DEFENSIFY
BUSINESS SECURITY SOLUTIONS

Attacks on OT systems

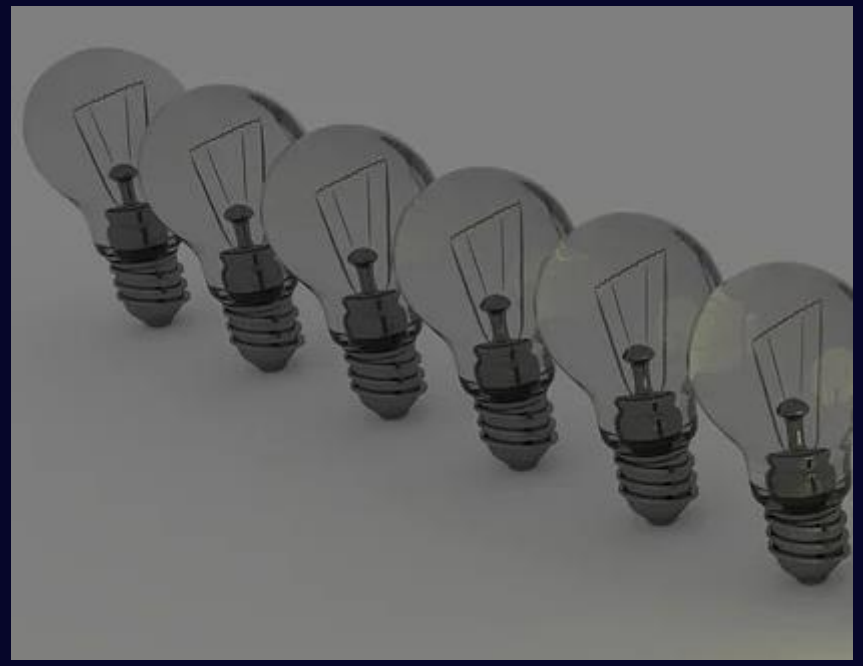
Ludwig Seitz, OT Security Specialist

February 2024

Agenda

1. Black Energy 2015
2. SektorCERT 2023
3. Norsk Hydro 2019

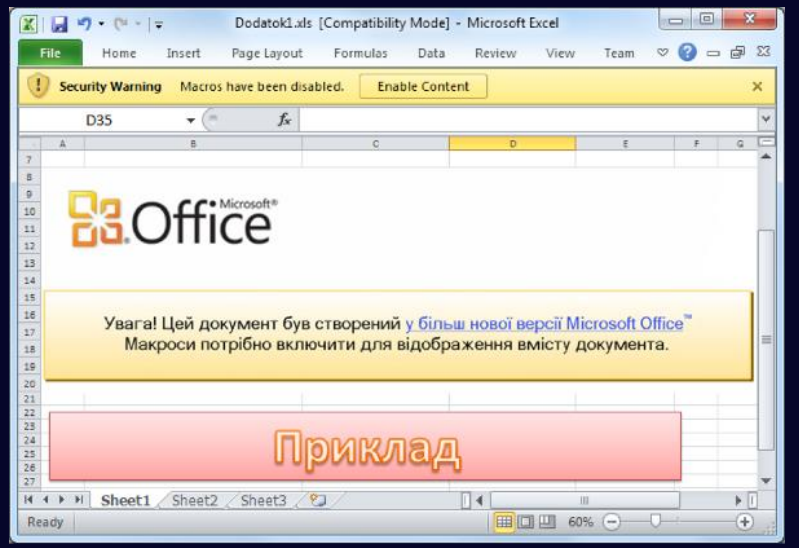
Black Energy 2015 - APT



Prykarpattyaoblernergo
Kyivoblenergo
Chernivtsioblenergo

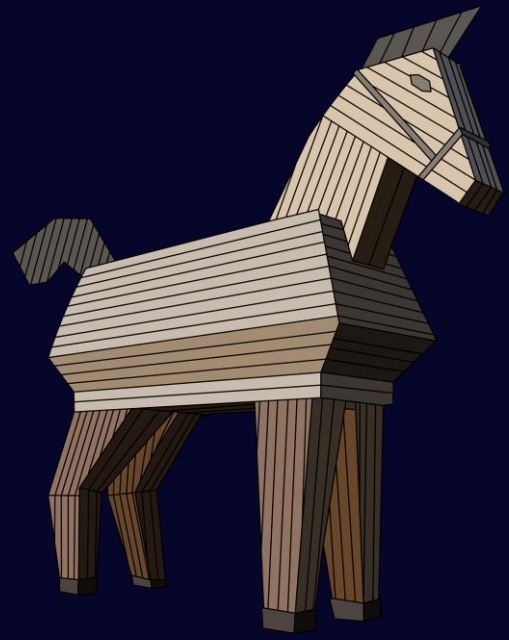
Prelude – IT Attack

1. OSINT
   - Find key persons, network architecture, hard/software
   - Around May 2014
2. Initial Access
   - Spearphishing campaign via email
