Ukraine Power Grid Attacks

Analysis of the 2015 and 2016 Cyber Attacks on Ukrainian Power Distribution

OT Security Learning Series

Document 411 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

The cyber attacks on Ukraine's power grid in December 2015 and December 2016 represent landmark events in the history of OT security. These attacks demonstrated that adversaries could successfully compromise power distribution systems and cause widespread outages affecting civilian populations.

Critical

The 2015 Ukraine attack was the first publicly confirmed cyber attack to cause a power outage. It proved that nation-state actors could and would target civilian critical infrastructure.

2 The 2015 Attack

2.1 Overview

Attribute	Details
Date	December 23, 2015
Target	Three Ukrainian power distribution companies
Duration	1–6 hours of outages
Impact	Approximately 225,000 customers without power
Malware	BlackEnergy 3, KillDisk
Attribution	Sandworm (Russian state-sponsored group)

2.2 Attack Timeline

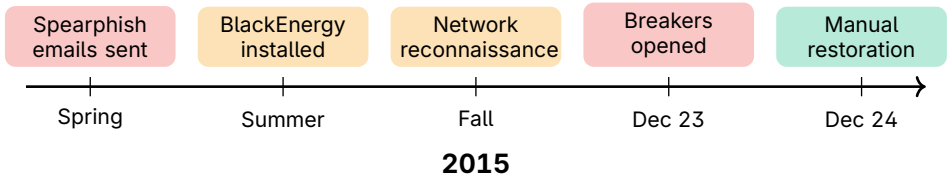

Figure 1: 2015 Ukraine Attack Timeline

2.3 Attack Chain

2015 Attack Sequence

1. **Initial Access:** Spear-phishing emails with malicious Word documents
2. **Persistence:** BlackEnergy malware established backdoor access
3. **Reconnaissance:** Months of network mapping and credential harvesting
4. **Lateral Movement:** Pivoted from IT networks to OT systems
5. **Execution:** Remote access to SCADA systems via hijacked VPNs
6. **Impact:** Operators watched as attackers opened breakers remotely
7. **Destruction:** KillDisk wiped systems, UPS firmware corrupted

2.4 Attack Execution Details

Warning

Attackers used legitimate remote access tools (VPNs, remote desktop) to control SCADA systems. They opened circuit breakers while operators watched helplessly, unable to regain control.

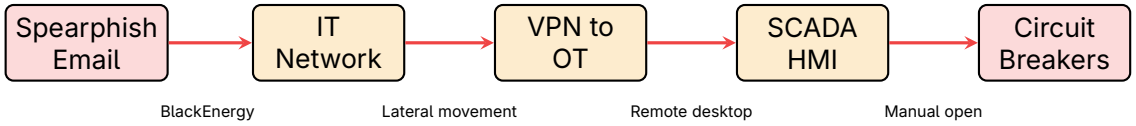

Figure 2: 2015 Ukraine Attack Path

The attackers demonstrated sophisticated operational planning:

- **Coordinated timing:** Attacked three utilities simultaneously
- **Denial of service:** Flooded utility call centers with fake calls
- **Persistence denial:** Corrupted serial-to-Ethernet converters
- **Recovery hindrance:** Deployed KillDisk to wipe workstations
- **UPS sabotage:** Modified UPS firmware to fail during recovery

2.5 Impact

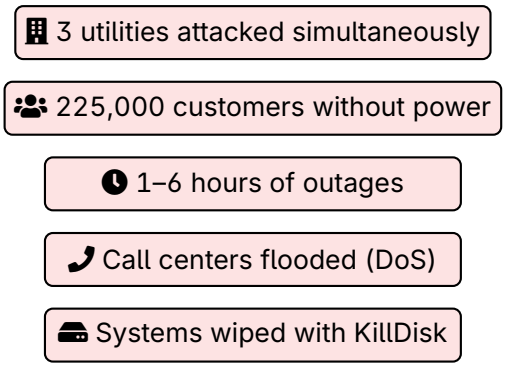

Figure 3: 2015 Attack Impact

2.6 Recovery

Power was restored within 1–6 hours through **manual operations**:

- Operators physically traveled to substations
- Breakers closed manually at each location
- Ukrainian grid design allowed for manual override capability
- Full IT system recovery took months

Tip

The ability to manually operate equipment was critical to rapid recovery. Modern fully-automated systems without manual override capabilities may be more vulnerable to prolonged outages.

