Oblenergo Attack Analysis

Russian Power Grid Attack

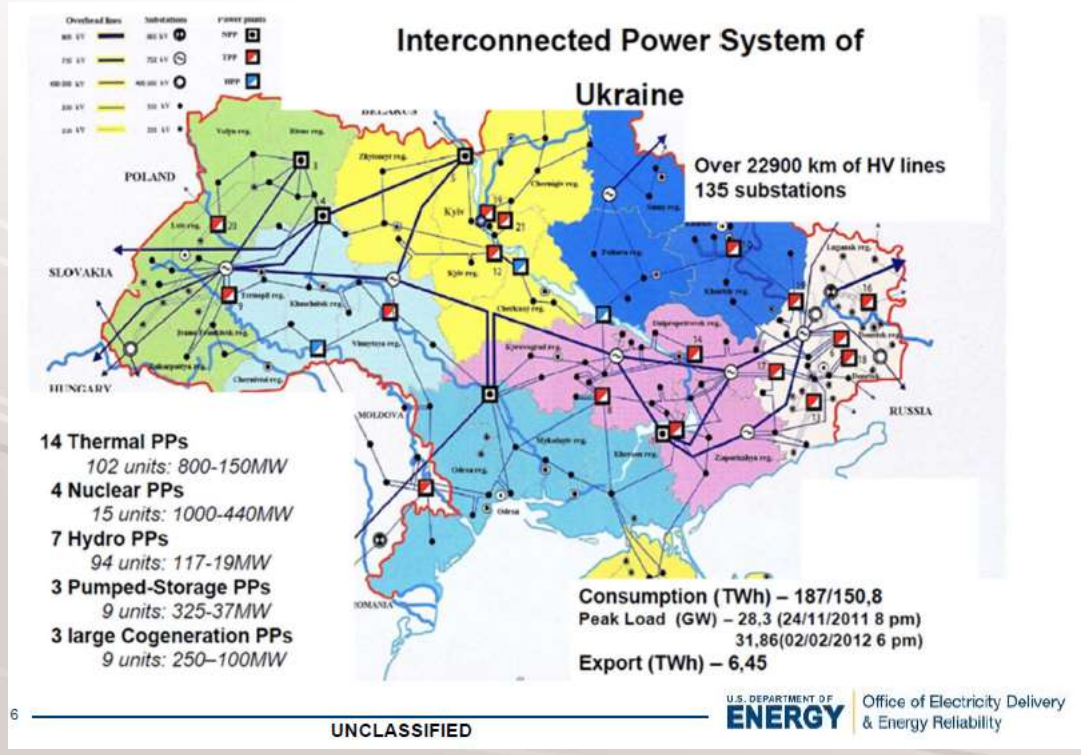
your energy partner®
OPPD
Omaha Public Power District

