INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-18 06:51 UTC

Multiple Data Breaches Reported by Breachsense: GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, First Cambodia

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0093
Type	Data Breach
Severity	HIGH
Affected Products	GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, First Cambodia
Published	2026-04-17
Discovery Source	Gemini

Executive Summary

On April 17, 2026, Breachsense reported data breaches affecting five organizations across fintech, financial services, physical security monitoring, municipal government, and banking: GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, and First Cambodia. Threat actors RansomEXX, DragonForce, and ShinyHunters are associated with this cluster of activity, though per-organization attribution remains unconfirmed. The cross-sector, cross-geography pattern indicates opportunistic or coordinated campaigns targeting organizations with varying security postures, with potential exposure of customer data, financial records, and operational information.

Technical Analysis

Five organizations were listed by Breachsense as breach victims on April 17, 2026. No CVE identifiers or CWE classifications are associated with this cluster. MITRE ATT&CK techniques mapped to this activity include: T1133 (External Remote Services), T1078 (Valid Accounts), T1486 (Data Encrypted for Impact), T1530 (Data from Cloud Storage), and T1657 (Financial Theft). RansomEXX is a sophisticated ransomware group known for enterprise and government targeting via legitimate remote access abuse and valid credential exploitation. DragonForce operates with both ransomware and hacktivist motivations, active since late 2023. ShinyHunters specializes in large-scale database and credential exfiltration, often via cloud storage misconfigurations or compromised development infrastructure. Attribution of specific actors to specific victims is unconfirmed at this time. Initial access vectors, exfiltrated record counts, ransom demands, and patch or remediation status are not confirmed in available source data. Source quality for this item is Tier 3 (Breachsense listing, RansomLook); no primary vendor advisories or law enforcement disclosures are available as of this writing. Confidence in actor

attribution is medium.

Action Checklist

1. Step 1: Containment. If your organization has a business relationship with GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, or First Cambodia, identify all shared credentials, API integrations, and data-sharing agreements with those entities and treat them as potentially compromised. Revoke or rotate any shared secrets immediately.
2. Step 2: Detection. Review authentication logs for anomalous access patterns tied to accounts used with affected organizations. Search for T1078 indicators: logins from unusual geolocations, off-hours access, or service accounts authenticating interactively. For T1530, audit cloud storage access logs for unexpected external reads or bulk downloads from buckets associated with these vendor relationships.
3. Step 3: Eradication. Force credential resets for any accounts shared with or exposed to affected organizations. Disable or quarantine API keys and OAuth tokens linked to these entities. If your organization uses Alert 360 for physical security monitoring, assess whether monitoring feeds or administrative consoles were accessible to the breach.
4. Step 4: Recovery. Validate that no lateral movement occurred from compromised third-party connections into your environment. Re-verify integrity of any data exchanged with affected organizations. Restore monitoring baselines and confirm that alerting on T1133 (external remote service abuse) and T1486 (ransomware precursors like shadow copy deletion) is active.
5. Step 5: Post-Incident. This cluster exposes third-party and supply chain risk gaps. Review your vendor risk management program against NIST SP 800-161 guidance. Confirm that third-party access is governed by least-privilege principles and that shared credential inventories exist and are auditable.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if any evidence confirms that PII, PHI, or financial account data transited between your organization and GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, or First Cambodia — the cross-sector nature of this cluster (banking, fintech, physical security) and association with RansomEXX, DragonForce, and ShinyHunters creates potential GDPR Article 33, FFIEC, and state breach notification triggers within 72-hour windows.
Recovery Notes	After revoking all vendor-linked credentials and API tokens, maintain enhanced logging on all external remote access points (VPN, RDP gateways, API endpoints) for a minimum of 30 days post-containment, with specific alerting on T1133 and T1078 indicators given the RansomEXX and DragonForce association — both groups are known to maintain persistent access for weeks before deploying ransomware or exfiltrating bulk data. Re-verify data integrity checksums for any datasets exchanged with First Cambodia (banking) and Empower Group (financial services) during the 90-day window preceding April 17, 2026, as DragonForce has been observed staging exfiltration over extended dwell periods. Confirm shadow copy and backup integrity weekly for 60 days, as RansomEXX specifically targets backup infrastructure.

