INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-13 06:40 UTC

Breach Notification Systems as Attack Surface: Disinformation, Extortion, and the Integrity of Public Incident Disclosure

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0451
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Maine Attorney General Breach Notification Portal; Instructure Canvas (LMS platform); Marquis (financial sector vendor serving 74+ US banks and credit unions); VRChat (impersonated); Discord (impersonated)
Published	2026-06-12T15:33:32
Discovery Source	Rss

Executive Summary

Three interconnected incidents have exposed a structural vulnerability in public breach disclosure infrastructure: fabricated breach filings disabled Maine's Attorney General notification portal, ShinyHunters has claimed a breach of Instructure Canvas affecting up to 275 million individuals (confirmed by Instructure), and a ransomware attack on financial vendor Marquis cascaded across 74 US banks and credit unions via shared credential exposure. The business risk is compound: organizations relying on the Maine portal for threat monitoring have lost a key intelligence resource, financial institutions face regulatory notification obligations from the Marquis supply-chain compromise, and the integrity of public incident disclosure as a threat intelligence source is actively degraded. Security and legal teams should treat breach notification data from the Maine AG portal with increased skepticism until identity verification controls are restored; cross-check any Maine portal entry against direct organizational confirmation before escalation. Your threat intelligence workflow, vendor access credentials in financial environments, and privileged account lifecycle should be immediately reviewed.

Technical Analysis

This campaign targets three distinct attack surfaces simultaneously. (1) Maine AG Portal Abuse: The portal auto-publishes breach submissions without submitter identity verification, mapped to CWE-287 (Improper

Authentication) and CWE-306 (Missing Authentication for Critical Function). Fabricated filings impersonating Discord and VRChat were published before detection, forcing a portal shutdown. Attack technique: T1565 (Data Manipulation) via fraudulent regulatory filings. (2) Instructure Canvas (ShinyHunters): Exploitation mapped to T1588 (Obtain Capabilities) and platform vulnerability category CWE-1026 (per vendor disclosure; specific CWE to be confirmed by Instructure). ShinyHunters claims exposure of data for up to 275 million individuals; Instructure has confirmed the breach occurred. Scope of confirmed data types not yet fully disclosed. (3) Marquis Ransomware, Financial Sector: Initial access via CVE-2024-40766 (SonicWall SonicOS improper access control, exploited by Akira ransomware group per prior CISA advisories), mapped to T1190 (Exploit Public-Facing Application). Contributing weaknesses: CWE-522 (Insufficiently Protected Credentials, SonicWall OTP seed exposure) and CWE-269 (Improper Privilege Management, stale privileged accounts not removed). Post-patch persistence achieved via T1078 (Valid Accounts) using stolen VPN credentials. Resecurity honeypot data identified 188,000 exfiltration requests routed through residential proxies (T1041). Akira and an unconfirmed group operating as 'Marquis' are involved; Marquis attribution remains medium confidence. SonicWall CVE-2024-40766 carries CVSS 7.5 per NVD; campaign-level severity (high) is driven by cascading supply-chain impact (74+ institutions) rather than individual CVE score. No additional CVE IDs are associated with the Maine portal or Canvas incidents in the provided source data.

Action Checklist

1. Step 1: Containment, Financial institutions using Marquis or any shared financial sector vendor should immediately audit active VPN and privileged account sessions; revoke credentials for any accounts not confirmed active and necessary, per NIST AC-2 (Account Management) and CIS 5.3 (Disable Dormant Accounts). If SonicWall VPN is in use, verify CVE-2024-40766 is patched and confirm OTP seed material has not been exposed.
2. Step 2: Detection, For Marquis/SonicWall exposure: review VPN authentication logs for sequences of failed login attempts without account lockout enforcement (control gap enabling T1110 Brute Force), off-hours privileged logins, and lateral movement from VPN ingress points. For Canvas/Instructure: monitor for credential stuffing attempts against Canvas SSO endpoints and watch for ShinyHunters data appearing in breach-trading forums. For Maine portal abuse: validate any breach notification sourced from the Maine AG portal against direct organizational confirmation before acting; treat unverified Maine portal entries as potentially fabricated until the portal resumes with authentication controls. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, (Marquis/SonicWall) Apply SonicWall patch for CVE-2024-40766 if not already applied; rotate all VPN credentials and OTP seeds; delete or disable all stale privileged accounts per CIS 5.3 and NIST AC-2. (Canvas) Await Instructure's official disclosure of affected data types and apply any platform patches issued; enforce MFA on all Canvas administrative and instructor accounts per CIS 6.5 (Require MFA for Administrative Access). (Maine portal) Remove the portal from automated threat intelligence feeds until identity verification controls are confirmed restored.
4. Step 4: Recovery, Verify no unauthorized VPN sessions persist post-credential rotation; confirm privileged account inventory is reconciled against active personnel per NIST AC-2. For financial institutions, validate Marquis vendor's incident scope against your data sharing agreement to scope notification obligations. Re-enable Maine AG portal monitoring only after public confirmation of authentication gating. Monitor for T1078 (Valid Accounts) reuse patterns for 30 days post-remediation per NIST AU-6.

