2025

ACW905 – CYBERWARFARE CAPSTONE PROJECT

Project Title: ERP-Focused Analysis of APT41's Intrusion Campaigns

By: Rachael Kivuti

EXECUTIVE SUMMARY

Enterprise Resource Planning (ERP) systems such as SAP, Oracle ERP and Microsoft Dynamics represent mission-critical digital infrastructure within modern organizations. These platforms support core business functions including financial processing, supply-chain coordination, human resources and enterprise authentication. Due to their central role and extensive integration with third-party vendors, cloud services and application programming interfaces (APIs), ERP systems present a highly attractive target for advanced persistent threat (APT) actors, particularly those conducting supply-chain and application-layer intrusion campaigns.

This capstone project focuses on APT41, a sophisticated Chinese state-aligned threat group known for its long-running involvement in software supply-chain compromise, exploitation of public-facing enterprise applications and abuse of trusted credentials and certificates. While APT41 has been widely documented in public threat intelligence reporting, existing analysis largely remains infrastructure-centric and does not sufficiently translate adversary behavior into ERP-specific defensive intelligence. This creates a gap for enterprise application security teams responsible for protecting SAP and other ERP platforms.

The primary objective of this project is to produce an ATT&CK-mapped intelligence dossier analyzing APT41's ERP-relevant supply-chain intrusion campaigns. To achieve this, the project consolidates and analyzes publicly available threat intelligence, vendor reports and advisories to profile APT41's strategic intent, operational patterns and intrusion lifecycle as it applies to enterprise application environments. Particular emphasis is placed on techniques such as supply-chain compromise (T1195), exploitation of public-facing applications (T1190), abuse of valid accounts (T1078), lateral movement via remote services (T1021), misuse of stolen certificates (T1550) and data staging through archive mechanisms (T1560).

In support of the primary objective, the project delivers a strategic technical analysis of APT41's intrusion lifecycle and its impact on ERP ecosystems. This analysis examines how APT41 uses trusted software components, application servers, integration mechanisms and privileged service accounts to achieve persistence and lateral movement within enterprise environments. The findings are structured using the MITRE ATT&CK framework to ensure consistency, traceability and applicability for defenders.

The project further produces ATT&CK-aligned mapping tables that link APT41's known behaviors to ERP-relevant techniques, commonly affected system components, defensive gaps and recommended mitigations. Building on this analysis, a concise ERP monitoring and mitigation priority brief is provided to highlight practical detection and defense considerations for SAP and enterprise application security teams.

All research conducted as part of this capstone is based exclusively on publicly available intelligence sources and vendor documentation, in strict compliance with ethical and containment protocols. No interaction with live ERP systems was performed. The resulting deliverables provide a structured, application-centric intelligence assessment intended to support enterprise defenders and decision-makers in understanding and mitigating the risk posed by APT41-style supply-chain intrusions targeting ERP environments.

TABLE OF CONTENTS

1. PROJECT BRIEFING

1.1 Project Codename

OPERATION VEILED SUPPLY-CHAIN

This codename reflects the covert and indirect nature of the threat examined in this project. It emphasizes the exploitation of trusted software supply chains and enterprise application ecosystems, where malicious activity is deliberately obscured behind legitimate vendors, updates, credentials and integrations.

1.2 Primary Warfighting Domain

Cyber Threat Intelligence and Enterprise Application Security (ERP / SAP)

This project is situated at the intersection of cyber threat intelligence and enterprise application security, with a specific focus on ERP platforms such as SAP. The warfighting domain emphasizes strategic intelligence analysis rather than offensive operations, examining how advanced persistent threats exploit application-layer trust and supply-chain dependencies within enterprise environments.

1.3 Situation Report (SITREP)

Enterprise Resource Planning systems aggregate some of the most sensitive and operationally critical assets within an organization. These platforms centralize business logic, financial data, supply-chain operations, authentication workflows and integration with third-party vendors and managed service providers. As a result, ERP systems operate within complex trust ecosystems that extend beyond organizational boundaries.

APT41 has demonstrated repeated success in abusing these trust relationships through a combination of software supply-chain compromise, exploitation of public-facing enterprise applications and the abuse of valid credentials and trusted certificates. Rather than relying on overt malware deployment, the group frequently leverages legitimate access paths and trusted components to blend malicious activity into normal business operations.