Forensic Artifacts	IdP sign-in logs (Okta System Log, Azure AD Sign-In Logs, or equivalent) filtered to service accounts and OAuth applications linked to GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, and First Cambodia — specifically capturing ASN, IP geolocation, device fingerprint, and MFA bypass events for the 90 days preceding April 17, 2026, which would reveal ShinyHunters credential-stuffing attempts using data from the breached organization datasets | AWS CloudTrail GetObject/ListBucket or Azure Monitor Blob storage read events on buckets and containers associated with affected vendor data exchanges — DragonForce and ShinyHunters both execute bulk cloud storage exfiltration (T1530) as a precursor to ransom or public leak, leaving high-volume GetObject sequences from novel IP addresses in cloud audit logs | Windows Security Event Log Event ID 4688 (Process Creation) and Sysmon Event ID 1 on hosts with Alert 360 physical security monitoring integrations, filtered for 'vssadmin', 'wmic shadowcopy', 'bcdedit', 'net use', and 'nltest' — these are documented RansomEXX pre-encryption commands that would appear on hosts where lateral movement succeeded from a compromised Alert 360 monitoring feed | API gateway access logs (Kong, AWS API Gateway, Azure APIM, or nginx access logs) for all endpoints authenticated by keys issued to GoTip (fintech) and First Cambodia (banking) integrations, specifically URI patterns showing bulk data retrieval, schema enumeration, or authentication token refresh loops indicative of automated credential exploitation following the breach | Firewall and proxy egress logs for outbound connections to Breachsense-reported infrastructure and known DragonForce/RansomEXX C2 IP ranges (cross-reference current CISA Known Exploited Vulnerabilities and threat actor infrastructure reports), particularly large outbound data transfers over HTTPS to non-CDN IPs from hosts in your environment that held third-party vendor session tokens

Per-Action IR Details

Step 1: Containment — If your organization has a business relationship with GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, or First Cambodia, identify all shared credentials, API integrations, and data-sharing agreements with those entities and treat them as potentially compromised. Revoke or rotate any shared secrets immediately.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (RS.MA-01: Execute IR plan in coordination with third parties; isolate affected connections before full scope is known)

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SC-12 (Cryptographic Key Establishment and Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Run 'Get-ADUser -Filter {Description -like "*GoTip*" -or Description -like "*Alert360*"} | Select Name,SamAccountName,Enabled' to locate accounts tagged to affected vendors. For API keys, grep your secrets vault exports or .env files: 'grep -rE "(gotip|alert360|empower|firstcambodia)" /etc/app/ ~/.env' and pipe results to a revocation queue. Use 'net user /active:no' to disable AD accounts immediately while rotation is pending.

Evidence: Before revoking, export current Active Directory account attributes and last-logon timestamps for all service accounts associated with GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, and First Cambodia using 'Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,ServicePrincipalNames | Export-Csv'. Capture OAuth token issuance logs from your IdP (Okta: System Log API; Azure AD: Sign-in logs filtered by application name) for the 30 days preceding April 17, 2026. Snapshot API gateway access logs showing all requests authenticated with keys linked to affected vendors before rotation destroys the audit trail.

