The 2016 Ukraine Power Grid Hacks

Overview:

In 2016 the Russian state-sponsored group of hackers called “Sandworm” hacked into Prykarpattyaoblenergo utility, a power company in western Ukraine. They used a type of hacking called “spear-phishing” to disrupt the power plants operations and caused a blackout that affected hundreds of thousands of Ukrainians for around 6 hours. The group orchestrated the attack for political reasons.

Tech Flaws:

The hacker group responsible for the attack prepared for months in advance. It is considered a more sophisticated attack, since the group was well funded and state sponsored. “Spear-phishing” emails were used to compromise corporate networks with malware. Workers at the power company were able to log in remotely to the SCADA network which controlled the grid and they weren’t required to use two-factor authentication. This allowed the hackers to hijack their credentials and gain access.

Solution Implemented:

Another attack was attempted in a similar fashion in 2022 as an act of terrorism during Russia’s invasion of Ukraine. This time it was thwarted for the most part. Cybersecurity groups have analyzed the malware used by Sandworm called “industroyer” and developed tools to fight against it. With attacks this sophisticated it’s difficult to create fool-proof solutions though.

References:

<https://www.wsj.com/articles/ukraine-thwarts-cyberattack-on-electric-grid-officials-say-11649794612>

<https://www.bbc.com/news/technology-35297464>

<https://www.bbc.com/news/technology-61085480>