INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:36 UTC

# Ransomware Attack Disrupts Digital Operations at Spain’s Port of Vigo

THREAT CAMPAIGN | HIGH

| | |
|---|---|
| SCC Item ID | SCC-CAM-2026-0122 |
| Type | Threat Campaign |
| Severity | HIGH |
| Affected Products | Port of Vigo digital infrastructure, cargo management systems, port services servers |
| Published | 2026-03-29 |
| Discovery Source | Gemini |

## Executive Summary

A ransomware attack hit the Port of Vigo, Spain's largest fishing port, encrypting cargo management systems and port services infrastructure. Cargo operations reverted to manual handling during recovery, creating measurable throughput delays at a facility central to Spain's fishing and trade supply chain. Threat actor identity and ransomware variant remain unconfirmed; the incident signals continued adversary focus on maritime critical infrastructure where operational downtime carries direct economic consequence.

## Technical Analysis

The attack encrypted systems supporting cargo management and port services at the Port of Vigo. No CVE is associated; this is an IT/OT infrastructure incident, not a disclosed software vulnerability. MITRE ATT&CK techniques mapped to available reporting: T1566 (Phishing) as probable initial access vector; T1078 (Valid Accounts) for potential credential-based persistence or lateral movement; T1486 (Data Encrypted for Impact) as the primary impact technique; T1490 (Inhibit System Recovery) to delay restoration; T1041 (Exfiltration Over C2 Channel) indicating possible data staging or exfiltration before encryption. No ransomware variant, group attribution, or specific IOCs have been publicly confirmed as of available reporting. Source quality score is 0.64 across five Tier 3 sources; findings should be treated as credible but unverified pending official disclosure from port authorities or Spanish national CSIRT (CCN-CERT). No CVSS scores or EPSS data are applicable.

## Action Checklist

1. Containment, Audit externally accessible management interfaces for port management systems and OT/IT integration layers. Isolate cargo management platforms from broader enterprise networks if not already segmented. Revoke and rotate all privileged credentials used for remote access to port operations

systems. Block inbound connections from unrecognized external IPs at perimeter and OT DMZ boundaries.

2. Detection, Search SIEM for indicators of T1486 and T1490: volume shadow copy deletion (vssadmin delete shadows), BCDEdit recovery disable commands, and rapid file rename or extension-change events across file servers. Review authentication logs for T1078 anomalies: off-hours logins, geographic anomalies, and service account usage outside normal baselines. Check email gateway logs for T1566 patterns: macro-enabled attachments, password-protected archives, and spoofed sender domains targeting operational staff.

3. Eradication, No confirmed ransomware variant or IOCs are publicly available for this incident. Apply general ransomware eradication methodology: rebuild compromised systems from known-clean images rather than attempting in-place disinfection. Verify backup integrity before restoration, confirm backups predate the earliest suspected intrusion timestamp. Remove any identified unauthorized accounts or persistence mechanisms discovered during forensic review.

4. Recovery, Restore cargo management systems in a staged sequence: validate network segmentation controls before reconnecting OT-adjacent systems. Monitor restored systems for re-encryption attempts or re-activation of lateral movement tools for a minimum of 72 hours post-restoration. Confirm that shadow copy and backup services are re-enabled and functioning. Validate that access controls and MFA enforcement are active on all restored accounts.

5. Post-Incident, This incident exposes three common control gaps in port and critical infrastructure environments: insufficient network segmentation between IT and OT systems, absence of MFA on remote access pathways, and reliance on backup infrastructure reachable from the production network. Map identified gaps to NIST CSF PR.AC, PR.DS, and RC.RP controls. Engage CCN-CERT (Spain's national CSIRT) if not already coordinating; they maintain sector-specific guidance for critical infrastructure operators under Spain's NIS2 transposition obligations.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to CCN-CERT and invoke NIS2 notification obligations immediately if forensic review confirms exfiltration of cargo manifests, vessel scheduling data, or crew personally identifiable information prior to encryption, or if OT systems controlling physical port operations (crane controls, vessel traffic management) show any evidence of ransomware propagation beyond the confirmed IT cargo management perimeter. |
| **Recovery Notes** | Restore cargo management systems in strict dependency order — validate IT/OT network segmentation controls at the OT DMZ firewall before reconnecting any system with interfaces to physical port operations; do not restore remote access pathways until MFA is confirmed enforced on all accounts. Maintain active Sysmon and enhanced audit logging on all restored systems for a minimum of 72 hours post-reconnection, with manual log review every 8 hours given the absence of a confirmed ransomware variant and unknown dwell period. Verify that all backup jobs complete successfully and that at least one full backup copy is confirmed offline or immutable before declaring recovery complete, addressing the identified gap of backup infrastructure reachable from the production network. |

