INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-31 06:09 UTC

ShinyHunters Publishes Data Allegedly Stolen from Charter Communications, Affecting Up to 4.9 Million Accounts

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0145
Type	Data Breach
Severity	HIGH
Affected Products	Charter Communications (Spectrum), customer account data; reported 4.9-13 million accounts depending on source
Published	1 day ago
Discovery Source	Serper

Executive Summary

ShinyHunters, a well-documented extortion group, has published data allegedly stolen from Charter Communications (Spectrum), the U.S. telecommunications provider. Reports indicate between 4.9 million and 13 million customer accounts may be affected, with personally identifiable information exposed. The breach creates direct risk of downstream fraud, regulatory scrutiny, and reputational harm for any organization whose employees or customers hold Spectrum accounts.

Technical Analysis

ShinyHunters has publicly released data allegedly exfiltrated from Charter Communications infrastructure. No CVE or specific technical vulnerability has been publicly attributed to the intrusion at this time. The attack maps to MITRE ATT&CK techniques: T1005 (Data from Local System), T1530 (Data from Cloud Storage), and T1586 (Compromise Accounts). Exposed data reportedly includes PII; the exact schema has not been publicly confirmed by Charter or an independent forensic firm. No CVSS score applies, this is a data breach disclosure, not a software vulnerability. Victim count discrepancy (4.9M vs. 13M) across SecurityWeek, BleepingComputer, and Techlicious suggests partial or staged disclosure. Root cause and initial access vector remain unconfirmed publicly as of the configuration date.

Action Checklist

1. Step 1: Containment. Audit any enterprise accounts tied to Charter/Spectrum services (billing portals, customer IDs, support accounts). Suspend or rotate credentials for service accounts or vendor contacts using Spectrum email domains or account identifiers. Reference NIST AC-2 (Account Management) to scope account review.
2. Step 2: Detection. Monitor for credential stuffing attempts against your perimeter using exposed PII as a lure. Review authentication logs for abnormal login patterns from unfamiliar IPs, particularly against externally exposed applications (NIST AU-6). Query SIEM for source IPs and domains associated with known ShinyHunters infrastructure, botnets, or command-and-control systems if your threat intelligence feeds carry tagged indicators. No specific hashes or domains are publicly confirmed at this time; treat IOC list as pending.
3. Step 3: Eradication. No patch applies. This is a third-party breach, not a software vulnerability in your environment. Eradication focus: revoke any shared or reused credentials that overlap with Charter account data. Enforce unique password policy per CIS 5.2 and disable any dormant accounts per CIS 5.3.
4. Step 4: Recovery. Validate that MFA is enforced on all externally exposed applications (CIS 6.3) and administrative access (CIS 6.5). Confirm audit logging is active and capturing authentication events per CIS 8.2 and NIST AU-2. Monitor for phishing campaigns using exposed PII to target your employees; ShinyHunters has historically used stolen data to enable follow-on social engineering.
5. Step 5: Post-Incident. Conduct a third-party vendor and supply-chain account review. Assess whether any employee PII present in the Charter dataset could enable spear-phishing or account takeover against your organization. Document control gaps against NIST AC-6 (Least Privilege) and AC-2 (Account Management). Evaluate integration of breach monitoring services (e.g., Have I Been Pwned, Flashpoint, or other threat intelligence platforms) into your threat intelligence program to track ongoing disclosure patterns.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if authentication logs confirm successful logins from credential stuffing attempts against accounts matching the Charter breach dataset, if employee PII confirmed in the ShinyHunters publication triggers state breach notification obligations (CCPA, NY SHIELD Act, or applicable state law), or if any third-party vendor account with privileged access to internal systems is identified in the breached dataset.
Recovery Notes	Post-containment, maintain elevated authentication monitoring for a minimum of 90 days given ShinyHunters' documented pattern of staging follow-on social engineering campaigns weeks to months after initial data publication. Verify MFA enforcement completion across all externally exposed applications before reducing alert thresholds — partial MFA rollout is the highest residual risk surface for credential stuffing from this dataset. Monitor threat intelligence feeds and breach forums for secondary publications or updated Charter datasets, as ShinyHunters has historically released data in tranches to maximize extortion leverage.

