INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:40 UTC

Global Enforcement Surge Sinkholed 45,000 IPs and Seized LeakBase: What Comes Next for Defenders

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0022
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	No specific vendor products; impersonated entities include financial institutions, casinos, payment processors, and government portals; affected communities include users of LeakBase (est. 142,000 members) and BreachForums successor ecosystem
Published	2026-03-14

Executive Summary

Interpol-coordinated operations (Operation Synergia II and Operation Serengeti) sinkholed approximately 45,000 malicious IP addresses, arrested over 745 suspects globally, and seized LeakBase, a criminal marketplace with an estimated 142,000 members that traded in stolen credentials, PII, and synthetic identity packages. Organizations in financial services, payment processing, and government sectors face elevated risk in the post-enforcement window, as displaced threat actors historically reconstitute within weeks via Telegram, new forums, or dark-web platforms. Immediate business risk includes a surge in credential stuffing, phishing campaigns, and bulk data dump releases as actors liquidate inventory before anticipated follow-on law enforcement action.

Technical Analysis

LeakBase operated as a successor to BreachForums, serving as a primary market for stolen credentials, PII, and synthetic identity packages. The platform and associated infrastructure supported tradecraft mapped to CWE-287 (Improper Authentication), CWE-308 (Use of Single-Factor Authentication), and CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). No CVE is assigned; this is a threat ecosystem disruption, not a software vulnerability event. MITRE ATT&CK coverage is broad: reconnaissance via T1591 (Gather Victim Org Information) and T1589 (Gather Victim Identity Information); resource development via T1583 (Acquire Infrastructure), T1584 (Compromise Infrastructure), T1586 (Compromise Accounts), T1588 (Obtain Capabilities), and T1608 (Stage Capabilities); initial access via T1078 (Valid Accounts) and T1566

(Phishing); credential access via T1539 (Steal Web Session Cookie) and T1111 (MFA Interception); collection via T1530 (Data from Cloud Storage); and financial crime via T1657 (Financial Theft). No IOCs have been publicly released by enforcement agencies as of publication. Historical precedent from BreachForums, Genesis Market, and RaidForums takedowns indicates actor migration to alternate infrastructure typically occurs within two to four weeks of enforcement action. Defenders should treat any identity data exposed on LeakBase as compromised and assume active exploitation attempts are in progress or imminent.

Action Checklist

1. Step 1, Immediate: Activate enhanced monitoring on authentication systems for credential stuffing patterns; apply rate limiting and account lockout thresholds if not already enforced; review MFA coverage across all externally accessible applications to address CWE-308 exposure.
2. Step 2, Detection: Query authentication logs for high-volume failed login attempts, logins from unfamiliar ASNs or geographies, and successful logins followed by unusual session behavior; cross-reference employee and customer email domains against known breach data sources (e.g., Have I Been Pwned API, commercial threat intel feeds) for LeakBase-associated exposure.
3. Step 3, Assessment: Inventory all services that accept username/password authentication without MFA; identify accounts belonging to users whose credentials may have circulated on LeakBase or predecessor forums; flag synthetic identity risk in onboarding and account recovery workflows, particularly in financial and payment-processing contexts.
4. Step 4, Communication: Brief the CISO and relevant business unit leads on the elevated post-enforcement risk window; notify fraud, identity, and customer support teams to expect increased account takeover attempts; if customer PII may be involved, engage legal and privacy counsel to assess notification obligations (this is a legal determination requiring qualified counsel).
5. Step 5, Long-term: Conduct a phishing simulation and awareness refresh targeting the credential-theft and social engineering TTPs associated with this ecosystem (T1566, T1598); review and strengthen identity verification controls to reduce synthetic identity fraud exposure; establish a recurring process to monitor dark-web and Telegram channels for re-emergence of displaced LeakBase actors and new forums; update incident response playbooks to include post-enforcement surge scenarios.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or law enforcement if forensic analysis of authentication logs reveals confirmed unauthorized account access (successful login from anomalous geography followed by account changes or data exfiltration), or if customer PII exposure is confirmed and privacy counsel advises notification — both warrant professional incident response and potential law enforcement briefing.
Recovery Notes	Post-containment recovery: (1) Force password reset for all users with exposure confirmed on LeakBase or with anomalous login history; enforce MFA re-enrollment across organization; (2) Monitor authentication logs for 90 days post-reset for renewed attack patterns to detect re-compromises or credential-reuse by displaced threat actors; (3) Conduct post-incident review within 30 days to document detection gaps, validate control effectiveness (rate-limiting, MFA, monitoring), update risk register, and archive forensic evidence per legal hold policy.