Although extensive public reporting exists on APT41's activities, most available intelligence remains generalized and infrastructure-focused. There is a lack of ERP-specific analysis that translates APT41's known tactics, techniques and procedures into practical detection and mitigation guidance for enterprise application security teams. This gap limits defenders' ability to effectively assess risk and prioritize controls within SAP and other ERP environments.

1.4 Problem Statement

Security teams responsible for protecting SAP and other ERP platforms lack an ATT&CK-aligned, application-centric intelligence assessment that contextualizes APT41's tradecraft within ERP architectures and integration layers. Existing threat intelligence does not sufficiently map adversary behavior to ERP-specific components such as application servers, middleware, background job frameworks and privileged service accounts. As a result, defenders face challenges in translating strategic threat reporting into actionable monitoring priorities and mitigation strategies tailored to enterprise application environments.

2. PROJECT OBJECTIVE

2.1 Primary Objective

To produce an ATT&CK-mapped intelligence dossier analyzing APT41's ERP-relevant supply-chain intrusion campaigns.

2.2 Secondary Objectives

a) To analyze APT41's intrusion lifecycle and ERP application impacts

To examine how APT41 achieves initial access, persistence, lateral movement and data exfiltration within ERP ecosystems, and to assess the operational impact of these activities on enterprise applications and business processes.

b) To Identify ERP-specific defensive monitoring priorities

To determine which ERP application-layer activities, authentication mechanisms and integration points present the highest detection value based on APT41's documented tradecraft.

c) To translate APT41 TTPs into actionable mitigation guidance for SAP environments

To provide practical, ERP-focused mitigation recommendations that align APT41's ATT&CK-mapped behaviors with defensive controls and security best practices relevant to SAP and similar enterprise application platforms.

3. ADVERSARY PROFILE: APT41

3.1 Threat actor overview

APT41, also publicly tracked under aliases such as Double Dragon and Winnti, is a highly sophisticated cyber threat group assessed to be Chinese state-aligned. The group is notable for conducting dual-purpose operations, combining long-term cyber espionage in support of strategic national objectives with financially motivated activities. This blended operational model distinguishes APT41 from many other advanced persistent threats and demonstrates a high degree of operational autonomy and technical maturity.

APT41 has been active for over a decade and has targeted a wide range of sectors, including technology, telecommunications, healthcare, logistics, software development and manufacturing. Of particular relevance to this project is the group's repeated focus on enterprise software vendors, managed service providers and trusted application ecosystems, making ERP platforms a natural downstream target of its operations.

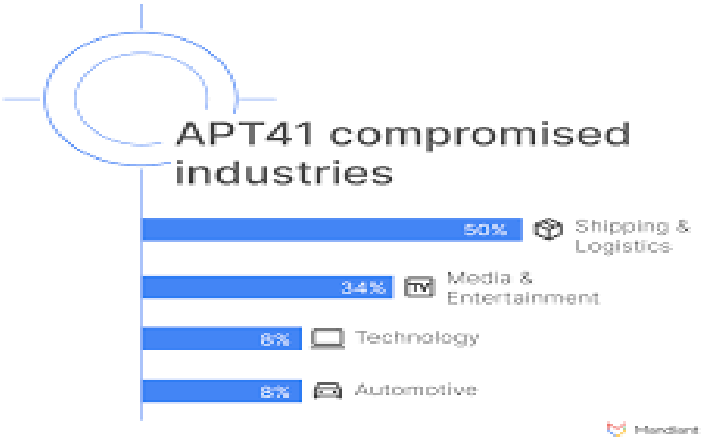


Figure 1: APT41 Targeted Sectors

3.2 Strategic objectives and intent

From an ERP-centric perspective, APT41's strategic objectives align closely with the exploitation of enterprise trust relationships. Rather than targeting ERP systems solely as end goals, the group frequently leverages them as strategic enablers for broader intelligence collection, operational persistence and lateral movement across enterprise environments.

