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

France: National Cybersecurity Agency Reports Ransomware Attack Drop in 2025

SECURITY ANALYSIS | INFORMATIONAL

SCC Item ID	SCC-STY-2026-0012
Type	Security Analysis
Severity	INFORMATIONAL
Affected Products	French public and private sector organizations (broad); specific sectors not confirmed from available data
Published	1 day ago
Discovery Source	Rss

Executive Summary

France's national cybersecurity agency ANSSI reported a measurable decline in ransomware attacks targeting French organizations in 2025, attributed in part to coordinated law enforcement operations that disrupted threat actor infrastructure. The finding signals that reported enforcement pressure can produce measurable results, though the underlying ransomware ecosystem remains active and adaptive. For security and risk leaders, this is a moment to reinforce defenses rather than reduce vigilance; historical patterns show ransomware groups reconstitute after disruption.

Technical Analysis

ANSSI's reported decline in French ransomware incidents during 2025 aligns with a broader pattern of law enforcement attrition against ransomware infrastructure observed globally over the same period. Operations targeting ransomware-as-a-service (RaaS) ecosystems, including affiliate networks, payment infrastructure, and negotiation portals, have demonstrated a measurable, if temporary, suppression effect on attack volume. The MITRE ATT&CK techniques associated with this story (T1486: Data Encrypted for Impact, T1489: Service Stop, T1490: Inhibit System Recovery) represent the terminal-phase execution playbook common across commodity and sophisticated ransomware operators alike. These TTPs have not changed materially despite enforcement pressure, meaning defensive posture against ransomware deployment mechanics remains as relevant as ever. ANSSI has historically tracked both criminal and state-adjacent ransomware activity targeting French critical infrastructure, including healthcare, local government, and industrial operators. While the specific sector breakdown and quantitative figures from the 2025 report are not fully confirmed from available source data, the directional finding is consistent with typical law enforcement trend reporting. A critical caveat applies: ANSSI incident counts reflect reported and confirmed cases. Underreporting, particularly in the private sector, means

the true decline may be smaller than agency data suggests, or may reflect improved response and containment rather than reduced attack attempts. Security teams should treat this as a positive signal, not a trend that justifies reduced investment in ransomware resilience. Law enforcement disruptions have historically been followed by regrouping; ransomware groups displaced by operations have been observed to reconstitute under new names or migrate to competing RaaS platforms.

Action Checklist

1. Step 1: Assess current ransomware resilience posture, verify that backup architecture follows 3-2-1 principles, backups are tested for restoration, and backup systems are isolated from primary network segments to prevent T1490 (Inhibit System Recovery) techniques from succeeding.
2. Step 2: Review detection coverage for T1486 (Data Encrypted for Impact), T1489 (Service Stop), and T1490, confirm SIEM or EDR rules are tuned to flag high-volume file rename or encryption activity, service termination targeting backup and security tools, and shadow copy deletion commands.
3. Step 3: Update threat model to account for post-disruption reconstitution risk; ransomware groups displaced by law enforcement frequently reband under new names or migrate to competing RaaS platforms. Adjust threat actor tracking accordingly rather than treating disrupted groups as eliminated.
4. Step 4: Brief leadership on the nuanced signal; a reported drop in French incidents is a positive law enforcement outcome, not evidence that ransomware risk has materially declined for your organization. Frame investment decisions against the persistent underlying threat.
5. Step 5: Monitor ANSSI's official website and Europol/Eurojust communications for confirmation of 2025 ransomware decline data and any associated operation disclosures, as these may surface new IOCs, affiliate TTPs, or sector-specific targeting patterns relevant to your environment.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and incident response leadership immediately if any detection rule in Step 2 fires with high confidence (>80%) on backup systems, shadow copy deletion commands, or service termination of backup agents; or if threat model review in Step 3 identifies IOC resurfacing matching historically disrupted groups — both warrant immediate containment readiness and potential external IR engagement.
Recovery Notes	Post-containment, prioritize: (1) restore from verified clean backup (3-2-1 validated in Step 1) to isolated environment, scan for reinfection before production reconnection; (2) revoke all credentials used during incident window, force password resets for accounts with access to backup systems; (3) review and patch vectors exploited (e.g., ProxyShell, Veeam CVEs) before restoration; (4) preserve forensic artifacts (memory dumps, disks, logs) for post-incident analysis and law enforcement collaboration; (5) update detection rules with IOCs and TTPs observed to prevent recurrence.

