INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-30 06:55 UTC

Over 14 million login credentials leaked from six ISPs in major data breach, here’s what we know

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0210
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Six unnamed Japanese ISPs, up to 14.2 million email/login accounts
Published	17 hours ago
Discovery Source	Serper

Executive Summary

According to TechRadar reporting (unconfirmed by affected ISPs or government authorities), a data breach affecting at least six Japanese internet service providers has resulted in the reported exposure of approximately 14.2 million email login credentials. The exact attack method has not been confirmed in available source material; reporting references infostealer activity or supply-chain compromise, but no official ISP or government statement has been issued. Organizations with employees or customers who hold accounts with Japanese ISPs face credential reuse and account takeover risk across enterprise systems.

Technical Analysis

Reported incident: approximately 14.2 million email login credentials exposed across at least six unnamed Japanese ISPs. No CVE identifier is associated with this breach. Relevant CWEs from item data: CWE-522 (Insufficiently Protected Credentials) and CWE-312 (Cleartext Storage of Sensitive Information), suggesting credential storage or transmission failures may be involved, though the exact technical vector is unconfirmed in available source material. MITRE ATT&CK techniques mapped in the item data include T1114 (Email Collection), T1586.002 (Compromise Accounts: Email Accounts), and T1078 (Valid Accounts), consistent with credential harvesting and subsequent account abuse scenarios. Attack vector, whether infostealer malware targeting ISP infrastructure, credential stuffing, or supply-chain compromise, is not confirmed. No patch or vendor advisory has been identified. Attribution to a specific threat actor is unconfirmed. All reporting appears to trace to a single originating TechRadar article; independent primary source confirmation from affected ISPs is pending.

Action Checklist

1. Step 1: Containment. Audit accounts for employees or customers who use Japanese ISP email addresses as login identifiers or recovery addresses on corporate systems; enforce password resets for any identified accounts per NIST AC-2 (Account Management) and CIS 6.3 (Require Multi-Factor Authentication).
2. Step 2: Detection. Query identity provider and SSO logs for anomalous login attempts originating from unfamiliar geolocations or IP ranges, particularly Japan-adjacent infrastructure; review for T1078 (Valid Accounts) abuse patterns such as off-hours logins, concurrent sessions, or logins from new device fingerprints (NIST AU-6, CIS 8.2).
3. Step 3: Eradication. Force credential rotation for any accounts confirmed to use ISP-origin email addresses as usernames or recovery contacts; apply NIST IA-4 (Identifier Management) and IA-5 (Authentication) controls; enforce credential rotation per CIS 5.4 (Remove Unnecessary Accounts); verify no shared passwords exist across enterprise systems using the exposed credentials.
4. Step 4: Recovery. Confirm MFA enrollment on all externally exposed applications and remote access points per CIS 6.3 and CIS 6.4; validate that account lockout policies are enforced per NIST AC-7 (Unsuccessful Logon Attempts); monitor affected accounts for 30 days post-reset for anomalous activity using NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Review credential storage and transmission controls against CWE-522 and CWE-312 findings; assess whether employee or customer accounts allow ISP email addresses as primary identifiers without MFA enforcement; document gaps and remediate per NIST AC-2 and CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal and privacy counsel if any confirmed unauthorized access to corporate systems is established using the leaked ISP credentials, or if affected accounts belong to employees in jurisdictions with mandatory breach notification obligations (EU GDPR 72-hour window, Japan APPI, US state notification laws), or if the organization lacks the IdP visibility to determine whether any of the 14.2 million leaked credentials match corporate account credentials — inability to rule out compromise is itself an escalation trigger.
Recovery Notes	Following credential rotation and MFA enforcement, monitor all formerly-ISP-email-linked accounts for 30 days minimum using IdP alert rules tuned for new source IP, new device fingerprint, off-hours authentication, and MFA fatigue patterns (repeated push denials followed by success), as threat actors who established OAuth persistence grants before rotation may retain access through authorized third-party app tokens that survived the password reset. Verify at day 7 and day 30 that no new OAuth application grants have been issued by affected accounts. If your organization provides services to Japanese consumers or has business relationships with any of the six unnamed ISPs, assess whether downstream customer accounts may also carry the same credential-reuse risk and whether contractual or regulatory notification obligations apply.