Key strategic objectives relevant to ERP environments include:

- Access to sensitive financial and supply-chain data
- Intelligence collection on business operations and trade relationships
- Establishment of long-term, covert access within trusted enterprise platforms
- Abuse of ERP systems as pivot points to downstream systems such as databases, identity providers and partner networks

APT41's emphasis on stealth and persistence makes ERP systems particularly valuable targets, as malicious activity can be concealed within normal business workflows and trusted application processes.

3.3 Operational characteristics

APT41 exhibits several operational characteristics that directly increase risk to ERP platforms:

- **Supply-chain centric targeting:** Frequent compromise of software vendors, application developers and update mechanisms.
- **Living-off-the-land techniques:** Heavy reliance on legitimate credentials, certificates and built-in system tools.
- **Application-layer persistence:** Use of web shells, modified application components and scheduled tasks within enterprise applications.
- **Operational patience:** Willingness to maintain access over extended periods to support intelligence objectives.

These characteristics reduce reliance on easily detectable malware and increase the difficulty of identifying malicious activity within complex ERP environments.

3.4 Historical campaigns relevant to ERP ecosystems

Multiple publicly reported APT41 campaigns demonstrate behaviors that directly affect ERP and enterprise application environments. These campaigns frequently involve the compromise of trusted software components that are subsequently distributed to downstream customers.

Common elements observed across campaigns include:

- Compromised software updates delivered through legitimate vendor channels
- Exploitation of public-facing enterprise applications, including Java-based application servers commonly used in ERP deployments
- Abuse of valid credentials and service accounts to access internal systems
- Use of signed malware or stolen certificates to evade detection

While not always explicitly labeled as "ERP attacks," these campaigns routinely place APT41 in positions of access that intersect with ERP infrastructure, middleware, and integration layers.

Table 1: Summary of Publicly Reported APT41 Campaigns with Relevance to ERP Environments

Campaign / Reporting Source	**Initial Access Vector**	**Enterprise Impact**	**ERP Relevance**
Supply-Chain Compromise of Software Vendors (Mandiant, CrowdStrike)	Compromise of legitimate software vendors and update mechanisms	Downstream organizations receive trojanized software updates, enabling stealthy initial access	ERP systems often integrate vendor-supplied components, plugins and updates, making them vulnerable to indirect compromise through trusted software supply chains
Exploitation of Public-Facing Enterprise Applications (Mandiant, CISA)	Exploitation of internet-facing Java-based and web application servers	Web shell deployment, persistent access and credential harvesting	SAP NetWeaver and similar ERP web components expose comparable application-layer attack surfaces when improperly patched or monitored
Abuse of Valid Credentials and	Use of stolen or compromised	Lateral movement and long-term	ERP platforms rely heavily on privileged service accounts

Campaign / Reporting Source	Initial Access Vector	Enterprise Impact	ERP Relevance
Service Accounts (CrowdStrike)	enterprise credentials	persistence without malware	and background users, making credential abuse particularly impactful
Use of Signed Malware and Stolen Certificates (ESET, Kaspersky)	Abuse of trusted digital certificates to sign malicious binaries	Evasion of endpoint detection and increased trust by security controls	ERP environments frequently rely on certificate-based trust for integrations, increasing the risk of malicious activity appearing legitimate
Targeting of Managed Service Providers (MSPs) (Mandiant)	Compromise of MSP infrastructure and administrative access	Broad access to multiple customer environments	ERP systems are often managed or monitored by MSPs, allowing attackers indirect access to ERP infrastructure through trusted administrators
Data Collection and Staging Operations (Multiple Vendor Reports)	Aggregation and archiving of sensitive enterprise data prior to exfiltration	Loss of intellectual property, financial, and operational data	ERP databases contain high-value financial and supply-chain data, making them prime targets for data staging and exfiltration activities

3.5 APT41 tradecraft in an ERP context

When mapped to ERP environments, APT41’s tradecraft reveals a consistent focus on trust abuse rather than exploitation of novel vulnerabilities.

The group frequently leverages:

- Public-facing ERP components (e.g., web interfaces, portals, application servers)
- Privileged ERP service accounts used for integrations and background processing
- Middleware and API connections linking ERP systems to external services
- Certificate-based trust mechanisms to legitimize malicious activity

This tradecraft aligns with ERP architectures that prioritize availability and integration, often at the expense of granular security monitoring.