5. Step 5: Post-Incident, This campaign exposes three persistent control gaps: (a) Absence of submitter identity verification in regulatory disclosure portals (CWE-306/CWE-287), advocate for authentication requirements in breach notification submissions to your state regulators; (b) Stale privileged account and credential lifecycle failures (CWE-269, CWE-522), implement quarterly privileged account review per NIST AC-2 and CIS 5.3; (c) Single-vendor dependency risk in financial sector supply chains, map vendor access to critical systems and apply D3-CRO (Credential Rotation) and D3-MFA (Multi-factor Authentication) countermeasures to all vendor-facing entry points.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and primary banking regulator (OCC, FDIC, NCUA, or state DFI as applicable) immediately if Marquis confirms your institution's customer PII or account credentials are within the compromised dataset, if any active unauthorized VPN session is identified post-CVE-2024-40766 assessment, or if a fabricated Maine AG portal filing referencing your organization is discovered — all three conditions independently trigger mandatory breach notification timelines under Gramm-Leach-Bliley Act and applicable state law.
Recovery Notes	After credential rotation and CVE-2024-40766 patching are confirmed, re-validate all SonicWall VPN policy rules to ensure no residual unauthorized access paths remain, as CVE-2024-40766's improper access control flaw may have permitted policy-bypass that survives credential rotation alone. Monitor Canvas SSO and API authentication logs continuously for 30 days for ShinyHunters-attributed credential-stuffing patterns using the newly exposed dataset, as threat actors routinely weaponize exfiltrated credentials within days of a confirmed breach claim. For financial institutions, do not restore normal Marquis vendor access until the vendor provides written attestation that the ransomware infection is fully eradicated and their credential infrastructure has been independently audited.
Forensic Artifacts	SonicWall VPN authentication syslog (UDP/514) — contains the pre-exploitation failed-then-successful authentication sequence characteristic of CVE-2024-40766 improper access control abuse; retain raw syslog files for the 90 days preceding incident discovery | SonicWall Active Connections Monitor export — timestamped session table capturing authenticated username, source IP, session duration, and bytes transferred for all VPN sessions active during the compromise window; this is the primary artifact for mapping Marquis-vector lateral movement | Windows Security Event Log from VPN-reachable hosts — Event ID 4624 (Logon Type 3/10), 4648 (Explicit Credential Use), and 4776 (Credential Validation) filtered to the VPN ingress IP range, documenting post-VPN lateral movement enabled by the Marquis shared-credential exposure | Instructure Canvas Admin Audit Log and API access log — bulk data export events, API token creation records, and OAuth grant events covering the period of ShinyHunters' claimed exfiltration; a 275M-record scrape would produce anomalous API call volume visible in rate-limit and request-count fields | Maine AG portal submission records — archived copies (screenshot plus HTTP response headers) of any breach notification filing referencing your organization, with submission timestamp and submitter metadata, establishing whether fabricated entries affected your organization's threat intelligence posture or triggered erroneous internal incident response actions

Per-Action IR Details

Step 1: Containment — Financial institutions using Marquis or any shared financial sector vendor should immediately audit active VPN and privileged account sessions; revoke credentials for any accounts not confirmed active and necessary, per NIST AC-2 (Account Management) and CIS 5.3 (Disable Dormant Accounts). If SonicWall VPN is in use, verify CVE-2024-40766 is patched and confirm OTP seed material has not been exposed.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Isolate affected systems and revoke access vectors to prevent further propagation while preserving evidence of compromise.