Forensic Artifacts	Windows Event Logs: 4688 (Process Creation), 4697 (Service Install), 4689 (Process Termination), 4690 (Backup Object Delete), 4720-4722 (Account Creation/Enabling) | Sysmon Event IDs: 1 (Process Creation, encryption tool execution), 11 (File Created, bulk renames/encryption), 17 (Pipe Created, lateral movement), 3 (Network Connection, C2 beaconing) | File System Artifacts: MFT ($MFT), USN Journal ($Extend\$UsnJrnl:$J) for file operation timeline, shadow copies ($SYSTEM Volume Information), alternate data streams (ADS) for malware staging | Memory Artifacts: Process dumps of encryption/service termination utilities, network sockets and connections (netstat -anob equivalent), loaded DLLs and code injection indicators | Network Artifacts: Firewall logs (outbound connections to C2, lateral movement RDP/SMB), DNS query logs (domain resolution patterns), VPN/proxy logs for external C2 communication | Application Logs: Backup software logs (failed jobs, access denials), security tool logs (AV/EDR detections, quarantine history), database transaction logs if applicable

Per-Action IR Details

Step 1: Assess current ransomware resilience posture, verify that backup architecture follows 3-2-1 principles, backups are tested for restoration, and backup systems are isolated from primary network segments to prevent T1490 (Inhibit System Recovery) techniques from succeeding.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: resource and tools); NIST 800-61r3 §4.4.4 (Recovery strategies)

Controls: NIST 800-53 CP-9 (Information System Backup), NIST 800-53 CP-10 (Information System Recovery and Reconstitution), NIST 800-53 SC-7 (Boundary Protection), CIS 3.14 (Backup and Disaster Recovery), CIS 11.1 (Backup and Recovery Practices)

Compensating: Without enterprise backup appliances: (1) Validate 3-2-1 manually — document two local copies on separate media (USB/NAS) and one offsite copy (encrypted cloud or external drive stored offsite); test restoration quarterly by recovering a sample dataset to isolated VM and verifying data integrity with checksums (SHA-256); (2) Isolate backups via air-gap (USB disconnected except during backup windows) or separate vLAN with no inbound RDP/SMB rules; restrict backup access to a dedicated service account with no domain admin rights; (3) Use open-source tools: Bacula, Veeam Community Edition (limited), or rsync + cron for incremental backups with immutable flag (chattr +i on Linux) post-backup.

Evidence: Capture backup logs (schedule, size, success/failure), last known good restore test results with timestamps, network segmentation rules (firewall ACLs, vLAN configs), backup service account permissions audit, and proof of offsite backup delivery (log entries from cloud provider or dated external drive inventory).

Step 2: Review detection coverage for T1486 (Data Encrypted for Impact), T1489 (Service Stop), and T1490, confirm SIEM or EDR rules are tuned to flag high-volume file rename or encryption activity, service termination targeting backup and security tools, and shadow copy deletion commands.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis); NIST 800-61r3 §3.2.4 (Indicator generation and signatures)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 SI-4(2) (Automated Tools for Real-Time Analysis), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), CIS 8.3 (Configure Data Loss Prevention), CIS 8.5 (Deploy File Integrity Monitoring), CIS 13.8 (Implement and Maintain File Integrity Monitoring)

Compensating: Without SIEM/EDR: (1) Enable Windows Event Logging (4688 Process Creation, 4697 Service Install, 4689 Process Termination) and export daily to a write-once log aggregation server; parse with grep/awk for patterns (vssadmin delete shadows, net stop, wmic logicaldisk, bcdedit /set {current} recoveryenabled no); (2) Monitor file system via Auditbeat (free, Elastic) or osqueryd for high I/O on system directories (/Windows, /ProgramFiles); alert on >100 file modifications/min in single directory; (3) Use Sysmon (free, Microsoft) on endpoints configured to log file creates/renames with hash matching and pipe creation; forward to central log collector; (4) Deploy Osquery (free, Facebook) with queries for service disablement (SELECT * FROM services WHERE status='stopped' AND name LIKE '%backup%') every 5 minutes.