3.6 MITRE ATT&CK alignment (overview)

APT41's behaviors affecting ERP systems can be consistently mapped to MITRE ATT&CK enterprise techniques.

The most ERP-relevant techniques include:

- T1195 – Supply Chain Compromise
- T1190 – Exploit Public-Facing Application
- T1078 – Valid Accounts
- T1021 – Remote Services
- T1550 – Use of Stolen Certificates
- T1560 – Archive Collected Data

These techniques form the analytical backbone for subsequent sections of this project.

3.7 Relevance to enterprise defenders

Understanding APT41 as an adversary is critical for ERP defenders because the group's operations frequently bypass traditional perimeter and endpoint-focused security controls. By exploiting trusted relationships and legitimate application behavior, APT41 demonstrates how ERP platforms can become silent enablers of broader intrusion campaigns.

This adversary profile establishes the foundation for the subsequent technical analysis of APT41's intrusion lifecycle and the development of ERP-specific monitoring and mitigation priorities.

4. APT41 INTRUSION LIFECYCLE ANALYSIS (ERP-Focused)

4.1 Overview of the Intrusion Lifecycle

APT41’s operations against enterprise environments follow a structured and adaptive intrusion lifecycle that prioritizes stealth, persistence and abuse of trusted relationships. When viewed through an ERP-focused lens, this lifecycle is characterized by indirect initial access, application-layer persistence and the exploitation of privileged enterprise integrations rather than overt exploitation of endpoint systems.

This section analyzes APT41’s intrusion lifecycle using the MITRE ATT&CK framework as an organizing structure, with emphasis on how each phase manifests within ERP and SAP-centric environments.

4.2 Initial Access: Supply-Chain and Application Exploitation

APT41 commonly achieves initial access through indirect compromise vectors that align closely with ERP ecosystems. Two primary access paths are consistently observed:

4.2.1 Supply-Chain Compromise (T1195)

APT41 has repeatedly compromised software vendors, development environments and update mechanisms, enabling malicious code to be distributed to downstream customers through trusted channels. In ERP environments, this presents a significant risk due to the widespread use of:

- Vendor-provided SAP add-ons and plugins
- Third-party integration components
- Automated update and patching mechanisms

Once a compromised component is introduced, malicious activity inherits the trust level of legitimate ERP software, reducing the likelihood of detection.

4.2.2 Exploitation of Public-Facing Enterprise Applications (T1190)

APT41 has also exploited vulnerabilities in internet-facing enterprise applications, particularly Java-based web platforms. ERP systems such as SAP NetWeaver expose comparable application-layer interfaces, including portals, web services and administrative consoles. Successful exploitation enables attackers to deploy web shells or gain direct access to application servers hosting ERP components.

Reference Point: Detailed technique-to-ERP mappings for T1195 and T1190 are presented in Section 5 (ATT&CK Mapping Table)

4.3 Execution and Persistence within ERP Environments

Following initial access, APT41 prioritizes persistence mechanisms that blend into normal enterprise application behavior.

4.3.1 Application-layer persistence

Rather than relying on traditional endpoint persistence techniques, APT41 often establishes persistence within:

- Application directories
- Web-accessible components
- Scheduled or background processes

In ERP environments, this may involve modified application files, abuse of background job frameworks, or persistence through legitimate service configurations. These techniques exploit the operational complexity of ERP platforms, where frequent changes and scheduled tasks are normal.

4.4 Privilege Escalation and Credential Abuse

APT41 places significant emphasis on credential-based access, minimizing the need for privilege escalation exploits.

4.4.1 Abuse of valid accounts (T1078)

The group routinely leverages compromised credentials, including:

- Administrative users
- Service accounts
- Integration and technical users

ERP platforms rely heavily on such accounts for automation, batch processing and system-to-system communication. Once obtained, these credentials provide broad access across ERP modules and connected systems with minimal risk of detection.

4.5 Lateral Movement through Trusted Integrations

4.5.1 Remote services and trust relationships (T1021)

APT41 exploits the interconnected nature of enterprise environments by moving laterally via trusted remote services. In ERP contexts, this includes:

- ERP application servers to databases
- ERP systems to identity providers
- ERP platforms to external partner systems

Because these connections are expected and often insufficiently monitored, lateral movement originating from ERP systems can appear indistinguishable from legitimate business activity.

