INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 06:45 UTC

France Titres Breach: 19 Million Identity Records Linked to National Document Infrastructure Now for Sale

DATA BREACH | CRITICAL | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0098
Type	Data Breach
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	ANTS (Agence nationale des titres sécurisés), ants.gouv.fr portal; French Ministry of the Interior identity and registration document systems
Published	2026-04-21T17:46:04
Discovery Source	Rss

Executive Summary

France Titres (ANTS), the French government agency responsible for issuing passports, national identity cards, driver's licenses, and immigration documents, confirmed a breach detected April 15, 2026, with a threat actor of unknown identity actively selling 19 million citizen records on hacker forums. Exposed data includes full names, dates and places of birth, home addresses, phone numbers, and account identifiers sourced from authoritative national identity infrastructure. The breach creates material downstream risk of large-scale identity fraud, synthetic identity campaigns, and targeted social engineering against French citizens, with potential cross-border exposure wherever French identity documents are accepted.

Technical Analysis

Affected system: ANTS portal (ants.gouv.fr) and associated French Ministry of the Interior identity and registration document infrastructure. Breach confirmed April 15, 2026. No CVE assigned. Root cause vector is unconfirmed; suspected contributors include CWE-284 (Improper Access Control) and CWE-522 (Insufficiently Protected Credentials), with CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) as the direct outcome. Relevant MITRE ATT&CK techniques mapped to threat actor post-breach activity: T1566 (Phishing), T1598 (Phishing for Information), T1078 (Valid Accounts), T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1585 (Establish Accounts), T1041 (Exfiltration Over C2 Channel). No patch or vendor advisory is available at this time; root cause remediation details have not been publicly disclosed. ANSSI and CNIL are actively involved in the response. Threat actor identity is unknown; data

is being actively marketed on hacker forums as of April 2026. Primary confirmed reporting from BleepingComputer and ANTS official channels; technical specifics of the attack vector remain unverified in public reporting.

Action Checklist

1. Containment: If your organization operates services that authenticate French citizens using ANTS-derived identity data (passport numbers, national ID card numbers, driver's license numbers), treat those identifiers as confirmed compromised. Flag accounts associated with French PII for enhanced verification until ANTS provides formal breach scope confirmation.
2. Detection: Monitor for anomalous authentication attempts referencing French national identifiers. Search SIEM logs for spikes in account creation, login attempts, or identity verification requests associated with French PII fields. Watch threat intelligence feeds and hacker forum monitoring services for your organization's domain or data appearing in proximity to this dataset.
3. Eradication: No patch is available; root cause has not been publicly confirmed. If your systems relied on ANTS-issued document numbers as a sole authentication factor, remove that single-factor dependency immediately. Enforce multi-factor authentication on any portal accepting French identity document inputs.
4. Recovery: Validate that no internal systems ingested or cached ANTS-sourced identity data in a manner that extended your own exposure surface. Review data minimization practices for French citizen PII held internally. Confirm CNIL notification obligations under GDPR Article 33 if your organization processed or holds any of the affected data categories.
5. Post-Incident: Conduct a control gap review against NIST SP 800-53 AC-2 (Account Management), IA-5 (Authenticator Management), and SC-28 (Protection of Information at Rest) controls. Evaluate whether third-party identity verification dependencies introduce breach propagation risk into your supply chain. Update threat models to account for high-confidence French citizen PII now circulating in criminal marketplaces.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal, DPO, and executive leadership if any internal data store is confirmed to have ingested ANTS-sourced PII, if anomalous authentication patterns matching MITRE T1078 (Valid Accounts) are detected against French citizen accounts, or if your organization's domain or data appears in proximity to the ANTS dataset sale thread on hacker forums — all three conditions trigger GDPR Article 33's 72-hour CNIL notification clock.
Recovery Notes	Post-containment, enforce continuous monitoring of authentication endpoints accepting French document identifiers for a minimum of 90 days, as threat actors who purchased the 19M record dataset will conduct account takeover campaigns on an extended timeline. Validate that all data minimization remediations are reflected in an updated GDPR Article 30 Records of Processing Activities entry. Re-verify MFA enforcement weekly for the first month using your IdP's admin audit log, as misconfigurations introduced during emergency remediation are a documented post-incident risk.

