INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-30 06:01 UTC

ShinyHunters Claims 350GB Haul from European Commission AWS Breach, SSO and Cloud Exposure Pattern Continues

DATA BREACH | HIGH | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0070
Type	Data Breach
Severity	HIGH
CVSS Base Score	9.5
Affected Products	European Commission Europa.eu cloud infrastructure (AWS-hosted); Okta SSO, Microsoft SSO, Google SSO integrations
Published	2026-03-30T02:42:58
Discovery Source	Rss

Executive Summary

ShinyHunters has claimed responsibility for a breach of the European Commission's Europa.eu cloud infrastructure hosted on AWS, alleging theft of 350GB of data including mail server contents, databases, and confidential documents. The Commission has confirmed the breach but states internal systems were not directly affected; cloud-hosted assets such as mail and databases typically contain operationally sensitive information. This incident follows a prior February 2026 breach of the same organization and signals that intergovernmental cloud tenants are active targets for data extortion; organizations sharing SSO integrations (Okta, Microsoft, Google) with the affected environment face elevated credential and token exposure risk.

Technical Analysis

The breach targeted the European Commission's AWS-hosted cloud environment, with ShinyHunters claiming exfiltration of approximately 350GB encompassing mail server data, databases, and confidential documents. No CVE is assigned; the attack surface maps to CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), and CWE-200 (Exposure of Sensitive Information). Named SSO providers, Okta, Microsoft Entra ID, and Google Workspace, appear in the exposure context, suggesting initial access likely involved credential theft, session token hijacking (T1539), or phishing for cloud credentials (T1566, T1598) against federated identity providers rather than direct AWS infrastructure exploitation. Relevant ATT&CK techniques include Valid Accounts: Cloud Accounts (T1078.004), Data from Cloud Storage (T1530), Email

Collection (T1114), Automated Exfiltration (T1020), Exfiltration Over Web Service (T1567), and Financial Motivated Extortion (T1657). ShinyHunters demonstrates a documented pattern, reported across threat intelligence platforms, of targeting SSO-federated cloud tenants; this is consistent with their prior Snowflake-adjacent campaign methodology. No patch is applicable; this is an authentication control and cloud configuration failure, not a software vulnerability. Patch status: N/A; remediation requires access control hardening and identity hygiene.