4.6 Defense Evasion through Trust Abuse

4.6.1 Use of stolen or misused certificates (T1550)

APT41 has a documented history of abusing stolen or compromised digital certificates to sign malicious components. This technique allows malicious activity to appear legitimate and bypass security controls.

ERP environments frequently rely on certificate-based trust for:

- Secure communications
- Application authentication
- Integration with external systems

This reliance amplifies the impact of certificate misuse within ERP ecosystems.

4.7 Data Collection, Staging and Exfiltration

4.7.1 Collection and archiving of ERP data (T1560

Once sufficient access is achieved, APT41 focuses on the collection of high-value enterprise data. ERP systems are particularly attractive due to their centralized storage of:

- Financial records
- Supply-chain data
- Business intelligence
- Intellectual property

Data is commonly staged and archived prior to exfiltration, reducing the likelihood of detection during transfer and enabling selective data theft aligned with strategic objectives.

4.8 Impact on ERP Ecosystems

The impact of APT41's intrusion lifecycle on ERP environments extends beyond data theft. Successful compromise can result in:

- Loss of financial and operational data confidentiality
- Undermining of enterprise trust relationships
- Potential manipulation of business processes
- Long-term exposure due to undetected persistence

These impacts highlight the need for ERP-specific threat intelligence and monitoring strategies rather than reliance on generic endpoint-focused defenses.

4.9 Summary of Lifecycle Analysis

APT41's intrusion lifecycle demonstrates a consistent preference for trust abuse, application-layer access, and credential-based operations, all of which align closely with ERP architectures. By mapping these behaviors to the MITRE ATT&CK framework within an ERP context, this analysis establishes a structured foundation for identifying defensive gaps and prioritizing monitoring and mitigation actions.

Table 2: ERP Impact Summary of APT41 Intrusion Lifecycle

Lifecycle Phase	**APT41 Behavior**	**ERP Components Affected**	**Operational / Strategic Impact**
Initial Access	Supply-chain compromise (T1195)	ERP plugins, add-ons, vendor-provided modules	Introduction of malicious components that inherit vendor trust, potential silent access
Initial Access	Exploitation of public-facing applications (T1190)	ERP web portals, admin consoles, API endpoints	Unauthorized access, possible deployment of web shells, immediate threat to critical interfaces
Persistence	Application-layer persistence	ERP background jobs, scheduled tasks, application directories	Long-term hidden access, risk of undetected manipulation of workflows
Credential Abuse	Use of valid accounts (T1078)	Privileged ERP service accounts, administrative users	Lateral movement, extended access without triggering endpoint alerts

Lifecycle Phase	**APT41 Behavior**	**ERP Components Affected**	**Operational / Strategic Impact**
Lateral Movement	Remote services (T1021)	ERP integrations, database connections, identity services	Expansion of attacker presence across ERP and connected systems, potential compromise of downstream processes
Evasion	Use of stolen certificates (T1550)	ERP certificate-based integrations, middleware	Malicious activity appears legitimate, bypassing trust-based controls and security monitoring
Collection & Exfiltration	Data staging and archiving (T1560)	ERP databases, financial tables, supply-chain records	Loss of sensitive data, intellectual property theft and operational disruption

5. MITRE ATT&CK TECHNIQUE MAPPING TABLES (ERP-Focused)

5.1 Purpose

This section presents a structured mapping of APT41's tactics, techniques and procedures (TTPs) against ERP environments, using the MITRE ATT&CK framework as a foundation. The mapping translates known adversary behaviors into ERP-relevant components, defensive gaps and recommended mitigations, providing actionable guidance for enterprise defenders.