| | |
|---|---|
| **Forensic Artifacts** | Windows Security Event Log (Event IDs 4624, 4625, 4648, 4697, 7045) from all cargo management servers — these will show the T1078 valid account abuse timeline, service installations used for persistence, and the authentication path the ransomware operator used to move from initial access to cargo management system compromise. \| Volume Shadow Copy Service state and VSS event logs (Application Event Log, VSS provider entries) from cargo management hosts — T1490 VSS deletion is a near-universal ransomware pre-encryption step and the exact 'vssadmin delete shadows /all /quiet' execution timestamp anchors the encryption initiation point in the incident timeline. \| File server MFT (Master File Table) from cargo management and port services servers — MFT analysis via tools like MFTECmd will reveal the mass file rename/extension-change timestamps characteristic of T1486 encryption, identify which directories were encrypted first (indicating ransomware execution origin point), and may recover file metadata even where encrypted files have been overwritten. \| Email gateway delivery and quarantine logs for the 60 days preceding incident discovery, specifically filtering on macro-enabled Office attachments (.xlsm, .docm), ISO/IMG files, and password-protected archives sent to Port of Vigo operational staff — ransomware operators targeting maritime logistics consistently use T1566.001 spearphishing with operational lures (customs documents, vessel manifests, freight invoices) tailored to port staff workflows. \| Network flow logs or firewall session logs at the OT DMZ boundary for the 90 days preceding discovery — maritime ransomware campaigns targeting port infrastructure have used extended dwell periods for reconnaissance of cargo scheduling systems before encryption; outbound connections from cargo management servers to non-standard external IPs during this window will identify C2 infrastructure even without a confirmed variant or public IOC set. |

### Per-Action IR Details

**Containment — Audit external-facing access points for port management systems and OT/IT integration layers. Isolate cargo management platforms from broader enterprise networks if not already segmented. Revoke and rotate all privileged credentials used for remote access to port operations systems. Block inbound connections from unrecognized external IPs at perimeter and OT DMZ boundaries.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy

**Controls:** NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** Without enterprise NAC: run 'netstat -ano' on cargo management servers to enumerate active external sessions; kill suspicious PIDs with 'taskkill /PID /F'. Use Windows Firewall CLI to block inbound ranges: 'netsh advfirewall firewall add rule name="OT_BLOCK" dir=in action=block remoteip='. For OT/IT boundary isolation without a managed switch, physically disconnect the trunk port linking the cargo management VLAN to the enterprise LAN and document the disconnection timestamp for the incident timeline.

**Evidence:** Before isolating, capture full netflow or tcpdump from the OT DMZ interface ('tcpdump -i -w vigo_otdmz_capture.pcap') to preserve lateral movement paths the ransomware used between IT cargo management systems and OT-adjacent port services servers. Export Windows Security Event Log from all cargo management hosts filtering Event ID 4624 (Logon) and 4648 (Explicit Credential Use) for the 30 days prior to incident discovery — ransomware operators frequently abuse valid remote access accounts (T1078) for days to weeks before detonation. Screenshot or export firewall connection state tables at perimeter and OT DMZ before rule changes overwrite session data.

**Detection — Search SIEM for indicators of T1486 and T1490: volume shadow copy deletion (vssadmin delete shadows), BCDEdit recovery disable commands, and rapid file rename or extension-change events across file servers. Review authentication logs for T1078 anomalies: off-hours logins, geographic anomalies, and service account usage outside normal baselines. Check email gateway logs for T1566 patterns: macro-enabled**

**attachments, password-protected archives, and spoofed sender domains targeting operational staff.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis

**Controls:** NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without SIEM: deploy Sysmon with SwiftOnSecurity config on cargo management servers immediately — Event ID 1 (Process Create) will capture 'vssadmin.exe delete shadows' and 'bcdedit.exe /set recoveryenabled no' command lines. Run this PowerShell one-liner on file servers to detect mass extension changes indicative of T1486 encryption activity: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4663} | Where-Object {$_.Message -match "\.encrypted|\.locked|\.[a-z]{5,8}$"} | Select-Object TimeCreated, Message | Export-Csv C:\IR\ext_changes.csv'. For T1078 auth anomaly detection without UEBA: export Security Event Log 4624 records and pivot in Excel or grep/awk on Linux for service account logons (Logon Type 3 or 10) occurring between 2200-0600 local Spain time (UTC+1).

