

Oblenergo Attack Analysis

Russian Power Grid Attack

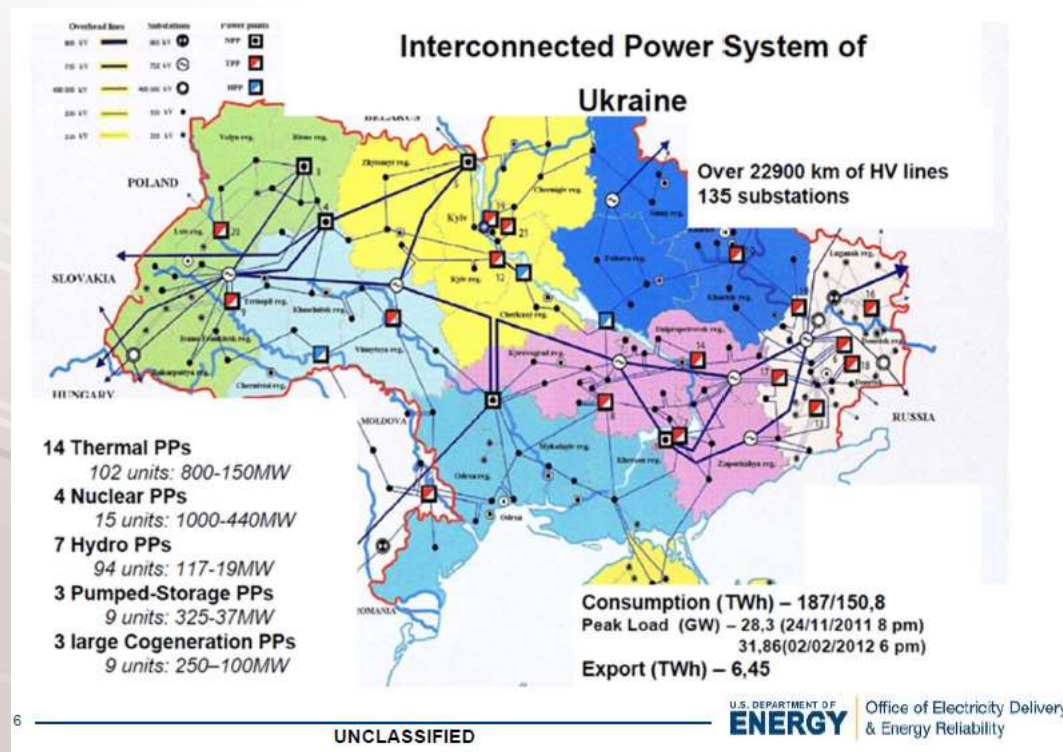


Ukraine Oblenergo Attacks

- What the HECK is an Oblenergo?
- The ICS Kill Chain
- Attack Rating
- Defending

