Cyberattacks on Ukraine's Power Grid 2015-2016 (Part 1)

Micro Learning Module
MLM-043-A

Industry	– Power
Principal Role	– Owner
Professional Role	– All
Enterprise Phase	– Master Planning

Soviet-style Electrical Substation
Wikimedia Creative Commons

Author

Vytautas Butrimas

Author's presented views do not represent the official position of NATO

Turn on your audio and click start to begin video

START

PRINT VERSION OF NARRATIVE

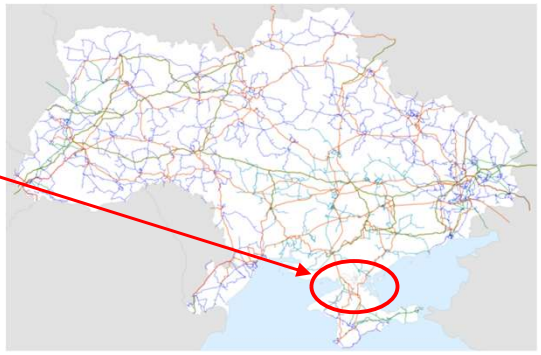
This module addresses *the first of two cyber attacks that targeted Ukraine's power grid in December 2015 and 2016*.
Its intended audience are CISOs, CEOs, CTOs of power utilities and other energy sector enterprises such as oil, gas, and nuclear.

Click the NEXT button when you are ready to advance to the next slide.

What led to events on December 23, 2015?

Russia's annexation of Ukraine's Crimea province (2014)

- In November 2015, an unknown group blew up pylons supporting electric supply to Crimea
- Demonstrators interfered with repair operations
- Russian Minister of Energy blamed Ukraine's Government



Ukraine Power Transmission Network
Wikimedia Creative Commons

PRINT VERSION OF NARRATIVE

The blackout in a region of Ukraine in 2015 occurred during a military conflict between Ukraine and Russia.
Russia's annexation of Ukraine's Crimea province (2014)
22 November 2015 -- an unknown group blew up some pylons that supported the electric power supply to Crimea. Demonstrators interfered with repair operations.
The Russian Minister of Energy blamed Ukraine's Government

What happened on December 23, 2015?

December 23, 2015

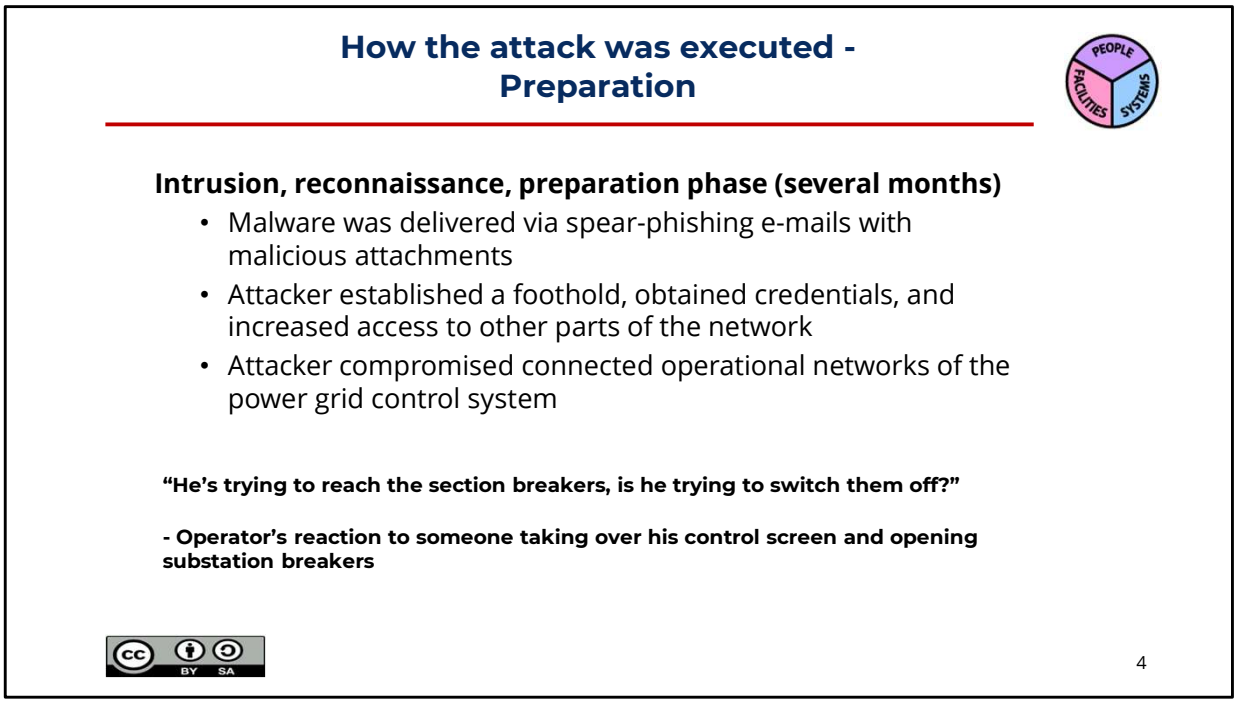
- Remote cyber intrusions at three electric power distribution companies…
- …caused a blackout impacting approximately 225,000 customers
- Power was restored after a few hours

Electrical Lineman
Wikimedia Creative Commons

PRINT VERSION OF NARRATIVE

On December 23, 2015, remote cyber intrusions at three regional electric power distribution companies (Oblenergos) caused a blackout impacting approximately 225,000 customers

Power was restored after a few hours via manual action.



