INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-29 18:26 UTC

Canadian Telecom Provider Telus Confirms Breach Involving Unauthorized Access and Extortion

DATA BREACH | HIGH | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0069
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Telus Digital (Canadian telecommunications provider, subsidiary of Telus Corporation)
Published	2026-03-27
Discovery Source	Gemini

Executive Summary

Telus Digital, the digital services subsidiary of Canadian telecom giant Telus Corporation, confirmed unauthorized access to its systems after threat actor group ShinyHunters claimed responsibility and alleged theft of approximately 1 petabyte of data. The full scope of exfiltrated data remains undisclosed, but potential exposure includes customer PII, internal credentials, and proprietary network data. Organizations with supply chain, vendor, or data-sharing relationships with Telus should assess third-party risk exposure and monitor for downstream credential or data abuse.

Technical Analysis

Telus Digital confirmed a breach attributed to ShinyHunters, a financially motivated threat actor group with a documented history of large-scale data theft and extortion targeting high-value organizations. The attack pattern aligns with MITRE ATT&CK techniques T1078 (Valid Accounts, likely initial access via compromised credentials), T1530 (Data from Cloud Storage), T1567 (Exfiltration Over Web Service), and T1657 (Financial Theft via extortion). CWE-284 (Improper Access Control) and CWE-200 (Exposure of Sensitive Information to Unauthorized Actor) align with the incident pattern based on credential abuse and overly permissive access controls. No CVE is associated with this incident; the breach appears to involve credential abuse and access control failures rather than a disclosed software vulnerability. The claimed exfiltration volume of 1 petabyte is unverified by Telus at time of reporting. Patch status and specific system scope have not been publicly disclosed. Sources: Reuters (2026-03-12), BleepingComputer, CybersecurityDive (2026-03-13).

Action Checklist

1. Containment, If your organization has active API integrations, data feeds, or shared authentication with Telus Digital systems, suspend or restrict those connections pending Telus confirmation of scope. Revoke any shared service account credentials or API keys provisioned by or for Telus Digital.
2. Detection, Review access logs for anomalous authentication events involving Telus-affiliated accounts, federated identity providers, or third-party SSO connections. Search for T1078 indicators: off-hours logins, geographic anomalies, or privilege escalation from service accounts linked to Telus. Check cloud storage access logs (T1530) for unexpected bulk read or export operations on data shared with or sourced from Telus systems.
3. Eradication, Rotate any credentials, tokens, or certificates shared with or issued by Telus Digital. If Telus Digital acts as a data processor or sub-processor for your organization, initiate your third-party incident notification procedure and request formal confirmation of scope from your Telus contact.
4. Recovery, Validate that rotated credentials and API keys are functioning correctly across dependent systems. Monitor downstream data pipelines or integrations that pull from Telus for anomalous data or unexpected schema changes that could indicate tampered data injection. Confirm no lateral movement indicators in your environment from any Telus-affiliated access paths.
5. Post-Incident, Evaluate third-party risk controls for telecom and digital services vendors: confirm contractual breach notification SLAs are defined, assess whether your vendor risk assessments require updated questionnaires for Telus, and review whether shared data with Telus falls under regulatory obligations (PIPEDA, provincial privacy laws, or applicable sector regulations) that trigger your own notification requirements.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if detection analysis confirms any Telus-affiliated account successfully authenticated to your systems after Telus Digital's breach disclosure date, if cloud storage logs show bulk export operations (T1530) on Telus-sourced data exceeding your baseline by more than 2x, or if shared data with Telus includes Canadian resident PII triggering PIPEDA mandatory notification obligations to the Office of the Privacy Commissioner.
Recovery Notes	Post-containment, maintain a 30-day heightened monitoring window on all systems and data pipelines that had active integrations with Telus Digital, specifically watching for ShinyHunters' known tactic of delayed credential use after exfiltration to establish persistence. Validate data integrity of all records received from Telus feeds using hash comparisons against pre-breach baselines, as the claimed 1 petabyte exfiltration scope creates material risk of tampered data re-injection as a secondary attack vector. Formally close the incident only after Telus provides written confirmation of breach scope and after your organization's PIPEDA notification obligations (if triggered) have been assessed and addressed.