3 The 2016 Attack (Industroyer/CrashOverride)

3.1 Overview

Attribute	Details
Date	December 17, 2016
Target	Ukrenergo transmission substation (Kyiv)
Duration	Approximately 1 hour outage
Impact	Portion of Kyiv without power
Malware	Industroyer / CrashOverride
Attribution	Sandworm (Russian state-sponsored group)

3.2 Attack Timeline

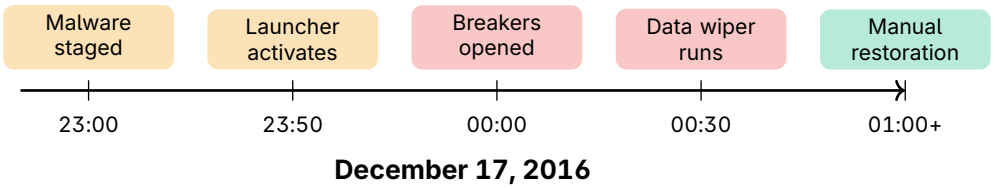

Figure 4: 2016 Ukraine Attack Timeline

3.3 Industroyer Malware

Critical

Industroyer was the first known malware specifically designed to attack power grid equipment. It included modules for four different industrial protocols, making it adaptable to various power system configurations.

Industroyer Protocol Modules

- **IEC 60870-5-101:** Serial communication protocol for telecontrol
- **IEC 60870-5-104:** TCP/IP version of 101 protocol
- **IEC 61850:** Substation automation standard
- **OPC DA:** Industrial data access protocol

3.4 Attack Capabilities

Industroyer demonstrated advanced capabilities:

- **Protocol-native attacks:** Spoke directly to substation equipment
- **No operator interaction needed:** Fully automated attack sequence
- **Modular design:** Easily adaptable to different targets
- **Data wiping:** Included destructive component
- **Potential for greater damage:** May have been a proof-of-concept

3.5 Comparison: 2015 vs 2016

Aspect	2015 Attack	2016 Attack
Attack Method	Remote desktop hijacking	Protocol-native malware
Human Involvement	Attackers manually operated SCADA	Automated malware execution
Sophistication	Used existing tools	Custom ICS malware
Scalability	Labor-intensive	Highly scalable
Target Level	Distribution (lower voltage)	Transmission (higher voltage)

4 Technical Analysis

4.1 Initial Compromise

Both attacks began with spear-phishing:

1. Targeted emails sent to utility employees
2. Malicious Microsoft Word documents with macros
3. BlackEnergy malware downloaded and installed
4. Backdoor access established for long-term persistence

4.2 Network Architecture Exploitation

Warning

The attackers exploited common weaknesses in IT/OT network architecture:

- VPN connections between corporate and operational networks
- Shared credentials between IT and OT systems
- Insufficient network segmentation
- Lack of multi-factor authentication

4.3 MITRE ATT&CK for ICS Mapping

Key techniques used (mapped to MITRE ATT&CK for ICS):

- **T0865:** Spearphishing Attachment (Initial Access)
- **T0859:** Valid Accounts (Persistence, Lateral Movement)
- **T0886:** Remote Services (Lateral Movement)
- **T0855:** Unauthorized Command Message (Execution)
- **T0831:** Manipulation of Control (Impact)

5 Lessons Learned

5.1 Key Takeaways

Key Point

Critical lessons from the Ukraine attacks:

1. **Spear-phishing remains effective:** Initial access through email
2. **IT/OT convergence creates risk:** VPNs bridged networks
3. **Credential theft enables pivoting:** Shared passwords exploited
4. **Manual operations saved the day:** Ability to operate without SCADA
5. **Attackers are patient:** Months of reconnaissance before attack
6. **Coordinated attacks multiply impact:** Multiple targets hit simultaneously

5.2 Defense Recommendations

- **Implement MFA:** Especially for remote access and VPNs
- **Segment networks:** Proper DMZ between IT and OT
- **Monitor OT traffic:** Detect anomalous commands and connections
- **Maintain manual capabilities:** Ensure equipment can be operated manually
- **Email security:** Advanced threat protection and user training
- **Incident response:** OT-specific plans and regular exercises

5.3 Industry Impact

The Ukraine attacks prompted significant changes:

- Increased investment in grid cybersecurity worldwide
- Development of ICS-specific threat intelligence sharing
- Enhanced regulatory focus on critical infrastructure protection
- Greater collaboration between utilities and government agencies

6 Further Reading

Technical Reports

- **SANS ICS** – Analysis of the Cyber Attack on the Ukrainian Power Grid
  https://www.sans.org/reading-room/whitepapers/ICS/
- **Dragos** – CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations
  https://www.dragos.com/resources/whitepaper/crashoverride-analyzing-the-malware-that-attacks-power-grids/
- **ESET** – Industroyer: Biggest threat to industrial control systems since Stuxnet
  https://www.eset.com/int/industroyer/

Government Resources

- **CISA** – ICS Alert: Cyber-Attack Against Ukrainian Critical Infrastructure
  https://www.cisa.gov/news-events/ics-alerts
- **US-CERT** – Alert TA17-163A: CrashOverride Malware
  https://www.cisa.gov/news-events/alerts