**Evidence:** Pull Windows Security Event ID 7045 (Service Installed) and 4697 from all cargo management hosts — ransomware groups commonly install services for persistence during the dwell period before encryption. Retrieve IIS or Apache access logs from the port services web servers for the 60 days preceding the incident, filtering for anomalous POST requests or URI paths inconsistent with normal cargo management API calls, which may reveal the initial access vector. Export email gateway quarantine and delivery logs for the 30 days prior, filtering on attachments with extensions .xlsm, .docm, .zip, .iso delivered to @apvigo.es or operational staff domains — T1566 phishing remains the predominant initial access vector for ransomware campaigns targeting port and logistics operators.

**Eradication — No confirmed ransomware variant or IOCs are publicly available for this incident. Apply general ransomware eradication methodology: rebuild compromised systems from known-clean images rather than attempting in-place disinfection. Verify backup integrity before restoration — confirm backups predate the earliest suspected intrusion timestamp. Remove any identified unauthorized accounts or persistence mechanisms discovered during forensic review.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication and Recovery

**Controls:** NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-2 (Baseline Configuration), NIST IR-4 (Incident Handling), CIS 4.6 (Securely Manage Enterprise Assets and Software)

**Compensating:** Without EDR for variant identification: submit memory dumps and encrypted file samples (with ransom note) to ID Ransomware (id-ransomware.malwarehunterteam.com) and No More Ransom (nomoreransom.org) to attempt variant identification before rebuilding — variant ID may reveal whether a decryptor exists and which threat actor group is responsible, informing whether CCN-CERT has specific intelligence. Run YARA rules from the RansomwareTracker or Malpedia community repositories against any preserved disk images before wiping: 'yara -r ransomware_rules.yar /mnt/compromised_image/'. Use 'reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' on all cargo management hosts to enumerate persistence before reimaging.

**Evidence:** Before reimaging any cargo management server, acquire a full forensic disk image using 'dc3dd if=/dev/sda of=/mnt/evidence/vigo_cargo_srv01.img hash=sha256 log=/mnt/evidence/vigo_cargo_srv01.log' or FTK Imager — the absence of a confirmed variant means post-incident variant attribution will depend entirely on artifacts preserved now. Capture the ransom note file (typically dropped in every encrypted directory) and one encrypted file sample per affected server before rebuilding; these are required for variant identification and potential law enforcement referral to Spain's Guardia Civil Cyber Crime Unit. Document the exact file paths and extensions of encrypted files on cargo management systems — the encryption scope defines the boundary between confirmed-compromised and potentially-clean systems and directly informs the restoration sequence.

**Recovery — Restore cargo management systems in a staged sequence: validate network segmentation controls before reconnecting OT-adjacent systems. Monitor restored systems for re-encryption attempts or re-activation of lateral movement tools for a minimum of 72 hours post-restoration. Confirm that shadow copy**

**and backup services are re-enabled and functioning. Validate that access controls and MFA enforcement are active on all restored accounts.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST CP-10 (System Recovery and Reconstitution), NIST SI-4 (System Monitoring), NIST IA-5 (Authenticator Management), NIST AU-4 (Audit Storage Capacity), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

**Compensating:** Without enterprise monitoring during the 72-hour watch window: configure Sysmon Event ID 11 (FileCreate) alerting on the restored cargo management servers using a PowerShell watcher script targeting directories that hold cargo manifest and vessel scheduling data — mass FileCreate events with unknown extensions signal re-encryption. Enable Windows VSS immediately post-restore via 'vssadmin create shadow /for=C:' on a scheduled task every 4 hours and verify via 'vssadmin list shadows'. For MFA enforcement without enterprise IAM: implement Windows Hello for Business or enforce TOTP via a self-hosted Authelia or Vaultwarden instance on the VPN gateway before any remote access is restored to cargo management systems.

**Evidence:** Before reconnecting any restored cargo management system to the port network, run 'Get-FileHash -Algorithm SHA256' against all restored system binaries and compare against the pre-incident baseline or known-good hashes from the vendor (port management software vendor documentation) — confirming integrity before reconnection is required per NIST 800-61r3 §3.5 and prevents reintroduction of a backdoor if backups were already compromised. Capture baseline netflow from restored systems during the 72-hour monitoring window to establish a clean behavioral profile; any outbound connection to non-port-operator IP ranges during this window should be treated as a re-infection indicator and trigger immediate re-isolation.

