INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-25 13:52 UTC

EU Organizations and Their Suppliers Face Intensified Ransomware Targeting as Gangs Shift Regional Focus

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0565
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	EU-based organizations and their third-party suppliers; critical infrastructure sectors
Published	2026-06-25T06:00:00
Discovery Source	Rss

Executive Summary

Ransomware operators are actively shifting targeting toward EU-based organizations and their supply chain partners. Threat intelligence reporting suggests this shift is driven by the regulatory environment: GDPR and NIS2 create compounding financial pressure (operational ransom plus regulatory fine exposure) that increases victim incentive to pay. High-value critical infrastructure targets and interconnected supplier networks expand lateral movement opportunity. Organizations in the EU, and non-EU companies with significant EU supplier relationships, face elevated risk of ransomware deployment across their third-party attack surface. The business risk is dual-layered: operational disruption from encryption plus regulatory fine exposure if a breach triggers data protection notification obligations.

Technical Analysis

This item documents a strategic regional targeting shift by ransomware operators toward EU organizations and their third-party suppliers, reported by Dark Reading and corroborated by threat intelligence analysis. No CVE is associated; the risk is operational and strategic rather than tied to a specific unpatched vulnerability. Representative weakness classes are CWE-693 (Protection Mechanism Failure) and CWE-284 (Improper Access Control), reflecting ransomware initial access and propagation patterns. Mapped MITRE ATT&CK techniques span the full ransomware kill chain: T1078 (Valid Accounts) and T1566 (Phishing) for initial access; T1190 (Exploit Public-Facing Application) for perimeter compromise; T1195 (Supply Chain Compromise) for third-party ingress; T1021 (Remote Services) for lateral movement; T1071 (Application Layer Protocol) for C2 communication; T1486 (Data Encrypted for Impact) and T1490 (Inhibit System Recovery) for impact. The GDPR

and NIS2 regulatory environment is a deliberate force multiplier: non-payment risks compounding fine exposure, incentivizing victims to pay rather than disclose. CVSS does not apply to campaign-level threat activity; priority score is 0.85 based on campaign-level strategic assessment.

Action Checklist

1. Step 1: Containment. Audit all third-party supplier connections and remote access paths immediately. Identify suppliers with access to production systems, sensitive data stores, or OT networks. Suspend or restrict any supplier connections that cannot be verified as MFA-enforced and monitored. Reference NIST AC-20 (Use of External Systems) and CIS 6.3 (Require MFA for Externally-Exposed Applications) for baseline gate criteria.
2. Step 2: Detection. Enable or verify logging across remote access gateways, VPN concentrators, and identity providers. Hunt for T1078 indicators: authentication events from unfamiliar geolocations, off-hours privileged logins, and service account authentications outside normal baselines. Baseline normal authentication patterns for 30 days before alerting on new ASNs or geolocations to reduce false positives. Review EDR telemetry for T1486 precursors: volume shadow copy deletion (vssadmin delete shadows), backup service termination, and mass file rename events. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication. Enforce least privilege across all accounts with third-party or remote access (NIST AC-6). Rotate credentials on any accounts identified as shared, default, or not rotated within the last 90 days (NIST IA-4: Credential Management). Patch all internet-facing systems with known exploitable vulnerabilities, prioritizing those mapped to T1190. Enforce MFA on all remote access paths (CIS 6.4: Require MFA for Remote Network Access; NIST IA-2: Authentication).
4. Step 4: Recovery. After any suspected compromise, restore from offline or immutable backups only. Validate backup integrity before restoration. Monitor restored systems for re-infection indicators: renewed shadow copy deletion activity, unexpected scheduled task creation, and anomalous outbound C2 traffic on application-layer protocols (T1071). Apply NIST AU-9 (Protection of Audit Information) controls to ensure recovery audit trails are not tampered.
5. Step 5: Post-Incident. Conduct a third-party risk review against CIS 1.1 (Enterprise Asset Inventory) to ensure all supplier-connected assets are inventoried and scoped. Map supply chain ingress points to NIST AC-17 (Remote Access) policy requirements and remediate gaps. Document NIS2 and GDPR notification thresholds and confirm incident response playbooks include regulatory notification timelines. Review separation of duties (NIST AC-5) for backup administration to prevent ransomware operators from disabling recovery mechanisms.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if any evidence of data exfiltration from GDPR-regulated personal data stores or NIS2-scoped critical infrastructure systems is confirmed, or if a supplier-side compromise is identified that has propagated to production OT or ICS networks, triggering mandatory 24-hour early warning obligations under NIS2 Article 23 to the relevant national competent authority.