Forensic Artifacts	IdP authentication logs (Okta System Log, Azure AD Sign-In Logs, Google Workspace Admin Audit) covering 30 days pre-disclosure: filter for accounts with Japanese ISP email domains (@ocn.ne.jp, @nifty.com, @so-net.ne.jp, @biglobe.ne.jp, @kddi.com, @softbank.ne.jp) as UPN, recovery address, or proxy address — source IPs, user-agents, and MFA outcomes are the primary indicators of credential-stuffing using the leaked 14.2 million records | OAuth application authorization grants issued by affected accounts in the 30 days preceding breach disclosure: attacker use of valid ISP credentials to authorize malicious OAuth apps is a known post-access persistence technique that survives password rotation and would appear in IdP OAuth consent logs | Active Directory password hash dump (DSInternals 'Get-ADReplAccount') for duplicate hash analysis: identifies whether leaked ISP passwords were reused verbatim on corporate AD accounts, providing direct evidence of credential reuse impact without requiring the plaintext password | VPN and remote access gateway authentication logs (Cisco ASA, Palo Alto GlobalProtect, Fortinet FortiGate, or equivalent): filter for authentication events from ASNs associated with Japanese ISPs (NTT AS4713, KDDI AS2516, SoftBank AS17676, IIJ AS2497) as source — successful VPN auth from these ASNs against affected account credentials would confirm active exploitation | Email gateway and mail server logs for any ISP-domain recovery address confirmation emails or password reset flows initiated from external IPs: if an attacker used leaked ISP email access to trigger corporate account recovery flows, these would appear as inbound reset-confirmation clicks or OTP requests originating from Japan-geolocated IPs in mail server access logs or email security gateway logs (Proofpoint, Mimecast, or O365 Message Trace)

Per-Action IR Details

Step 1: Containment — Audit accounts for employees or customers who use Japanese ISP email addresses as login identifiers or recovery addresses on corporate systems; enforce password resets for any identified accounts per NIST AC-2 (Account Management) and CIS 5.3 (Disable Dormant Accounts).

NIST Phase: Containment

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

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

Compensating: Export user account lists from Active Directory using 'Get-ADUser -Filter * -Properties EmailAddress,ProxyAddresses | Where-Object {$_.EmailAddress -match "\.jp$" -or $_.ProxyAddresses -match "\.jp$"}' to identify ISP-domain email addresses (e.g., @ocn.ne.jp, @nifty.com, @so-net.ne.jp, @biglobe.ne.jp). Cross-reference against password recovery fields in your IdP (Okta, Azure AD, Google Workspace admin console) using bulk export. A 2-person team can complete this audit in a single shift using PowerShell and spreadsheet diffing.

Evidence: Before forcing password resets — which invalidate active session tokens and may destroy live session evidence — export all active session tokens and last-login metadata from your IdP (Okta System Log, Azure AD Sign-In Logs, or Google Workspace Admin Audit Log) for the identified accounts. Capture current session list via IdP API or admin console export. Record source IPs, user-agent strings, and device fingerprints for any session active within the past 72 hours on ISP-email-linked accounts, as these may represent attacker sessions established using the leaked credentials before your detection.

Step 2: Detection — Query identity provider and SSO logs for anomalous login attempts originating from unfamiliar geolocations or IP ranges, particularly Japan-adjacent infrastructure; review for T1078 (Valid Accounts) abuse patterns such as off-hours logins, concurrent sessions, or logins from new device fingerprints (NIST AU-6, CIS 8.2).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query Azure AD Sign-In Logs via Microsoft Graph CLI: 'az monitor activity-log list --filter "eventTimestamp ge 2025-01-01"' or use the Azure AD portal's Sign-In report filtered by country. For Okta, use the System Log API with query 'eventType eq "user.session.start" and outcome.result eq "SUCCESS"' and filter results in PowerShell for JP/AS-region IP ranges using a free IP geolocation database (ip-api.com bulk CSV). Flag accounts showing logins from ASNs associated with Japanese ISPs (KDDI AS2516, NTT AS4713, SoftBank AS17676) concurrent with or immediately preceding logins from your organization's known IP space — this pattern is consistent with credential-stuffing using the leaked 14.2 million records.

Evidence: This is a detection step that does not alter live system state on corporate infrastructure; however, capture a point-in-time snapshot of all active IdP sessions for ISP-email-linked accounts before analysts begin querying — active attacker sessions may be terminated by the query activity alerting the threat actor. Preserve raw IdP log exports (Okta syslog JSON, Azure AD signin-logs CSV, or Google Workspace audit JSON) covering at minimum 30 days prior to breach disclosure. Key artifacts: source IP per authentication event, MFA challenge outcome (success/bypass/not-required), device fingerprint or user-agent string, and session duration for accounts matching Japanese ISP email domains.

Step 3: Eradication — Force credential rotation for any accounts confirmed to use ISP-origin email addresses as usernames or recovery contacts; apply D3-CRO (Credential Rotation) and D3-CH (Credential Hardening) across affected identity stores; verify no shared passwords exist across enterprise systems using the exposed credentials.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Use 'Have I Been Pwned' k-anonymity API (api.pwnedpasswords.com) to check whether any enterprise passwords match entries in known breach corpuses — hash the candidate passwords with SHA-1, send the first 5 characters, and compare returned suffixes without transmitting the full hash. For internal shared-password detection without an enterprise PAM tool, run a password audit on your Active Directory using the free DSInternals PowerShell module ('Get-ADReplAccount' + 'Test-PasswordQuality') to identify duplicate password hashes across accounts, flagging any that match hashes from publicly circulated credential dumps associated with Japanese ISP breaches.