Step 2: Detection — Review authentication logs for anomalous access patterns tied to accounts used with affected organizations. Search for T1078 indicators: logins from unusual geolocations, off-hours access, or service accounts authenticating interactively. For T1530, audit cloud storage access logs for unexpected external reads or bulk downloads from buckets associated with these vendor relationships.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (DE.AE-02: Analyze potentially adverse events; DE.AE-03: Correlate information from multiple sources including IdP, cloud storage, and network logs)

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)

Compensating: For T1078 (Valid Accounts) detection without SIEM: on Windows, query Security Event Log for Event ID 4624 (successful logon) with LogonType 10 (RemoteInteractive) or 3 (Network) filtered to service accounts linked to affected vendors — 'Get-WinEvent -FilterHashtable @{LogName="Security";Id=4624} | Where-Object {$_.Message -match ""}'. For T1530 (Cloud Storage Object Collection) on AWS: 'aws s3api get-bucket-logging' to verify logging is enabled, then pull CloudTrail events with 'aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=GetObject' filtered to buckets shared with affected orgs. Deploy the Sigma rule 'win_susp_interactive_logon_service_account.yml' against exported Windows Security logs using Hayabusa or Chainsaw locally.

Evidence: Collect IdP sign-in logs for all accounts authenticated against GoTip, Empower Group, and Alert 360 integrations for 60 days prior to April 17, 2026, specifically flagging logins from ASNs not previously seen for those accounts (ShinyHunters and DragonForce have been observed using residential proxy infrastructure). Pull AWS CloudTrail or Azure Monitor logs for S3/Blob storage GetObject and ListBucket events on buckets containing data exchanged with affected vendors. Export Windows Security Event ID 4648 (Explicit Credential Use) and 4672 (Special Privileges Assigned) for service accounts to detect credential stuffing attempts using credentials exposed in the GoTip or First Cambodia breach datasets.

Step 3: Eradication — Force credential resets for any accounts shared with or exposed to affected organizations. Disable or quarantine API keys and OAuth tokens linked to these entities. If your organization uses Alert 360 for physical security monitoring, assess whether monitoring feeds or administrative consoles were accessible to the breach.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (RS.MA-01: Remove threat actor footholds; verify all access paths associated with compromised third parties are closed before recovery begins)

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST CM-2 (Baseline Configuration), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For Alert 360 physical security console exposure: document all IP addresses and user accounts with access to Alert 360 administrative interfaces by reviewing access control lists in the Alert 360 portal and correlating with your firewall outbound rules ('netstat -an | grep '). Enumerate all OAuth applications authorized by accounts linked to affected vendors using Microsoft Graph: 'Get-MgUserOauth2PermissionGrant -UserId ' or equivalent Okta API call. Use 'dsacls' or 'icacls' to verify no file share permissions were granted to Alert 360-associated service accounts that persist post-reset.

Evidence: Before disabling Alert 360 console access, screenshot or export the full audit log from the Alert 360 administrative portal showing all logins, configuration changes, and video/sensor access events for the 90 days prior to April 17, 2026 — RansomEXX has been observed leveraging physical security system access for reconnaissance in pre-ransomware stages. Capture OAuth token issuance and refresh events for all Alert 360-integrated accounts. For Empower Group and First Cambodia (financial services entities), collect any FTP/SFTP transfer logs or EDI transaction logs that reflect data exchanged with those organizations, as DragonForce targets financial data for exfiltration prior to encryption.

Step 4: Recovery — Validate that no lateral movement occurred from compromised third-party connections into your environment. Re-verify integrity of any data exchanged with affected organizations. Restore monitoring baselines and confirm that alerting on T1133 (external remote service abuse) and T1486 (ransomware precursors like shadow copy deletion) is active.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (RC: Execute recovery plan, verify environment integrity, restore monitoring baselines before returning systems to production)

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For T1133 (External Remote Services) detection: audit firewall rules and VPN gateway logs for any persistent remote access sessions originating from Alert 360 monitoring IP ranges or Empower Group/GoTip API server addresses — run 'grep -E "" /var/log/firewall.log | awk '{print $1,$2,$5,$6}' | sort | uniq -c | sort -rn'. For T1486 ransomware precursor detection (associated with RansomEXX): deploy Sysmon Event ID 1 (Process Create) filtering on 'vssadmin delete shadows', 'wmic shadowcopy delete', and 'bcdedit /set recoveryenabled no' — these are RansomEXX pre-encryption TTPs. Verify shadow copies are intact: 'vssadmin list shadows' on all servers that had connectivity to affected vendor systems.