   - MS Office documents with macrovirus
   - May 2014 – June 2015



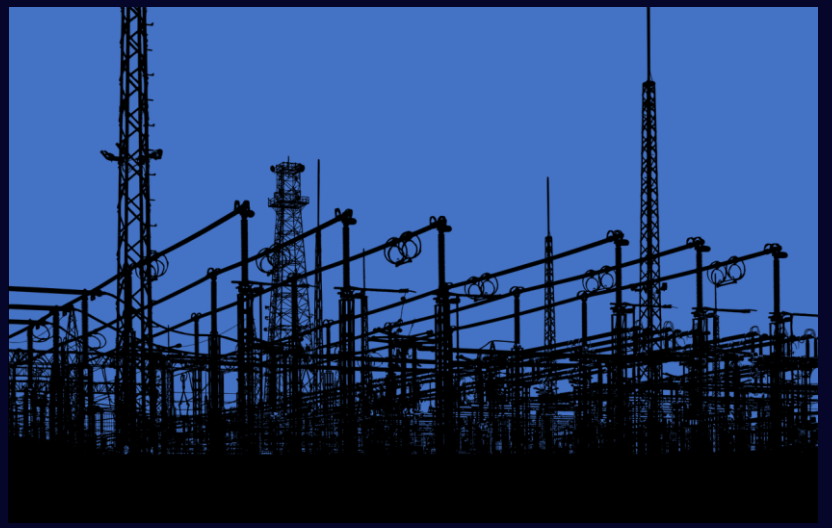
Prelude – IT Attack

3. Deliver Remote Access Trojan
   - Establish C2 channel → persistence
   - Evade detection
4. Lateral Movement
   - Discover IT architecture
   - Harvest credentials



OT Attack Preparation

5. OT Reconnaissance
   - Discover OT architecture
   - Hardware & software
   - Processes
6. Prepare Attack
   - Malicious firmware for serial2ethernet converters
   - Scheduled UPS disruption



OT Attack Execution

December 23rd 2015 (late afternoon)