Action Checklist

1. Recommended: Audit all active Okta, Microsoft Entra ID, and Google Workspace sessions for anomalous cloud API access; revoke suspicious OAuth tokens and active SSO sessions for AWS tenants immediately. If your organization federates identity into AWS via any of these providers, treat access logs as potentially compromised until reviewed.
2. Recommended: Query AWS CloudTrail for anomalous GetObject, ListBuckets, and CopyObject calls, particularly from unfamiliar IP ranges or user agents. In Okta, review System Log (requires Okta Administrator access) for events: user.session.impersonation.initiate, app.oauth2.token.grant, and policy.evaluate_sign_on failures followed by successes. In Microsoft Entra ID, audit Sign-in logs for impossible travel, unfamiliar device compliance state, and service principal consent grants. Cross-reference against ShinyHunters-associated infrastructure where IOCs become available.
3. Recommended: Enforce phishing-resistant MFA (FIDO2/WebAuthn) on all SSO provider accounts with AWS federation; remove SMS and TOTP as fallback options for privileged roles. Rotate all AWS IAM access keys and SSO application credentials. Review and remove excessive OAuth application permissions granted to third-party apps in Okta, Entra ID, and Google Workspace. Enforce least-privilege on AWS S3 bucket policies and disable public access where not operationally required.
4. Recommended: Validate that CloudTrail logging is enabled across all AWS regions and accounts, including S3 data event logging. Confirm GuardDuty is active and review findings for the prior 30 days. Verify that no unauthorized IAM roles, users, or cross-account trust relationships were created during the suspected access window. Restore any modified bucket policies from known-good configuration baselines.
5. Post-Incident: This incident exposes three recurring control gaps: absence of phishing-resistant MFA on federated identity providers, insufficient monitoring of cloud API data access patterns, and over-permissive OAuth token grants. Map these gaps to NIST SP 800-53 controls IA-2(6) (Phishing-Resistant MFA), AC-2 (Account Management), AU-2 and AU-12 (Audit Logging), and SC-28 (Protection of Information at Rest). Update your cloud incident response playbook to include SSO provider compromise as an initial access vector requiring parallel investigation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal counsel immediately if CloudTrail S3 data event logs confirm GetObject or CopyObject operations against buckets containing PII, employee data, or regulated information during the suspected breach window — GDPR Article 33 imposes a 72-hour supervisory authority notification deadline from the point the organization becomes aware of a personal data breach, and ShinyHunters' claimed 350GB haul from a cloud-hosted mail server and database environment creates high probability of personal data exposure.
Recovery Notes	Do not declare recovery complete until all three of the following are verified: (1) No unauthorized IAM roles, users, access keys, or cross-account trust relationships exist that were created after the earliest suspected compromise date; (2) CloudTrail data event logging is confirmed active across all AWS regions and accounts, including S3 object-level logging — ShinyHunters-pattern operations are undetectable without data events enabled; (3) All SSO-federated applications in Okta, Entra ID, and Google Workspace have been audited for OAuth scope grants and FIDO2/WebAuthn enforcement is confirmed active for all privileged roles. Maintain elevated monitoring of AWS CloudTrail, GuardDuty, and Okta System Log for a minimum of 30 days post-containment — ShinyHunters has demonstrated a pattern of returning to previously breached environments (as evidenced by the February 2026 and March 2026 Europa.eu incidents) when initial eviction is incomplete.
Forensic Artifacts	AWS CloudTrail S3 data event logs — GetObject, CopyObject, and ListBuckets calls with sourceIPAddress, userAgent, requestParameters.key, and responseElements fields: the primary artifact establishing exfiltration scope and attacker enumeration pattern consistent with ShinyHunters bulk-harvest TTPs | AWS CloudTrail AssumeRoleWithSAML and AssumeRoleWithWebIdentity events — captures the federated credential chain from Okta/Entra ID/Google through to temporary AWS session tokens, establishing which SSO provider was the initial access vector and which IAM roles were assumed during the breach | Okta System Log entries for app.oauth2.token.grant.access_token and user.session.impersonation.initiate events targeting the AWS SAML/OIDC application — primary evidence of identity-layer exploitation preceding AWS API abuse | AWS VPC Flow Logs showing large outbound TCP sessions (sustained high-volume transfers consistent with 350GB exfiltration) to non-AWS IP space during off-hours — corroborates the claimed data volume and provides destination IP evidence for ShinyHunters infrastructure attribution | Microsoft Entra ID unified audit log entries for Add app role assignment to service principal and Consent to application events — ShinyHunters has used illicit OAuth consent grants as a persistence and re-entry mechanism in prior SSO-federated cloud breach campaigns, and these entries survive credential rotation if the application grant itself is not revoked

Per-Action IR Details

Containment — Audit all active Okta, Microsoft Entra ID, and Google Workspace sessions for anomalous cloud API access; revoke suspicious OAuth tokens and active SSO sessions for AWS tenants immediately. If your organization federates identity into AWS via any of these providers, treat access logs as potentially compromised until reviewed.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected resources, preserve evidence, and prevent further unauthorized access while maintaining operational continuity

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without enterprise SIEM: (1) Export Okta System Log via API using `curl -H 'Authorization: SSWS {token}' 'https://{org}.okta.com/api/v1/logs?filter=eventType+eq+"app.oauth2.token.grant"&limit=1000'` and parse with jq for unfamiliar IP ranges. (2) In AWS Console, run `aws iam list-users --output json` and `aws iam list-access-keys --user-name {user}` for every federated role; cross-reference last-used timestamps. (3) Use Google Workspace Admin

SDK Reports API to pull `token` activity events for the past 30 days at no cost. (4) For Entra ID, use the free Microsoft Entra sign-in log export (CSV) filtered on AWS-federated service principal IDs. Assign one analyst per IdP to parallelize.

Evidence: BEFORE revoking any tokens, preserve: (1) Full Okta System Log export covering the 72-hour window prior to discovery — specifically events `user.session.impersonation.initiate`, `app.oauth2.token.grant.access_token`, and `app.oauth2.as.token.exchange` tied to the AWS SAML/OIDC application integration. (2) AWS CloudTrail `AssumeRoleWithSAML` and `AssumeRoleWithWebIdentity` events showing which federated principals were used to obtain temporary AWS credentials — capture the `sourceIPAddress`, `userAgent`, and `requestParameters.roleArn` fields. (3) Microsoft Entra ID sign-in logs for the service principal corresponding to your AWS SSO application — export before any conditional access policy changes purge entries. (4) Google Workspace Token audit log showing OAuth scope grants to AWS-integrated apps. These are ephemeral and may roll over; capture before revocation actions overwrite session state.