Forensic Artifacts	Windows Security Event Log (Event IDs 4624, 4625, 4648, 4720, 4722, 4723, 5379) or Linux /var/log/auth.log and /var/log/secure — captures all authentication attempts, account changes, and MFA events | Web application authentication logs (IIS/Apache access and error logs, custom application authentication traces) — captures HTTP-based login attempts and session anomalies | Mailbox forwarding and delegation rules (Exchange: Get-MailboxForwarding; Unix mail: .forward files) — detects account takeover persistence mechanisms | Browser history and download artifacts (Chrome/Edge: %APPDATA%\Local\Google\Chrome\User Data\Default\History; Firefox: places.sqlite; Safari: ~/Library/Safari/) — reveals access to breach databases or credential marketplaces by administrative users | DNS query logs and proxy logs for domains like haveibeenpwned.com, Telegram, BreachForums successor sites — indicates organization's breach database reconnaissance and threat actor communication

Per-Action IR Details

Step 1, Immediate: Activate enhanced monitoring on authentication systems for credential stuffing patterns; apply rate limiting and account lockout thresholds if not already enforced; review MFA coverage across all externally accessible applications to address CWE-308 exposure.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase: tools, training, and preventive controls)

Controls: NIST AC-2 (Account Management), NIST AC-7 (Unsuccessful Login Attempts), NIST IA-2 (Authentication), CIS 5.4 (Account Lockout), CIS 6.1 (MFA)

Compensating: Without enterprise WAF: (1) Configure OS-level rate limiting using iptables (Linux) or netsh (Windows) to drop connections exceeding 10 failed auth attempts per minute per source IP; (2) Set account lockout via local Group Policy (Windows: GPOE > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies) to lock after 5 failures for 30 minutes; (3) Monitor auth logs with grep/awk for patterns: grep 'Failed password\|Invalid user' /var/log/auth.log | awk -F'[=]' '{print $(NF-3)}' | sort | uniq -c | sort -rn | head -20; (4) Implement TOTP-based MFA on SSH using libpam-google-authenticator or equivalent for critical accounts; (5) Use open-source tools like Fail2ban to auto-block IPs after threshold.

Evidence: Baseline authentication log volume and source IP geographies before enforcement; export current MFA enrollment status per account; capture current rate-limiting and lockout policy configuration (via auditpol, Get-AuditPolicy, or /etc/security/limits.conf); take screenshots of AD/LDAP account properties showing current MFA status; document existing WAF/load-balancer rules if present.

Step 2, Detection: Query authentication logs for high-volume failed login attempts, logins from unfamiliar ASNs or geographies, and successful logins followed by unusual session behavior; cross-reference employee and customer email domains against known breach data sources (e.g., Have I Been Pwned API, commercial threat intel feeds) for LeakBase-associated exposure.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (detection and analysis: determine whether an incident has occurred)

Controls: NIST SI-4 (Information System Monitoring), NIST AU-6 (Audit Review, Analysis, and Reporting), NIST CA-7 (Continuous Monitoring), CIS 8.1 (Audit Log Storage), CIS 8.2 (Audit Log Transmission)