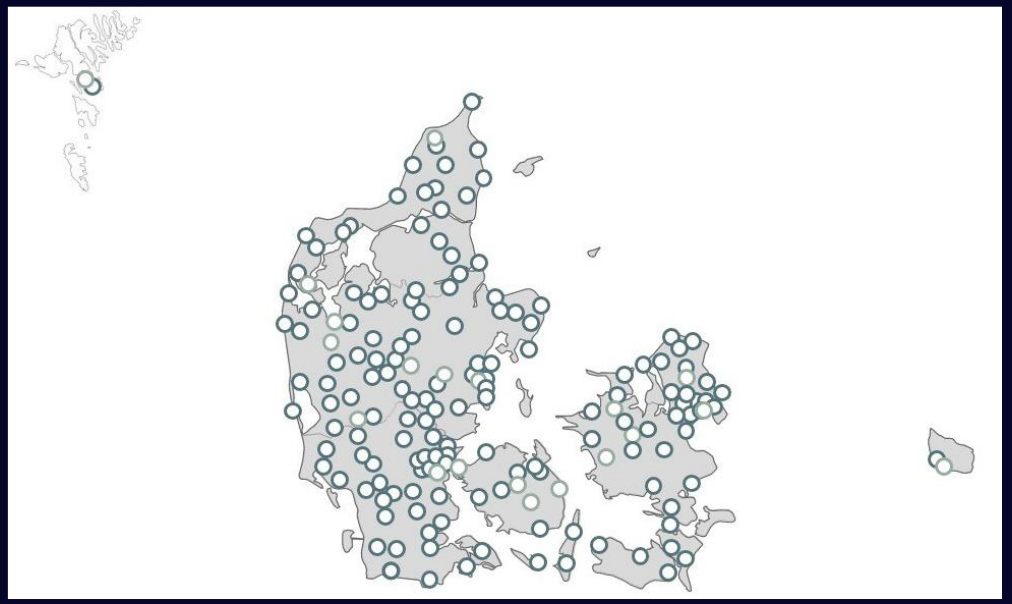
7. Manual shutdown of substations
   - Remote desktop → operator's SCADA
8. Brick field devices
9. Emergency power shutdown
10. DoS against operator call center
11. Erase all computers (KillDisk)

Aftermath

- >200.000 customers affected
- Power restored within ~6 hours
  - Fall-back to manual operations
- More oblenergos hacked
  - Unclear why only 3 targeted

SektorCERT - 2023

- Danish cybersecurity organization
- Non-profit, owned & funded by critical infrastructure companies
- Monitors their members' infrastructure



SektorCERT's 270 network sensors

Prelude – Vulnerable equipment

- April 25th
  - Critical vulnerability in common firewall
  - SektorCERT warns its members to patch
- May 1st
  - SektorCERT issues additional warning

First Attack – APT?

- May 11th
  - Coordinated attack on 16 Danish energy companies
  - Very stealthy approach
  - 11 immediately compromised
  - SektorCERT detected the attacks…
  - … and managed to stop them by end of the night

Second Wave

- May 22nd 14:44
  - Alarm: suspicious firmware download
  - New Zero-days used
  - Possibly different attacker
  - Compromised assets used for DDoS

→ Victim forced to isolate & operate manually

Second Wave - ctd

- May 22nd 18:13
  - Next attack detected
- May 23rd 18:43
  - Next attack detected
  - Compromised asset used for brute force attack

→ Victims also go to manual operations

More Waves

- May 24th
  - Zyxel discloses new vulnerabilities
- 10:27-10:58
  - 4 more attacks
- 15:59
  - New type of attack
  - Member didn’t know they had the vulnerable firewall

Even More Waves

- 24th May 19:02
  - Communication to APT server detected
- 25th May
  - 3 more attacks
- 30th May
  - Exploit code public
  - Many follow-up attacks

APT: Advanced Persistent Threat (Hacker suspected to be associated to a government)

Sandworm: Hacker group suspected to work for Russian military intelligence

Conclusions

- Coordinated & stealthy attacks, APT?
  - → Critical infrastructure is a target
- Attacks prevented/mitigated
  - → Network visibility useful
- No visible effect for Danish public
  - … but manual operation necessary