Ukraine Oblenergo Attacks

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

An Oblenergo is a …

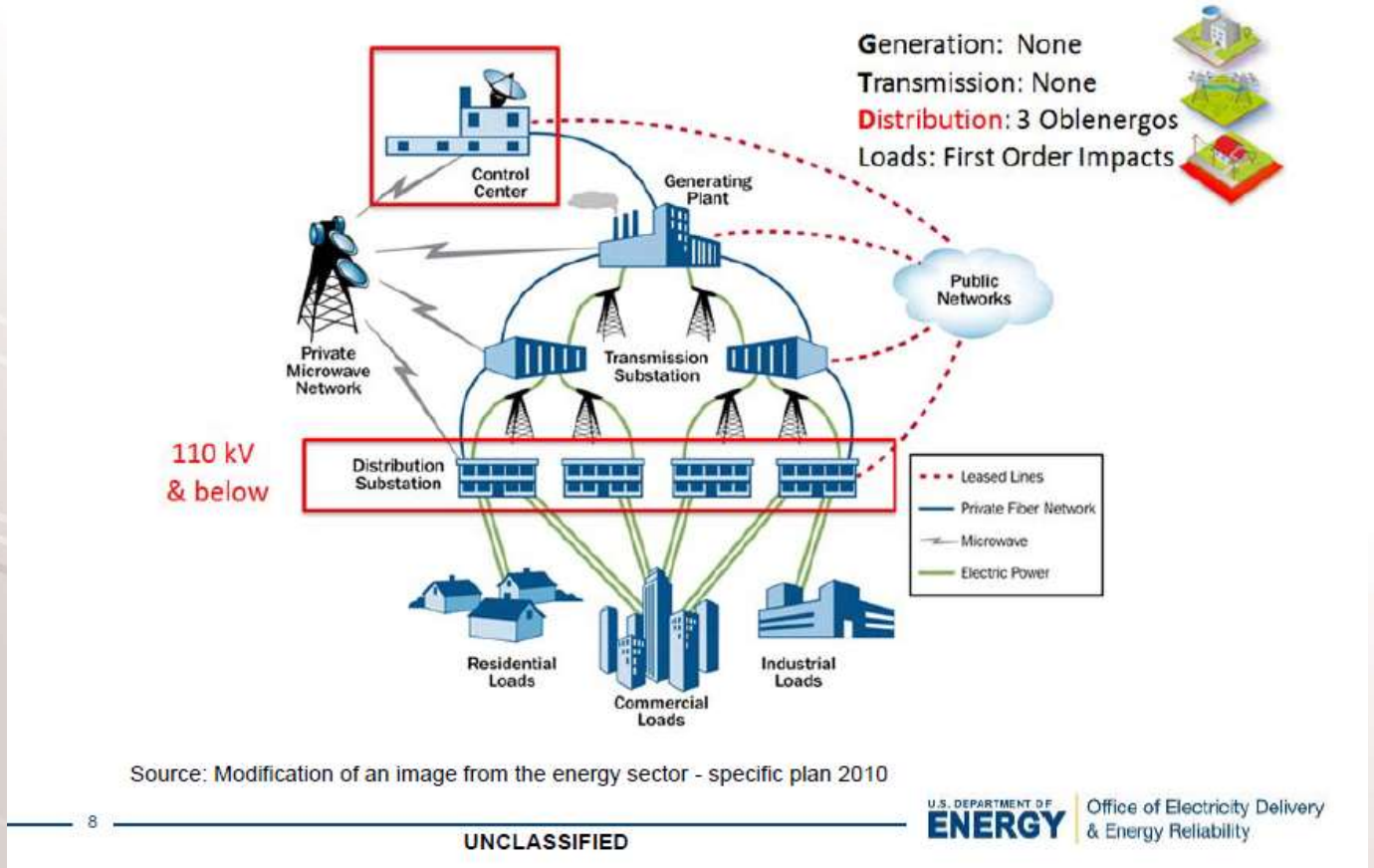
- Regional power distribution entity.
- This matters because the attackers disrupted 3 different oblenergos … it