**Post-Incident — This incident exposes three common control gaps in port and critical infrastructure environments: insufficient network segmentation between IT and OT systems, absence of MFA on remote access pathways, and reliance on backup infrastructure reachable from the production network. Map identified gaps to NIST CSF PR.AC, PR.DS, and RC.RP controls. Engage CCN-CERT (Spain's national CSIRT) if not already coordinating — they maintain sector-specific guidance for critical infrastructure operators under Spain's NIS2 transposition obligations.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity

**Controls:** NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AU-11 (Audit Record Retention), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-6 (Incident Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** Without a GRC platform for gap mapping: use the CISA Maritime Cybersecurity Standards publication and ENISA's 'Guidelines on Maritime Cybersecurity' (freely available) as the baseline for port-specific control gap documentation. Build the lessons-learned report in a structured template referencing the three identified gaps — segmentation, MFA, offline backups — with specific remediation owners, target dates, and validation criteria. Submit the incident report to CCN-CERT via their LUCIA platform (the Spanish national incident reporting portal) and request the NIS2 sector-specific advisory package for port operators; CCN-CERT has published guidance under Spain's RD-Ley 12/2018 (NIS transposition) that directly addresses IT/OT segmentation requirements for critical maritime infrastructure.

**Evidence:** Compile the complete incident timeline from first forensic artifact (earliest suspicious Event ID or log entry) through recovery completion — this timeline is the primary deliverable for CCN-CERT reporting under Spain's NIS2 obligations and must be preserved in write-protected storage per NIST AU-11 (Audit Record Retention). Retain all forensic disk images, memory captures, ransom notes, encrypted file samples, and network packet captures for a minimum of 3 years to support potential Guardia Civil criminal investigation and future threat intelligence sharing with ENISA's maritime sector working group.

## Detection Guidance

In the absence of confirmed IOCs for this incident, detection should focus on behavioral TTPs mapped from the MITRE techniques. For T1486 (Data Encrypted for Impact): alert on mass file modification events, unexpected changes to file extensions, and Encrypting File System (EFS) activity on servers not configured for EFS use. For T1490 (Inhibit System Recovery): monitor for execution of 'vssadmin delete shadows /all', 'wbadmin delete catalog', or 'bcdedit /set recoveryenabled no'; these commands are rarely legitimate in port operations environments. For T1078 (Valid Accounts): correlate authentication logs against baseline behavioral profiles, flag service accounts authenticating interactively, accounts logging in from new hosts or geolocations, and privilege escalation events outside change windows. For T1566 (Phishing): review email gateway telemetry for delivery of macro-enabled Office documents, ISO/IMG attachments, and HTML smuggling payloads targeting operations or logistics staff. For T1041 (Exfiltration Over C2 Channel): monitor for anomalous outbound traffic volumes, especially to newly registered domains or IPs with no prior connection history. No confirmed hashes, domains, or IP indicators are available for this incident at time of reporting.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| DOMAIN | `not confirmed` | No IOCs have been publicly disclosed for this incident as of available reporting. This field will be updated if official attribution or IOC releases are made by CCN-CERT or the Port of Vigo. | LOW |

## Framework Mappings

### MITRE-ATTACK

- **T1490** — Inhibit System Recovery
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1041** — Exfiltration Over C2 Channel

### NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

**NIST-CSF-2**

- **RS.MI-01** — Incidents are contained

**HIPAA-SECURITY**

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

**ISO-27001-2022**

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1490 | Inhibit System Recovery | Impact |
| T1078 | Valid Accounts | Defense-Evasion |
| T1486 | Data Encrypted for Impact | Impact |
| T1566 | Phishing | Initial-Access |
| T1041 | Exfiltration Over C2 Channel | Exfiltration |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Ransomware attack disrupts operation at major Spanish fishing port** | https://therecord.media/port-of-vigo-ransomware | T3 |
| **Cyberattack on the Port of Vigo: what happened and why it matters** | https://www.apolocybersecurity.com/en/blog-posts/ciberataque-al-pue... | T3 |

| Source | URL | Tier |
|---|---|---|
| **Ransomware Attack Disrupts Operations at Spain's Port of Vigo** | https://securityboulevard.com/2026/03/ransomware-attack-disrupts-op... | T3 |
| **Port of Vigo Cyberattack Disrupts Cargo Systems - The Cyber Express** | https://thecyberexpress.com/port-of-vigo-cyberattack-disrupts-systems/ | T3 |
| **Ransomware Attack Disrupts Digital Operations at Spain's Port of Vigo** | https://beyondmachines.net/event_details/ransomware-attack-disrupts... | T3 |



Generated 2026-03-29 18:36 UTC by TJS Security Command Center