Forensic Artifacts	Authentication provider logs (Azure AD Sign-In, Okta System Log, or AD Security Event IDs 4624/4625/4648) filtered for accounts matching @spectrum.net and @charter.com domains — these reveal whether breached credentials were used to authenticate into your environment before or after ShinyHunters' publication date | Web application and reverse proxy access logs (Nginx/Apache/IIS) showing high-frequency POST requests to authentication endpoints from single source IPs, consistent with automated credential stuffing tooling (SentryMBA, OpenBullet) commonly used to operationalize ShinyHunters datasets | Email gateway quarantine logs and SMTP header records for inbound messages referencing Spectrum/Charter account themes post-publication — ShinyHunters-linked actors have used stolen telecom PII to craft convincing account-verification phishing lures targeting the same victim organizations | VPN and remote access gateway authentication logs showing any third-party vendor or contractor accounts affiliated with Charter/Spectrum that authenticated to your environment, along with source IP geolocation data to identify anomalous access patterns | Identity provider MFA bypass and legacy authentication protocol logs (Basic Auth, SMTP AUTH, IMAP) — credential stuffing attacks against organizations following this breach type specifically target legacy protocol endpoints that bypass modern MFA enforcement, leaving a distinct authentication pattern in provider logs

Per-Action IR Details

Step 1: Containment — Audit any enterprise accounts tied to Charter/Spectrum services (billing portals, customer IDs, support accounts). Suspend or rotate credentials for service accounts or vendor contacts using Spectrum email domains or account identifiers. Reference NIST AC-2 (Account Management) to scope account review.

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Export your Active Directory or identity provider account list and grep for @spectrum.net, @charter.com, or @chartercom.com email domains: `Get-ADUser -Filter * -Properties EmailAddress | Where-Object {$_.EmailAddress -match 'spectrum|charter'} | Select Name,EmailAddress,Enabled | Export-Csv accounts_audit.csv`. For Linux/LDAP environments: `ldapsearch -x -b 'dc=yourdomain,dc=com' mail | grep -iE 'spectrum|charter'`. Force password resets via `net user /logonpasswordchg:yes` for any matches. Document all findings in a dated change log.

Evidence: Before suspending accounts, capture: (1) Identity provider or AD last-logon timestamps for all Spectrum/Charter-affiliated accounts — export via `Get-ADUser -Filter * -Properties LastLogonDate,EmailAddress`; (2) Service account usage logs showing which internal systems those accounts authenticated to within the past 90 days; (3) Any vendor portal access logs or SSO federation logs showing Charter/Spectrum account identifiers. This establishes a pre-containment baseline and documents whether any matched accounts were recently active, which would indicate potential active exploitation.

Step 2: Detection — Monitor for credential stuffing attempts against your perimeter using exposed PII as a lure. Review authentication logs for abnormal login patterns from unfamiliar IPs, particularly against externally exposed applications (NIST AU-6). Query SIEM for source IPs associated with ShinyHunters infrastructure if threat intel feeds carry tagged IOCs. No specific hashes or domains are publicly confirmed at this time — treat IOC list as pending.

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-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, implement these targeted detections: (1) For credential stuffing against web applications, parse your web server or reverse proxy access logs for high-frequency POST requests to /login, /auth, or /signin endpoints from single IPs — `awk '$6=="POST" && $7~/login|auth|signin/' /var/log/nginx/access.log | awk '{print $1}' | sort | uniq -c | sort -rn | head -20`. (2) For Windows environments, query Security Event Log for Event ID 4625 (Failed Logon) and 4648 (Explicit Credential Use) clustered by source IP using: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625} | Group-Object {$_.Properties[19].Value} | Sort-Object Count -Descending`. (3) Deploy the Sigma rule 'Credential Stuffing - Multiple Failed Logins' (sigma/rules/web/web_multiple_failed_auth.yml) against exported logs using sigma-cli with the generic backend if no SIEM is available. (4) Check threat intel feeds such as AlienVault OTX (free) for ShinyHunters-tagged IOCs and cross-reference against firewall deny logs.