Forensic Artifacts	Application authentication logs covering 90 days pre- and 30 days post-April 15, 2026: filter for HTTP POST requests to identity verification or account creation endpoints containing French document number patterns (passport regex [A-Z0-9]{9}, CNI regex [0-9]{12}) — these establish whether compromised ANTS records were weaponized against your platform | IdP (Identity Provider) audit logs (Keycloak audit DB, Azure AD Sign-In logs, Okta System Log): extract all account creation and authentication events for users with country_code=FR or document_type IN (passport_fr, CNI, permis) — look for success events from anomalous IPs or unusual device fingerprints consistent with T1078 abuse of the leaked dataset | Database transaction logs for any table storing French citizen PII fields (nom, prenom, date_naissance, lieu_naissance, adresse, telephone, numero_document): extract INSERT/UPDATE timestamps and source application identifiers to establish whether your organization's data holdings overlap with the 19M records confirmed in the ANTS breach | API gateway or WAF request logs for identity verification endpoints: look for high-frequency calls from single IPs or ASNs submitting varied French document numbers — a pattern of sequential or bulk document number submissions is a direct indicator of credential stuffing using the ANTS dataset, consistent with T1110 (Brute Force) / T1078 (Valid Accounts) | Data pipeline and ETL job logs for any workflow that consumed ANTS-sourced identity feeds or third-party identity verification API responses: these logs establish your organization's upstream data lineage from ANTS infrastructure and are required evidence for scoping your own secondary exposure and GDPR Article 33 notification obligations

Per-Action IR Details

Containment — If your organization operates services that authenticate French citizens using ANTS-derived identity data (passport numbers, national ID card numbers, driver's license numbers), treat those identifiers as potentially compromised. Flag accounts associated with French PII for enhanced verification until ANTS provides formal breach scope confirmation.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Export your user account table and filter for accounts where identity_document_type IN ('passport_fr','carte_identite','permis_conduire') or country_code = 'FR'. Flag those accounts in your IdP (Keycloak, FreeIPA, or AD) by adding a 'step_up_required' attribute via PowerShell Set-ADUser or ldapmodify. Force re-authentication with a second factor (SMS OTP, TOTP) on next login. If no IdP attribute is available, build a deny-list text file and run it against your auth logs with: grep -Ff compromised_ids.txt auth.log | awk '{print $1,$2,$9}' > flagged_sessions.txt

Evidence: Before flagging accounts, snapshot your identity provider's account table including last_login, creation_date, document_number_hash, and associated_IP. Export IdP audit logs (e.g., /var/log/keycloak/keycloak.log or Azure AD Sign-In logs) covering 90 days prior to April 15, 2026 to establish a pre-breach authentication baseline. Preserve this baseline in write-once storage before any account modifications alter the audit trail.

Detection — Monitor for anomalous authentication attempts referencing French national identifiers. Search SIEM logs for spikes in account creation, login attempts, or identity verification requests associated with French PII fields. Watch threat intelligence feeds and hacker forum monitoring services for your organization's domain or data appearing in proximity to this dataset.

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-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run this directly against your web server or application auth logs: grep -E '(passport|carte_nationale|permis|document_number)' /var/log/nginx/access.log | awk '{print $1}' | sort | uniq -c | sort -rn > fr_doc_spikes.txt. For Windows IIS, use: Get-WinEvent -LogName 'Microsoft-IIS-Logging/Logs' | Where-Object {$_.Message -match 'FR_ID|passeport|CNI'} | Export-Csv auth_anomalies.csv. For threat intel monitoring without budget, configure a free RSS or API alert via abuse.ch, Have I Been Pwned's domain search API, or MISP community feeds filtered on the ANTS breach tag. Set a daily cron to diff new IOC feeds against your domain name and known data field schemas.

Evidence: Query application authentication logs for the 30 days following April 15, 2026 for: (1) HTTP POST requests to identity verification endpoints (/api/verify, /auth/document, or equivalent) with French document number patterns (passport: [A-Z0-9]{9}, CNI: [0-9]{12}); (2) spikes in 200 OK responses on new account registration flows tied to French PII; (3) source IP clustering — multiple French document numbers verified from the same IP or ASN within a short window, consistent with MITRE ATT&CK T1078 (Valid Accounts) abuse using stolen credentials from this dataset.

Eradication — No patch is available; root cause has not been publicly confirmed. If your systems relied on ANTS-issued document numbers as a sole authentication factor, remove that single-factor dependency immediately. Enforce multi-factor authentication on any portal accepting French identity document inputs.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST IA-2 (Identification and Authentication — Organizational Users), NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Audit every application that accepts French government document numbers as an authentication input: grep -r 'passport_number\|document_id\|cni_number\|permis_number' /var/www/ --include='*.php' --include='*.py' --include='*.js' -l to locate the code paths. For each identified endpoint, immediately enforce a mandatory second factor. If your app framework cannot enforce MFA natively, place an nginx auth_request module or a Cloudflare Access zero-trust policy in front of those endpoints with TOTP as the gate. Document every change in a change log with timestamp and approver for CNIL audit readiness.

Evidence: Before removing the single-factor dependency, capture the current authentication configuration as a forensic baseline: export your application's auth configuration files (e.g., /etc/app/auth.conf, Django settings.py AUTH_PASSWORD_VALIDATORS block, or Apache mod_auth config), hash them with sha256sum, and store in an incident evidence folder. This documents the pre-remediation state if the root cause investigation later implicates your configuration as part of a supply-chain exposure path from the ANTS dataset.