Detection — Query AWS CloudTrail for anomalous GetObject, ListBuckets, and CopyObject calls, particularly from unfamiliar IP ranges or user agents. In Okta, review System Log for events: user.session.impersonation.initiate, app.oauth2.token.grant, and policy.evaluate_sign_on failures followed by successes. In Microsoft Entra ID, audit Sign-in logs for impossible travel, unfamiliar device compliance state, and service principal consent grants. Cross-reference against ShinyHunters-associated infrastructure where IOCs become available.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources, establish timeline of attacker activity, and assess scope of data exposure

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM: (1) AWS CloudTrail Insights is free within CloudTrail — enable it to auto-flag unusual `GetObject` and `ListBuckets` call volumes. (2) Run this AWS CLI query targeting S3 data events: `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=GetObject --start-time 2026-02-01 --output json | jq '.Events[] | select(.CloudTrailEvent | fromjson | .sourceIPAddress | test("YOUR_KNOWN_CIDR") | not)'`. (3) Deploy the free Sigma rule `aws_cloudtrail_s3_data_exfiltration.yml` (SigmaHQ repository) against exported CloudTrail JSON logs using the `sigma convert` CLI tool with grep/jq backend. (4) For Okta, use the free Okta System Log search UI filtered on `eventType eq "user.session.impersonation.initiate" OR eventType eq "app.oauth2.token.grant"` covering the period since the confirmed February 2026 ShinyHunters EC breach.

Evidence: Before pivoting to containment actions that may alter log state: (1) AWS CloudTrail S3 data event logs — specifically `GetObject` and `CopyObject` events on buckets containing mail server exports or database snapshots, with full `requestParameters`, `sourceIPAddress`, `userAgent`, and `responseElements` fields preserved in raw JSON. (2) Okta System Log entries matching ShinyHunters' known pattern of MFA bypass via SSO token theft — look for `policy.evaluate_sign_on` failure immediately followed by success from the same session context, indicating policy downgrade or phishing-resistant MFA bypass. (3) AWS IAM credential report (`aws iam generate-credential-report`) capturing last-used timestamps for all access keys — ShinyHunters operations typically involve programmatic key use for bulk S3 enumeration before targeted exfiltration. (4) VPC Flow Logs for large outbound data transfers (>1GB sessions) to non-AWS IP space during off-hours — consistent with the claimed 350GB exfiltration volume. (5) Entra ID unified audit log entries for `Add app role assignment to service principal` and `Consent to application` — ShinyHunters has used illicit OAuth consent grants to maintain persistence across SSO-federated environments.

Eradication — Enforce phishing-resistant MFA (FIDO2/WebAuthn) on all SSO provider accounts with AWS federation; remove SMS and TOTP as fallback options for privileged roles. Rotate all AWS IAM access keys and SSO application credentials. Review and remove excessive OAuth application permissions granted to third-party apps in Okta, Entra ID, and Google Workspace. Enforce least-privilege on AWS S3 bucket policies and disable public access where not operationally required.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all threat actor footholds, revoke compromised credentials, remediate the conditions that enabled initial access and persistence

Controls: NIST IA-2(6) (Identification and Authentication — Phishing-Resistant MFA), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST SI-2 (Flaw Remediation), NIST SC-28 (Protection of Information at Rest), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise IAM governance tooling: (1) Enumerate all AWS IAM access keys older than 90 days using `aws iam list-users --output json | jq -r '.Users[].UserName' | xargs -I{} aws iam list-access-keys --user-name {}` — rotate any key that touched S3 data events during the suspect window. (2) Audit Okta OAuth grants for AWS-integrated apps via `GET /api/v1/apps/{appId}/grants` API endpoint — revoke any grant with `offline_access` or `s3:*` equivalent scopes not tied to an approved integration. (3) Apply AWS S3 Block Public Access at the account level using `aws s3control put-public-access-block --account-id {ID} --public-access-block-configuration BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true`. (4) For FIDO2 enforcement without enterprise Okta license, configure Okta's free-tier Authentication Policy to require `FIDO2_WEBAUTHN` authenticator class for the AWS SAML app specifically.

