OT Supply Chain Attacks

Threats Through Trusted Vendors and Components

OT Security Learning Series

Document 422 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Supply chain attacks target organizations indirectly by compromising trusted vendors, software, hardware, or service providers. In OT environments, these attacks are particularly dangerous because industrial systems often rely on specialized vendors with deep access to critical infrastructure, and security updates are applied infrequently due to operational constraints.

Supply chain attacks exploit the trust relationships between organizations and their suppliers. Rather than attacking a hardened target directly, adversaries compromise a weaker link in the supply chain, then leverage that access to reach their ultimate target.

For OT environments, supply chain risks are amplified by:

- Long equipment lifecycles (15–25 years)
- Vendor remote access for maintenance and support
- Limited visibility into vendor security practices
- Delayed patching due to operational requirements
- Dependence on specialized, sometimes sole-source vendors

2 Types of Supply Chain Attacks

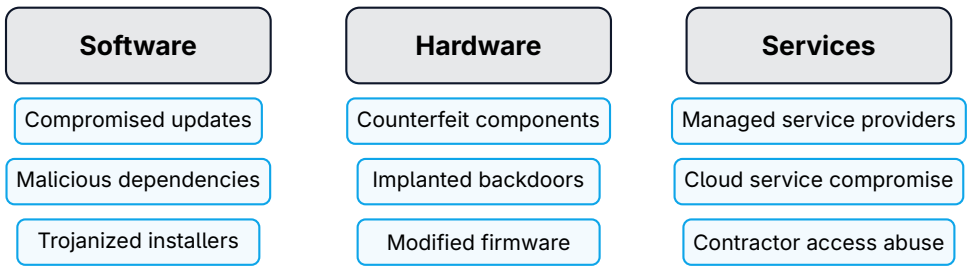

Figure 1: Categories of supply chain attacks

2.1 Software Supply Chain

Software supply chain attacks compromise the development, build, or distribution processes:

- **Build System Compromise** – Injecting malware during software compilation
- **Update Mechanism Hijacking** – Distributing malware through legitimate update channels
- **Dependency Confusion** – Exploiting package managers to install malicious libraries

- **Code Repository Attacks** – Compromising source code repositories

2.2 Hardware Supply Chain

Hardware attacks introduce malicious modifications during manufacturing or distribution:

- **Counterfeit Components** – Substandard or modified parts entering the supply chain
- **Firmware Implants** – Malicious code embedded in device firmware
- **Hardware Trojans** – Circuits added during manufacturing for later exploitation

2.3 Service Provider Attacks

Attackers compromise managed service providers (MSPs) or contractors to reach multiple targets:

- **MSP Compromise** – Attacking IT/OT service providers to access client networks
- **Remote Access Abuse** – Exploiting vendor VPN or remote support tools
- **Credential Theft** – Stealing vendor credentials for customer systems

3 Notable OT Supply Chain Incidents

3.1 Havex / Dragonfly (2013–2014)

Attribute	Details
Attack Vector	Trojanized ICS vendor software installers
Targets	Energy sector, ICS software users
Method	Compromised legitimate download sites of ICS vendors
Malware Capability	OPC server scanning, data exfiltration
Attribution	Energetic Bear / Dragonfly (Russia-linked)

Table 1: Havex/Dragonfly campaign summary

Attackers compromised the websites of at least three ICS software vendors, replacing legitimate installers with trojanized versions. The Havex malware specifically targeted OPC servers to map industrial networks.

Critical

Havex demonstrated that attackers could compromise ICS environments by targeting the vendors that asset owners trust implicitly. Users downloading software from official vendor websites received malware.

3.2 NotPetya (2017)

While primarily known as ransomware, NotPetya was a supply chain attack that devastated OT operations:

- **Vector:** Compromised update mechanism of M.E.Doc (Ukrainian accounting software)

- **OT Impact:** Maersk shipping operations halted, Merck pharmaceutical manufacturing stopped, FedEx TNT logistics disrupted
- **Damage:** Over $10 billion in total damages globally

3.3 SolarWinds / SUNBURST (2020)

Attribute	Details
Attack Vector	Trojanized SolarWinds Orion software updates
Scope	18,000+ organizations downloaded compromised updates
Duration	March–December 2020 (9 months undetected)
OT Relevance	Orion widely used to monitor OT network infrastructure
Attribution	APT29 / Cozy Bear (Russia-linked)

Table 2: SolarWinds/SUNBURST campaign summary

3.4 Kaseya VSA (2021)

The REvil ransomware group exploited vulnerabilities in Kaseya's VSA remote management software:

- Compromised MSPs using Kaseya to manage client systems
- Ransomware deployed to 1,500+ downstream organizations
- Demonstrated cascading impact through service provider relationships

3.5 3CX Supply Chain Attack (2023)

A trojanized version of the 3CX desktop application was distributed through official channels:

- Attackers first compromised Trading Technologies software
- Used that access to compromise 3CX build environment
- Multi-stage supply chain attack (supply chain of a supply chain)

4 OT-Specific Attack Vectors

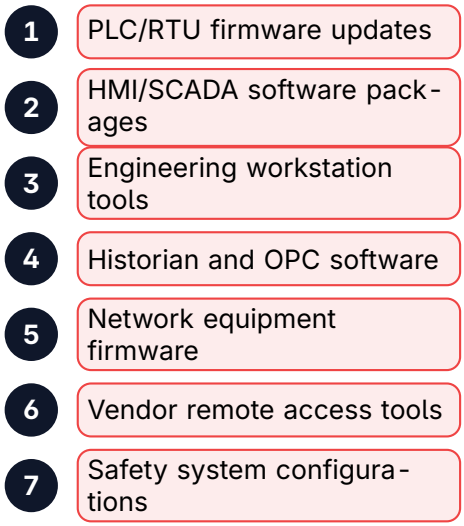

Figure 2: OT-specific supply chain attack vectors

4.1 Vendor Remote Access

Many OT vendors require persistent or on-demand remote access for support:

Warning

Vendor remote access connections often bypass security controls and provide direct access to OT networks. A compromised vendor can use legitimate credentials and tools to access multiple customer sites.

4.2 Embedded Systems and Firmware

OT devices present unique supply chain risks:

- Firmware updates are infrequent and difficult to verify
- Limited ability to inspect embedded system code
- Long device lifecycles mean vulnerabilities persist
- Counterfeit components may contain backdoors

5 Defense Strategies

5.1 Vendor Risk Management

- **Security Assessments** – Evaluate vendor security practices before procurement
- **Contractual Requirements** – Include security obligations in vendor contracts

- **Continuous Monitoring** – Track vendor security posture over time
- **Incident Notification** – Require vendors to report security incidents

5.2 Software Integrity Verification

Control	Implementation
Hash Verification	Verify checksums before installation
Code Signing	Require and validate digital signatures
SBOM Analysis	Review Software Bill of Materials for dependencies
Staged Deployment	Test updates in isolated environment first
Network Segmentation	Limit blast radius of compromised software

Table 3: Software integrity controls

5.3 Remote Access Controls

- Implement jump servers for all vendor access
- Require multi-factor authentication
- Enable session recording and monitoring
- Use time-limited access with explicit approval
- Segment vendor access from critical systems

Key Point

Adopt a zero-trust approach for vendor access: verify identity, limit access scope, monitor all activity, and assume any vendor could be compromised. Never allow persistent, unmonitored vendor connections to OT networks.

5.4 Hardware Supply Chain Security

- Purchase from authorized distributors only
- Inspect components for signs of tampering
- Verify firmware integrity before deployment
- Maintain inventory of hardware provenance
- Consider trusted supplier programs

6 Summary

Key Takeaways

- **Indirect Attack Path:** Supply chain attacks compromise trusted vendors to bypass direct security controls, making them effective against hardened OT environments
- **Multiple Vectors:** Attacks can target software updates, hardware components, or service provider relationships
- **OT Amplification:** Long lifecycles, vendor dependencies, and limited patching make OT especially vulnerable
- **Historical Impact:** Havex, NotPetya, SolarWinds, and Kaseya demonstrate real-world consequences for industrial operations
- **Defense in Depth:** Combine vendor risk management, integrity verification, access controls, and network segmentation
- **Zero Trust for Vendors:** Treat all vendor access as potentially compromised; verify, limit, and monitor continuously

7 Further Reading

Government Resources

- **CISA Supply Chain Risk Management** – Guidance for critical infrastructure
  https://www.cisa.gov/supply-chain-compromise
- **NIST Cybersecurity Supply Chain Risk Management** – C-SCRM practices
  https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

Standards

- **NIST SP 800-161** – Supply Chain Risk Management Practices
  https://csrc.nist.gov/pubs/sp/800/161/r1/final
- **IEC 62443-2-4** – Security program requirements for IACS service providers
  https://webstore.iec.ch/publication/34421

Books

- Andress & Winterfeld – *Cyber Warfare: Techniques, Tactics and Tools* (Auerbach)
- Kouns & Minoli – *Information Technology Risk Management in Enterprise Environments* (Wiley)

Part of the OT Security Learning Series