Norsk Hyrdo - 2019

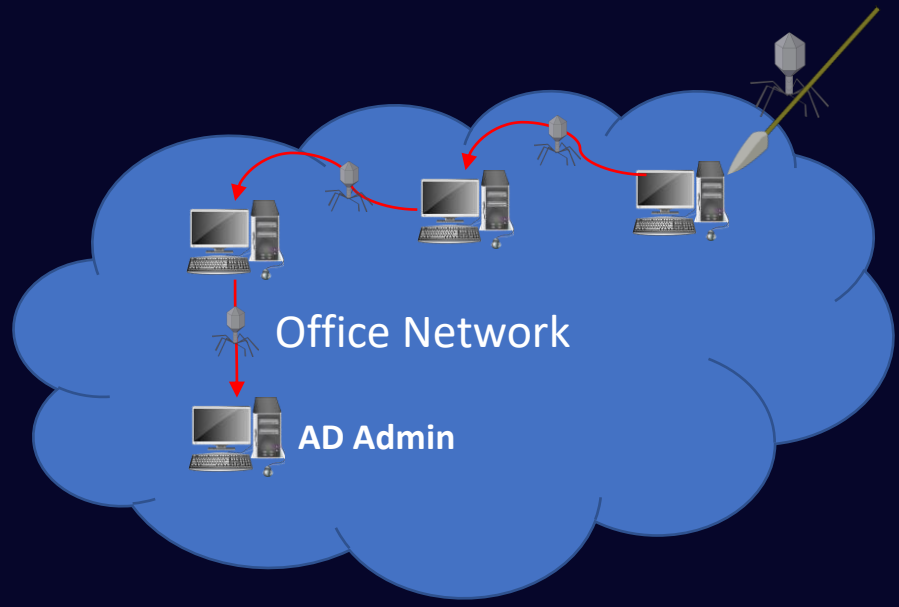
- One of the largest Aluminium producers worldwide
- Hydro- & solar-power
- 32000 empolyees
- Operations in 40 countries
- Revenue (2022): 208 B NOK

Cybercriminal Attack

- January 2019 – Initial access
  - Spearphishing campaign
  - Malicious email attachments
  - Spoofed trusted customer sender address

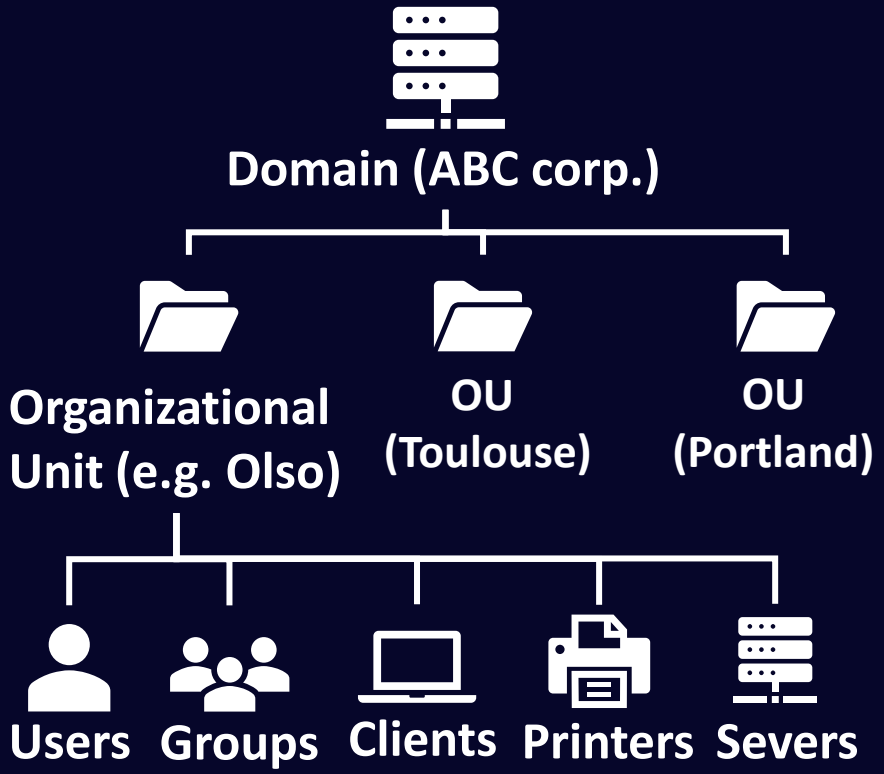
→ IT computer compromised

- January – March – Lateral movement
  - Attackers gain access to Active Directory