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Run `Get-VpnConnection` and `Get-NetTCPConnection -State Established` on Windows VPN concentrator or gateway hosts to enumerate live sessions; cross-reference against an HR-sourced active personnel list exported to CSV. For SonicWall specifically, pull the Active Connections Monitor export from the SonicOS GUI (Monitor > Active Connections) before terminating any session. Use a PowerShell one-liner to dump active AD accounts with last-logon older than 45 days: `Search-ADAccount -AccountInactive -TimeSpan 45 -UsersOnly | Select-Object Name,LastLogonDate | Export-Csv stale_accounts.csv`.

Evidence: Before revoking any VPN session or rotating OTP seeds, capture: (1) Full SonicWall VPN session table export (Active Connections Monitor) including source IP, authenticated username, session start time, and bytes transferred — this documents which accounts were active at time of compromise; (2) Windows Security Event Log Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use) filtered to Logon Type 3 (Network) and Type 10 (RemoteInteractive) from the VPN ingress period; (3) `netstat -ano` output and running process list (`tasklist /svc`) from any host reached via VPN lateral movement; (4) OTP seed database file path and last-modified timestamp before any rotation — exposure of seeds (not just tokens) is the Marquis/SonicWall-specific risk from CVE-2024-40766's improper access control flaw.

Step 2: Detection — For Marquis/SonicWall exposure: review VPN authentication logs for account lockout events (absent lockout policy per T1110), off-hours privileged logins, and lateral movement from VPN ingress points. For Canvas/Instructure: monitor for credential stuffing attempts against Canvas SSO endpoints and watch for ShinyHunters data appearing in breach-trading forums. For Maine portal abuse: validate any breach notification sourced from the Maine AG portal against direct organizational confirmation before acting; treat unverified portal entries as potentially fabricated until the portal resumes with authentication controls. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlate log sources across VPN, SSO, and external intelligence feeds to characterize scope of Marquis credential exposure, Canvas data theft, and Maine portal integrity compromise.

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: For Marquis/SonicWall: parse SonicWall syslog output (UDP/514) with `grep` or PowerShell `Select-String` for authentication failure strings followed by success from the same source IP within a 5-minute window — this is the credential-stuffing pattern absent lockout controls. For Canvas SSO: configure free Cloudflare or nginx access log parsing to flag >20 failed OAuth/SAML assertions per source IP per minute against Canvas login endpoints. For Maine portal abuse: maintain a private spreadsheet cross-referencing any Maine AG portal filing that names your organization against direct email/phone confirmation with the filing entity — free and achievable with two analysts.

Evidence: This step does not alter live state; capture the following as the detection record: (1) SonicWall authentication syslog entries showing Event ID patterns for failed then successful auth from the same IP (CVE-2024-40766 exploitation artifact); (2) Canvas SSO/SAML assertion logs from Instructure's admin console showing unusual volume of authentication requests or bulk data export events — ShinyHunters operations typically involve large API scrapes preceding exfiltration; (3) Maine AG portal submission metadata (filing timestamps, submitter email domains, IP addresses if obtainable via public records request) for any filing referencing your organization, to

establish whether the entry is fabricated; (4) Threat-intel feed entries or forum posts referencing 'ShinyHunters Canvas' or 'Marquis bank credentials' on dark-web adjacent forums (BreachForums, Telegram) — document URLs and timestamps as intelligence artifacts, do not download raw data.

Step 3: Eradication — (Marquis/SonicWall) Apply SonicWall patch for CVE-2024-40766 if not already applied; rotate all VPN credentials and OTP seeds; delete or disable all stale privileged accounts per CIS 5.3 and NIST AC-2. (Canvas) Await Instructure's official disclosure of affected data types and apply any platform patches issued; enforce MFA on all Canvas administrative and instructor accounts per CIS 6.5 (Require MFA for Administrative Access). (Maine portal) Remove the portal from automated threat intelligence feeds until identity verification controls are confirmed restored.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Remove the specific vulnerability (CVE-2024-40766 unpatched SonicWall, exposed OTP seeds, stale privileged accounts) that enabled initial access and persistence across the Marquis supply-chain vector.