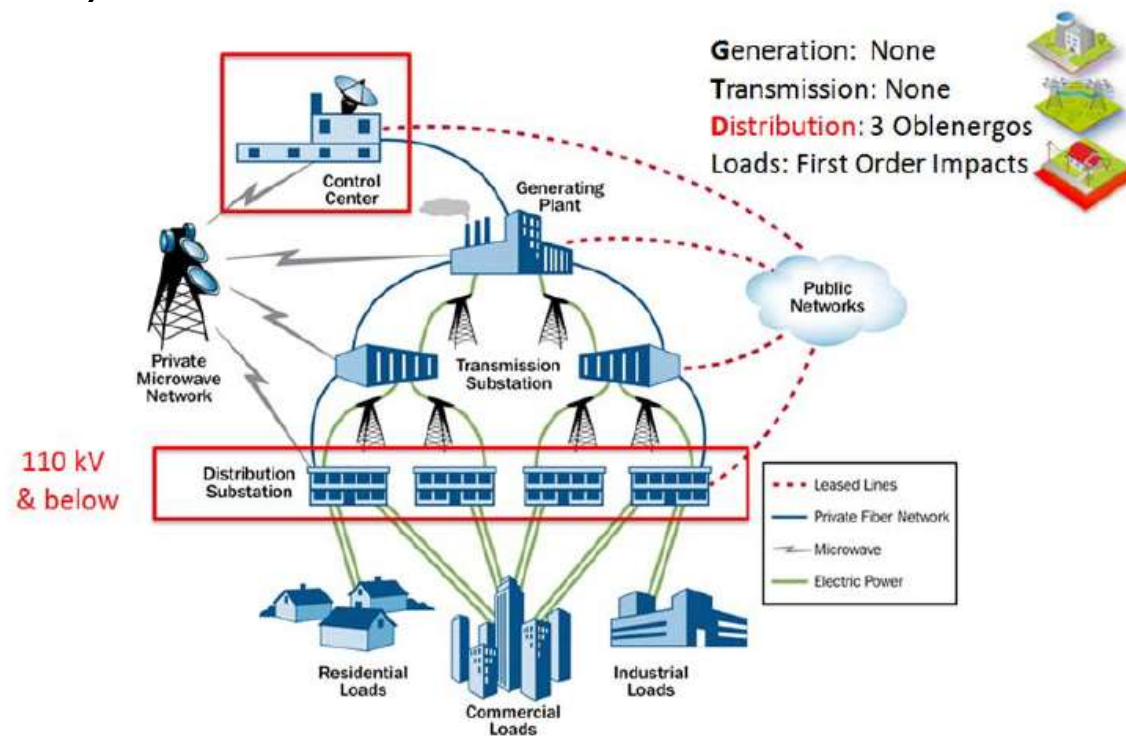
An Oblenergo is a ...

- Regional power distribution entity.
- This matters because the attackers disrupted 3 different oblenergos ... it would be similar to attacking OPPD, NPPD, and MidAmerican at the same time.



The ICS Kill Chain

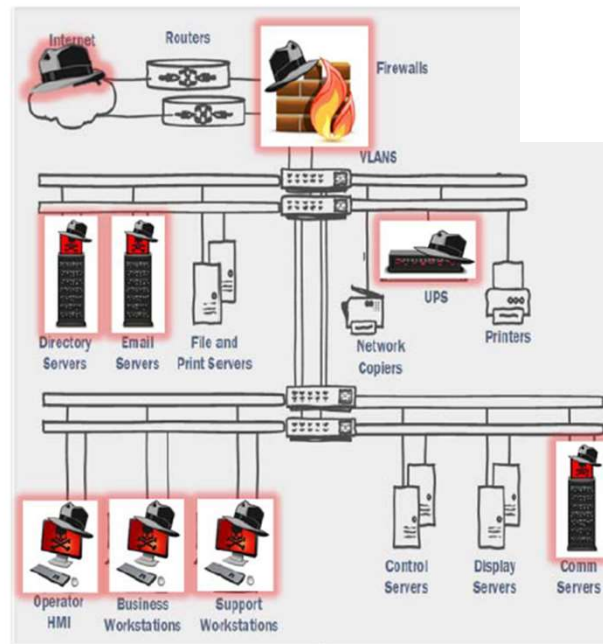
- Targeted the distribution networks (impacted 225,000 customers)



Source: Modification of an image from the energy sector - specific plan 2010

Attack Steps Summary

- Infect, Foothold, C2
- Harvest Credentials
- Achieve Persistence & IT Control
- Discover SCADA, Devices, Data
- Develop Attack Concept of Operation (CONOP)
- Position
- Execute Attack
 - SCADA/DMS Dispatcher Client/WS Hijacking
 - Malicious firmware uploads
 - KillDisk Wiping of WS & Servers
 - UPS Disconnects & TDoS

