Industroyer / CrashOverride

Analysis of Grid-Targeting Malware

OT Security Learning Series

Document 413 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Industroyer (also known as CrashOverride) is sophisticated malware specifically designed to attack electric power grids. It was used in the December 2016 cyberattack on Ukraine's power grid, causing a blackout in Kyiv that affected approximately one-fifth of the city's power consumption.

Critical

Industroyer is only the second known malware (after Stuxnet) specifically designed to disrupt physical industrial processes. It demonstrates nation-state capability to attack critical infrastructure.

1.1 Incident Overview

Attribute	Details
Date	December 17, 2016
Target	Ukrenergo (Ukrainian power transmission)
Location	Pivnichna substation, Kyiv region
Impact	Approximately 200MW load disconnected, 1-hour outage
Attribution	Sandworm Team (Russian GRU Unit 74455)
Discovery	ESET and Dragos (June 2017)

2 Malware Architecture

2.1 Modular Design

Industroyer uses a highly modular architecture:

Component Structure

- **Main backdoor:** C2 communication, orchestration
- **Additional backdoor:** Persistence mechanism
- **Launcher:** Executes payloads at scheduled time
- **Payload modules:** Protocol-specific attack components
- **Data wiper:** Destroys evidence and damages systems

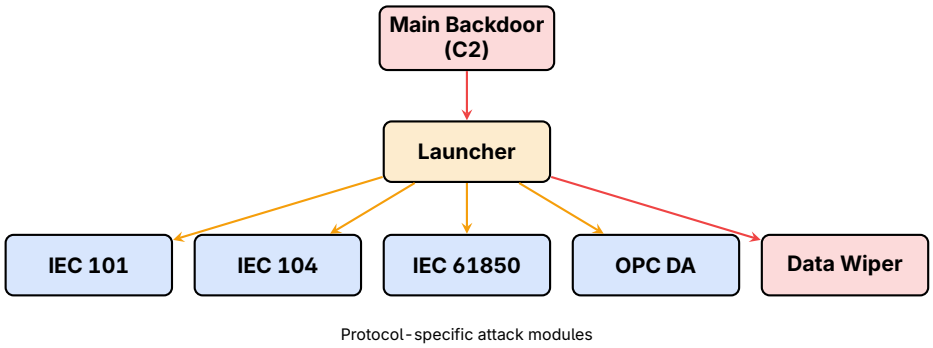

Figure 1: Industroyer Modular Architecture

2.2 ICS Protocol Modules

The malware includes four payload modules targeting industrial protocols:

Protocol	Attack Capability
IEC 60870-5-101	Serial communication with RTUs
IEC 60870-5-104	TCP/IP communication with RTUs (primary attack vector)
IEC 61850	Substation automation, GOOSE messaging
OPC DA	Data access to SCADA historians and HMIs

Warning

The inclusion of multiple protocol modules shows extensive knowledge of power grid systems. This indicates significant reconnaissance and development resources.

3 Attack Sequence

3.1 Attack Timeline

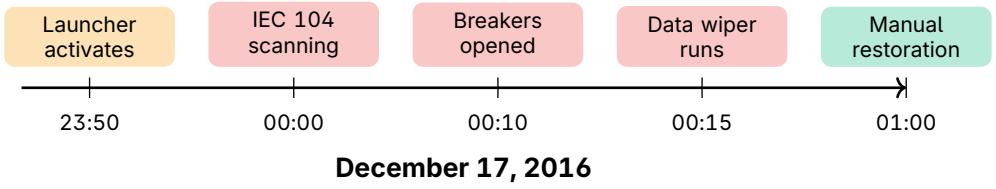

Figure 2: Industroyer Attack Timeline

3.2 Kill Chain

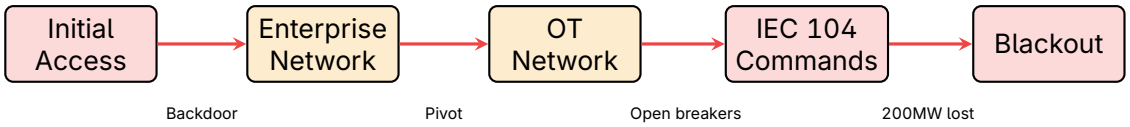

Figure 3: Industroyer Attack Path

1. **Initial access:** Spearphishing or supply chain compromise
2. **Lateral movement:** Spread through enterprise network
3. **OT network access:** Pivoted to control system network
4. **Reconnaissance:** Mapped network and identified targets
5. **Staging:** Deployed malware components
6. **Execution:** Launched attack at midnight local time
7. **Impact:** Opened circuit breakers, caused blackout
8. **Cleanup:** Data wiper attempted to destroy evidence