Forensic Artifacts	IAM/IdP federation logs: SAML assertion logs or OAuth token issuance records from your identity provider (Azure AD, Okta, Ping) where the issuer or audience field references Telus Digital's tenant or domain — these establish whether ShinyHunters-obtained Telus credentials were used to authenticate into your environment via federated trust | API gateway access logs filtered on Telus-affiliated client IDs: specifically HTTP 200 responses with response body sizes in the top 5th percentile, which would indicate bulk data retrieval consistent with T1530 (Data from Cloud Storage) using valid but compromised Telus-issued API keys | Cloud storage audit logs (AWS CloudTrail S3 data events, Azure Storage diagnostic logs, or GCP Cloud Storage Data Access logs) for GetObject, CopyObject, and ListBucket operations on buckets containing Telus-sourced or Telus-shared data — the 1 petabyte claimed exfiltration volume makes bulk read operations the primary artifact to isolate | Network flow records (NetFlow, VPC Flow Logs, or Azure NSG flow logs) showing connection history to Telus Digital IP ranges or ASN (AS852 — TELUS Communications) for the 90 days preceding breach disclosure, preserving source IP, destination IP, bytes transferred, and session duration to reconstruct any outbound data staging activity | Secrets vault access audit logs (HashiCorp Vault audit log, AWS Secrets Manager CloudTrail events for GetSecretValue) for all secrets tagged or named with Telus Digital references — last-access timestamps on these entries reveal whether an adversary with Telus Digital network access enumerated and retrieved your organization's stored credentials during the breach window

Per-Action IR Details

Containment — If your organization has active API integrations, data feeds, or shared authentication with Telus Digital systems, suspend or restrict those connections pending Telus confirmation of scope. Revoke any shared service account credentials or API keys provisioned by or for Telus Digital.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected components and prevent further damage while preserving evidence

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management) — disable or suspend Telus-provisioned service accounts, NIST SC-7 (Boundary Protection) — block or null-route Telus Digital API endpoints at the network boundary, CIS 6.2 (Establish an Access Revoking Process) — immediately revoke access for Telus-affiliated accounts and API keys, CIS 4.4 (Implement and Manage a Firewall on Servers) — apply firewall rules blocking outbound connections to Telus Digital IP ranges

Compensating: On Linux/macOS: run `ss -tunap | grep ` to enumerate active connections, then use `iptables -I OUTPUT -d -j DROP` to block outbound traffic immediately. On Windows: use `netstat -ano | findstr ` to identify connections, then block via `netsh advfirewall firewall add rule name='Block-TelusDigital' dir=out action=block remoteip=`. Revoke API keys via your API gateway's admin console or by invalidating tokens in your IAM store directly. Document timestamps of each revocation action.

Evidence: Before revoking, capture: (1) a full export of your IAM/directory service showing all accounts, service principals, or OAuth clients with 'telus' in the display name, UPN, or issuer field; (2) your API gateway access logs (e.g., AWS API Gateway CloudWatch logs, Kong access logs, or nginx access.log) for the prior 90 days filtered on Telus-affiliated client IDs or API keys — specifically look for bulk data export patterns (HTTP 200 responses with unusually large response body sizes); (3) network flow records (NetFlow/IPFIX or VPC Flow Logs) for all traffic to/from Telus Digital ASN or documented IP ranges for the same 90-day window, preserving them before connection termination removes active session state.

