INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-29 14:00 UTC

ShinyHunters Breaches Charter Communications via Vishing and Salesforce Exfiltration, Exposing 4.9M Accounts

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0142
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Charter Communications (Spectrum), Microsoft Entra (identity platform), Salesforce (CRM/data platform)
Published	2026-05-29T04:29:40
Discovery Source	Rss

Executive Summary

ShinyHunters compromised Charter Communications (Spectrum) in early April 2026 by using a voice phishing call to manipulate an employee into surrendering Microsoft Entra credentials, then using that access to exfiltrate personally identifiable information on approximately 4.9 million customer accounts from Charter's Salesforce environment. The attack required no software vulnerability, it exploited authentication process gaps and the absence of phishing-resistant MFA on identity and SaaS platforms. Charter disputes ShinyHunters' claims that sensitive telecommunications records were stolen, but the disclosure conflict itself creates regulatory and reputational exposure regardless of what data was ultimately taken.

Technical Analysis

Attack vector: vishing (T1566.004) targeting a Charter Communications employee to harvest Microsoft Entra (cloud identity) credentials. The threat actor leveraged the compromised cloud account (T1078.004, Valid Accounts: Cloud Accounts) to authenticate to Charter's Salesforce CRM instance and exfiltrate PII on approximately 4.9 million customers (T1213, Data from Information Repositories; T1530, Data from Cloud Storage). No CVE is associated; the breach exploited process and authentication weaknesses. Applicable CWEs: CWE-287 (Improper Authentication), CWE-308 (Use of Single-Factor Authentication), CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). Additional MITRE techniques: T1657 (Financial Theft, consistent with ShinyHunters' monetization pattern), T1078 (Valid Accounts, general),

T1586.002 (Compromise Accounts: Email Accounts, possible preparatory step). No patch exists; remediation requires control improvements across identity, telephony verification, and SaaS access governance. This incident demonstrates a known TTP of identity-layer compromise against SaaS environments; ShinyHunters' targeting of Salesforce specifically warrants monitoring for similar campaigns in the broader threat landscape.