3.3 IEC 104 Attack Details

The IEC 60870-5-104 module performed these actions:

- Scanned network for IEC 104 devices
- Enumerated Information Object Addresses (IOAs)
- Sent unauthorized commands to open circuit breakers
- Issued single-point and double-point commands
- Toggled breakers repeatedly to prevent manual restoration

3.4 Attack Timeline

Time	Event
23:50	Launcher component activates
00:00	IEC 104 module begins scanning
00:05	Unauthorized commands sent to breakers
00:10	Multiple substations affected
00:15	Data wiper activates
01:00+	Manual restoration begins

4 Technical Analysis

4.1 Main Backdoor

- Written in C++, compiled for Windows
- Communicates via HTTPS to C2 servers
- Uses Tor for anonymization (optional)
- Supports file upload/download, shell commands
- Configurable via XML configuration files

4.2 Launcher Component

Tip

The launcher uses Windows scheduled tasks to execute payloads at a specific time. This allows attackers to:

- Coordinate attacks across multiple systems
- Execute during low-staffing periods (midnight)
- Maintain operational security until attack time

4.3 Data Wiper

The wiper component:

- Overwrites files with random data
- Targets Windows registry and system files
- Attempts to make systems unbootable
- Designed to hamper forensic investigation

5 Comparison with 2015 Attack

Aspect	2015 Attack	2016 (Industroyer)
Method	Manual (remote desktop)	Automated malware
Protocols used	Proprietary SCADA	IEC 104, IEC 61850
Scale	3 utilities, 225,000 affected	1 utility, smaller impact
Sophistication	Medium	High
Reusability	Low (manual)	High (modular)
Recovery impact	Firmware damage	Data wiping

Information

Industroyer represents an evolution from manual attacks to automated, repeatable capabilities. The modular design allows rapid adaptation to different targets.

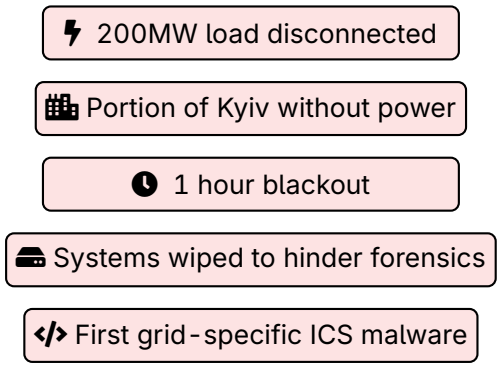

Figure 4: Industroyer Attack Impact

6 Detection and Defense

6.1 Indicators of Compromise

Key detection opportunities:

- Unusual IEC 104 traffic patterns or command sequences
- Unauthorized connections to RTU/IED addresses
- Scheduled tasks created with suspicious names
- Tor network connections from OT systems
- File modifications in system directories

6.2 Defensive Measures

Key Point

Recommended defenses:

- Network segmentation between IT and OT
- ICS-aware intrusion detection systems
- Application whitelisting on SCADA servers
- Monitoring of IEC 104/61850 protocol traffic
- Offline backups of critical configurations
- Incident response plans for grid emergencies

6.3 Protocol-Specific Protections

- **IEC 62351:** Security extensions for IEC 60870-5 and 61850
- **Command validation:** Verify commands against expected operations
- **Rate limiting:** Detect rapid command sequences

- **Access control:** Restrict which systems can send commands

7 Lessons Learned

1. **Automation increases risk:** Malware can attack faster than humans respond
2. **Protocol knowledge is weaponized:** Attackers invest in understanding ICS protocols
3. **Defense in depth is essential:** Single controls are insufficient
4. **Visibility matters:** Many victims lacked monitoring capability
5. **Recovery planning is critical:** Manual restoration procedures saved the day

8 Further Reading

Technical Reports

- **ESET** – Industroyer Analysis
  https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
- **Dragos** – CrashOverride Report
  https://www.dragos.com/resources/whitepaper/crashoverride-analyzing-the-malware-that-attacks-power-grids/

Government Resources

- **CISA** – ICS-CERT Alerts
  https://www.cisa.gov/news-events/ics-alerts

Books

- Andy Greenberg – *Sandworm* (Doubleday)