Evidence: Collect Windows Event Logs (4688, 4697, 4689, 4690 deleted object), Sysmon Event IDs 1 (Process Creation, T1486 encryption tools), 11 (File Created, renamed files), 17 (Pipe Created, T1570 lateral movement), 3 (Network Connection, beaconing); /var/log/audit/audit.log on Linux for execve syscalls and unlink; file system change logs from any FIM tool; network logs showing DNS queries to ransomware command infrastructure.

Step 3: Update threat model to account for post-disruption reconstitution risk; ransomware groups displaced by law enforcement frequently reband under new names or migrate to competing RaaS platforms. Adjust threat actor tracking accordingly rather than treating disrupted groups as eliminated.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Incident Determination); NIST 800-61r3 §3.2.5 (Incident documentation and notification)

Controls: NIST 800-53 RA-3 (Risk Assessment), NIST 800-53 PM-7 (Integrated Information Security Risk Management Program), NIST 800-53 SI-4(16) (Automated Threat Recognition), CIS 1.1 (Govern the Use of Organizational Assets), CIS 14.1 (Establish and Maintain a Security Awareness Program)

Compensating: Maintain a living threat actor registry (spreadsheet or wiki) documenting: (1) known ransomware group names, aliases, and rebranding history (cross-reference MITRE ATT&CK groups, Ransomware.live, Dark Web Forum archives); (2) associated IOCs (C2 domains, server IPs, file hashes) and their operational window; (3) observed RaaS platform affiliations and migration patterns; (4) sector/geography targeting; (5) TTP overlap (e.g., ProxyShell exploitation, Veeam backup targeting); update weekly from open-source threat feeds (URLhaus, abuse.ch, Shodan queries for known C2 signatures); flag any IOC resurfacing or naming overlap as likely rebrand.

Evidence: Capture current threat model document (date, actor list, assessed likelihood), IOC inventory with source and confidence level, any detections matching historically disrupted group IOCs (domain resolutions, file hashes, network connections), and external threat intelligence reports (CISA AA, vendor advisories) referencing post-disruption reconstitution.

Step 4: Brief leadership on the nuanced signal; a reported drop in French incidents is a positive law enforcement outcome, not evidence that ransomware risk has materially declined for your organization. Frame investment decisions against the persistent underlying threat.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4.4.1 (Lessons Learned); NIST 800-61r3 §2.3.6 (Security awareness and training)

Controls: NIST 800-53 PM-1 (Information and Communications Technology (ICT) Governance), NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 AT-1 (Security Awareness and Training Policy), CIS 17.1 (Define and Maintain a Cyber Risk Register), CIS 17.2 (Assess Risk Explicitly)

Compensating: Prepare a one-page risk position statement for leadership that includes: (1) French law enforcement disruption statistics (ANSSI-reported, externally verified); (2) global ransomware incident volume 2024–2025 (cite Statista, SonicWall, Emsisoft reports showing persistent ecosystem); (3) RaaS market health assessment (number of active platforms, affiliate recruitment activity); (4) organization's sector/geography risk elevation vs. French average (if available from Ransomware.live or sector-specific sources); (5) conclusion: no material risk reduction for this org; (6) recommended investment priorities (backup resilience, detection tuning, incident response retainer).

Evidence: Collect ANSSI press releases and official statements, external threat intelligence summaries (Gartner, Forrester, Mandiant reports on 2025 ransomware outlook), internal risk register showing ransomware as persistent threat, and any incident history (prior attacks, near-misses) specific to your organization or sector.

