Ransomware in OT Environments

Understanding and Defending Against Industrial Ransomware Attacks

OT Security Learning Series

Document 423 | February 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Ransomware has evolved from a nuisance targeting individual computers to a critical threat against industrial infrastructure. When ransomware strikes OT environments, the consequences extend beyond data loss to physical safety hazards, environmental damage, and disruption of essential services.

Ransomware attacks against industrial organizations have increased dramatically in recent years. Unlike traditional IT ransomware that primarily impacts data availability, attacks on OT environments can halt production lines, disrupt critical infrastructure, and create safety hazards. The convergence of IT and OT networks has expanded the attack surface, making industrial systems more accessible to ransomware operators.

2 IT vs OT Ransomware Impact

The impact of ransomware differs significantly between IT and OT environments:

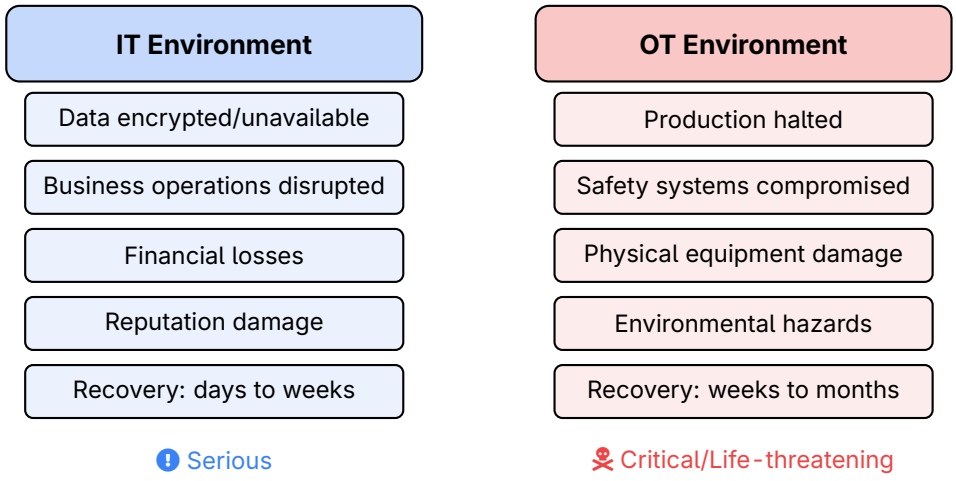


Figure 1: Comparison of ransomware impact on IT vs OT environments

Critical

In OT environments, ransomware can cause physical consequences: halted production, damaged equipment, safety incidents, and even loss of life. The stakes are fundamentally different from traditional IT ransomware.

3 Ransomware Attack Chain in OT

Understanding how ransomware reaches OT systems is essential for defense:

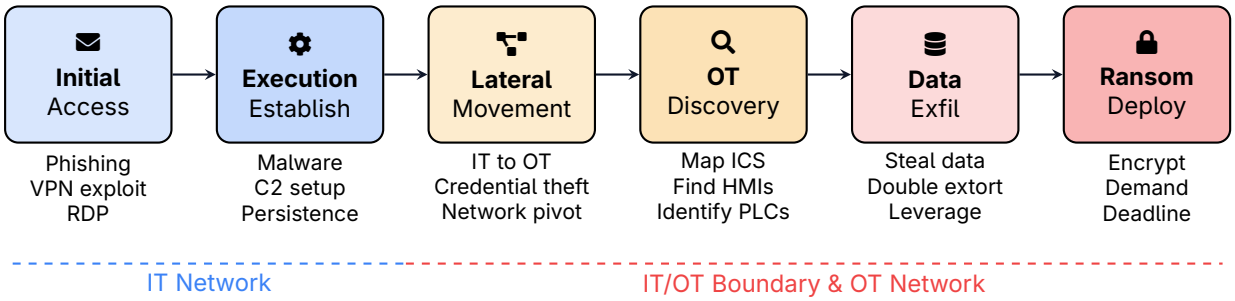


Figure 2: Typical ransomware attack chain targeting OT environments

3.1 Attack Phases Explained

1. **Initial Access** – Attackers gain foothold via phishing, exploiting VPN vulnerabilities, or compromised RDP
2. **Execution & Persistence** – Malware establishes command and control, creates persistence mechanisms
3. **Lateral Movement** – Attackers move through IT network, harvest credentials, pivot toward OT
4. **OT Discovery** – Reconnaissance of industrial systems, identifying HMIs, historians, engineering workstations
5. **Data Exfiltration** – Stealing sensitive data for double extortion leverage
6. **Ransomware Deployment** – Encryption of systems, ransom demand issued

4 Common Attack Vectors

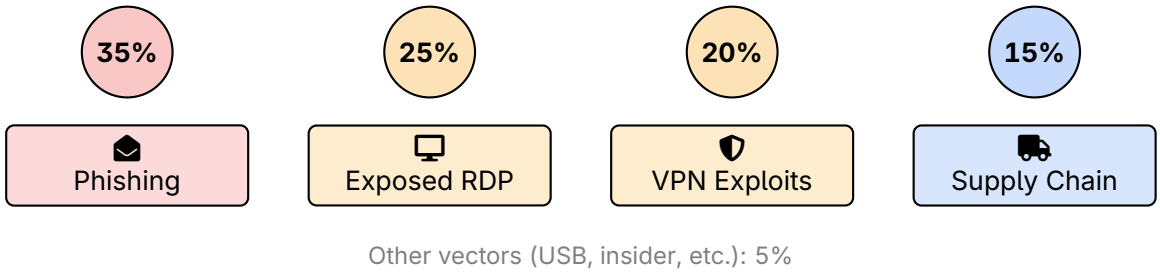


Figure 3: Common initial access vectors for OT ransomware (approximate distribution)

5 Major OT Ransomware Incidents

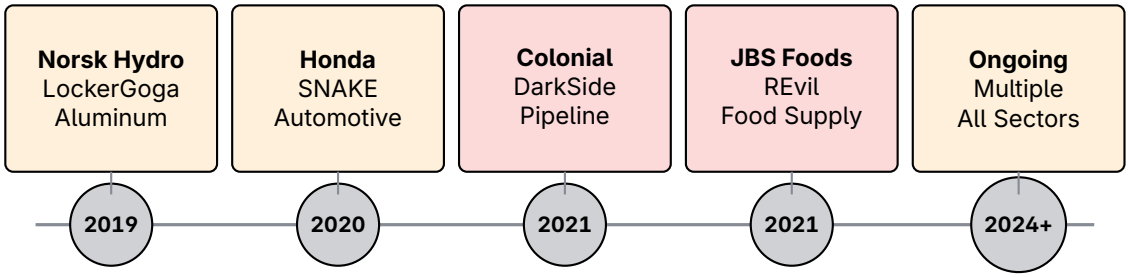


Figure 4: Timeline of significant OT ransomware incidents

5.1 Colonial Pipeline (2021)

Warning

The Colonial Pipeline attack demonstrated how IT ransomware can force OT shutdowns. Although the ransomware only infected IT systems, the company shut down pipeline operations as a precaution, causing fuel shortages across the US East Coast.

- **Attack vector:** Compromised VPN credentials (no MFA)
- **Ransomware:** DarkSide
- **Impact:** 5,500-mile pipeline shutdown for 6 days
- **Ransom:** $4.4 million paid (partially recovered)
- **Lesson:** IT/OT interdependencies can force OT shutdowns

5.2 Norsk Hydro (2019)

- **Attack vector:** Phishing email with infected attachment
- **Ransomware:** LockerGoga
- **Impact:** Global aluminum production halted, manual operations for weeks
- **Cost:** $70+ million in losses
- **Response:** Refused to pay ransom, transparent public communication

