INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:44 UTC

BridgePay Ransomware Attack Triggers Widespread Payments Disruption

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0010
Type	Threat Campaign
Severity	HIGH
Affected Products	BridgePay (U.S. payments platform provider); downstream clients and dependent entities, specific versions not identified in available sources
Published	1 month ago

Executive Summary

A ransomware attack against BridgePay, a U.S. payment processing platform provider, has disrupted operations across multiple dependent organizations. The attack follows a deliberate pattern of targeting payment infrastructure and managed service providers to amplify downstream impact beyond the primary victim. Organizations that rely on BridgePay for payment processing should assess service continuity exposure and activate third-party incident response procedures.

Technical Analysis

BridgePay, a U.S.-based payments platform provider, was struck by ransomware resulting in cascading service disruption to downstream clients. No specific ransomware group has been attributed in available open sources; BridgePay has not made a public attribution statement as of the sources reviewed. MITRE ATT&CK techniques associated with this incident type include T1190 (Exploit Public-Facing Application), T1486 (Data Encrypted for Impact), and T1657 (Financial Theft or unauthorized fund transfers). Initial access vector is unconfirmed. No CVE identifier is associated with this campaign; it does not appear to exploit a specific named vulnerability. No IOCs (hashes, IPs, domains) have been confirmed in available open sources at this time. Source quality for this item is limited (T3 sources only; source quality score 0.64), technical details should be treated as preliminary pending official disclosure from BridgePay or authoritative reporting. No patch status is applicable as this is an operational incident, not a software vulnerability.

Action Checklist

1. Step 1, Immediate: Confirm BridgePay service status directly with your account representative or BridgePay's official communications channel; activate contingency payment processing procedures if

service is degraded.

2. Step 2, Detection: Review network logs and EDR telemetry for anomalous lateral movement, large-scale file encryption activity, or unusual outbound connections consistent with T1486 (Data Encrypted for Impact) and T1190 (Exploit Public-Facing Application) behavior patterns.

3. Step 3, Assessment: Inventory all systems, workflows, and data flows with direct or indirect dependency on BridgePay; assess potential exposure of payment data transiting the platform and determine whether cardholder data or PII may be at risk.

4. Step 4, Communication: Notify relevant internal stakeholders (finance, legal, compliance, executive leadership) of potential payment processing disruption; if cardholder data exposure is possible, engage legal and privacy counsel to assess breach notification obligations under PCI DSS and applicable state law.

5. Step 5, Long-term: Conduct a third-party risk review of all payment processing and MSP dependencies; validate that vendor contracts include incident notification SLAs and that your organization has documented business continuity procedures for critical payment provider failures, consistent with NIST SP 800-53 SA-9 (External System Services) and CP-2 (Contingency Plan) controls.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm if forensic analysis reveals data exfiltration (confirmed file staging/transfer), lateral movement to production databases, or if payment data exposure is confirmed and your organization lacks breach response experience or legal resources.
Recovery Notes	After containment: (1) Validate remediation by re-running detection scans (EDR queries, file system scans) to confirm malware/lateral movement artifacts are gone. (2) Restore payment processing from clean backup or validated systems; reconcile all transactions processed during outage window against financial records. (3) Implement compensating controls until root cause is known: enhanced network monitoring for BridgePay connections, mandatory MFA for payment system access, daily file integrity checks on payment database servers.
Forensic Artifacts	Windows Security Event Log (Event ID 4688 Process Creation, 4624 Logon, 4625 Failed Logon, 4720 User Created) | Sysmon logs (Event ID 1 Process Creation, 3 Network Connection, 11 File Create) | Web server access logs (Apache access.log, IIS W3SVC) with HTTP status codes and request paths | Network PCAP or proxy logs showing DNS queries, outbound connections, and data transfer volumes | Application logs from payment systems (transaction timestamps, API calls to BridgePay, error codes)

Per-Action IR Details

Step 1, Immediate: Confirm BridgePay service status directly with your account representative or BridgePay's official communications channel; activate contingency payment processing procedures if service is degraded.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation Phase)

Controls: NIST 800-53 CP-2 (Contingency Plan), NIST 800-53 SA-9 (External System Services), CIS 4.2 (Address Unauthorized Software)

Compensating: Maintain a documented contact list (spreadsheet with email, phone, incident escalation contact) for BridgePay support updated quarterly. Establish a manual payment processing procedure documented in a runbook:

alternative payment gateway login credentials, batch processing instructions, and transaction reconciliation steps executable without API integration.