Recovery — Validate that no internal systems ingested or cached ANTS-sourced identity data in a manner that extended your own exposure surface. Review data minimization practices for French citizen PII held internally. Confirm CNIL notification obligations under GDPR Article 33 if your organization processed or holds any of the affected data categories.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-12 (Information Management and Retention), NIST SC-28 (Protection of Information at Rest), NIST IR-6 (Incident Reporting), NIST AU-11 (Audit Record Retention), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.4 (Enforce Data Retention), CIS 3.5 (Securely Dispose of Data)

Compensating: Run a data discovery scan using the free tool 'grep' or 'ripgrep' across your databases and file stores to locate cached French PII: rg -e '[A-Z0-9]{9}' -e '[0-9]{12}' -e 'France|français|ANTS' /data/cache/ /data/uploads/ /data/exports/ --type json --type csv -l. For databases, query: SELECT table_name, column_name FROM information_schema.columns WHERE column_name ILIKE '%passport%' OR column_name ILIKE '%national_id%' OR column_name ILIKE '%document_num%'; to identify tables holding the affected data categories. For GDPR Article 33 timeline compliance (72-hour notification to CNIL), use the CNIL's official online notification portal — do not estimate your obligation; confirm with your DPO.

Evidence: Document all data stores where French citizen PII fields (full name, DOB, birthplace, address, phone, document number) were ingested, including ETL pipeline logs, API gateway request logs showing inbound PII payloads, database transaction logs showing INSERT/UPDATE operations on citizen record tables, and any data lake or S3-equivalent bucket access logs. These artifacts establish your organization's actual exposure surface and are required evidence for any CNIL investigation or GDPR Article 33 notification package.

Post-Incident — Conduct a control gap review against NIST SP 800-53 AC-2 (Account Management), IA-5 (Authenticator Management), and SC-28 (Protection of Information at Rest) controls. Evaluate whether third-party identity verification dependencies introduce breach propagation risk into your supply chain. Update threat models to account for high-confidence French citizen PII now circulating in criminal marketplaces.

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 AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST SC-28 (Protection of Information at Rest), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Conduct a tabletop exercise scenario: 'A threat actor purchases the ANTS 19M record dataset and attempts account takeover against our French citizen users using document numbers as knowledge-based authentication answers.' Map every gap identified to the three controls listed. For supply chain risk, build a one-page dependency map listing every third-party identity verification vendor (e.g., Onfido, Jumio, or equivalent) your organization uses and whether those vendors rely on ANTS-issued document number validation — email each vendor asking for their breach impact statement specific to the April 2026 ANTS incident. File responses as evidence.

Evidence: Lessons learned package must include: (1) a timeline of when your organization first ingested ANTS-derived identity fields and from which source; (2) the full account list of French citizen users with associated document types used for authentication; (3) any threat intelligence reports from hacker forum monitoring services showing your organization's data or domain correlated with the ANTS dataset sale thread; (4) the pre- and post-incident authentication configuration diffs generated during eradication; (5) all CNIL/GDPR Article 33 notification correspondence and timestamps.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) have been publicly attributed to this breach as of available reporting. Detection focus should shift to downstream abuse indicators. Monitor for: (1) Unusual spikes in new account registrations using French address formats or French phone number prefixes (+33). (2) Credential stuffing patterns against portals that accept French national ID or passport numbers as authenticators. (3) Inbound phishing campaigns impersonating ANTS, the French Ministry of the Interior, or CNIL, particularly emails requesting document re-verification or portal credential updates. (4) Dark web and hacker forum monitoring for your organization's domains, employee emails, or partner identifiers appearing alongside this dataset. SIEM queries should target: repeated failed authentication from new IP ranges against accounts with French PII attributes; anomalous document verification API call volumes; and new account creation bursts tied to French address or phone fields. Flag and escalate any communications purporting to originate from ants.gouv.fr that were not initiated by your users.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/french-govt-agency-confirms-breach-as-hacker-offers-to-sell-data/`	Primary news reporting confirming ANTS breach and active sale of 19 million records on hacker forums — T3 source, human validation recommended	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1598** — Phishing for Information
- **T1078** — Valid Accounts
- **T1213** — Data from Information Repositories
- **T1114** — Email Collection
- **T1566** — Phishing
- **T1530** — Data from Cloud Storage
- **T1585** — Establish Accounts
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **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
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.2** — Use Unique Passwords

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1598	Phishing for Information	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1213	Data from Information Repositories	Collection
T1114	Email Collection	Collection
T1566	Phishing	Initial-Access
T1530	Data from Cloud Storage	Collection
T1585	Establish Accounts	Resource-Development
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/french-govt-agency-c...	T3
Personal data protection - France Titres (ANTS)	https://ants.gouv.fr/home/personal-data	T3
Scam emails sent to authorized automotive professionals en	https://immatriculation.ants.gouv.fr/home/all-the-news/scam-emails-...	T3
Home - France Titres (ANTS)	https://ants.gouv.fr/home	T3
General Terms and Conditions of Use - France Titres (ANTS)	https://ants.gouv.fr/home/general-terms-and-conditions-of-use	T3

Generated 2026-04-22 06:45 UTC by TJS Security Command Center