5.2 ATT&CK Technique Mapping Table

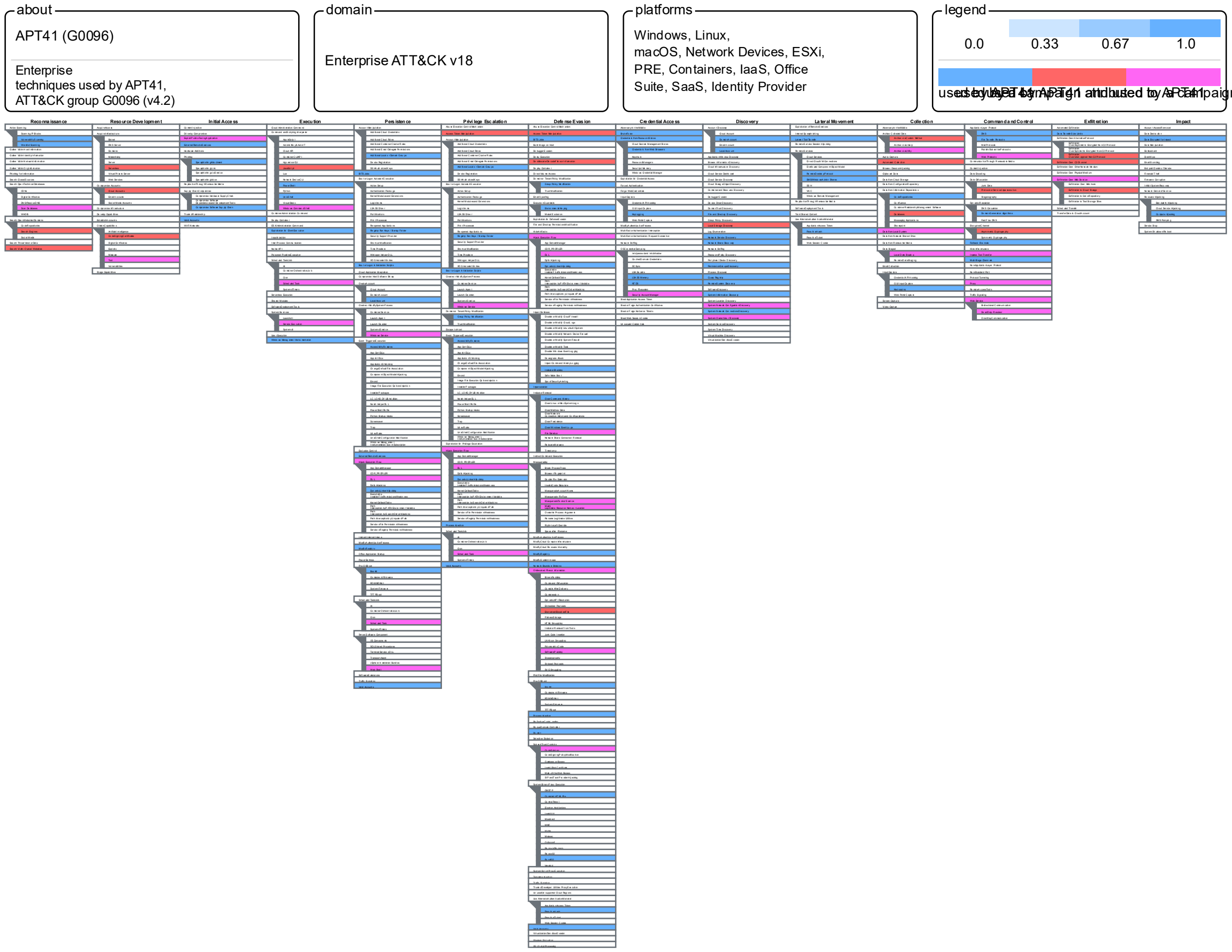
Table 3: Mapping of APT41's ATT&CK techniques to ERP components, highlighting defensive gaps and mitigation recommendations tailored to enterprise application security

ATT&CK ID / Technique	**Description / ERP Context**	**ERP Components Affected**	**Defensive Gaps Identified**	**Recommended Mitigations**
T1195 – Supply Chain Compromise	Malicious software distributed via trusted vendor channels	ERP plugins, add-ons, integration modules	Over-reliance on vendor-supplied components; lack of validation of updates	Vendor verification, digital signature validation, software inventory monitoring
T1190 – Exploit Public-Facing Application	Exploitation of ERP web interfaces or administrative portals	ERP web portals, admin consoles, API endpoints	Limited patching; insufficient monitoring of web-facing components	Regular patching, web application firewalls (WAF), portal/API activity monitoring
T1078 – Valid Accounts	Use of stolen or compromised credentials	ERP privileged accounts, service accounts	Overuse of high-privilege	Multi-factor authentication,