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.5 (Require MFA for Administrative Access), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For CVE-2024-40766 patching on SonicWall: follow SonicWall PSIRT advisory steps directly from MySonicWall portal — apply firmware update to SonicOS 7.0.1-5035 or later for Gen 7 devices, or 6.5.4.15 or later for Gen 6/6.5 devices. OTP seed rotation: export the current seed database, delete all TOTP/HOTP seed records from the SonicWall local database, and re-provision using a new shared secret — distribute new enrollment QR codes via out-of-band channel (SMS or physical). For Canvas MFA without enterprise SSO: use Instructure's native Canvas MFA settings under Admin > Authentication to enforce TOTP for all admin roles — free and built-in.

Evidence: Before applying the SonicWall patch or rotating OTP seeds (actions that alter system state), capture: (1) Full SonicWall firmware version string and configuration export (`.exp` file via SonicOS export) as a pre-patch baseline; (2) Complete dump of all provisioned VPN user accounts including creation date, last-authentication timestamp, and associated group memberships — documents the stale account population that enabled Marquis-vector lateral movement; (3) Memory image of the SonicWall management process if forensic capability exists, as CVE-2024-40766 is an improper access control flaw that may have exposed credential material in process memory; (4) Canvas admin audit log export (Admin > Logging) covering the 90 days prior to ShinyHunters' claimed exfiltration date, capturing bulk data export events, API token generation, and role escalation — these are the specific artifacts a 275M-record scrape would produce.

Step 4: Recovery — Verify no unauthorized VPN sessions persist post-credential rotation; confirm privileged account inventory is reconciled against active personnel per NIST AC-2. For financial institutions, validate Marquis vendor's incident scope against your data sharing agreement to scope notification obligations. Re-enable Maine AG portal monitoring only after public confirmation of authentication gating. Monitor for T1078 (Valid Accounts) reuse patterns for 30 days post-remediation per NIST AU-6.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore verified-clean VPN and privileged account posture, confirm vendor incident scope for regulatory scoping, and re-introduce intelligence feeds only after Maine portal integrity is confirmed.

Controls: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Post-rotation verification: run `Get-NetTCPConnection -State Established | Where-Object {$_.LocalPort -eq 4433}` (SonicWall SSL-VPN default port) to confirm zero active sessions survive credential rotation. For privileged account reconciliation without an IDM platform, export AD privileged group memberships (`Domain Admins`, `Enterprise Admins`, vendor-specific OUs) via `Get-ADGroupMember -Recursive` and diff against the HR active personnel CSV captured in Step 1. For 30-day Valid Accounts reuse monitoring, deploy a free Sigma rule (sigma rule `win_security_account_reuse_after_rotation`) against Windows Security Event Log using `chainsaw` or

`Hayabusa` — both are free CLI EVTX analysis tools.

Evidence: This step modifies monitoring configuration (re-enabling feeds, reconciling accounts); before re-enabling Maine AG portal entries in threat intel tooling, document: (1) A screenshot or archived copy of the Maine AG portal's public status page confirming authentication controls are restored — this is the verification artifact for re-enabling the feed; (2) Marquis vendor-provided incident scope letter or breach notification (obtain in writing) specifying data types, affected institution list, and compromise window — required to determine your organization's independent notification obligation under Gramm-Leach-Bliley Act or state breach notification law; (3) 30-day VPN authentication log baseline post-rotation, capturing all Event ID 4624 Logon Type 3 events, to establish a clean comparative baseline for Valid Accounts reuse detection.

Step 5: Post-Incident — This campaign exposes three persistent control gaps: (a) Absence of submitter identity verification in regulatory disclosure portals (CWE-306/CWE-287) — advocate for authentication requirements in breach notification submissions to your state regulators; (b) Stale privileged account and credential lifecycle failures (CWE-269, CWE-522) — implement quarterly privileged account review per NIST AC-2 and CIS 5.3; (c) Single-vendor dependency risk in financial sector supply chains — map vendor access to critical systems and apply D3-CRO (Credential Rotation) and D3-MFA (Multi-factor Authentication) countermeasures to all vendor-facing entry points.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conduct lessons-learned review addressing the three structural gaps this campaign exposed — regulatory portal integrity, privileged credential lifecycle, and financial-sector third-party dependency concentration.