Detection — Review access logs for anomalous authentication events involving Telus-affiliated accounts, federated identity providers, or third-party SSO connections. Search for T1078 indicators: off-hours logins, geographic anomalies, or privilege escalation from service accounts linked to Telus. Check cloud storage access logs (T1530) for unexpected bulk read or export operations on data shared with or sourced from Telus

systems.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate log data across sources to identify indicators of compromise and determine scope of unauthorized access

Controls: NIST IR-5 (Incident Monitoring) — track and document all anomalous authentication events tied to Telus-federated identities, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review authentication and storage access logs at increased frequency given active breach disclosure, NIST SI-4 (System Monitoring) — monitor for T1078 (Valid Accounts) and T1530 (Data from Cloud Storage) indicators in real time, NIST AU-2 (Event Logging) — confirm logging is enabled for federated SSO authentication events and cloud object storage access, CIS 8.2 (Collect Audit Logs) — verify audit logs for cloud storage and identity provider are centralized and intact

Compensating: For Azure AD/Entra ID: run `Get-AzureADAuditSignInLogs | Where-Object {$_.UserDisplayName -like '*telus*' -or $_.AppDisplayName -like '*telus*'}` and filter on `RiskState -ne 'none'` or `LocationCity` outside expected geographies. For AWS: use `aws cloudtrail lookup-events --lookup-attributes AttributeKey=Username,AttributeValue=` and separately run `aws s3api list-buckets` followed by `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=GetObject` filtered on buckets containing Telus-shared data. For on-prem: query Windows Security Event Log for Event ID 4648 (explicit credential logon) and 4672 (special privilege assigned) where the account name matches Telus service account naming conventions. Use the free Sigma rule `win_susp_service_account_interactive_login.yml` against collected logs if a local Sigma-compatible parser (e.g., sigmac + Splunk or chainsaw) is available.

Evidence: Capture before analysis modifies state: (1) Azure AD/Entra ID or Okta sign-in logs for all federated identity events from Telus Digital's IdP tenant for the 90 days preceding the breach disclosure date, paying specific attention to SAML assertions or OAuth token issuances with Telus as the issuer; (2) AWS S3 server access logs or GCP Cloud Storage audit logs (Data Access log type: DATA_READ) for any buckets tagged or named as containing Telus-sourced data — filter for ListBucket, GetObject, or CopyObject operations with response sizes exceeding your normal baseline; (3) your CASB or proxy logs for HTTP GET/POST requests to Telus Digital API hostnames (e.g., *.telus.com, *.telusdigital.com) showing anomalous payload sizes or frequencies consistent with T1530 bulk exfiltration.

Eradication — Rotate any credentials, tokens, or certificates shared with or issued by Telus Digital. If Telus Digital acts as a data processor or sub-processor for your organization, initiate your third-party incident notification procedure and request formal confirmation of scope from your Telus contact.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all components of the incident from the environment, including compromised credentials and untrusted trust relationships

Controls: NIST IR-4 (Incident Handling) — execute eradication phase of incident response plan including credential invalidation, NIST IA-5 (Authenticator Management) — rotate all authenticators (passwords, tokens, certificates, API keys) associated with Telus Digital trust relationships, NIST IR-6 (Incident Reporting) — notify appropriate internal and external stakeholders per the IR plan when a third-party processor is confirmed as the breach source, NIST SA-9 (External System Services) — re-evaluate third-party service agreements and data processor obligations in light of confirmed breach, CIS 5.2 (Use Unique Passwords) — enforce immediate rotation of all shared or Telus-issued credentials to unique values meeting password policy

Compensating: Enumerate all credentials linked to Telus Digital using a secrets inventory approach: search your password manager or secrets vault (e.g., HashiCorp Vault: `vault list secret/telus`, or AWS Secrets Manager: `aws secretsmanager list-secrets | jq '.SecretList[] | select(.Name | contains("telus"))'`) and rotate each. For TLS/mTLS certificates issued by or for Telus, use `openssl x509 -in -noout -issuer -subject -dates` to identify and prioritize expiry/revocation. Draft the third-party notification using your existing DPA (Data Processing Agreement) template — if none exists, reference PIPEDA Breach of Security Safeguards Regulations s.6 as the mandatory reporting threshold and document the gap for the post-incident review.