PRINT VERSION OF NARRATIVE

Intrusion, reconnaissance, preparation phase (several months)

- Malware was delivered via spear phishing emails with malicious attachments
- The attacker established a foothold, obtained credentials, and increased his access to other parts of the network
- A way was found into the connected operational networks of the power grid control system

"He's trying to reach the section breakers, is he trying to switch them off?"

- Operator's reaction at someone taking over his control screen and opening substation breakers

https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

How the attack was executed

Execution phase

- Access to SCADA control was used to remotely open breakers at >30 substations
- Serial-to-ethernet servers were disabled with bad firmware
- UPS was disabled with bad firmware
- Wiper malware was applied to workstations
- Denial-of-service attack was conducted against the utility's telephone system

Response of the power utility operator

- Went to manual control after loss of SCADA
- Engineers traveled to substations to close breakers

PRINT VERSION OF NARRATIVE

Execution phase

- Access to SCADA control was used to remotely open breakers at over 30 substations
- Serial-to-ethernet servers compromised/disabled with bad firmware resulted in operator loss of view and control (an operator's worst nightmare)
- UPS was disabled with bad firmware
- Wiper malware was applied to workstations
- In parallel with the main attach, a denial-of-service (DoS) attack targeted the operator's telephone system. Customers could not report a loss of service.

Response of the power utility

- Went to manual restoration (closing breakers) at the affected substations after losing remote monitoring and control capability
- Engineers and other support staff traveled to each of the affected

substations to manually close the breakers

Key Messages

- Think of your operations as a target and be prepared.
- Political conflicts can spill over into industrial operations.
- The cyber intruder seeks to avoid detection and the presence may only become apparent after an attack has been executed.
- Internet-connected business networks must be separated from control networks.
- Remote access policies should be strictly enforced
- Capability to monitor equipment and control networks for anomalous behavior is required for early detection of and response to a breach.
- Refer to ISA/IEC 62443 Part 3-3: System security requirements and security levels.

Remote Electrical Substation
Wikimedia Public Domain

PRINT VERSION OF NARRATIVE

The following are the key messages to take away from this MLM:

Think of your operations as a target and be prepared.

Political conflicts can spill over into industrial operations. Your operations may get “caught in the crossfire”.

The cyber intruder seeks to avoid detection and the presence may only become apparent after an attack has been executed.

Internet-connected business networks must be separated from control networks.

Remote access policies should be strictly and actively controlled.

Capability to monitor equipment and control networks for anomalous behavior is required for early detection and response to a breach.

You may find it useful to refer to ISA/IEC 62443 3-3 Security for industrial automation and control systems Part 3-3: System security requirements and security levels for ways to defend against and improve the resilience of critical systems to advanced cyber attacks.

Further Information

- Related MLMs
  - Cyberattacks on Ukraine's Power Grid 2015-2016 Part 2
- References:
  - https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack
  - ISA/IEC 62443 3-3 Security for industrial automation and control systems Part 3-3: System security requirements and security levels
  - Grid operators description of the attack on December 23rd https://www.youtube.com/watch?v=bV47gBsrDkc
  - https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

PRINT VERSION OF NARRATIVE

Select the Resources tab (at the top of the screen) to view and/or print this MLM, including the speaker notes. Some people like to review the slides and written narrative after listening to the micro learning module. Some like to print them and follow along as they listen to the video. It's up to you.

Author – Vytautas Butrimas

Vytautas Butrimas has been working in defense and cyber security roles for over 30 years including:

- Vice-minister at the Ministry of Communications and Informatics, Republic of Lithuania responsible for Information Society programs.
- Defense Policy and Planning Director, Lithuanian Ministry of National Defense (MoND) responsible for preparing the first Military Defense Strategy.
- Deputy Director responsible for IT security at the Communications and Information System Service (CISS) responsible for preparing the first National Defense System Cybersecurity Strategy
- Chief Adviser for the MoND of Lithuania with a focus on cybersecurity policy, including the national task force that wrote the Lithuanian Law on Cybersecurity
- Member (Presidential appointee) of the National Communications Regulatory Service's Council (RTT-Coucil)
- Cybersecurity Subject Matter Expert for the NATO Energy Security Center of Excellence (NATO ENSECCOE) who performed a Cyber Risk Study of the ICS Used in the NATO Central Europe Pipeline System (CEPS)