5.3 JBS Foods (2021)

- **Attack vector:** Unknown initial access
- **Ransomware:** REvil
- **Impact:** Meat processing plants closed in US, Australia, Canada

- **Ransom:** $11 million paid
- **Lesson:** Food supply chain vulnerability to cyber attacks

6 OT-Specific Ransomware

While most OT ransomware incidents involve IT-focused malware spreading to OT, some variants specifically target industrial systems:

Ransomware	Target	Characteristics
EKANS/SNAKE	ICS processes	Kills ICS-specific processes before encryption
MegaCortex	Enterprise/OT	Targets domain controllers, spreads to OT
LockerGoga	Industrial	Aggressive encryption, disables network adapters
Ryuk	Enterprise/OT	Big game hunting, targets large organizations
Conti	Critical infra	RaaS model, healthcare and industrial targets

Table 1: Ransomware variants that have impacted OT environments

6.1 EKANS/SNAKE Analysis

Critical

EKANS (SNAKE spelled backwards) was the first ransomware designed with ICS awareness. It contains a kill list of industrial processes including GE Proficy, Honeywell HMI, and Fanuc automation software—terminating them before encryption.

7 Defense Strategy

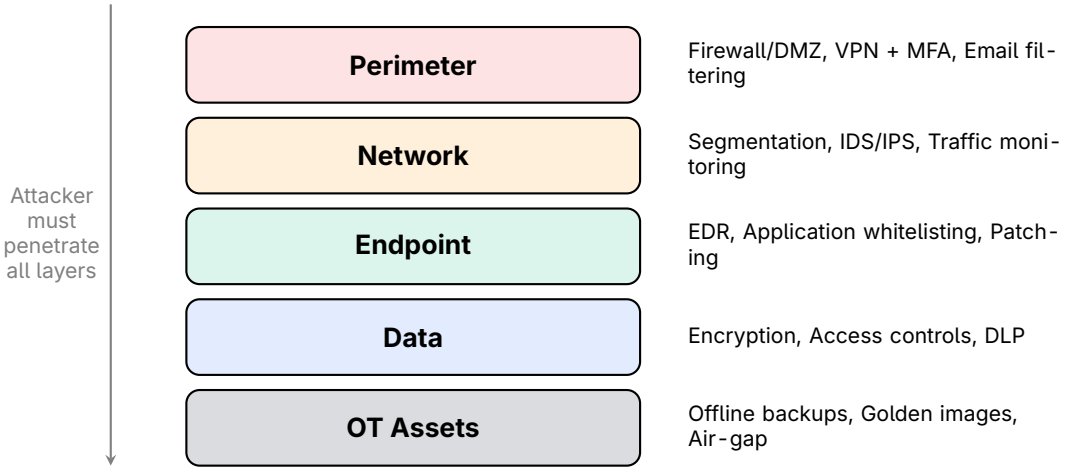


Figure 5: Defense-in-depth strategy for OT ransomware protection

7.1 Prevention Controls

Key Point

The best defense against ransomware is preventing initial access. Focus on the most common vectors: phishing, exposed RDP, and VPN vulnerabilities.

Network Security:

- Implement proper IT/OT segmentation with industrial DMZ
- Disable unnecessary RDP; if required, use VPN + MFA
- Deploy email filtering with attachment sandboxing
- Maintain strict firewall rules between zones

Endpoint Protection:

- Application whitelisting on OT systems
- Endpoint detection and response (EDR) where compatible
- Disable macros in Office documents
- Regular patching of IT systems (prioritize internet-facing)

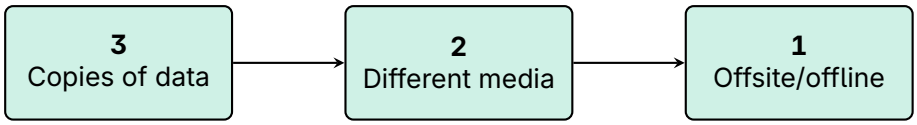
Access Control:

- Multi-factor authentication for all remote access
- Privileged access management (PAM)
- Principle of least privilege
- Regular credential rotation

7.2 Detection Capabilities

- Network traffic analysis for anomalies
- Monitor for reconnaissance activities
- Alert on lateral movement indicators
- Watch for mass file modifications
- Honeypots and deception technology

7.3 Backup and Recovery



Critical: Test restoration regularly and keep backups offline/air-gapped

Figure 6: The 3-2-1 backup rule for ransomware resilience

OT-Specific Backup Considerations:

- Backup PLC programs and configurations
- Preserve HMI graphics and setpoints
- Document network configurations
- Store golden images for rapid rebuild
- Test restoration procedures regularly

8 Incident Response

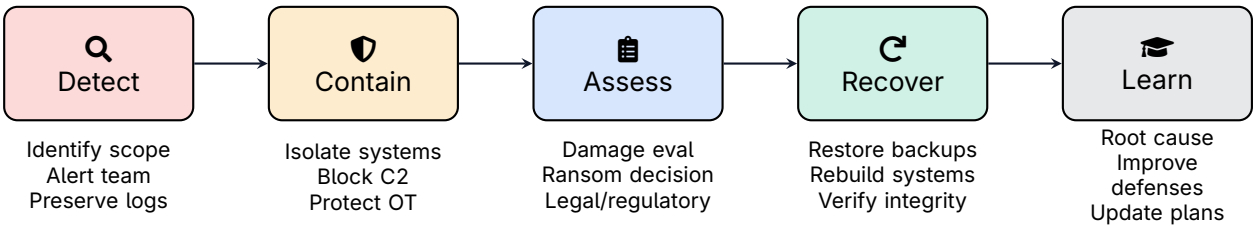


Figure 7: OT ransomware incident response phases

8.1 To Pay or Not to Pay?

Warning

The decision to pay ransom is complex and should involve legal, business, and technical considerations. Paying does not guarantee recovery and may fund future attacks.

Considerations against paying:

- No guarantee of decryption key
- May fund criminal/terrorist organizations
- Encourages future attacks

- Potential legal implications (sanctions)

Considerations for paying:

- Safety-critical systems at risk
- No viable backup recovery option
- Cost of downtime exceeds ransom
- Critical infrastructure service restoration

9 Regulatory Landscape

Recent regulations have increased reporting requirements for ransomware attacks on critical infrastructure:

- **CIRCIA (US)** – 72-hour reporting for critical infrastructure incidents
- **NIS2 (EU)** – 24-hour early warning, 72-hour incident report
- **TSA Security Directives** – Pipeline cybersecurity requirements
- **SEC Rules** – Material cybersecurity incident disclosure

10 Summary

Key Takeaways

- **OT ransomware has physical consequences** – safety hazards, equipment damage, environmental impact
- **Most attacks start in IT** and spread to OT through lateral movement
- **Common vectors:** phishing (35%), exposed RDP (25%), VPN exploits (20%)
- **Prevention focus:** IT/OT segmentation, MFA, email filtering, patching
- **Offline backups are critical** – include PLC programs and configurations
- **Incident response planning** must address OT-specific considerations
- **Ransom payment** is a business decision with no guaranteed outcome

11 Further Reading

Standards and Guidelines

- **CISA Ransomware Guide** – Best practices for prevention and response
  https://www.cisa.gov/stopransomware

- **NIST Cybersecurity Framework** – Risk management guidance
  https://www.nist.gov/cyberframework

Resources

- **No More Ransom Project** – Decryption tools and prevention advice
  https://www.nomoreransom.org/
- **CISA ICS Advisories** – Industrial control system alerts
  https://www.cisa.gov/news-events/ics-advisories

Reports

- Dragos – *Year in Review: ICS/OT Cybersecurity*
- Mandiant – *M-Trends Annual Threat Report*
- IBM – *X-Force Threat Intelligence Index*

Part of the OT Security Learning Series