Action Checklist

1. Step 1: Containment. Immediately audit Microsoft Entra sign-in logs for anomalous authentication events in March-April 2026, focusing on impossible travel, unfamiliar device registrations, and token issuance outside normal business hours. Suspend any accounts showing suspicious activity and revoke active sessions. In Salesforce, run a Data Export audit and review Setup Audit Trail for unauthorized data access or API calls during the same window. Reference: NIST IR-6 (Incident Reporting), NIST AC-2 (Account Management).
2. Step 2: Detection. Query Microsoft Entra audit logs for: new MFA method registrations, conditional access policy bypasses, OAuth token grants to unfamiliar applications, and sign-ins from Tor exit nodes or anonymizing infrastructure. In Salesforce, review Login History and API Usage reports for accounts accessing large record volumes or bulk data exports. Reference: NIST AU-2 (Audit Events), NIST AC-2 (Account Management). Behavioral indicator: single account accessing millions of CRM records in a compressed time window is a high-confidence IOC.
3. Step 3: Eradication. Enforce phishing-resistant MFA (FIDO2/hardware keys) on all Microsoft Entra accounts with Salesforce access, replacing SMS or voice-call OTP which are bypassed by vishing. Reference: NIST IA-5 (Authenticator Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access). In Salesforce, implement IP allowlisting, restrict Data Export permissions to named roles, and audit Connected Apps for unauthorized OAuth integrations. Apply credential hardening and multifactor enforcement controls.
4. Step 4: Recovery. Validate that all compromised accounts have been rotated and re-enrolled with phishing-resistant MFA per NIST IA-5 (Authenticator Management). Confirm Salesforce connected app permissions have been reviewed and reduced to least-privilege (NIST AC-6). Re-run Salesforce Data Export audit and verify no residual unauthorized access paths remain. Monitor Microsoft Entra Identity Protection risk detections continuously for 30 days post-remediation. Reference: CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process).
5. Step 5: Post-Incident. Conduct a vishing-specific tabletop exercise targeting help desk and identity reset workflows, as ShinyHunters' known entry vector is manipulating support and IT staff over phone calls. Implement out-of-band verification requirements for any identity reset, MFA enrollment change, or privileged access request initiated via phone or messaging. Review Salesforce data access governance: apply CIS 3.3 (Configure Data Access Control Lists) and NIST AC-3 (Access Enforcement) to restrict bulk record access by role. Add this incident pattern to your threat intelligence feed as an active TTP for SaaS-targeted vishing campaigns.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to legal counsel, executive leadership, and external breach counsel if Salesforce Data Export logs confirm more than 500 records of California-resident PII were accessed without authorization, triggering mandatory CCPA breach notification obligations, or if analysis reveals the compromised Entra account had access to systems beyond Salesforce (e.g., billing, network infrastructure), expanding the blast radius beyond the initial 4.9M customer scope.
Recovery Notes	Before returning any remediated accounts to production, verify FIDO2 or number-matched Authenticator enrollment is confirmed in Entra and that Salesforce Connected App OAuth tokens have been fully revoked and re-issued only to approved integrations under least-privilege scopes. Monitor Entra Identity Protection risk detections and Salesforce Login History daily for a minimum of 30 days post-remediation, with particular attention to any new sign-ins from IPs associated with ShinyHunters infrastructure (cross-reference against threat intel feeds such as AbuseIPDB and your ISAC). Given ShinyHunters' pattern of selling exfiltrated data on criminal forums within weeks of a breach, initiate dark web monitoring for Charter/Spectrum customer data appearing in breach marketplaces as an indicator of whether the exfiltrated dataset has been published.
Forensic Artifacts	Microsoft Entra Sign-In Logs (retention: 30 days free tier, 90 days P1/P2) — specifically the entries showing the initial vishing-compromised authentication event with fields IPAddress, DeviceDetail.DeviceId, TokenIssuedAt, and ConditionalAccessStatus='notApplied', which document the exact moment and mechanism of the credential-based Entra compromise by ShinyHunters. | Salesforce EventLogFile — ReportExport and BulkApi event types for the April 2026 window, which record the USER_ID, SOURCE_IP, ROWS_PROCESSED, and ENTITY_NAME for each bulk data operation, providing the definitive forensic record of the 4.9M customer record exfiltration from Charter's CRM environment. | Salesforce Setup Audit Trail (downloadable CSV from Setup > View Setup Audit Trail) — captures Connected App authorizations, Data Export permission grants, and profile changes made by the compromised account during the attacker's dwell time, establishing the full scope of Salesforce-side persistence mechanisms. | Microsoft Entra Audit Logs filtered on 'Register security info' and 'Update user — StrongAuthenticationRequirements' event categories — records any MFA method additions (e.g., attacker-controlled authenticator app enrollment) made after the vishing-obtained credentials were used, evidencing post-compromise persistence establishment in the identity platform. | Help desk ticketing system or call log records from the social engineering timeframe — the primary evidence artifact for the vishing attack vector itself, capturing the caller ID, timestamp, request type (password reset or MFA change), and processing staff identity that ShinyHunters exploited to initiate the entire compromise chain.

Per-Action IR Details

Step 1: Containment — Immediately audit Microsoft Entra sign-in logs for anomalous authentication events in March-April 2026, focusing on impossible travel, unfamiliar device registrations, and token issuance outside normal business hours. Suspend any accounts showing suspicious activity and revoke active sessions. In Salesforce, run a Data Export audit and review Setup Audit Trail for unauthorized data access or API calls during the same window. Reference: NIST IR-6 (Incident Reporting), AC-2 (Account Management).