would be similar to attacking OPPD, NPPD, and MidAmerican at the same time.



your energy partner
OPPD
Omaha Public Power District

The ICS Kill Chain

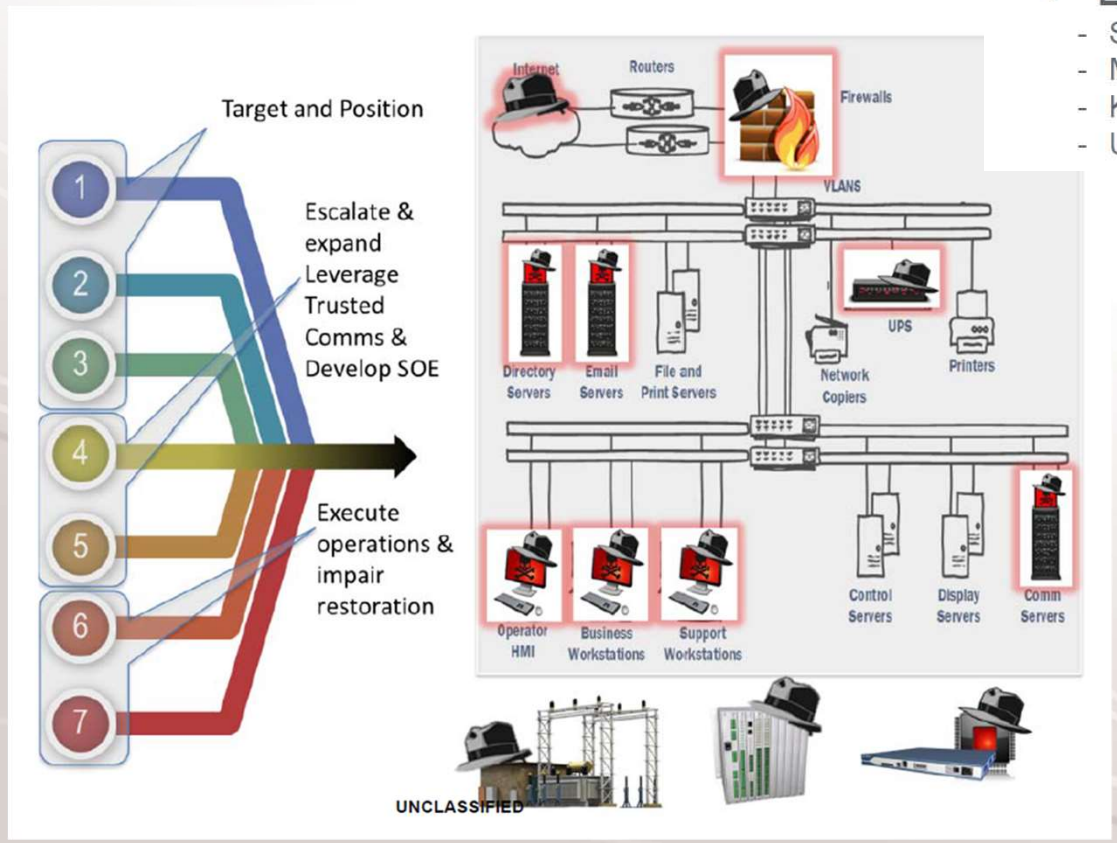
- Targeted the distribution networks (impacted 225,000 customers)