Evidence: Before rotating credentials (which destroys forensic state): (1) Snapshot all AWS IAM `LastUsedDate` fields for every access key via `aws iam get-access-key-last-used --access-key-id {key}` — this establishes which keys were active during the breach window attributed to ShinyHunters. (2) Export the full list of OAuth application grants from Okta, Entra ID, and Google Workspace with grant timestamps and scopes — ShinyHunters has used over-permissive OAuth tokens as persistence mechanisms post-initial-access to avoid triggering re-authentication. (3) Capture current AWS S3 bucket policies and ACLs via `aws s3api get-bucket-policy --bucket {name}` and `aws s3api get-bucket-acl --bucket {name}` for all buckets — preserve as baseline evidence of the permissive state that enabled the alleged 350GB exfiltration. (4) Document all existing AWS IAM roles with `sts:AssumeRole` trust policies pointing to Okta, Entra ID, or Google as SAML/OIDC providers before any policy modifications.

Recovery — Validate that CloudTrail logging is enabled across all AWS regions and accounts, including S3 data event logging. Confirm GuardDuty is active and review findings for the prior 30 days. Verify that no unauthorized IAM roles, users, or cross-account trust relationships were created during the suspected access window. Restore any modified bucket policies from known-good configuration baselines.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation, verify integrity of configurations, and confirm no attacker persistence mechanisms remain

Controls: NIST IR-4 (Incident Handling), NIST AU-4 (Audit Storage Capacity), NIST AU-9 (Protection of Audit Information), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without AWS Security Hub or commercial CSPM: (1) Validate CloudTrail coverage across all regions using `aws cloudtrail describe-trails --include-shadow-trails --output json | jq '.[].TrailARN'` and confirm `IsMultiRegionTrail: true` and `IncludeGlobalServiceEvents: true` for each. (2) Check S3 data event logging gaps: `aws cloudtrail get-event-selectors --trail-name {name}` — ShinyHunters-style bulk exfiltration is invisible without data events enabled. (3) Enumerate IAM roles created after your earliest suspected compromise date: `aws iam list-roles --output json | jq --arg d '2026-02-01' '.Roles[] | select(.CreateDate > $d)'`. (4) Use the free AWS Config `iam-root-access-key-check` and `s3-bucket-public-read-prohibited` managed rules if AWS Config is enabled — both are zero-cost managed rules that flag the control gaps this incident exploited. (5) For cross-account trust validation, run `aws iam list-roles --output json | jq '.Roles[] | select(.AssumeRolePolicyDocument.Statement[].Principal.AWS != null)'` to surface any unexpected external account trust relationships added during the breach window.

Evidence: During recovery validation, preserve as post-incident evidence: (1) AWS Config configuration history snapshots for all IAM roles and S3 bucket policies modified during the suspected access window — these show the delta between pre-breach and post-breach configuration state. (2) GuardDuty finding archive for the 30-day review period — specifically `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration`, `Recon:IAMUser/UserPermissions`, and `Exfiltration:S3/ObjectRead.Unusual` finding types that would correspond to ShinyHunters' enumeration and exfiltration TTPs. (3) CloudTrail `CreateRole`, `AttachRolePolicy`, `CreateUser`, and

`CreateAccessKey` events within the breach window — these are the persistence artifacts ShinyHunters would leave if they established footholds beyond the initial SSO session.

Post-Incident — This incident exposes three recurring control gaps: absence of phishing-resistant MFA on federated identity providers, insufficient monitoring of cloud API data access patterns, and over-permissive OAuth token grants. Map these gaps to NIST SP 800-53 controls IA-2(6) (Phishing-Resistant MFA), AC-2 (Account Management), AU-2 and AU-12 (Audit Logging), and SC-28 (Protection of Information at Rest). Update your cloud incident response playbook to include SSO provider compromise as an initial access vector requiring parallel investigation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned review, control gap remediation, playbook updates, and threat intelligence sharing to improve detection of future ShinyHunters-pattern attacks