Step 5: Monitor ANSSI's official website and Europol/Eurojust communications for confirmation of 2025 ransomware decline data and any associated operation disclosures, as these may surface new IOCs, affiliate TTPs, or sector-specific targeting patterns relevant to your environment.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Indicators and Anomalies); NIST 800-61r3 §3.2.4 (Indicator generation and signatures)

Controls: NIST 800-53 RA-3(1) (Risk Assessment | Threat and Vulnerability Identification), NIST 800-53 SI-4(7) (Information System Monitoring | Automated Response), NIST 800-53 SI-5 (Security Alerts, Advisories, and Directives), CIS 4.3 (Address Unauthorized Software), CIS 15.1 (Establish and Maintain an Incident Response Infrastructure)

Compensating: Set up automated monitoring without paid threat intelligence: (1) Subscribe to free RSS feeds from ANSSI (anssi.gouv.fr/communiques), Europol press releases, and CISA Alerts; pipe to a monitoring tool (e.g., Feedly, Zapier free tier, or cron job with curl + grep); set keywords (ransomware, operation, disruption, IOC); (2) Maintain a saved search on Twitter/X for @anssi_fr, @Europol, and @CISAgov with notifications for retweets/mentions; (3) Periodically query VirusTotal Intelligence (free tier limited) or abuse.ch for emerging C2 domains; (4) Subscribe to Shodan alerts for known ransomware C2 IPs; (5) Document any disclosed IOCs (domains, IPs, file hashes) in threat actor registry; cross-reference against EDR/firewall logs within 48 hours of disclosure.

Evidence: Collect historical monitoring logs (search history, subscription confirmations), IOC disclosures from official sources (screenshots, archived URLs), internal detection results (any hits on newly disclosed IOCs), and timeline correlation (when IOC disclosed vs. when observed in your environment).

Detection Guidance

Because this story reports a trend decline rather than an active incident, detection guidance focuses on hardening against the confirmed TTPs (T1486, T1489, T1490) that remain active regardless of enforcement outcomes. Log sources to prioritize: Windows Event Logs (Event IDs 7036, 7040 for service state changes tied to T1489; VSS deletion activity via vssadmin or wmic for T1490), EDR telemetry for mass file extension changes or encryption-pattern write operations (T1486), and PowerShell/cmd execution logs for shadow copy deletion one-liners. Behavioral patterns to hunt: processes spawning vssadmin delete shadows or wbadmin delete catalog outside of authorized maintenance windows; backup agent services stopping without a corresponding change ticket; high file I/O rates combined with uniform file extension changes across multiple directories in a short window. Policy gaps to audit: verify that backup service accounts are not reachable via lateral movement paths from workstation-tier endpoints; confirm that endpoint protection is configured to prevent tampering with its own service (self-protection mode enabled). No confirmed IOCs are available from the source data for this story.

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1489** — Service Stop
- **T1490** — Inhibit System Recovery

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **IR-4** — Incident Handling

NIST-CSF-2

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

HIPAA-SECURITY

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

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1489	Service Stop	Impact
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
Infosecurity Magazine	https://www.infosecurity-magazine.com/news/france-anssi-ransomware-...	T3
National Cybersecurity Agency Reports Ransomware Attack Drop in ...	https://www.dataproof.co.za/index.php/2026/03/11/france-national-cy...	T3
France's Cybersecurity Agency Reports Ransomware Attack Drop in ...	https://x.com/TheCyberSecHub/status/2031775477107732814	T3
National Cybersecurity Agency Reports Ransomware Attack Drop in ...	https://www.socdefenders.ai/item/fbfa76a4-1bc2-41fd-8aae-a1e333fdf3e0	T3
National Cybersecurity Agency Reports Ransomware Attack Drop in ...	https://www.instagram.com/p/DVweix3kyWT/	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 2026-03-29 18:36 UTC by TJS Security Command Center