ATT&CK ID / Technique	**Description / ERP Context**	**ERP Components Affected**	**Defensive Gaps Identified**	**Recommended Mitigations**
			accounts; lack of anomaly detection	credential rotation, audit logging
T1021 – Remote Services	Lateral movement via trusted remote connections	ERP integration points, database links, identity services	Insufficient monitoring of internal trust relationships	Network segmentation, audit of remote access sessions, anomaly detection
T1550 – Use of Stolen Certificates	Signing malicious activity to bypass security	ERP certificate-based integrations, middleware	Poor certificate lifecycle management	Certificate inventory, monitoring, revocation procedures
T1560 – Archive Collected Data	Staging or archiving high-value ERP data prior to exfiltration	ERP databases, financial tables, supply-chain records	Limited monitoring of internal data movement	Data loss prevention (DLP), ERP audit log monitoring, anomaly detection on archiving

5.3 Visual Mapping

5.3.1 ERP-ATT&CK Matrix Diagram



about

APT41 (G0096)

Enterprise
techniques used by APT41,
ATT&CK group G0096 (v4.2)

domain

Enterprise ATT&CK v18

platforms

Windows, Linux,
macOS, Network Devices, ESXi,
PRE, Containers, IaaS, Office
Suite, SaaS, Identity Provider

legend

0.0	0.33	0.67	1.0

Figure 2: ERP-focused ATT&CK techniques visualized in the MITRE Enterprise Matrix (MITRE ATT&CK, 2025).

For a clear view of the ATT&CK matrix, see here: Enterprise matrix. *Download the image for a high-resolution view.*

6. ERP MONITORING AND MITIGATION PRIORITY BRIEF

6.1 ERP-Specific defensive gaps and risks

Defensive Gap	**Description / ERP Context**	**Risk / Threat Behavior**
Over-trusted third-party SAP plugins	ERP systems often rely on vendor-supplied add-ons, plugins and middleware without sufficient verification	Initial access via supply-chain compromise (T1195); hidden malware; long-term persistence
Insufficient logging of application-layer authentication	Limited or inconsistent logging of ERP user and service account activity	Credential abuse (T1078); undetected lateral movement; privilege escalation
Weak monitoring of RFC, OData, and API misuse	ERP integrations with databases, middleware, and external systems often lack anomaly detection	Lateral movement (T1021); data exfiltration; exploitation of trusted integrations
Poor separation of ERP application and OS-level telemetry	Lack of correlation between application-layer and OS/network telemetry	Reduced detection of persistence, malware, or abnormal system behavior; attackers bypass application-focused monitoring

6.2 ERP Monitoring Priorities

Based on the gaps above, the following ERP components and behaviors should be prioritized for monitoring:

ERP Component / Layer	Monitoring Focus
Third-party plugins	Plugin integrity checks, installation logs, vendor verification alerts
Authentication & Service Accounts	Detailed login records, service account activity, anomaly detection
RFC, OData, APIs	Rate limiting, usage patterns, anomalous activity detection across integrations
Application + OS telemetry	Correlation of ERP application, OS and network logs; centralized alerts for suspicious activity

6.3 Recommended Mitigation Strategies

a) **Vendor validation and control**: Verify all third-party ERP components before deployment; maintain software inventory and check digital signatures.

b) **Enhanced logging & audit:** Enable detailed application-layer authentication logging; monitor privileged accounts; implement anomaly detection.

c) **Integration monitoring:** Monitor RFC, OData and API usage; alert on unusual activity; correlate across system layers.

d) **Telemetry correlation:** Aggregate ERP application, OS and network logs in SIEM for holistic detection.

e) **Role-Based access controls:** Enforce least privilege and separation of duties (SoD) for all ERP users and service accounts.

f) **Patch & configuration management:** Regularly update ERP systems and third-party components to reduce exploitable vulnerabilities.

g) **Data Loss Prevention (DLP):** Implement monitoring and alerts for unusual data export, archiving or movement.