Parenthesis: Active Directory

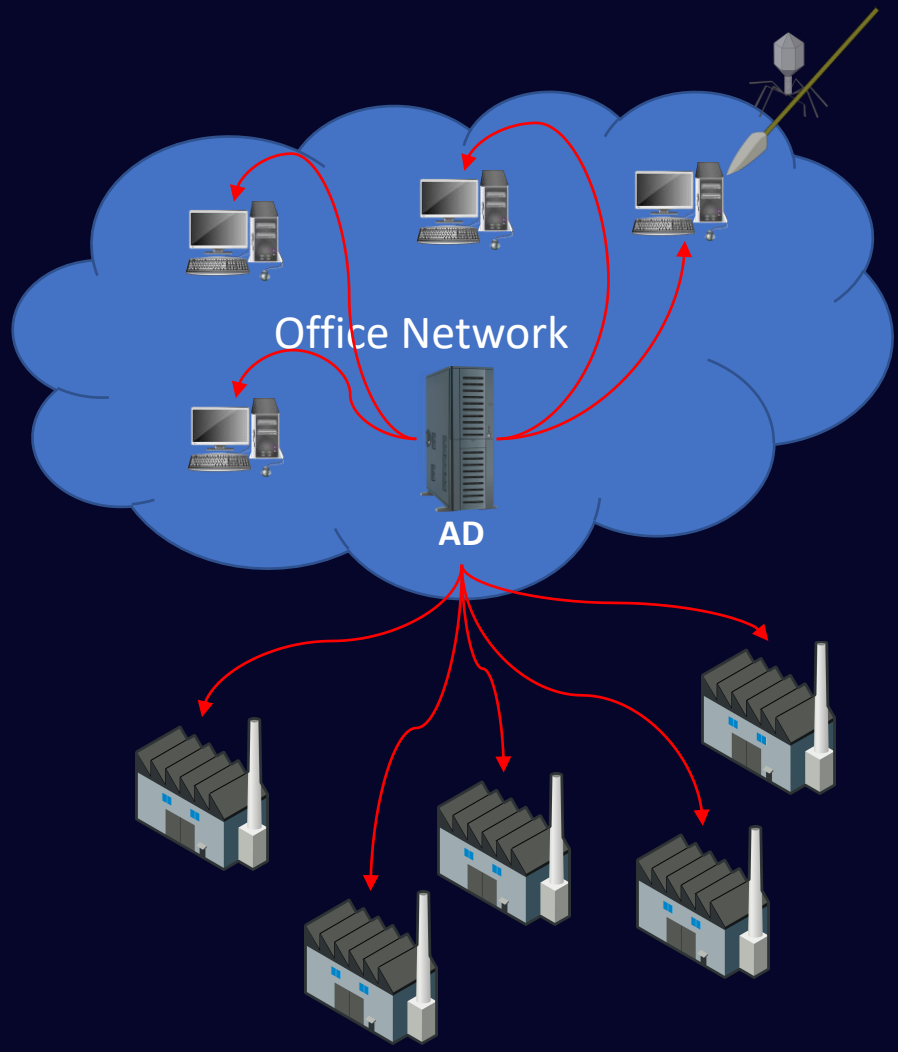
- Service for managing accounts & configuration
  - Very popular in Microsoft environments
- Feature spotlight: Group Policies
  - Manages configuration for groups of objects, e.g., computer, printers, users
  - Can push software installations



Danger, Will Robinson!