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Quarterly privileged account review without IDM: schedule a cron job or Windows Scheduled Task to run `Get-ADGroupMember -Recursive -Identity 'Domain Admins' | Get-ADUser -Properties LastLogonDate` and email results to the security team — zero-cost and repeatable. For vendor access mapping without a TPRM platform, maintain a shared spreadsheet (template: vendor name, systems accessed, access method, credential type, last-reviewed date, MFA enforced Y/N) reviewed quarterly. For advocacy to state regulators on Maine portal authentication: draft a formal comment letter referencing the fabricated filing incident and citing NIST SP 800-63B (Digital Identity Guidelines) as the authentication standard regulators should require for portal submissions.

Evidence: Post-incident documentation artifacts to retain for lessons-learned and regulatory response: (1) Full timeline of fabricated Maine AG portal filings referencing your organization (if any), including submission timestamps and comparison against your actual incident history — demonstrates the disinformation risk concretely; (2) Pre- and post-remediation privileged account inventory diff showing accounts disabled or deleted as a result of this incident — demonstrates control gap closure for auditors; (3) Marquis vendor incident report and your institution's data-sharing agreement, retained together — establishes the third-party dependency scope for future vendor risk assessments; (4) Written record of any regulatory communications (state AG, FFIEC, NCUA) triggered by Marquis cascade exposure — required for compliance documentation under applicable financial sector breach notification requirements.

Detection Guidance

Three detection workstreams apply. (1) SonicWall/Marquis: Query VPN authentication logs for sequences of failed login attempts without account lockout enforcement (control gap enabling T1110 Brute Force); flag successful logins from IP ranges associated with residential proxy services; alert on privileged account activity from accounts inactive for 45+ days. Cross-reference against Resecurity's reported residential proxy exfiltration pattern (188,000 requests). Apply D3-LAM (Local Account Monitoring) for stale account activity. (2) Canvas/ShinyHunters: Monitor breach-trading forums and paste sites for Instructure or Canvas credential

dumps; enable anomaly detection on Canvas API authentication endpoints for credential stuffing patterns; alert on bulk data export events from Canvas administrative accounts. (3) Maine portal disinformation: Implement a validation step in your threat intelligence pipeline that cross-checks Maine AG portal entries against direct issuer confirmation before routing to analysts or escalation workflows. Flag any Maine portal entry referencing an organization without corroborating source before treating as actionable. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) for logging requirements supporting these queries.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Residential proxy network infrastructure (specific IPs not disclosed in source data)`	Resecurity honeypot identified 188,000 exfiltration requests routed through residential proxies; treat unusual volume from residential IP ranges targeting VPN or API endpoints as a behavioral IOC	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1036** — Masquerading
- **T1498** — Network Denial of Service
- **T1486** — Data Encrypted for Impact
- **T1110** — Brute Force
- **T1565** — Data Manipulation
- **T1190** — Exploit Public-Facing Application
- **T1566** — Phishing
- **T1588** — Obtain Capabilities
- **T1659** — Content Injection
- **T1078** — Valid Accounts

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **5.2** — Use Unique Passwords
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1036	Masquerading	Defense-Evasion
T1498	Network Denial of Service	Impact
T1486	Data Encrypted for Impact	Impact
T1110	Brute Force	Credential-Access
T1565	Data Manipulation	Impact
T1190	Exploit Public-Facing Application	Initial-Access
T1566	Phishing	Initial-Access
T1588	Obtain Capabilities	Resource-Development
T1659	Content Injection	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/maine-disables-data-...	T3
	https://www.bleepingcomputer.com/news/security/hackers-claim-resecu...	T3
	https://www.bleepingcomputer.com/news/security/instructure-confirms...	T3
	https://www.bleepingcomputer.com/news/security/marquis-data-breach-...	T3
Maine disables data breach notification portal after fake disclosures	https://www.bleepingcomputer.com/news/security/maine-disables-data-...	T3

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 2026-06-13 06:40 UTC by TJS Security Command Center