OT Security Incidents

Overview of Notable Attacks on Industrial Control Systems

OT Security Learning Series

Document 400 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

The history of attacks on Operational Technology (OT) and Industrial Control Systems (ICS) provides valuable lessons for security professionals. Understanding how past incidents occurred helps organizations identify vulnerabilities and implement effective defenses.

Information

This document provides an overview of significant OT/ICS security incidents, covering attack patterns, common vectors, and key lessons learned from historical attacks on industrial control systems.

1.1 Why Study Past Incidents?

- **Learn from mistakes:** Understanding attack vectors helps prevent similar incidents
- **Identify patterns:** Many attacks share common techniques and entry points
- **Justify investments:** Real-world examples demonstrate the need for OT security
- **Improve detection:** Knowledge of attack behaviors aids in building detection capabilities

2 Timeline of Major Incidents

Year	Incident	Impact
2010	Stuxnet	Destroyed Iranian uranium enrichment centrifuges
2014	German Steel Mill	Physical damage to blast furnace
2015	Ukraine Power Grid	225,000 customers lost power
2016	Ukraine Power Grid (Industroyer)	Power outage in Kyiv
2017	TRITON/TRISIS	Targeted safety instrumented systems
2017	NotPetya	Global disruption, $10B+ damages
2019	LockerGoga (Norsk Hydro)	Aluminum production halted
2020	SolarWinds	Supply chain compromise affecting OT vendors
2021	Colonial Pipeline	Fuel supply disruption, US East Coast
2021	Oldsmar Water	Attempted manipulation of water treatment
2021	JBS Foods	Meat processing shutdown
2022	Viasat/Ukraine	Satellite communications disrupted

3 Attack Categories

3.1 Nation-State Attacks

Characteristics of Nation-State Attacks

- Highly sophisticated and well-resourced
- Often target critical infrastructure
- May remain undetected for extended periods
- Focus on espionage, sabotage, or pre-positioning

Examples: Stuxnet, Ukraine Power Grid attacks, TRITON

3.2 Ransomware and Criminal Attacks

Characteristics of Criminal Attacks

- Financially motivated
- Often opportunistic rather than targeted
- IT systems compromised, OT affected indirectly
- Growing trend of targeting industrial sectors

Examples: Colonial Pipeline, JBS Foods, Norsk Hydro

3.3 Insider Threats

Characteristics of Insider Threats

- Authorized access misused
- May be malicious or unintentional
- Difficult to detect with perimeter security
- Can cause significant damage due to system knowledge

Examples: Maroochy Shire sewage spill (2000)

4 Common Attack Vectors

Warning

Most OT security incidents do not begin with direct attacks on OT systems. Attackers typically compromise IT networks first, then pivot to OT environments.

4.1 Initial Access Methods

1. **Spear Phishing:** Targeted emails to employees with access to OT networks
2. **Remote Access:** Compromised VPNs, RDP, or vendor connections
3. **Supply Chain:** Compromised software updates or vendor tools
4. **Removable Media:** USB drives crossing air-gap boundaries

5. **Internet-Exposed Systems:** Misconfigured devices accessible from internet

4.2 Lateral Movement to OT

1. **Dual-Homed Systems:** Engineering workstations connected to both networks
2. **Historian Servers:** Data replication paths between IT and OT
3. **Shared Credentials:** Same passwords used across IT and OT systems
4. **Flat Networks:** Lack of segmentation allowing direct access

5 Key Lessons Learned

Key Point

Recurring themes across major incidents:

1. Network segmentation failures enabled lateral movement
2. Lack of visibility into OT network traffic
3. Insufficient monitoring and logging
4. Weak authentication and access controls
5. Delayed patching of known vulnerabilities
6. Inadequate incident response planning for OT

6 Further Reading

Reports and Analysis

- **CISA ICS Advisories**
  https://www.cisa.gov/news-events/ics-advisories
- **MITRE ATT&CK for ICS**
  https://attack.mitre.org/techniques/ics/
- **Dragos Year in Review Reports**
  https://www.dragos.com/year-in-review/

Standards

- **NIST Cybersecurity Framework**
  https://www.nist.gov/cyberframework
- **IEC 62443 Series**
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Part of the OT Security Learning Series