p0wnd

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

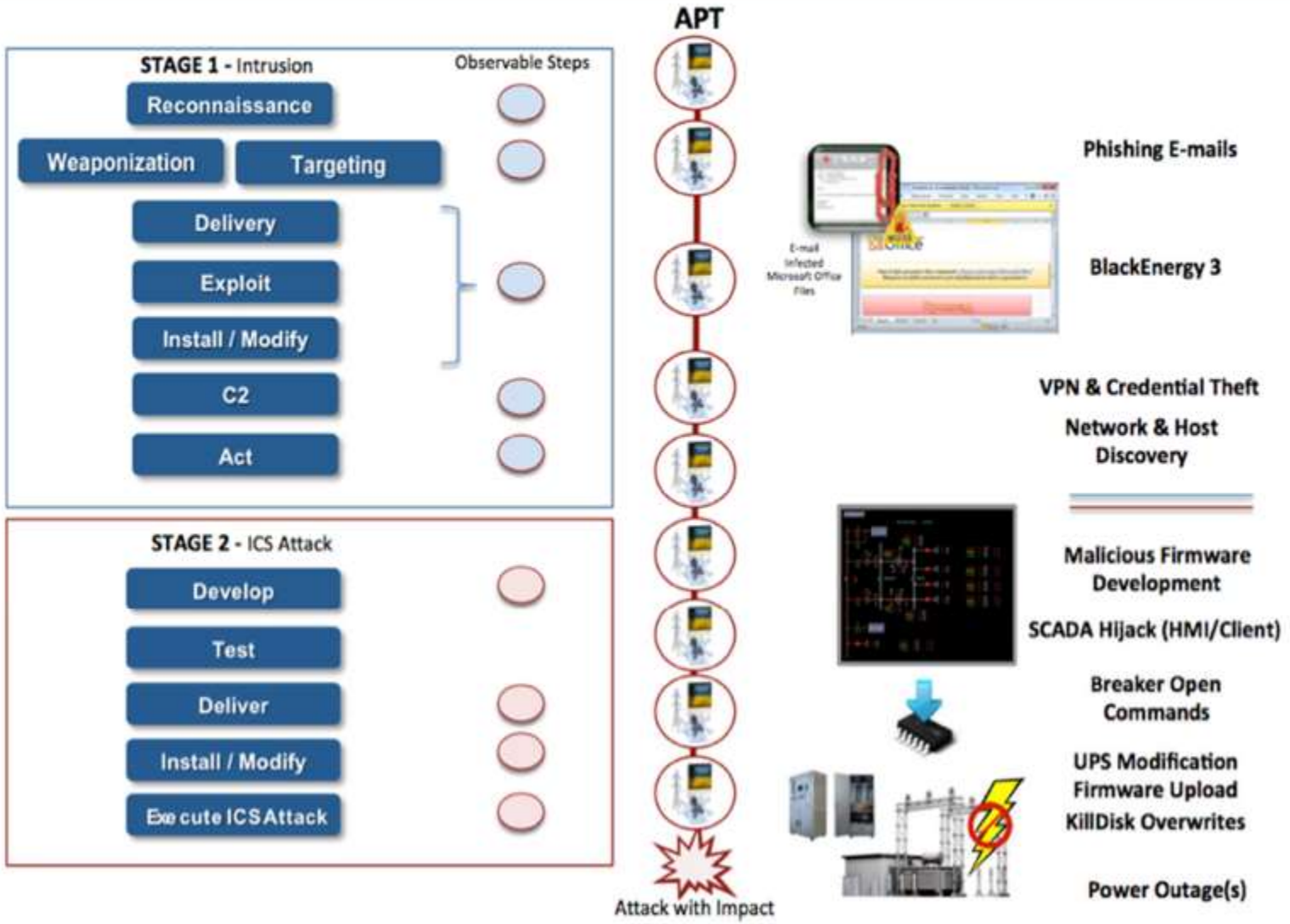


your energy partner
OPPD
Omaha Public Power District

p0wnd

Technical Components

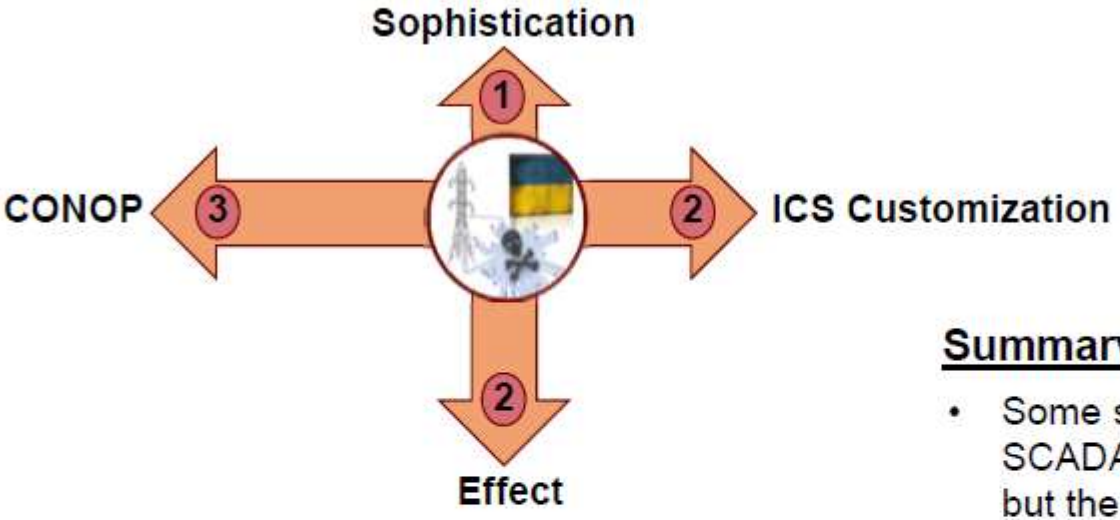
- Spear phishing to gain access to the business networks
- Identification of BlackEnergy 3 at each Oblenergos
- Adversary theft of credentials from the business networks
- Use of VPNs to enter the ICS network
- Use of existing remote access tools within the environment or issuing commands directly from 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

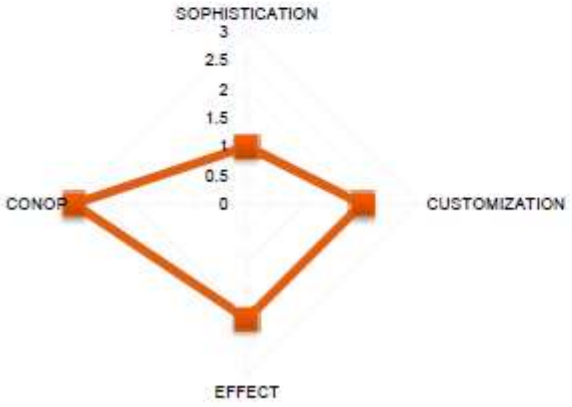


How Sophisticated Was It?