Compensating: (1) Export auth logs to CSV: Windows Event Viewer > filter Event ID 4625 (failed login) and 4624 (successful login), export to CSV; Linux: journalctl -u sshd -o short-iso > auth_export.csv or grep from /var/log/auth.log; (2) Cross-reference source IPs against MaxMind GeoIP2 free tier (import IPs and check geography mismatches); (3) Query Have I Been Pwned API programmatically: for each user email, call https://haveibeenpwned.com/api/v3/breachedaccount/{email} and parse response for 'LeakBase' or similar; (4) Hunt for session anomalies manually: grep 'Accepted password\|Accepted publickey' /var/log/auth.log and correlate timestamp-to-timestamp to identify rapid re-logins or unusual source patterns; (5) Use free OSINT: query Telegram @leakbase_official archives or BreachForums successor databases directly (via OSINT frameworks like Maltego Community or manual search) to identify your domain's presence.

Evidence: Full authentication logs (Windows Event Viewer Security log Event IDs 4624, 4625, 4648, 4720; /var/log/auth.log with full timestamps and source IPs) spanning at least 90 days pre-enforcement and 30 days post-enforcement; export of all user mailbox forwarding rules (Exchange: Get-Mailbox | Get-MailboxForwarding; Linux: postfix virtual file); browser history and download artifacts from any administrative accounts showing breach database access; DNS query logs for have-i-been-pwned.com or threat intel feed domains; list of all externally accessible authentication endpoints (VPN, RDP, OWA, etc.) and their log sources.

Step 3, Assessment: Inventory all services that accept username/password authentication without MFA; identify accounts belonging to users whose credentials may have circulated on LeakBase or predecessor forums; flag synthetic identity risk in onboarding and account recovery workflows, particularly in financial and payment-processing contexts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.5 (incident categorization and initial response) and NIST 800-53 §IA-4 (Identifier Management)

Controls: NIST IA-4 (Identifier Management), NIST IA-5 (Authentication), NIST AC-2 (Account Management), CIS 5.1 (Inventory and Control of Enterprise Software), CIS 6.2 (Address Unauthorized Software)

Compensating: (1) Inventory non-MFA services: conduct port scans (nmap -p 22,3389,443,8080,5985 -sV) to identify accessible services; query firewall rules (iptables -L -n or Windows Firewall Get-NetFirewallRule) to list externally exposed ports; (2) For each service, check MFA capability: SSH (grep 'ChallengeResponseAuthentication' /etc/ssh/sshd_config; test with 'ssh -v user@host' and observe auth methods offered); RDP (query Registry HKLM\\System\\CurrentControlSet\\Control\\SecurityProviders\\SCHANNEL); web applications (test login with tool like Burp Suite Community to check for TOTP/U2F in response); (3) Identify exposed users: export all user directories (Active Directory: Get-ADUser -Filter * -Properties * | Select-Object samAccountName, mailNickname; LDAP: ldapsearch -x cn=* mail > users.txt); (4) Cross-reference exposed users against HIBP and BreachForums: write Python loop calling HIBP API or manually search dark-web archives for your email domain; (5) Flag synthetic identity risk by auditing account creation records: export user creation timestamps and source (AD: Get-ADUser -Filter * -Properties whenCreated, Created; review onboarding tickets for verification evidence); identify accounts created without photo ID verification or with mismatched account recovery email.

Evidence: Complete export of all active user accounts with creation date, last logon, MFA status, and privilege level (AD: Get-ADUser -Filter {Enabled -eq $true} -Properties *; LDAP: ldapsearch -x); list of all applications and services accepting password authentication, mapped to account systems (AD, LDAP, custom databases); onboarding records for accounts created in past 12 months (from HR system, ticketing system, or account provisioning logs); account recovery audit log showing password resets and email/phone verification attempts; financial transaction logs correlated to suspicious accounts (if available); export of all federated identity sources and their MFA requirements (if using Okta, Ping, etc.).