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without Entra Identity Protection P2 licensing, use the Microsoft Entra free Sign-In Logs export via Graph API: run 'Get-MgAuditLogSignIn -Filter "createdDateTime ge 2026-03-01" | Export-Csv entra_signin_audit.csv'

using the Microsoft.Graph PowerShell module. For Salesforce without a SIEM, navigate to Setup > Login History and export to CSV, then use Excel or Python pandas to filter rows where 'Login Type' equals 'API' or 'Remote Access 2.0' and 'Source IP' falls outside your known corporate IP ranges. Revoke all active Salesforce sessions via Setup > Session Management for flagged users.

Evidence: Capture BEFORE suspending accounts: (1) Full Entra Sign-In Log export for the March–April 2026 window including fields UserPrincipalName, IPAddress, DeviceDetail, TokenIssuedAt, ConditionalAccessStatus, and RiskLevelDuringSignIn — this preserves the vishing-originated session chain before revocation destroys it. (2) Salesforce Setup Audit Trail (Setup > View Setup Audit Trail > Download) covering the same window, which records Data Export jobs, Connected App authorizations, and profile permission changes made by the compromised Entra-federated account. (3) Microsoft Entra audit log entries for 'Register security info' and 'Update user' events, which capture any MFA method additions the attacker may have made after credential surrender to establish persistence.

Step 2: Detection — Query Microsoft Entra audit logs for: new MFA method registrations, conditional access policy bypasses, OAuth token grants to unfamiliar applications, and sign-ins from Tor exit nodes or anonymizing infrastructure. In Salesforce, review Login History and API Usage reports for accounts accessing large record volumes or bulk data exports. Correlate against D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) principles. Behavioral indicator: single account accessing millions of CRM records in a compressed time window is a high-confidence IOC.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use the free Microsoft Entra workbook 'Sign-ins using legacy authentication' and the 'Risky Sign-ins' report available under Entra ID Protection (free tier shows limited signals). For deeper free analysis, export Entra logs to JSON via Graph API and run the open-source 'AzureADAssessment' PowerShell tool (Microsoft GitHub) to surface OAuth app grants and conditional access gaps. For Salesforce, query the EventLogFile object via Salesforce REST API using the ReportExport and ApiTotalUsage event types — filter for rows where ROWS_PROCESSED exceeds 50,000 in a single session, which aligns with bulk exfiltration of 4.9M records. Cross-reference Salesforce login source IPs against the free Tor exit node list at 'dan.me.uk/torlist' using a simple bash diff.

Evidence: Capture BEFORE tuning any detection rules: (1) Salesforce EventLogFile records for 'ReportExport', 'BulkApi', and 'ContentTransfer' event types during the April 2026 window — these are the specific log types that would record the ShinyHunters exfiltration of 4.9M customer records and are only retained for 24 hours on free Salesforce tiers, requiring immediate export. (2) Microsoft Entra OAuth 2.0 token grant logs filtered on 'Add delegated permission grant' and 'Consent to application' audit categories, which capture any third-party app the attacker authorized to maintain persistent API access to Salesforce data post-compromise. (3) Entra Conditional Access sign-in logs with ConditionalAccessStatus='notApplied' or 'failure', scoped to the Salesforce enterprise app registration, revealing the specific policy gap ShinyHunters exploited to authenticate without phishing-resistant MFA.

Step 3: Eradication — Enforce phishing-resistant MFA (FIDO2/hardware keys) on all Microsoft Entra accounts with Salesforce access, replacing SMS or voice-call OTP which are bypassed by vishing. Reference: NIST IA-5 (Authenticator Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access). In Salesforce, implement IP allowlisting, restrict Data Export permissions to named roles, and audit Connected Apps for unauthorized OAuth integrations. Apply D3-MFA and D3-CH (Credential Hardening) countermeasures.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IA-5 (Authenticator Management), NIST IA-2 (Identification and Authentication — Organizational Users), NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For teams that cannot immediately deploy FIDO2 hardware keys (cost/procurement delay), enforce Microsoft Authenticator with number matching and additional context as an interim phishing-resistant upgrade — configure via Entra ID > Authentication Methods > Microsoft Authenticator > Enable 'Require number matching'. Disable SMS and voice OTP methods organization-wide using the PowerShell command 'Update-MgPolicyAuthenticationMethodPolicy' targeting the 'Voice' and 'Sms' method types and setting state to 'disabled'. In Salesforce, restrict the 'Data Export' user permission to a named 'Data Steward' profile using Setup > Profiles, and revoke it from all other profiles including System Administrator until re-evaluated — this directly closes the bulk export vector ShinyHunters used.