Evidence: Collect Windows Security Event ID 4769 (Kerberos Service Ticket Request) and 4625 (Failed Logon) for lateral movement indicators from any host that shared connectivity with Alert 360 feeds or API endpoints. For RansomEXX lateral movement validation, review Sysmon Event ID 3 (Network Connection) logs for unexpected SMB (port 445) or RDP (port 3389) connections initiated from hosts with third-party vendor integrations. Capture 'net share', 'net use', and scheduled task exports ('schtasks /query /fo LIST /v') from affected hosts to identify persistence mechanisms that may have been planted during the breach window before your organization completed containment.

Step 5: Post-Incident — This cluster exposes third-party and supply chain risk gaps. Review your vendor risk management program against NIST SP 800-161 guidance. Confirm that third-party access is governed by least-privilege principles and that shared credential inventories exist and are auditable.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (GV, ID: Lessons learned, update policies, improve detection for third-party risk vectors identified in this incident cluster)

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SA-9 (External System Services), NIST RA-3 (Risk Assessment), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Build an auditable shared-credential inventory using a free password manager with team vaulting (Bitwarden Teams free tier) or a structured CSV under version control in a private Git repo, tagged by vendor name with last-rotation date. For least-privilege validation of third-party accounts, run 'Get-ADGroupMember -Identity "Domain Admins" -Recursive | Where-Object {$_.Description -match "vendor|api|svc"}' to identify over-privileged service accounts. Schedule a quarterly review task using a cron job or Windows Task Scheduler that emails a CSV export of all vendor-associated accounts with their privilege levels and last-active dates to the security team.

Evidence: Compile a full timeline of all third-party access events across GoTip, Empower Group, Alert 360, Abfall-kreis-kassel.de, and First Cambodia integrations from IdP logs, firewall logs, and API gateway logs into a single incident timeline document — this serves as both the lessons-learned input and evidence for any regulatory breach notification obligations triggered by PII exposure through these relationships. Retain all collected logs per NIST AU-11 (Audit Record Retention) requirements for a minimum of three years given the financial services and municipal government entities involved (Empower Group, First Cambodia, Abfall-kreis-kassel.de may trigger GDPR, FFIEC, or local data protection notification obligations).

Detection Guidance

No confirmed IOCs are available for this breach cluster. Detection should focus on behavioral indicators aligned to mapped ATT&CK techniques. For T1078 (Valid Accounts): alert on authentication events from accounts associated with the five affected organizations, particularly service accounts or shared credentials. For T1133 (External Remote Services): review VPN, RDP, and remote access gateway logs for connections originating from the affected organizations' IP ranges or user accounts. For T1486 (Data Encrypted for Impact): monitor for VSS deletion commands (vssadmin delete shadows), rapid file renaming with unfamiliar extensions, and

high-volume file write activity on shared drives. For T1530 (Cloud Storage Access): audit S3, Azure Blob, and GCS access logs for bulk GET or LIST operations from external principals. For T1657 (Financial Theft): review transaction approval workflows and wire transfer logs for anomalous approvals, particularly if Empower Group or First Cambodia are counterparties. RansomLook (ransomlook.io) and Breachsense (breachsense.com/breaches/) should be monitored for updated victim postings and any published data samples that may contain your organization's data.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1530** — Data from Cloud Storage
- **T1657** — Financial Theft

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **SI-4** — System Monitoring

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1530	Data from Cloud Storage	Collection
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
The Most Recent Data Breaches in 2026 - Breachsense	https://www.breachsense.com/breaches/	T3
Recent posts - RansomLook	https://www.ransomlook.io/recent	T3
Data Breach Examples: 30 Biggest Security Incidents Ever	https://www.breachsense.com/blog/data-breach-examples/	T3
Breachsense: Data Breach & Dark Web Monitoring	https://www.breachsense.com/	T3
Data breaches in December 2025	https://www.breachsense.com/breaches/2025/december/	T3

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-18 06:51 UTC by TJS Security Command Center