Evidence: Preserve before and during detection activity: (1) Web application access logs (Apache/Nginx/IIS) covering the 30 days prior to the ShinyHunters publication date — ShinyHunters typically stages data exfiltration weeks before public release, so pre-publication activity may be present in logs; (2) Authentication provider logs (Azure AD Sign-In logs, Okta System Log, or on-prem AD Event ID 4625/4624/4648) filtered for accounts matching known Charter/Spectrum customer email patterns; (3) VPN gateway authentication logs showing geographic anomalies or impossible travel from accounts that may appear in the breached dataset; (4) Firewall or proxy logs showing outbound connections to paste sites (pastebin.com, rentry.co, breachforums domains) which ShinyHunters commonly uses for data publication and victim communication.

Step 3: Eradication — No patch applies. This is a third-party breach, not a software vulnerability in your environment. Eradication focus: revoke any shared or reused credentials that overlap with Charter account data. Enforce unique password policy per CIS 5.2 and disable any dormant accounts per CIS 5.3.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential reuse detection without enterprise tooling: (1) Use the haveibeenpwned.com API (free tier available) to check whether corporate email addresses appear in the Charter/Spectrum breach or prior ShinyHunters datasets — `curl 'https://haveibeenpwned.com/api/v3/breachedaccount/{email}' -H 'hibp-api-key: YOUR_KEY'` in a loop over your employee email list. (2) Export all accounts with passwords older than 90 days using `Get-ADUser -Filter {PasswordLastSet -lt (Get-Date).AddDays(-90)} -Properties PasswordLastSet` and force resets for any that intersect with Spectrum/Charter email domains. (3) Audit for dormant accounts with `Get-ADUser -Filter {LastLogonDate -lt (Get-Date).AddDays(-45) -and Enabled -eq $true} -Properties LastLogonDate` and disable per CIS 5.3 threshold. Document each revocation with timestamp for regulatory evidence.

Evidence: Before revoking credentials, capture: (1) A timestamped export of all active accounts and their last authentication event — this is your pre-eradication baseline for regulatory documentation if a breach notification obligation is later triggered; (2) Any password manager or SSO configuration files showing credential sharing between Charter-affiliated accounts and internal systems — specifically look for service account configurations in task schedulers, CI/CD pipelines, and monitoring tools that may use shared credentials; (3) Log evidence of any accounts that were successfully authenticated after the ShinyHunters publication date, which would indicate credential stuffing success and elevates incident severity.

Step 4: Recovery — Validate that MFA is enforced on all externally exposed applications (CIS 6.3) and administrative access (CIS 6.5). Confirm audit logging is active and capturing authentication events per CIS 8.2 and NIST AU-2. Monitor for phishing campaigns using exposed PII to target your employees — ShinyHunters has historically used stolen data to enable follow-on social engineering.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-8 (Spam Protection), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 8.2 (Collect Audit Logs)

Compensating: MFA validation without enterprise IAM tooling: (1) Enumerate all externally exposed applications (VPN, webmail, cloud consoles, remote desktop gateways) and verify MFA enrollment per account using provider-native reports — for Azure AD: `Get-MgReportAuthenticationMethodUserRegistrationDetail | Where-Object {$_.IsMfaRegistered -eq $false}`. (2) For phishing detection targeting Charter-exposed PII, deploy email header analysis on incoming mail using free tools — configure your mail gateway or use `spamassassin -t < suspicious_email.eml` to score inbound messages referencing Spectrum account themes. (3) Enable Sysmon Event ID 1 (Process Creation) and Event ID 22 (DNS Query) to detect phishing payload execution; use the SwiftOnSecurity Sysmon config as a baseline. (4) Alert employees via internal communication about spear-phishing risk specific to Charter/Spectrum account holders — include sample lure language ShinyHunters has historically used (account verification, data exposure notices).

Evidence: During recovery, preserve: (1) Email gateway logs and quarantine queues for the 30 days post-publication, filtering for subject lines referencing 'Spectrum', 'Charter', 'account verification', 'data breach notification', or 'password reset' — these are ShinyHunters-consistent social engineering lures; (2) MFA enrollment audit reports from your identity provider showing any MFA bypass events (Event ID 18 in Azure AD conditional access logs) or legacy authentication protocol usage (SMTP AUTH, Basic Auth) that bypasses MFA; (3) DNS query logs for domains typosquatting spectrum.net or charter.com (e.g., spectrurn.net, chartercomm.com) which ShinyHunters and downstream threat actors commonly register post-publication to support credential harvesting campaigns.