Evidence: Capture BEFORE revoking OAuth tokens and Connected Apps: (1) Full list of Salesforce Connected Apps with OAuth tokens currently active, exported via Setup > Connected Apps OAuth Usage — preserves evidence of any persistent OAuth application the attacker registered for ongoing access after the initial vishing compromise. (2) Microsoft Entra Enterprise Applications list filtered to the Salesforce SAML/OIDC app, with all assigned users and their last token issuance timestamps — documents the full blast radius of which accounts could have been pivoted through the compromised identity. (3) Salesforce Permission Set and Profile assignments for any accounts touched during the incident window, captured via 'SELECT Id, PermissionSetId, AssigneeId FROM PermissionSetAssignment' SOQL query — ShinyHunters may have elevated permissions on the compromised account to enable bulk export.

Step 4: Recovery — Validate that all compromised accounts have been rotated and re-enrolled with phishing-resistant MFA per D3-CRO (Credential Rotation). Confirm Salesforce connected app permissions have been reviewed and reduced to least-privilege (NIST AC-6). Re-run Salesforce Data Export audit and verify no residual unauthorized access paths remain. Monitor Microsoft Entra Identity Protection risk detections continuously for 30 days post-remediation. Reference: CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST CP-10 (System Recovery and Reconstitution), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 6.1 (Establish an Access Granting Process)

Compensating: Without Entra Identity Protection P2 for continuous risk monitoring, configure a free Logic App alert using the Entra Sign-In Logs diagnostic setting forwarded to Azure Monitor — create an alert rule on 'riskLevelDuringSignIn ne none' to fire on any future risky sign-in at zero cost beyond Log Analytics ingestion. In Salesforce, implement a free Transaction Security Policy (available in all Salesforce editions) at Setup > Transaction Security > Policies — create a policy using the 'Data Export' event type that blocks exports exceeding 10,000 records and sends an email alert, directly mitigating the bulk exfiltration technique used in this breach. Run 'Get-MgUser -Filter "accountEnabled eq true" | Where-Object {$_.LastSignInDateTime -lt (Get-Date).AddDays(-45)}' monthly to enforce CIS 5.3 for dormant Entra accounts.

Evidence: Capture BEFORE closing the incident: (1) Salesforce Data Export history log showing all completed export jobs for the past 90 days, including the job owner, record count, and timestamp — establishes the definitive exfiltration timeline and confirms no additional export jobs ran after containment. (2) Microsoft Entra audit log export showing 'Reset user password' and 'Update user — StrongAuthenticationRequirements' events for all remediated accounts, confirming credential rotation and FIDO2/phishing-resistant MFA enrollment completion as evidence of eradication. (3) Salesforce Connected Apps OAuth usage report post-remediation, confirming revocation of any non-approved app tokens — validates no persistent OAuth backdoor survives the recovery phase.

Step 5: Post-Incident — Conduct a vishing-specific tabletop exercise targeting help desk and identity reset workflows — ShinyHunters' known entry vector is manipulating support and IT staff over phone calls. Implement out-of-band verification requirements for any identity reset, MFA enrollment change, or privileged access request initiated via phone or messaging. Review Salesforce data access governance: apply CIS 3.3 (Configure Data Access Control Lists) and NIST AC-3 (Access Enforcement) to restrict bulk record access by role. Add this incident pattern to your threat intelligence feed as an active TTP for SaaS-targeted vishing campaigns.