7. DECEPTION PROTOTYPE

Prototype Name: ERP Threat Telemetry Correlation Model (ETTCM)

7.1 Purpose

The ETTCM is a log-centric, ERP-focused defensive framework designed to detect, analyze and respond to APT41-related intrusion behaviors in ERP systems. By correlating SAP application logs, operating system telemetry, and network flows, this conceptual prototype demonstrates how defenders can:

- Identify ATT&CK-aligned TTPs without relying on exploit execution.
- Detect credential abuse, lateral movement and supply-chain compromise attempts.
- Provide actionable alerts and intelligence for security operations teams.

7.2 Core Components

Component	**Description**	**ERP Relevance**
SAP Security Audit Log Ingestion	Collects authentication events, transaction logs, role modifications and service account activity	Detects T1078 (Valid Accounts), unusual access patterns
Operating System Telemetry	Monitors system-level events such as process creation, file access and scheduled jobs	Supports detection of T1021 (Remote Services), T1550 (Use of Stolen Certificates)
Network Flow Collection	Captures internal and outbound network traffic from ERP servers, including API and RFC calls	Flags abnormal lateral movement, data exfiltration (T1560) and suspicious external communications
Deception Service Accounts	Dummy ERP accounts and service identities designed to attract attacker activity	Early detection of credential abuse; verifies alerts from log correlations
ATT&CK-Tagged Detection Rules	Rules and correlation logic mapping ERP telemetry to specific TTPs	Ensures automated mapping of behavior to MITRE ATT&CK framework for monitoring and reporting

7.3 Operational Workflow

a) Telemetry Collection
   - Logs from SAP applications, OS and network sensors are ingested into a centralized correlation engine.
   - Data normalization ensures all events can be analyzed consistently.

b) Behavioral Correlation
   - Detection rules match telemetry patterns against ATT&CK-mapped behaviors.
   - For example, simultaneous API abuse + suspicious service account activity triggers a T1021 / T1078 alert.

c) Deception Integration
   - Deception accounts are monitored for login attempts or unauthorized access.
   - Any interaction with these accounts generates high-confidence alerts.

d) Alerting & Reporting
   - Correlated events generate a prioritized alert list for SOC teams.
   - Visual dashboards can highlight high-risk ERP components, affected TTPs and potential attacker pathways.

e) Continuous Improvement
   - The framework is modular: new ATT&CK techniques, ERP modules or vendor components can be integrated into rules.
   - Supports scenario testing and “what-if” analysis in a controlled, conceptual environment.

REFERENCES

[1] N. Fraser et al., *APT41: A Dual Espionage and Cyber Crime Operation*, Mandiant/FireEye, Aug. 2019. Available: https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf Google Cloud

[2] MITRE, *APT41, Wicked Panda, Brass Typhoon, BARIUM, Group G0096*, MITRE ATT&CK. Available: https://attack.mitre.org/groups/G0096/ MITRE ATT&CK

[3] "Defending Against Software Supply Chain Attacks," Cybersecurity and Infrastructure Security Agency (CISA), Apr. 2021. Available: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf CISA

[4] CISA, *Defending Against Software Supply Chain Attacks* (online resource). Available: https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks CISA

[5] "APT41 DUST, Campaign C0040," MITRE ATT&CK Campaigns. Available: https://attack.mitre.org/campaigns/C0040/ MITRE ATT&CK

[6] "C0017, Campaign C0017," MITRE ATT&CK Campaigns. Available: https://attack.mitre.org/campaigns/C0017/ MITRE ATT&CK

[7] "Defending Against Software Supply Chain Attacks," Security Affairs, Apr. 2021. Available: https://securityaffairs.com/117286/hacking/cisa-nist-supply-chain-attacks.html Security Affairs

[8] SAP Security Notes & CVEs 2025: Analysis & Threats, Onapsis Blog, Jul. 22, 2025. Available: https://onapsis.com/blog/critical-sap-security-notes-cves-2025/ Onapsis

[9] Kaspersky, *APT41 Targets Southern African Organisation in Espionage Attack*, Jul. 21, 2025. Available: https://www.kaspersky.com/about/press-releases/kaspersky-apt41-targets-southern-african-organisation-in-espionage-attack Kaspersky

[10] "Advanced persistent threat," *Wikipedia*, accessed Dec. 14, 2025. Available: https://en.wikipedia.org/wiki/Advanced_persistent_threat Wikipedia