Evidence: Before rotating credentials, preserve for forensic chain of custody: (1) a timestamped export of all secrets vault entries referencing Telus Digital, including creation date, last rotation date, and last access date — this establishes whether ShinyHunters could have had access to long-lived credentials; (2) certificate transparency logs (query crt.sh for your organization's domains) to identify any certificates issued by Telus Digital's PKI that may need revocation; (3) your current Data Processing Agreement and vendor risk assessment for Telus Digital, which will be needed for PIPEDA notification timeline calculations and to determine whether your organization independently triggers breach notification obligations.

Recovery — Validate that rotated credentials and API keys are functioning correctly across dependent systems. Monitor downstream data pipelines or integrations that pull from Telus for anomalous data or unexpected schema changes that could indicate tampered data injection. Confirm no lateral movement indicators in your environment from any Telus-affiliated access paths.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation, verify integrity of restored components, and monitor for recurrence

Controls: NIST IR-4 (Incident Handling) — execute recovery phase including verification that all eradication actions were successful before restoring connectivity, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of data received from Telus Digital pipelines to detect potential tampered data injection, NIST SI-4 (System Monitoring) — maintain heightened monitoring for lateral movement (T1021) from any Telus-affiliated network segments or re-established connections, NIST AU-12 (Audit Record Generation) — ensure audit logging remains active and at increased verbosity during the recovery monitoring window, CIS 7.2 (Establish and Maintain a Remediation Process) — document recovery actions and validate against the remediation process for completeness

Compensating: Validate credential rotation by testing each API integration endpoint with the new credentials and logging HTTP response codes — a 401 on old credentials and 200 on new credentials confirms successful rotation. For data pipeline integrity, implement a hash-based data validation step: compute SHA-256 checksums on a representative sample of records received from Telus feeds post-recovery and compare against pre-breach baselines stored locally. Use osquery to hunt for lateral movement indicators: `SELECT * FROM processes WHERE parent IN (SELECT pid FROM processes WHERE name IN ('svchost.exe','winlogon.exe')) AND name NOT IN ()` on hosts that had Telus-affiliated service account access. Run this query daily for 30 days post-recovery.

Evidence: Capture during recovery monitoring window: (1) API gateway response logs showing successful authentication of rotated credentials — preserve these as proof of eradication completion; (2) data pipeline ingestion logs from your ETL system (e.g., Apache NiFi provenance repository, AWS Glue job logs, or custom ingestion script stdout/stderr) for the first 30 days post-recovery, specifically flagging any record counts, field types, or encoding anomalies inconsistent with the pre-breach data schema from Telus feeds; (3) Windows Security Event ID 4624 (successful logon) and 4625 (failed logon) logs filtered on logon type 3 (network) and 10 (remote interactive) for any accounts that previously held Telus-affiliated credentials, to detect adversary persistence through credential reuse from the ShinyHunters exfiltration.

Post-Incident — Evaluate third-party risk controls for telecom and digital services vendors: confirm contractual breach notification SLAs are defined, assess whether your vendor risk assessments require updated questionnaires for Telus, and review whether shared data with Telus falls under regulatory obligations (PIPEDA, provincial privacy laws, or applicable sector regulations) that trigger your own notification requirements.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons learned, update policies and controls, and share intelligence to improve future response posture

Controls: NIST IR-4 (Incident Handling) — update the incident handling capability and procedures based on lessons learned from the Telus Digital breach response, NIST IR-8 (Incident Response Plan) — revise the IR plan to incorporate third-party breach notification triggers and PIPEDA-specific response timelines, NIST SA-9 (External System Services) — update vendor assessment criteria to require explicit breach notification SLAs and data processor obligations for all telecom and digital services providers, NIST RA-3 (Risk Assessment) — reassess residual risk from Telus Digital relationship given confirmed unauthorized access and undisclosed scope, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update vendor risk scoring methodology to account for supply chain breach exposure as demonstrated by the ShinyHunters Telus incident