Step 4, Communication: Brief the CISO and relevant business unit leads on the elevated post-enforcement risk window; notify fraud, identity, and customer support teams to expect increased account takeover attempts; if customer PII may be involved, engage legal and privacy counsel to assess notification obligations (this is a legal determination requiring qualified counsel).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.3.2 (notification to external entities); NIST 800-53 §IR-4 (Incident Handling) and §CA-7 (Continuous Monitoring)

Controls: NIST IR-1 (Incident Response Policy), NIST IR-4 (Incident Handling), NIST CA-7 (Continuous Monitoring), CIS 18.1 (Incident Response Program)

Compensating: (1) Create a one-page threat brief: include Operation Synergia II/Serengeti summary, LeakBase member count (142,000), your organization's exposure category (if known), elevated attack window duration (typically 30–90 days post-enforcement), and three recommended mitigations; distribute to C-suite via secure email; (2) Activate incident response team: send Slack/Teams alert to Security, Fraud, Identity, and Support teams with template: 'Elevated credential-stuffing risk expected for next 60 days. Report unusual login patterns (GEO-anomalies, rapid failures, failed 2FA) to Security@domain immediately. See [brief link].'; (3) Brief customer support: create knowledge

base article on account takeover signs (multiple failed logins, password reset emails they didn't initiate, unauthorized transactions) and escalation path; (4) For legal/privacy: prepare incident summary with data elements at risk (email, phone, SSN if present), affected user count (estimated), and query legal: 'Does our applicable state/federal privacy law (CCPA, GDPR, state breach notification law) require notification for credential exposure without confirmed breach of *our* systems?' Document their written response and retain legal privilege; do not proceed with customer notification without written legal sign-off.

Evidence: Incident response plan template and escalation matrix (document who briefs whom and timeline); roster of fraud, security, and customer support leads with contact information; list of applicable privacy laws by jurisdiction of affected users (CCPA for CA, GDPR for EU, etc.); sample breach notification template from legal/compliance department (to ensure consistency); evidence of legal consultation (email chain or meeting notes confirming notification guidance); customer communication drafts (to be sent only after legal approval).

Step 5, Long-term: Conduct a phishing simulation and awareness refresh targeting the credential-theft and social engineering TTPs associated with this ecosystem (T1566, T1598); review and strengthen identity verification controls to reduce synthetic identity fraud exposure; establish a recurring process to monitor dark-web and Telegram channels for re-emergence of displaced LeakBase actors and new forums; update incident response playbooks to include post-enforcement surge scenarios.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 (Post-Incident Activities) and §3.4 (Eradication and Recovery); NIST 800-53 §AT-3 (Role-Based Security Training) and §CA-7 (Continuous Monitoring)

Controls: NIST AT-2 (Security Awareness and Training), NIST AT-3 (Role-Based Security Training), NIST CA-7 (Continuous Monitoring), NIST IR-3 (Incident Response Training), CIS 14.7 (User Security Awareness Program)

Compensating: (1) Phishing simulation: use free tools (Gophish, Phish.Report community, or simple manual campaigns) to send 10 test emails impersonating LeakBase/BreachForums actors offering 'stolen credential packages' or requesting password resets; track click-through and credential entry rates; brief users failing >20% of tests; repeat monthly; (2) Awareness refresh: create 15-minute video or email series explaining T1566 (phishing with malware, credential harvesting) and T1598 (phishing for information) with LeakBase case examples; require completion by all staff; (3) Identity verification hardening: for financial services, implement out-of-band verification on account recovery (SMS or hardcoded security questions, not email-based reset); for payment processors, require MFA for all account changes (password, email, phone); audit current processes against NIST IA-5r5 guidance; (4) Dark-web monitoring: subscribe to free Telegram feed aggregators (e.g., IntelligenceX, Shodan) or set Google Alerts for 'LeakBase,' 'BreachForums,' and actor handles (e.g., 'pompompurin,' 'xenutax'); assign one person to check weekly; document findings in threat intel database; (5) Playbook update: add new IR playbook section: 'Post-Enforcement Credential-Stuffing Surge — Detection Triggers' (5+ failed logins in 10 min, ASN change, MFA failure spikes), 'Immediate Actions' (rate-limit, MFA enforcement, customer comms), and 'Recovery' (password reset campaign, fraud review); schedule IR drill testing playbook quarterly.

