Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again

Published: 2022-11-28 · Archived: 2026-04-05 16:41:38 UTC

Industroyer2 – a new version of the only malware to ever trigger electricity blackouts – was deployed in Ukraine amidst the ongoing Russian invasion. Like in 2016 with the original Industroyer, the aim of this recent cyberattack was to cause a major blackout – this time against two million+ people and with components amplifying the impact, making recovery harder. We believe the malware authors and attack orchestrators are the notorious Sandworm APT group, attributed by the US DoJ to Russia's GRU. Our talk covers the technical details: our reverse engineering of Industroyer2, and a comparison with the original. Industroyer is unique in its ability to communicate with electrical substation ICS hardware – circuit breakers and protective relays – using dedicated industrial protocols. While Industroyer contains implementations of four protocols, Industroyer2 "speaks" just one: IEC-104. Presented by Robert Lipovsky & Anton Cherepanov Full Abstract & Presentation Materials: https://www.blackhat.com/us-22/briefi...