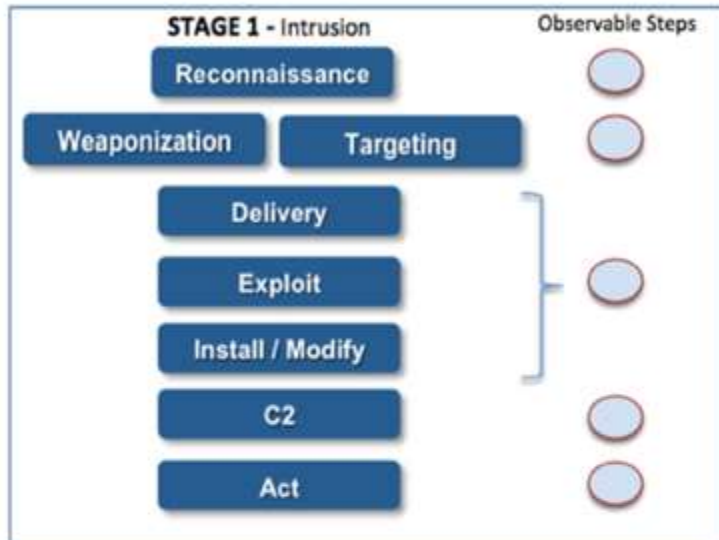


UNCLASSIFIED

p0wnd

Technical Components

- Spear phishing to gain access to the business networks
- Identification of BlackEnergy 3 at each Oblenergos
- Adversary theft of credentials from the business networks
- Use of VPNs to enter the ICS network
- Use of existing remote access tools within the environment or issuing commands directly from a remote station capable of issuing commands similar to an operator HMI
- Serial to Ethernet communications devices impacted at a firmware level
- Use of a modified KillDisk to erase
- Utilizing UPS systems to impact connected load with a scheduled service outage
- Telephone Denial of Service attack on the call center



APT



Attack with Impact



Phishing E-mails

BlackEnergy 3

VPN & Credential Theft

Network & Host Discovery



Malicious Firmware Development

SCADA Hijack (HMI/Client)

Breaker Open Commands

UPS Modification
Firmware Upload

KillDisk Overwrites



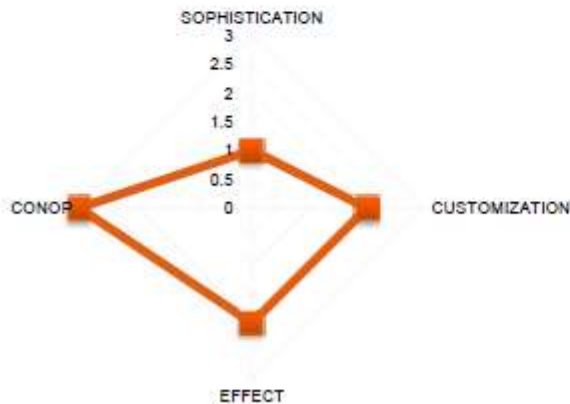
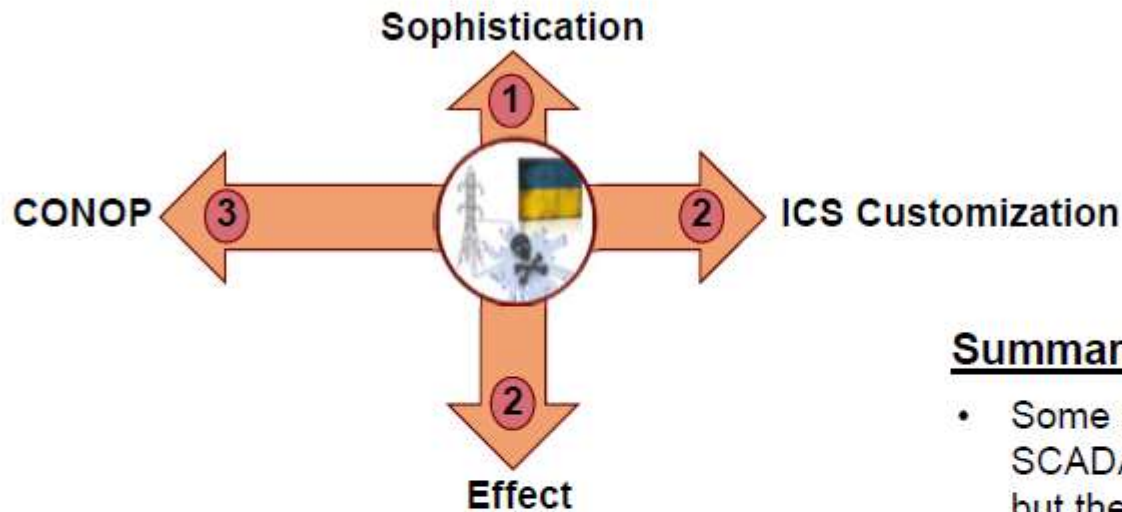
Power Outage(s)

How Sophisticated Was It?