Evidence: Before contacting BridgePay, capture: (1) current network connectivity to BridgePay endpoints (ping, tracert, DNS resolution), (2) screenshots of BridgePay dashboard showing last successful transaction timestamp, (3) system time on your servers to rule out local clock skew, (4) copies of any official BridgePay status page communications received in past 24 hours.

Step 2, Detection: Review network logs and EDR telemetry for anomalous lateral movement, large-scale file encryption activity, or unusual outbound connections consistent with T1486 (Data Encrypted for Impact) and T1190 (Exploit Public-Facing Application) behavior patterns.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis Phase - Determine whether an incident has occurred)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-2 (Audit Events), CIS 8.2 (Configure Centralized Log Management), CIS 8.8 (Log Events to Central Storage)

Compensating: Without EDR: (1) Windows Event Log 4688 (Process Creation) exported via `wevtutil qe Security /q:*[System[(EventID=4688)]] /f:text > processes.txt` on each endpoint, filtered for anomalous encryption utilities (certutil, cipher.exe, tar.exe with high-entropy files). (2) Network traffic: use Zeek (free, open-source) or tcpdump to capture PCAP, analyze with Suricata rules for ransomware C2 signatures. (3) File system: scan with YARA rules targeting common ransomware encryption patterns (CheckPoint, Kaspersky publish free rules). (4) Manual log review: examine web server access logs (Apache/IIS) for exploitation attempts: SQL injection, path traversal, unpatched application endpoints.

Evidence: Capture BEFORE analysis: (1) Process Creation logs (Windows Event ID 4688, Sysmon Event ID 1) from 72 hours before disruption to present. (2) File modification logs: MFT (Master File Table) snapshot or fsutil USN journal extract. (3) Network traffic PCAP (full packet capture or at minimum DNS queries, outbound connection logs). (4) PowerShell transcription logs (if enabled) or alternative: command-line audit logs (Windows Event ID 4103). (5) Web server access logs with full request paths and response codes.

Step 3, Assessment: Inventory all systems, workflows, and data flows with direct or indirect dependency on BridgePay; assess potential exposure of payment data transiting the platform and determine whether cardholder data or PII may be at risk.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment, Eradication, and Recovery Phase - short-term containment)

Controls: NIST 800-53 SA-9 (External System Services), NIST 800-53 IA-4 (Identifier Management), NIST 800-53 SC-7 (Boundary Protection), CIS 1.1 (Inventory and Control of Enterprise Assets)

Compensating: Map dependencies manually: (1) Search Active Directory for service accounts with 'bridgepay' or 'payment' in name; query SQL Server and application config files for connection strings. (2) Interview stakeholders: finance team (which transactions touch BridgePay?), developers (which APIs/integrations?), network team (which firewall rules allow BridgePay traffic?). (3) Grep application code repos for BridgePay API endpoints, variable names, hardcoded IPs. (4) Data flow diagram: draw on whiteboard or Google Sheets linking systems → BridgePay → payment recipients. (5) Query database logs for data exfiltration: SELECT statements from payment tables, timestamp range matching attack window.

Evidence: Capture BEFORE inventory: (1) Network configuration files (/etc/hosts, DNS records, firewall rules, NAT tables). (2) Application configuration files (config.xml, .env files, appsettings.json) from all servers with payment functionality. (3) Service account credential material location (if stored in files, vaults, or key management systems). (4) Database transaction logs showing data accessed during suspected compromise window. (5) API call logs showing requests to BridgePay endpoints with timestamps and payloads.

Step 4, Communication: Notify relevant internal stakeholders (finance, legal, compliance, executive leadership) of potential payment processing disruption; if cardholder data exposure is possible, engage legal and privacy counsel to assess breach notification obligations under PCI DSS and applicable state law.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Preparation Phase - notification procedures) and §3.2.2 (Detection and Analysis Phase - reporting)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-4 (Incident Handling), CIS 6.1 (Establish an Incident Response Process)

Compensating: Use your documented incident communication plan (required by policy): (1) Pre-write notification templates for finance (payment processing status, estimated recovery time), legal (data exposure assessment, breach notification timeline), and executive (business impact, stakeholder communications). (2) Establish a war room: daily call at fixed time (e.g., 9 AM) with attendees listed in advance. (3) Use a shared tracking document (Google Sheet, Excel) to log: questions raised, decisions made, action owners, deadlines. (4) Assign one person as communications lead to centralize message consistency. (5) For PCI/breach assessment, consult your contract's payment processor liability clause and state data breach notification laws (usually 30–60 days). Frame legal conversation as: 'Do we meet breach definition under state law? What is our notification timeline?'