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IA-2(6) (Identification and Authentication — Phishing-Resistant MFA), NIST AC-2 (Account Management), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SC-28 (Protection of Information at Rest), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without a GRC platform or formal lessons-learned tooling: (1) Conduct a structured 60-minute post-incident review using NIST 800-61r3 §4 as an agenda template — document the three control gaps identified in this step as formal findings with owners and due dates. (2) Add a ShinyHunters-specific detection rule to your Okta System Log monitoring: alert on any sequence of `policy.evaluate_sign_on` failure → success within 5 minutes from the same `actor.id` targeting an AWS-federated app. Implement as a free Okta Workflow or a Sigma rule processed against log exports. (3) File the three control gaps (phishing-resistant MFA, cloud API monitoring, OAuth over-permission) as tracked items in any free project management tool (GitHub Issues, Jira free tier) with NIST control cross-references for audit evidence. (4) Subscribe to ShinyHunters IOC feeds via free OSINT sources (IntelX, Hudson Rock, Breach Forums monitoring via threat intel aggregators) to enable early warning if your organization's data surfaces.

Evidence: For the lessons-learned record and any regulatory notification obligations: (1) Timeline reconstruction from CloudTrail, Okta System Log, and Entra ID unified audit log — establish first-observed unauthorized API call, peak exfiltration window (correlated against VPC Flow Log outbound volume spikes), and last attacker action before containment. (2) Data classification inventory for all S3 buckets accessed during the breach window — required to assess whether the 350GB-pattern exfiltration scope included PII, PHI, or regulated data triggering GDPR Article 33 (72-hour supervisory authority notification) or equivalent obligations. (3) Documentation of the OAuth application permission state at time of breach versus post-remediation — this delta constitutes the control gap evidence required for formal gap remediation tracking under NIST IR-8 (Incident Response Plan) update requirements.

Detection Guidance

Primary detection surface is AWS CloudTrail combined with your SSO provider's audit logs. In CloudTrail, alert on: high-volume S3 GetObject or CopyObject events from a single principal in a short window; ConsoleLogin events from IPs outside expected geographic ranges; CreateAccessKey or AttachUserPolicy calls not initiated through your approved provisioning pipeline. In Okta System Log, query for: eventType eq 'user.session.start' AND outcome.result eq 'SUCCESS' combined with preceding failures; eventType eq 'app.oauth2.as.token.grant' for unexpected application grants. In Microsoft Entra ID Sign-in Logs, filter for: RiskState = 'atRisk' or RiskLevel = 'high'; conditionalAccessStatus = 'failure' followed by 'success' within the same session window. Behavioral indicator to prioritize: large outbound data transfers from AWS S3 to external endpoints, especially via presigned URL generation (CloudTrail: GeneratePresignedUrl). As of 2026-03-27 (incident confirmation date), no confirmed IOCs for this incident have been publicly released; monitor threat intelligence feeds (ISAC, Mandiant, Recorded Future) for ShinyHunters infrastructure indicators as they are released.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`europa.eu (victim infrastructure — do not block)`	Confirmed breach target; reference only for internal log correlation against any outbound connections initiated from your environment to this domain during the breach window.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft
- **T1566** — Phishing
- **T1020** — Automated Exfiltration
- **T1078** — Valid Accounts
- **T1213** — Data from Information Repositories
- **T1539** — Steal Web Session Cookie
- **T1078.004** — Cloud Accounts
- **T1598** — Phishing for Information
- **T1530** — Data from Cloud Storage
- **T1567** — Exfiltration Over Web Service
- **T1586** — Compromise Accounts
- **T1114** — Email Collection

NIST-800-53R5

- **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-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

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(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1566	Phishing	Initial-Access
T1020	Automated Exfiltration	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1213	Data from Information Repositories	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1078.004	Cloud Accounts	Defense-Evasion
T1598	Phishing for Information	Reconnaissance
T1530	Data from Cloud Storage	Collection

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1586	Compromise Accounts	Resource-Development
T1114	Email Collection	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/european-commission-...	T3
European Commission's Data Stolen in Hack on AWS ...	https://www.bloomberg.com/news/articles/2026-03-27/european-commiss.. .	T2
European Commission Reports Cyberattack on AWS as ...	https://finance.yahoo.com/sectors/technology/articles/european-comm...	T3
Hackers Stole 350GB From the European Commission's ...	https://www.gblock.app/articles/european-commission-aws-cloud-breach	T3
■ The European Commission has confirmed a data breach ...	https://www.instagram.com/p/DWgE9MhCZm5/	T3

Generated 2026-03-30 06:01 UTC by TJS Security Command Center