Recorded Future Intelligence Brief: Attack on Ukrainian Critical Infrastructure

February 22, 2016

Executive Summary:

Unauthorized access to Ukrainian critical infrastructure systems left 200,000+ citizens without power for several hours on December 23, 2015.

The strategically sophisticated attack utilized multiple attack vectors and tools. A spear phish email was used to deliver the BlackEnergy Trojan, which enabled persistent access to Ukrainian industrial control system (ICS) networks. A data destroying component KillDisk was used to erase system logs while a Distributed Denial of Service (DDoS) was conducted to disrupt telecommunication services and delay response. Finally, a previously unknown backdoor in the OpenSSH protocol Dropbear was used to pass data. The unauthorized users manipulated a human-machine interface (HMI) to physically switch relays off and disrupt power.

Although no definitive attribution has been made, the attack's sophistication and coordination implies it was carried out by a nation-state sponsored group. Notably, the source code for most of the attack components is available for purchase and download on the open Web, and it's no longer far fetched that a similar attack could be conducted by non-nation-state sponsored groups for criminal purposes.

Incident Highlights:

- **Event Category**: Critical Infrastructure Breach
- **Attack Method(s)**: Spear phish, Trojan, DDoS, Zero-day vulnerability
- **Severity**: High
    - Power disrupted for 200,000+ Ukrainian citizens.
    - Latest proof that malware can have tangible physical effects.
- **Actor(s)**: Unknown. Suspected Russian nation-state sponsored (Sandworm).
- **Response**: The Ukrainian government noted Russian infrastructure used in the attack but has not directly accused the Russian government; responses from U.S. officials have ranged from pointed implication of Russia to hesitation over inconclusive evidence.
- **Recommended Actions**:
    - End-user education remains paramount to preventing unauthorized access.
    - Disallow emails with embedded macros.
    - Utilize IP and port whitelisting and blacklisting.
    - Adhere to data redundancy and offsite storage best practices.