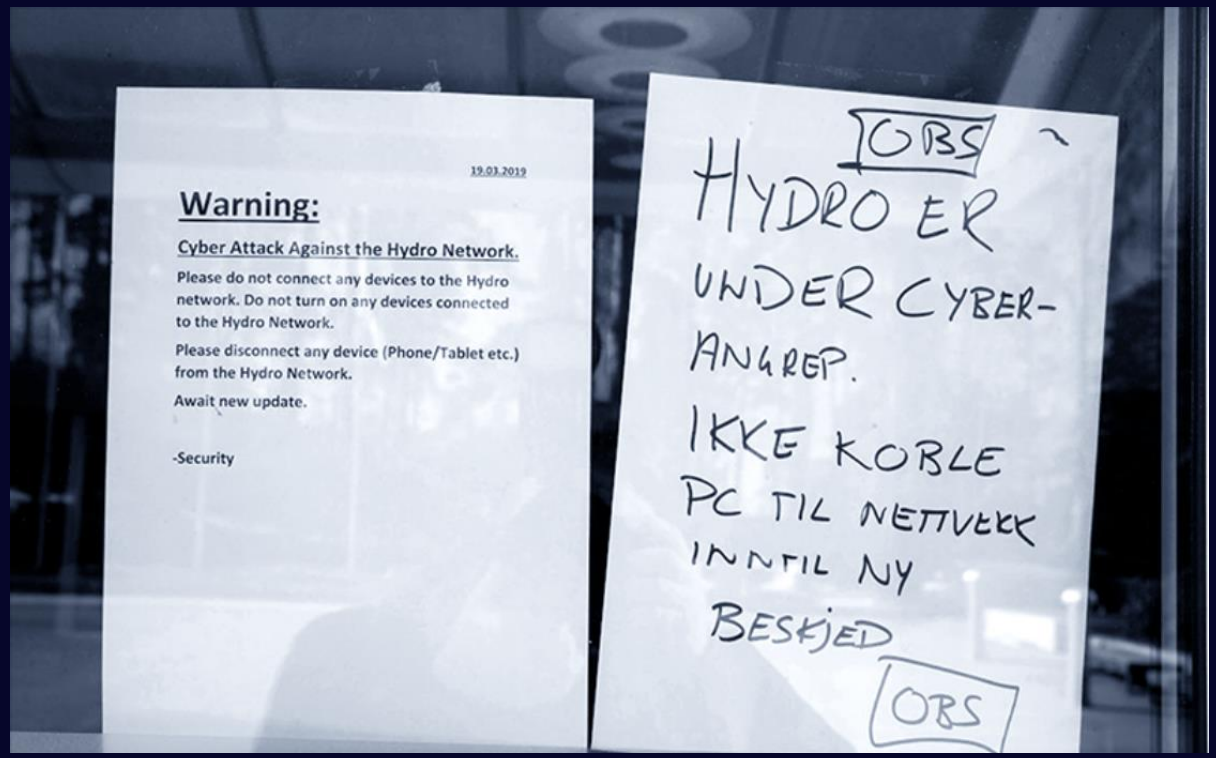
Cybercriminal Attack

- March 19th 2019 – Attack execution
  - Ransomware spread via AD to all connected computers
  - Video from Hydro
- Norsk Hydro reaction
  - Didn't pay ransom
  - Hired external help
  - Went public



Aftermath

- Factories in “manual mode”
- Estimated losses: 500-650 M NOK
- Cyber insurance paid out a small fraction (~ 6%)
- Full recovery took several months



Lessons learned

- SektorCERT & Black Energy
  - Critical infrastructure vulnerable
  - Attacks can be very stealthy
  - Network monitoring helps!
- Norsk Hydro
  - Industry is a target
  - Preparation saves money
  - Openness is appreciated

DEFENSIFY
BUSINESS SECURITY SOLUTIONS

THANK YOU!

Ludwig Seitz
E: ludwig.seitz@defensify.se
W: www.defensify.se

February 2024