Recovery Notes	Restore only from backups predating the earliest confirmed indicator of compromise, not the earliest observed ransomware detonation — EU-targeting ransomware operators frequently maintain dwell times of 14-45 days before encryption to ensure backup poisoning. Verify restored systems by running YARA rules for known ransomware dropper signatures and checking for residual scheduled tasks and WMI subscriptions before reconnecting to production networks or supplier-facing segments. Maintain elevated monitoring on restored systems and all supplier access paths for a minimum of 30 days post-recovery, with specific alerting on any recurrence of shadow copy deletion commands, backup service termination, or outbound connections to newly registered domains, which are consistent with re-infection attempts by the same operator.
Forensic Artifacts	Windows Security Event Log Event IDs 4624, 4625, 4648, and 4688 from domain controllers and VPN-terminating systems covering supplier account authentication activity — specifically logon type 3 and 10 events from supplier source IP ranges during off-hours, which indicate valid-account initial access consistent with this campaign's supply chain entry vector | Volume Shadow Copy Service (VSS) deletion records: Sysmon Event ID 1 for `vssadmin.exe delete shadows /all /quiet`, `wbadmin.exe delete catalog -quiet`, and `bcdedit.exe /set {default} recoveryenabled no` — the specific command-line sequence used by ransomware operators to destroy recovery options before encryption detonation | Ransom note file artifacts deposited across encrypted directory trees — document full file paths, filenames, and hash values to identify ransomware family and variant for cross-referencing against Europol EC3 No More Ransom decryptor availability and to establish which threat group is operating the campaign | Identity provider (Entra ID, Okta, AD FS) conditional access and sign-in logs showing supplier account authentications, legacy authentication protocol usage (NTLM, basic auth), and any MFA bypass or registration events — critical for establishing whether the initial access was credential-based or MFA-bypassed, which determines the scope of the credential rotation required | Scheduled task and WMI subscription persistence artifacts: output of `schtasks /query /fo LIST /v` and `Get-WMIObject -Namespace root\subscription -Class __EventFilter` collected from all hosts in the supplier-accessible network segment — ransomware operators targeting EU supply chains commonly plant WMI subscriptions and scheduled tasks during the dwell period to survive partial remediation and re-establish access post-recovery

Per-Action IR Details

Step 1: Containment — Audit all third-party supplier connections and remote access paths immediately. Identify suppliers with access to production systems, sensitive data stores, or OT networks. Suspend or step-down any supplier connections that cannot be verified as MFA-enforced and monitored. Reference NIST AC-20 (Use of External Systems) and CIS 6.3 (Require MFA for Externally-Exposed Applications) for baseline gate criteria.

NIST Phase: Containment

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

Controls: NIST AC-20 (Use of External Systems), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Export active VPN sessions using `show vpn-sessiondb` (Cisco ASA) or equivalent gateway CLI; cross-reference against an approved supplier access register maintained in a spreadsheet. For suppliers using RDP or jump hosts, pull active sessions via `query session /server:` on Windows. Disable unverified supplier accounts immediately via `net user /active:no` or equivalent AD command. A 2-person team can divide by supplier tier: one handles identity verification calls, the other executes suspensions.

Evidence: Before suspending any supplier connection, capture: (1) active VPN session tables including source IPs, user accounts, session duration, and bytes transferred — export via gateway CLI or syslog before terminating; (2)

Windows Security Event Log Event ID 4624 (Successful Logon) and 4625 (Failed Logon) filtered for supplier account UPNs across all domain controllers for the prior 14 days; (3) firewall flow logs showing supplier source IP ranges communicating with production and OT network segments; (4) identity provider (Entra ID, Okta, AD FS) sign-in logs for all third-party accounts, including conditional access policy bypass events. Ransomware operators targeting EU supply chains frequently use supplier VPN credentials as initial access — this session state is volatile and gone once accounts are disabled.

Step 2: Detection — Enable or verify logging across remote access gateways, VPN concentrators, and identity providers. Hunt for T1078 indicators: authentication events from unfamiliar geolocations, off-hours privileged logins, and service account authentications outside normal baselines. Review EDR telemetry for T1486 precursors: volume shadow copy deletion (vssadmin delete shadows), backup service termination, and mass file rename events. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 1 (Process Create) for `vssadmin.exe`, `wbadmin.exe`, `bcdedit.exe`, and `net stop` targeting backup services (VSS, Veeam Transport, Windows Backup). Use the Sigma rule `win_ransomware_shadow_copy_deletion.yml` converted to Windows Event Log XML queries if no SIEM is available. For authentication hunting without a SIEM, run: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624} | Export-Csv auth_events.csv` and filter for logon type 3 (network) or 10 (remote interactive) from supplier account SAMAccountNames during off-hours. For identity provider logs without EDR, pull Entra ID sign-in logs via Microsoft Graph API using a free tenant account.