RESPONSE: Just enough

Rating this Attack



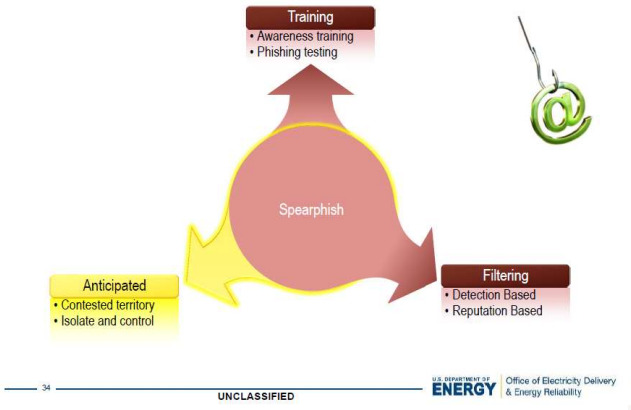


Summary

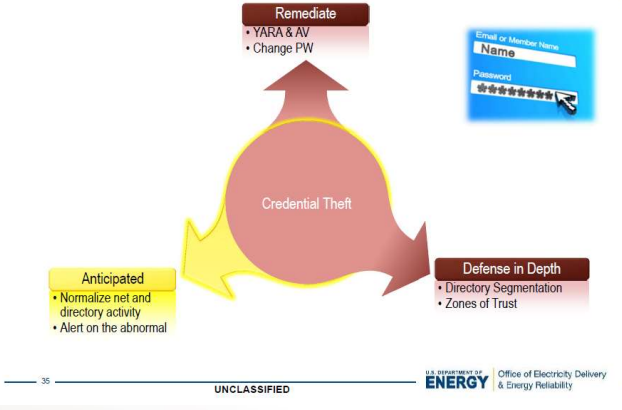
- Some sophistication in the SCADA/DMS hijacking method but the majority of it was not
- Rogue client hijacking demonstrated some customization
- Electricity outage in three service territories restored in hours
- A complex and successful attack plan

Mitigation

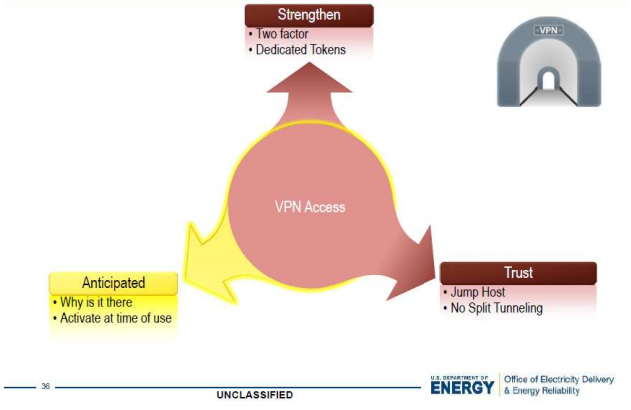
Spearphish



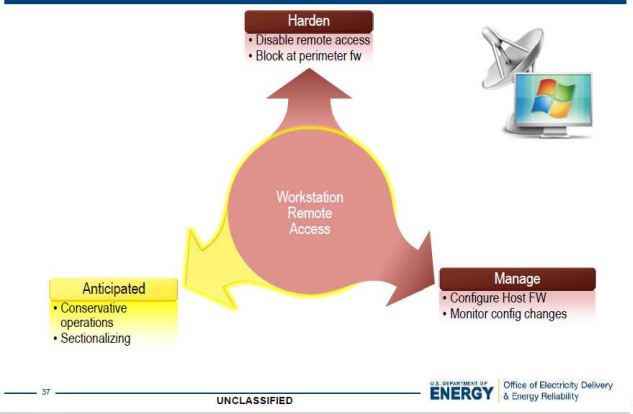
Credential Theft



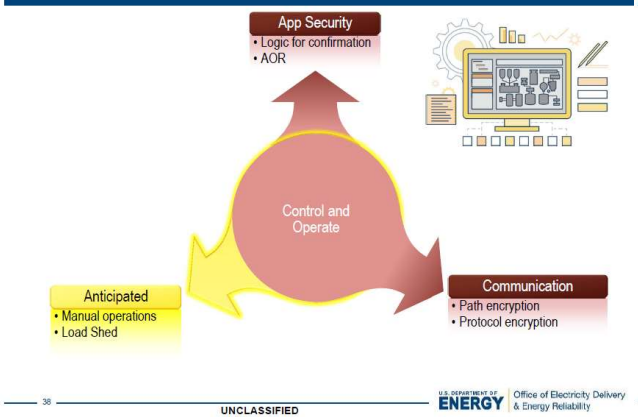
VPN Access



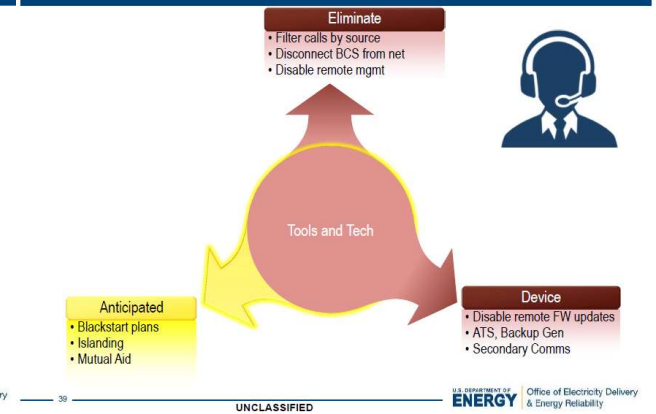
Remote Access



Control



Tools and Tech



your energy partner
OPPD
Omaha Public Power District

питання
Questions

your energy partner
OPPD
Omaha Public Power District