Targeting the Ukrainian Electrical Grid

Ryan Dozier, William Droge, Kyle Krause, Danniel Wayland

Threat Intelligence 100

Secure|Set Acedemy

A. Dubey

October 18, 2019

(synopsis)

Identifing Russian Objectives (Droge)

Russian Targeting Development (Wayland)

Russian Targeting Plan (Wayland)

*Identify your targets by type (e.g. Deliberate / Dynamic, etc).*

Key Cyber Terrain used by Russians (Droge)

*Reconnaissance/ Weaponization/ Delivery/ Exploitation/ Installation/ C2/ Action*

Russian information requirements (IR)s (Dozier)

1. Ukrainian electrical grid system overview.

2. Ukrainian Entry and Exit nodes to ISP for all electrical systems to be attacked.

3. Private internal routing systems, i.e. SCADA networks, fiber, microwave communication between sites.

4. Allow work from home access, VPN.

5. Vulnerability to a spear-phishing campaign to install malware to allow for persistent access and command and control.

6. Common operating systems, types of firmware to target and weaponize malware for most effective coverage of systems.

Annex A : Russian CCIRs, PIR, FFIR, and EEFI (Dozier)

**CCIR**

**PIR**

1. Intrusion Detection Systems/Firewalls

2. Mean time to detection

3. Actions on objective after reconnaissance

**FFIR**

1. Ability to maintain access without detection

2. Ability to deploy wide accessing malware that can control multiple operating systems

3. Types of communication internal to the Ukrainian network

**EEFI**

1. Who is targeting the electrical grid

2. Non-attribution of malware signature

Annex B: Russian Collection Synchronization Plan (Krause)

*Use the example in the slide deck as the baseline. Use the references provided in the reading for further explanation. This will be*

References