Compensating: For teams without a dedicated GRC platform: create a vendor risk register entry for Telus Digital in a spreadsheet documenting: (a) data categories shared (PII, credentials, network data), (b) applicable regulation (PIPEDA Breach of Security Safeguards Regulations — mandatory notification to OPC if real risk of significant harm), (c) contractual breach notification SLA found or absent in your DPA, and (d) date of next vendor reassessment (recommend 90 days). Use the OPC's publicly available PIPEDA self-assessment tool to determine whether your organization independently triggers notification obligations. Draft an updated vendor questionnaire section specifically addressing data breach response procedures and ShinyHunters-style extortion scenarios for all telecom/digital services vendors in your supply chain.

Evidence: Assemble the post-incident evidence package: (1) the complete incident timeline log from initial Telus breach disclosure through your recovery validation, documenting every action with timestamps — required for PIPEDA notification submissions if triggered; (2) your current DPA with Telus Digital and any sub-processor agreements, marked against the data categories potentially exposed in the ShinyHunters claim (customer PII, internal credentials, proprietary network data) to determine notification obligations under PIPEDA s.10.1; (3) the updated vendor risk assessment for Telus Digital, including the gap analysis against your prior assessment, which documents organizational learning per NIST 800-61r3 §4 lessons-learned requirements. Worth noting this touches regulatory notification obligations under PIPEDA — you may want to verify with qualified Canadian privacy counsel whether your organization independently triggers mandatory breach reporting to the OPC and affected individuals.

Detection Guidance

No confirmed IOCs have been publicly released by Telus or attributed threat intelligence sources at time of reporting. Detection should focus on behavioral indicators consistent with ShinyHunters' TTPs. Monitor for: (1) T1078, authentication events from Telus-affiliated accounts outside normal business hours or originating from unexpected geographies; failed login spikes followed by successful authentication on the same account. (2) T1530, bulk cloud storage access or export events on buckets or repositories with Telus access permissions; look for high-volume GetObject or ListBucket API calls in AWS CloudTrail, or equivalent in Azure Monitor or GCP audit logs. (3) T1567, large outbound data transfers to unfamiliar external endpoints, particularly to file-sharing or cloud hosting services. (4) T1657, monitor for extortion-related communications referencing Telus data in dark web forums or threat actor channels; ShinyHunters has historically listed stolen data on BreachForums. SIEM query approach: correlate Telus-affiliated user or service account activity with anomalous data access volume and outbound transfer events within the same session. Note: detection guidance will require refinement as Telus releases further incident details.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not publicly disclosed at time of reporting`	No confirmed IOCs released by Telus or authoritative threat intelligence sources as of 2026-03-13. Monitor threat intelligence feeds and Telus official communications for updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft

- **T1530** — Data from Cloud Storage
- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts

NIST-800-53R5

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

OWASP-TOP10-2021

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

CIS-V8

- **6.1**
- **6.2**
- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1530	Data from Cloud Storage	Collection
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Telus Digital confirms hack as ShinyHunters claims credit for ...	https://www.cybersecuritydive.com/news/telus-digital-cyberattack-sh...	T3
Telus says it is investigating hack of its systems - Reuters	https://www.reuters.com/business/media-telecom/telus-says-it-is-inv...	T2
Canadian Telecom Telus Says It's Investigating Cyber Breach	https://www.insurancejournal.com/news/international/2026/03/13/8618...	T3
Telus Digital confirms breach after hacker claims 1 petabyte data theft	https://www.bleepingcomputer.com/news/security/telus-digital-confir...	T3
Telus hacked: Cybersecurity incident, unauthorized access : r/Koodo	https://www.reddit.com/r/Koodo/comments/1rscywb/telus_hacked_cybers...	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 18:26 UTC by TJS Security Command Center