Evidence: This is a read/analyze step that does not alter live state, but log evidence must be preserved before any subsequent containment actions. Capture and preserve: (1) Windows Security Event Log Event IDs 4688 (Process Creation with command line) filtered for `vssadmin delete shadows`, `bcdedit /set {default} recoveryenabled no`, and `wbadmin delete catalog`; (2) Sysmon Event ID 1 for `vssadmin.exe`, `taskkill.exe` targeting backup processes, and `ren` or PowerShell `Rename-Item` mass execution sequences; (3) VPN concentrator authentication logs showing supplier account source geolocations and session timing anomalies; (4) Windows Event ID 7045 (New Service Installed) and 4698 (Scheduled Task Created) which ransomware operators use for persistence before detonation; (5) identity provider conditional access logs for any policy bypass or legacy authentication protocol (NTLM, basic auth) usage by supplier accounts, which EU-targeting ransomware groups exploit to bypass MFA.

Step 3: Eradication — Enforce least privilege across all accounts with third-party or remote access (NIST AC-6). Rotate credentials on any accounts identified as shared, default, or not rotated within the last 90 days (D3-CRO: Credential Rotation). Patch all internet-facing systems with known exploitable vulnerabilities, prioritizing those mapped to T1190. Enforce MFA on all remote access paths (CIS 6.4: Require MFA for Remote Network Access; D3-MFA).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For credential rotation without a PAM tool: script bulk AD password resets using `Set-ADAccountPassword` for all service accounts and supplier-linked accounts; export the target account list via `Get-ADUser -Filter {LastPasswordSet -lt (Get-Date).AddDays(-90)} -Properties LastPasswordSet`. For least privilege remediation without an IAM platform: run `Get-ADGroupMember 'Domain Admins'` and `Get-ADGroupMember 'Remote Desktop Users'` to identify over-privileged accounts, then remove supplier accounts from privileged groups via `Remove-ADGroupMember`. For internet-facing patch prioritization without a vulnerability scanner: cross-reference CISA KEV catalog (free, at cisa.gov/known-exploited-vulnerabilities-catalog) against installed software versions from

`winrm` inventory or `wmic product get name,version`.

Evidence: CRITICAL — volatile evidence must be captured before credential rotation, privilege changes, or patching, as each action destroys live forensic state. Before rotating credentials: (1) acquire full memory dump of any host suspected of active compromise using WinPmem or ProcDump on the LSASS process (`procdump -ma lsass.exe lsass.dmp`) to preserve in-memory credential material that ransomware operators may have harvested; (2) capture `netstat -ano` and `Get-NetTCPConnection` output to document active C2 or lateral movement connections before network changes; (3) export all active session tokens and OAuth refresh tokens from identity providers before invalidation — these show which supplier accounts were actively authenticated and to which resources; (4) collect registry hive exports (`reg export HKLM\SYSTEM` and `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`) for persistence mechanisms ransomware operators plant before detonation. Patching internet-facing systems without prior memory and process capture will destroy evidence of pre-existing exploitation.

Step 4: Recovery — After any suspected compromise, restore from offline or immutable backups only. Validate backup integrity before restoration. Monitor restored systems for re-infection indicators: renewed shadow copy deletion activity, unexpected scheduled task creation, and anomalous outbound C2 traffic on application-layer protocols (T1071). Apply NIST AU-9 (Protection of Audit Information) controls to ensure recovery audit trails are not tampered.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Validate backup integrity before restoration by computing SHA-256 hashes of backup archives and comparing against checksums recorded at backup creation time: `Get-FileHash -Algorithm SHA256 `. For post-restoration re-infection monitoring without EDR: deploy Sysmon on restored hosts immediately on first boot (before domain rejoining) and monitor Event ID 1 for the same shadow copy deletion and backup service termination commands used in Step 2 hunting. Monitor outbound C2 traffic using Wireshark or Windows Firewall logging (`netsh advfirewall set allprofiles logging filename C: w.log`) with alerting on unusual outbound connections on ports 443, 80, and 8443 to non-CDN destinations, which EU-targeting ransomware groups use for application-layer C2.

Evidence: Before initiating restoration, capture from the compromised system (if still accessible): (1) complete disk image using FTK Imager or `dd` to preserve encryption artifacts and ransomware binary drop locations (common paths: `C:\ProgramData\`, `C:\Windows\Temp\`, user `%APPDATA%` directories); (2) Windows Event Log Event IDs 4698 and 4702 (Scheduled Task Created/Modified) to document persistence mechanisms that must be removed before restoration is considered clean; (3) `schtasks /query /fo LIST /v` and `Get-ScheduledTask` output to enumerate all scheduled tasks, as ransomware operators targeting EU supply chains frequently plant recurring tasks to re-download payloads after partial remediation; (4) ransom note file paths and filenames (document but do not open) as they identify the specific ransomware family and variant, which informs whether a decryptor exists and which law enforcement body (Europol EC3, national CERTs) has jurisdiction for NIS2 notification purposes.