Evidence: Capture BEFORE notification: (1) Forensic timeline: when was disruption first detected, when was BridgePay notified, when did you learn of ransomware? (2) Data exposure scope: what data transited BridgePay during the attack window (card numbers, expiration, CVC, cardholder names/addresses)? (3) Encryption status: was data encrypted, tokenized, or in plaintext? (4) Affected customer count: how many transactions/records are potentially exposed? (5) PCI compliance status: do you have a current P2PE attestation, or were you storing card data outside compliance scope?

Step 5, Long-term: Conduct a third-party risk review of all payment processing and MSP dependencies; validate that vendor contracts include incident notification SLAs and that your organization has documented business continuity procedures for critical payment provider failures, consistent with NIST SP 800-53 SA-9 (External System Services) and CP-2 (Contingency Plan) controls.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.3 (Post-Incident Activities) and NIST 800-53 SA-9, CP-2

Controls: NIST 800-53 SA-3 (System Development Life Cycle), NIST 800-53 SA-9 (External System Services), NIST 800-53 CP-2 (Contingency Plan), CIS 6.5 (Manage Service Provider Relationships)

Compensating: Create a vendor risk assessment spreadsheet: columns = vendor name, service criticality (critical/high/medium/low), contract review date, has SLA for incident notification (Y/N), has RTO/RPO defined (Y/N), backup provider exists (Y/N), last breach assessment date. (1) Audit contracts: search for 'incident', 'notification', 'breach', 'SLA', 'RTO' to confirm 24–48 hour notification language. (2) Document contingency: write a runbook for each critical vendor failure: alternative payment gateway login, batch processing procedures, transaction reconciliation steps. (3) Test annually: conduct a tabletop exercise where you simulate BridgePay failure and walk through your contingency procedures (do they work?). (4) Maintain a secondary payment processor account (even if unused) as active backup.

Evidence: Capture for post-incident review: (1) List of all current third-party payment/MSP contracts with signature dates and SLA appendices. (2) Records of previous vendor security incidents and how they were handled. (3) Vendor security questionnaires (SOC 2 Type II reports, penetration test results, vulnerability assessments). (4) Internal business continuity test results (last 12 months) showing whether contingency procedures were validated. (5) Audit trail of vendor risk assessments conducted (dates, findings, remediation status).

Detection Guidance

No confirmed IOCs are available from open sources at this time. Detection should focus on behavioral indicators consistent with ransomware TTPs mapped to this incident. Monitor for: (1) mass file rename or encryption events on endpoints and file servers (T1486); (2) anomalous authentication attempts or exploitation attempts against internet-facing applications (T1190); (3) unexpected outbound data transfers or connections to newly observed external IPs prior to encryption events (potential exfiltration staging); (4) unauthorized fund transfers, unusual payment reversals, account modifications, or anomalous transaction patterns within payment

processing systems or downstream banking connections (T1657). For organizations integrated with BridgePay via API or direct network connection, review firewall and proxy logs for unexpected traffic originating from BridgePay IP ranges. SIEM query logic should target high-volume file modification events within short time windows (e.g., >500 file writes in 60 seconds from a single process). Subscribe to BridgePay's official security communications and monitor FS-ISAC for threat intelligence updates specific to this incident.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not confirmed`	No IOCs attributed to this campaign in available open sources at time of publication. This field will be updated when authoritative indicators are released.	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Paymentsjournal	https://www.paymentsjournal.com/the-latest-wave-of-ransomware-attac...	T3
The Latest Wave of Ransomware Attacks: As Widespread as Possible	https://www.linkedin.com/posts/cyber-news-live_the-latest-wave-of-r...	T3
Dec 2025: Biggest Cyber Attacks, Ransomware Attacks and Data ...	https://www.cm-alliance.com/cybersecurity-blog/dec-2025-biggest-cyb...	T3
Data Breaches 2025: Biggest Cybersecurity Incidents So Far	https://www.pkware.com/blog/recent-data-breaches	T3
The State of Ransomware 2025 - BlackFog	https://www.blackfog.com/the-state-of-ransomware-2025/	T3

Generated 2026-03-29 18:44 UTC by TJS Security Command Center