RESPONSE: Just enough



Rating this Attack



Summary

- Some sophistication in the SCADA/DMS hijacking method but the majority of it was not
- Rogue client hijacking demonstrated some customization
- Electricity outage in three service territories restored in hours
- A complex and successful attack plan

Mitigation

| | | |
|--|--|--|
| <h3>Spearphish</h3> <ul style="list-style-type: none"> Training <ul style="list-style-type: none"> Awareness training Phishing testing Remediate <ul style="list-style-type: none"> YARA & AV Change PW Anticipated <ul style="list-style-type: none"> Contested territory Isolate and control Filtering <ul style="list-style-type: none"> Detection Based Reputation Based <p>UNCLASSIFIED</p> <p>U.S. DEPARTMENT OF ENERGY Office of Electricity Delivery & Energy Reliability</p> | <h3>Credential Theft</h3> <ul style="list-style-type: none"> Remediate <ul style="list-style-type: none"> YARA & AV Change PW Defense in Depth <ul style="list-style-type: none"> Directory Segmentation Zones of Trust Anticipated <ul style="list-style-type: none"> Normalize net and directory activity Alert on the abnormal Trust <ul style="list-style-type: none"> Jump Host No Split Tunneling <p>UNCLASSIFIED</p> <p>U.S. DEPARTMENT OF ENERGY Office of Electricity Delivery & Energy Reliability</p> | <h3>VPN Access</h3> <ul style="list-style-type: none"> Strengthen <ul style="list-style-type: none"> Two factor Dedicated Tokens Trust <ul style="list-style-type: none"> Jump Host No Split Tunneling Anticipated <ul style="list-style-type: none"> Why is it there Activate at time of use Trust <ul style="list-style-type: none"> Jump Host No Split Tunneling <p>UNCLASSIFIED</p> <p>U.S. DEPARTMENT OF ENERGY Office of Electricity Delivery & Energy Reliability</p> |
| <h3>Remote Access</h3> <ul style="list-style-type: none"> Harden <ul style="list-style-type: none"> Disable remote access Block at perimeter fw Manage <ul style="list-style-type: none"> Configure Host FW Monitor config changes Anticipated <ul style="list-style-type: none"> Conservative operations Sectionalizing Manage <ul style="list-style-type: none"> Configure Host FW Monitor config changes <p>UNCLASSIFIED</p> <p>U.S. DEPARTMENT OF ENERGY Office of Electricity Delivery & Energy Reliability</p> | <h3>Control</h3> <ul style="list-style-type: none"> App Security <ul style="list-style-type: none"> Logic for confirmation AOR Communication <ul style="list-style-type: none"> Path encryption Protocol encryption Anticipated <ul style="list-style-type: none"> Manual operations Load Shed Communication <ul style="list-style-type: none"> Path encryption Protocol encryption <p>UNCLASSIFIED</p> <p>U.S. DEPARTMENT OF ENERGY Office of Electricity Delivery & Energy Reliability</p> | <h3>Tools and Tech</h3> <ul style="list-style-type: none"> Eliminate <ul style="list-style-type: none"> Filter calls by source Disconnect BCS from net Disable remote mgmt Device <ul style="list-style-type: none"> Disable remote FW updates ATS, Backup Gen Secondary Comms Anticipated <ul style="list-style-type: none"> Blackstart plans Islanding Mutual Aid Device <ul style="list-style-type: none"> Disable remote FW updates ATS, Backup Gen Secondary Comms <p>UNCLASSIFIED</p> <p>U.S. DEPARTMENT OF ENERGY Office of Electricity Delivery & Energy Reliability</p> |



ПИТАННЯ Questions