Step 5: Post-Incident — Conduct a third-party risk review against CIS 1.1 (Enterprise Asset Inventory) to ensure all supplier-connected assets are inventoried and scoped. Map supply chain ingress points to NIST AC-17 (Remote Access) policy requirements and remediate gaps. Document NIS2 and GDPR notification thresholds and confirm incident response playbooks include regulatory notification timelines. Review separation of duties (NIST AC-5) for backup administration to prevent ransomware operators from disabling recovery mechanisms.

NIST Phase: Post Incident

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

Controls: NIST AC-17 (Remote Access), NIST AC-5 (Separation Of Duties), NIST AC-2 (Account Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 6.2 (Establish an Access Revoking Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For third-party asset inventory without a CMDB: build a supplier access register in a spreadsheet that captures supplier name, accounts provisioned, systems accessible, MFA status, last access review date, and

contractual data processing basis under GDPR Article 28. For NIS2 notification timeline tracking without GRC software: create a dated incident log with a 24-hour early warning threshold and 72-hour notification threshold for significant incidents to the relevant national CSIRT (per NIS2 Article 23), with a calendar reminder triggered at incident declaration. For separation of duties on backup administration: create a separate AD group `Backup_Admins` and verify no account in that group overlaps with `Domain Admins` or supplier-linked accounts using `Compare-Object (Get-ADGroupMember Backup_Admins) (Get-ADGroupMember 'Domain Admins') -Property SamAccountName`.

Evidence: Post-incident evidence preservation for regulatory and lessons-learned purposes: (1) retain all VPN, identity provider, and firewall logs covering the incident window for a minimum of 12 months to satisfy NIS2 Article 23 supervisory authority requests and GDPR Article 33 documentation obligations — export and write-protect log archives immediately; (2) preserve the full incident timeline document including first indicator timestamp, containment action timestamps, and notification timestamps to demonstrate NIS2 72-hour notification compliance to the relevant national competent authority; (3) retain ransom note, encrypted file samples (in a quarantined, password-protected archive), and any attacker communications as evidence for Europol EC3 or national law enforcement referral; (4) document which supplier accounts were active during the compromise window and what data stores they accessed — this is the GDPR Article 33 personal data breach assessment foundation and must be preserved as a controller-processor incident record.

Detection Guidance

Focus detection on the ransomware pre-deployment phase, where dwell time creates the detection window. Key signals by technique: T1078 (Valid Accounts), alert on authentication from new ASNs or geolocations for privileged accounts, especially service accounts; baseline normal patterns for 30 days before alerting to reduce false positives; flag concurrent sessions from geographically separated IPs. T1566 (Phishing), monitor email gateway logs for malicious attachment delivery and link-click events; correlate with endpoint process creation events following email client activity. T1195 (Supply Chain Compromise), baseline supplier VPN and API authentication patterns; alert on deviations in access time, volume, or accessed resource types. T1021 (Remote Services), alert on lateral movement via RDP, WMI, or SMB from non-standard source hosts, particularly from third-party-associated network segments. T1486 (Data Encrypted for Impact) precursors, monitor for vssadmin.exe, wbadmin.exe, or bcdedit.exe execution with deletion or disable arguments; high-volume file rename or extension-change events across shared drives. T1490 (Inhibit System Recovery), alert on backup service stops, task scheduler manipulation targeting backup jobs, and firewall rule additions blocking backup infrastructure. Log sources: Windows Security Event Log (Event IDs 4624, 4625, 4648, 4672), EDR process telemetry, VPN/remote access gateway logs, email security platform, and cloud identity provider sign-in logs. NIST AU-2 and AU-12 define the event types that should be captured to support this detection posture.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1071** — Application Layer Protocol
- **T1190** — Exploit Public-Facing Application
- **T1490** — Inhibit System Recovery
- **T1021** — Remote Services

- **T1195** — Supply Chain Compromise

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **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
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access
T1071	Application Layer Protocol	Command-And-Control
T1190	Exploit Public-Facing Application	Initial-Access
T1490	Inhibit System Recovery	Impact
T1021	Remote Services	Lateral-Movement
T1195	Supply Chain Compromise	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cybersecurity-analytics/europe-evolves-...	T3
Vulnerabilities - NVD - National Institute of Standards and Technology	https://nvd.nist.gov/vuln	T1
What Is a Security Vulnerability? Definition, Types, and How They're ...	https://www.picussecurity.com/resource/glossary/what-is-a-security-...	T3
Software vendor refuses to fix security vulnerability - what to do?	https://security.stackexchange.com/questions/264626/software-vendor...	T3

Source	URL	Tier
Content Security Policy (CSP) Not Implemented - Invicti	https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/c...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-25 13:51 UTC by TJS Security Command Center