Evidence: Volatile capture REQUIRED before credential rotation: export the complete list of all active OAuth tokens, SAML assertions, API keys, and refresh tokens associated with affected accounts from your IdP before revoking — rotation invalidates these and destroys evidence of attacker-established persistence. Additionally, query your IdP for any third-party application authorizations (OAuth grants) made by affected accounts in the past 30 days; attackers using valid ISP credentials may have granted OAuth access to attacker-controlled apps as a persistence mechanism that survives a password reset. Preserve this data to artifact storage before executing any rotation.

Step 4: Recovery — Confirm MFA enrollment on all externally exposed applications and remote access points per CIS 6.3 and CIS 6.4; validate that account lockout policies are enforced per NIST AC-7 (Unsuccessful Logon Attempts); monitor affected accounts for 30 days post-reset for anomalous activity using NIST AU-6 (Audit Record Review, Analysis, and Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Validate MFA enrollment gaps using IdP admin bulk-export (Azure AD: 'Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}'; Okta: Users API filtered by 'provider.type ne "OKTA" and status eq "ACTIVE"'). For the 30-day monitoring period without a SIEM, configure free IdP alert rules for affected account UPNs: in Azure AD, use Conditional Access named locations to flag logins outside known corporate IPs; in Google Workspace, use the Alert Center for 'Suspicious login' events. Create a daily cron job or scheduled task to pull

and diff IdP login reports for the affected account list, alerting on any new source IP, new device, or MFA-bypass event.

Evidence: Recovery actions (MFA enforcement policy changes, lockout policy updates) alter system configuration rather than live session state, so volatile capture is not required at this step. However, before closing the incident window, preserve a baseline snapshot of MFA enrollment status for all affected accounts (exported from IdP as a timestamped CSV) and current account lockout policy settings (exported from AD via 'Get-ADDefaultDomainPasswordPolicy') to establish the verified-clean baseline for post-incident comparison during the 30-day watch period.

Step 5: Post-Incident — Review credential storage and transmission controls against CWE-522 and CWE-312 findings; assess whether employee or customer accounts allow ISP email addresses as primary identifiers without MFA enforcement; document gaps and remediate per NIST AC-2 and CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a manual identity-store configuration review: audit your IdP's accepted email domain allowlist to determine whether third-party consumer ISP domains (e.g., @nifty.com, @ocn.ne.jp, @biglobe.ne.jp) can be used as primary identifiers without MFA enforcement. Document findings in a structured gap register. Use OWASP ASVS v4 Section 2 (Authentication) as a free checklist framework to assess credential storage, transmission, and recovery controls against what the Japanese ISP breach revealed about ISP-side weaknesses — regardless of confirmed attack vector, the breach demonstrates that externally-held credentials used as corporate recovery contacts are an uncontrolled dependency.

Evidence: No volatile evidence at risk at this phase — post-incident activity operates on preserved artifacts from earlier phases. The primary evidence inputs for this review are: (1) the IdP audit log exports captured during detection_analysis, (2) the OAuth grant inventory captured before credential rotation, (3) the MFA enrollment baseline snapshot from recovery, and (4) the final account inventory showing which accounts had Japanese ISP email domains as identifiers or recovery contacts. These collectively form the forensic record supporting the gap assessment and any required regulatory breach notification documentation.

Detection Guidance

Query identity provider, SSO, and email gateway logs for accounts using Japanese ISP domain email addresses as login identifiers or recovery addresses. Look for T1078 indicators: successful logins from new IP ranges, geographic anomalies, concurrent sessions across disparate locations, or logins at unusual hours following the breach disclosure window (per NIST AU-6, CIS 8.2). Monitor identity and access logs to flag accounts with sudden privilege escalation or configuration changes post-login. No specific IOCs (IP addresses, hashes, domains) have been published in available source material; detection must rely on behavioral anomaly patterns rather than signature-based matching. Monitor for T1586.002 indicators: externally created or hijacked email accounts used to initiate password resets on enterprise systems.

Framework Mappings

MITRE-ATTACK

- **T1114** — Email Collection
- **T1586.002** — Email Accounts
- **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

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1114	Email Collection	Collection
T1586.002	Email Accounts	Resource-Development
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Techradar	https://www.techradar.com/pro/security/over-14-million-login-creden...	T3

Source	URL	Tier
16 billion passwords exposed in colossal data breach - Cybernews	https://cybernews.com/security/billions-credentials-exposed-infoste...	T2

Generated 2026-06-30 06:55 UTC by TJS Security Command Center