Evidence: Baseline phishing click-through and credential-entry rates before simulation; record of all staff completing awareness training (LMS export or email delivery receipts); current identity verification procedure documentation (compare to NIST IA-5 baseline); copy of updated IR playbook with new post-enforcement section and version control metadata; evidence of dark-web monitoring setup (Telegram subscription, Google Alert confirmation, or paid feed contract); incident debrief notes documenting lessons learned from this operation.

Detection Guidance

No enforcement-released IOCs are publicly available as of publication. Detection relies on behavioral and volumetric signals. In authentication logs: alert on more than 10 failed login attempts per account within 5 minutes; alert on successful logins preceded by 5 or more failures; alert on logins from IP addresses registered to hosting or VPN ASNs that do not match the account's baseline geography. In web application logs: look for high-volume POST requests to login endpoints with low success rates, characteristic of credential stuffing tools. For email security: monitor for phishing lure themes impersonating financial institutions, payment processors,

and government portals consistent with T1566 and T1598; inspect for lookalike domains registered against your brand. For cloud storage (T1530): alert on bulk download activity or permission changes on data repositories outside normal operational hours. Subscribe to Interpol and CISA advisories for IOC releases as enforcement agencies publish findings. Commercial threat intelligence platforms with dark-web monitoring coverage may surface LeakBase data samples or migration indicators before public disclosure.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`leakbase[.]io`	Primary LeakBase forum domain; seized by law enforcement. Block at DNS and proxy as a precaution; any traffic to this domain post-seizure may indicate compromise or user activity.	HIGH
DOMAIN	`leakbase[.]cx`	Alternate LeakBase domain reported in open sources; treat as associated infrastructure. Verify current resolution status before drawing conclusions from DNS hits.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1591** — Gather Victim Org Information
- **T1598** — Phishing for Information
- **T1078** — Valid Accounts
- **T1588** — Obtain Capabilities
- **T1589** — Gather Victim Identity Information
- **T1608** — Stage Capabilities
- **T1539** — Steal Web Session Cookie
- **T1566** — Phishing
- **T1584** — Compromise Infrastructure
- **T1586** — Compromise Accounts
- **T1583** — Acquire Infrastructure
- **T1657** — Financial Theft
- **T1530** — Data from Cloud Storage
- **T1111** — Multi-Factor Authentication Interception

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)

- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **CP-9** — System Backup
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3**
- **6.4**
- **6.5**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1591	Gather Victim Org Information	Reconnaissance

Technique ID	Technique Name	Tactic
T1598	Phishing for Information	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1588	Obtain Capabilities	Resource-Development
T1589	Gather Victim Identity Information	Reconnaissance
T1608	Stage Capabilities	Resource-Development
T1539	Steal Web Session Cookie	Credential-Access
T1566	Phishing	Initial-Access
T1584	Compromise Infrastructure	Resource-Development
T1586	Compromise Accounts	Resource-Development
T1583	Acquire Infrastructure	Resource-Development
T1657	Financial Theft	Impact
T1530	Data from Cloud Storage	Collection
T1111	Multi-Factor Authentication Interception	Credential-Access

Sources

Source	URL	Tier
Security News	https://staging.techjacksolutions.com/news/security-news/police-sin...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/police-sinkholes-45-...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/police-arrests-651-s...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/police-arrests-20-su...	T3
Synthetic Identities - Institute for Financial Integrity	https://finintegrity.org/synthetic-identities/	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 2026-03-29 18:40 UTC by TJS Security Command Center