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 AT-2 (Literacy Training and Awareness), NIST AC-3 (Access Enforcement), NIST PM-16 (Threat Awareness Program), CIS 3.3 (Configure Data Access Control Lists), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Run the vishing tabletop using the free CISA Tabletop Exercise Package (CTEP) framework — customize a scenario where a caller impersonates an IT vendor and requests an Entra password reset and MFA re-enrollment, targeting your help desk staff directly. Document the out-of-band verification procedure as a one-page runcard: all phone-initiated identity changes require the requester to authenticate via a pre-shared employee PIN verified in your HR system before any Entra action is taken — implementable with zero tooling cost. For Salesforce role-based access governance, use the free Salesforce Optimizer report (Setup > Optimizer) to identify profiles with excessive Data Export, API Enabled, and View All Data permissions, then document a quarterly review cadence per CIS 7.2.

Evidence: Capture for post-incident reporting and threat intel: (1) Help desk call logs or ticketing system records (ServiceNow, Jira, or email) from March–April 2026 showing any password reset or MFA change requests initiated via phone — these are the primary evidence of the ShinyHunters vishing call and document the social engineering timeline for regulatory notification and lessons-learned reporting. (2) Salesforce field history tracking and record access logs for the customer account object, confirming exactly which PII fields (name, address, SSN, account number) were accessed and exported — required for state breach notification determinations under laws such as CCPA and for calculating the precise regulatory exposure of 4.9M affected customers. (3) Microsoft Entra audit log entries for the specific help desk or IT administrator account that processed the vishing-induced credential reset, capturing the 'Reset user password' and 'Update user' events that initiated the compromise chain — essential for root cause analysis and playbook refinement.

Detection Guidance

Microsoft Entra: Query sign-in logs for new device registrations, MFA method changes, conditional access policy failures, and token grants during the March-April 2026 window. Alert on: sign-ins from IP ranges associated with anonymizing infrastructure, impossible travel events, and OAuth grants to unfamiliar first-party or third-party applications. Salesforce: Review Login History for accounts that accessed abnormally large record volumes, and check Setup Audit Trail for Data Export jobs, permission set changes, or Connected App authorizations not initiated by known administrators. Reference: NIST AU-2 (Audit Events), NIST AC-2 (Account Management). Behavioral IOC: a single identity accessing millions of CRM records within hours is a strong indicator of bulk exfiltration consistent with this TTP (T1213, T1530). For vishing detection, review telephony and help desk ticketing logs for social engineering attempts targeting MFA resets or password recovery, as ShinyHunters specifically exploits these workflows. Cross-reference new MFA enrollments or account unlocks against the initiating call or ticket record.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/charter-communications-data-breach-affects-49-million-accounts/`	Primary reporting source — BleepingComputer coverage of the Charter Communications breach	HIGH

Framework Mappings

MITRE-ATTACK

- **T1213** — Data from Information Repositories
- **T1078.004** — Cloud Accounts
- **T1657** — Financial Theft
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1566.004** — Spearphishing Voice
- **T1586.002** — Email Accounts

NIST-800-53R5

- **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)
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

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
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1213	Data from Information Repositories	Collection
T1078.004	Cloud Accounts	Defense-Evasion
T1657	Financial Theft	Impact
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion
T1566.004	Spearphishing Voice	Initial-Access
T1586.002	Email Accounts	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/charter-communicatio...	T3
	https://www.bleepingcomputer.com/news/security/charter-communicatio...	T3
	https://www.bleepingcomputer.com/news/security/european-space-agenc...	T3
	https://www.bleepingcomputer.com/news/security/european-commission-...	T3
Charter Communications - Data Breach - Scott+Scott	https://scott-scott.com/consumer-cases/charter-communications-data-...	T3

Generated 2026-05-29 14:00 UTC by TJS Security Command Center