Step 5: Post-Incident — Conduct a third-party vendor and supply-chain account review. Assess whether any employee PII present in the Charter dataset could enable spear-phishing or account takeover against your organization. Document control gaps against NIST AC-6 (Least Privilege) and AC-2 (Account Management). Consider adding breach monitoring services to your threat intelligence program.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Third-party exposure assessment without commercial breach monitoring: (1) Use the free HIBP API or DeHashed (limited free tier) to enumerate organizational email domains against known ShinyHunters breach datasets — automate with a bash script iterating over your employee email list. (2) Review vendor access to your systems: query your VPN and remote access gateway logs for third-party contractor accounts and cross-reference against Charter/Spectrum email domains identified in Step 1. (3) Update your threat intelligence program by subscribing to CISA Known Exploited Vulnerabilities feed (free) and configuring RSS alerts for ShinyHunters mentions on threat intel platforms such as OTX AlienVault. (4) Document lessons learned in a structured after-action report addressing: (a) how many internal accounts intersected with the Charter dataset, (b) MFA coverage gaps discovered in Step 4, (c) time-to-detect for credential stuffing indicators from Step 2 — this feeds directly into NIST 800-61r3 §4 lessons learned requirements.

Evidence: Post-incident evidence to preserve for lessons learned and potential regulatory documentation: (1) Final account audit report showing all Spectrum/Charter-affiliated accounts reviewed, actions taken, and timestamps — required for regulatory response if breach notification obligations apply under state PII laws (CCPA, SHIELD Act) triggered by employee data exposure; (2) Threat intelligence enrichment records documenting whether any ShinyHunters IOCs were confirmed in your environment during the detection phase — absence of evidence is also evidence and should be documented; (3) Vendor access review records showing third-party accounts with access to sensitive internal systems, cross-referenced against the Charter breach scope, to support supply chain risk assessment under NIST RA-3 (Risk Assessment).

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) have been publicly released for this incident as of reporting. Detection focus should shift to downstream threat indicators: (1) Credential stuffing, monitor authentication logs

for high-volume failed logins against externally facing portals, particularly from distributed IP ranges. (2) Spear-phishing precursors, flag inbound emails referencing Spectrum, Charter, or account-related lures targeting employees. (3) Account enumeration, review NIST AU-6 audit logs for unusual account lookups or access attempts using PII patterns consistent with telecom customer data (name + address + account number combinations). If your threat intelligence platform ingests ShinyHunters-tagged indicators, create alerting rules now. BleepingComputer and SecurityWeek are likely to publish IOCs if they surface; monitor those sources. Apply NIST AC-2 (Account Management) and AU-6 (Audit Review) controls to privileged accounts as a precautionary measure.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/charter-communications-data-breach-affects-49-million-accounts/`	BleepingComputer reporting on breach disclosure — monitor for IOC updates as investigation matures	LOW
URL	`https://www.securityweek.com/charter-communications-data-breach-could-impact-nearly-5-million/`	SecurityWeek primary reporting — source for victim count of approximately 5 million	LOW

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft
- **T1530** — Data from Cloud Storage
- **T1586** — Compromise Accounts

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

NIST-800-53R5

- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1530	Data from Cloud Storage	Collection
T1586	Compromise Accounts	Resource-Development

Sources

Source	URL	Tier
	https://www.securityweek.com/charter-communications-data-breach-cou...	T3
Charter Communications Data Breach Could Impact Nearly 5 Million -	https://x.com/SecurityWeek/status/2060403262386274313	T3
Charter Communications data breach affects 4.9 million accounts	https://www.bleepingcomputer.com/news/security/charter-communicatio...	T3
Charter confirms Spectrum data breach: 13 million customers exposed	https://www.techlicious.com/blog/spectrum-charter-data-breach-shiny...	T3
Charter Communications Data Breach Could Impact Nearly 5 Million	https://www.linkedin.com/posts/garettm_charter-communications-data-...	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 2026-05-31 06:09 UTC by TJS Security Command Center