharing and Analysis Center.

ISight said Sandworm was also behind previously reported attacks on Ukrainian officials, EU and NATO members as well as media companies in Ukraine.

Original url:
https://www.themoscowtimes.com/2016/01/08/us-firm-blames-russian-sandworm-hackers-for-ukraine-power-outage-a51394