A Tale of Two Indestroyers: It was the Season of Darkness
“By using terror and cold, the Russians want to break our spirit and unity. They believe that cold will become their most effective weapon of subjugation, so they are trying to destroy our power generation facilities. They are also trying to break up our national power grid by targeting substations so that even if there is power, it cannot be transferred from one part of the country to another”

- Yaroslav Demchenkov, Ukraine’s deputy energy minister

A timeline between Russia and Ukraine

1992: Treaty of Friendship

2004: The Orange Revolution in Ukraine

2008: Ukraine applies for NATO membership

2014 (Feb-Mar): Russia annexes Crimea

2014 (Jul): Malaysian airlines flight shot down over eastern Ukraine

2015: Cyberattack against Ukraine’s power grid

2016: Use of Industroyer in cyberattack

2018: Russian cyberattacks on Ukrainian government websites

2021: Cyberattacks against Ukrainian government websites

2022: Use of Industroyer 2 in cyberattack during military operation

Rising tension

Military operations

Cyber warfare
The power grid

Two primary objectives:
- Synchronized generation
- Power transmission

Control Room

Generation  Transmission Substation  Distribution Substation
Synchronization

Try to keep all the generated energy at the same frequency and voltage.
Power transmission

• Balance the produced energy with the consumption

• Send the energy where needed
Substation communications

- Control Room
- Substation
- Remote Terminal Unit
- Intelligent Electronic Devices
  - IEC-101
  - IEC-104
  - GOOSE (IEC-61850)
  - MMS (IEC-61850)
Most reasonable target to cause a blackout
Military strikes against power facilities (Oct 2022)

<table>
<thead>
<tr>
<th>Substations</th>
<th>Power plants</th>
<th>Administrative buildings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lviv oblast</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Dnipropetrovsk oblast</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Khmelnytskyi oblast</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Kharkiv oblast*</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Kyiv</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Kirovohrad oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Kyiv oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Mykolaiv oblast*</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Rivne oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Sumy oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Vinnytsia oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Volyn oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Zhytomyr oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Zaporizhzhia oblast*</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Ivano-Frankivsk oblast</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Kherson oblast*</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Verified incidents of damage by oblast (Oct/2022 – Apr/2023)

2015 Attack

Known exploit

Remote desktop

HMI

Manual control
How to safely study a malware targeting a physical system?

- Binary analysis
  - (Encryption / Obfuscation techniques)
- Reverse engineering / Disassembly
- Identify system calls
- Execution in a sandbox
  - Execution analysis
  - Network analysis
    - Traffic / Protocol analysis
    - Behavioral analysis (Industrial Control - centered)

Previous efforts
Safely testing the malware
Sandbox architecture
Industroyer 1 a.k.a. CrashOverride (2016)

Communication with C&C

Main Backdoor

Additional Backdoor

Launcher

Orchestration & Cleanup

Data Wiper

Payloads for each Industrial Control protocol:

- IEC-104
- IEC-101
- OPCDA
- IEC-61850 (MMS)
Deployment
Remote attack

- Configurable targets
- Configurable attack pattern
- Multi-threaded attack
Local attack

- Semi-autonomous attack
- Scanning capabilities
- No configuration needed
Industroyer 2 (2022)

- Stand-alone executable
- Hard-coded configuration
- Single communication protocol (IEC-104)
- Single-shot attack (No infinite loop)
Industroyer 2 deployment
Timing

Each payload has a different timing and behavior.
Evolution of Russian cyber attacks

- 2015 - Remote access attack
- 2016 - Industroyer 1 Various payloads
- 2016 - Industroyer 2 Targeted payload
- 2022 - Industroyer 2 Targeted payload
- 2022 - Industroyer 2 Semi-Autonomous
- 2023 - Malicious MicroSCADA scripts
Questions?