INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

LeakBase Admin Arrested in Russia After U.S.-Led Takedown of 142,000-Member Credential Marketplace

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0102
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	N/A, LeakBase cybercrime platform (no specific vendor products affected); victims span global organizations and individuals whose credentials were traded on the platform
Published	2026-03-25
Discovery Source	Rss

Executive Summary

U.S. authorities (DOJ), Europol, and Russian law enforcement dismantled LeakBase, a stolen credential marketplace that served over 142,000 members and hosted hundreds of millions of compromised credentials, financial records, and corporate documents since 2021. The platform's alleged administrator, a Russian national operating under aliases including Chucky and beakdaz, was arrested in Taganrog, Russia. Organizations whose employee or customer credentials were traded on LeakBase remain exposed to account takeover attacks and fraud until those credentials are identified and rotated.

Technical Analysis

LeakBase operated as a large-scale credential trading marketplace from 2021 until its dismantlement in early 2026. The platform aggregated credentials from third-party breaches and infostealer campaigns, supplying downstream threat actors conducting account takeover (ATO) operations and fraud. No specific CVE applies; the platform's supply chain exploited weak credential hygiene in victim environments mapped to CWE-255 (Credentials Management Errors), CWE-522 (Insufficiently Protected Credentials), and CWE-308 (Use of Single-factor Authentication). Relevant MITRE ATT&CK techniques include T1110.004 (Credential Stuffing), T1078 and T1078.004 (Valid Accounts: Cloud Accounts), T1539 (Steal Web Session Cookie), T1586.001 and T1586.002 (Compromise Accounts: Social Media/Email Accounts), T1589.001 (Gather Victim Identity Information: Credentials), T1650 (Acquire Access), T1567 (Exfiltration Over Web Service), and T1657 (Financial Theft). The administrator used aliases Chucky, beakdaz, Chuckies, and Sqlrip. No patch exists; remediation is

defensive, credential rotation, MFA enforcement, and credential exposure monitoring. Sources: DOJ press release (T1), Europol press release (T1).

Action Checklist

1. Step 1, Immediate: Submit your organization's domains and email address ranges to Have I Been Pwned (haveibeenpwned.com) and your identity threat monitoring vendor to identify credentials exposed via LeakBase or its source breaches.
2. Step 2, Immediate: Force password resets for any accounts identified as exposed; prioritize privileged accounts, service accounts, and accounts with access to financial or customer data.
3. Step 3, Detection: Review authentication logs for credential stuffing indicators, high-volume failed logins, logins from anomalous geographies or ASNs, and successful logins preceded by repeated failures, correlated with T1110.004.
4. Step 4, Detection: Hunt for T1078 and T1078.004 abuse: successful authentications outside normal working hours, impossible travel events, and first-time access to sensitive resources from accounts that have not recently been used.
5. Step 5, Assessment: Audit MFA coverage across all externally accessible services; accounts lacking MFA are the primary downstream risk vector from credential marketplace operations. Map gaps against CWE-308.
6. Step 6, Assessment: Inventory third-party SaaS applications where employees use corporate email addresses as usernames; these are high-value ATO targets if credentials were traded on LeakBase.
7. Step 7, Communication: Notify affected users whose credentials were confirmed exposed; provide clear password reset instructions and guidance on recognizing phishing follow-on attempts.
8. Step 8, Long-term: Implement or validate continuous credential monitoring against dark web and breach corpus feeds to reduce mean time to detection for future exposures.
9. Step 9, Long-term: Enforce passwordless or phishing-resistant MFA (FIDO2/passkeys) for all privileged and externally accessible accounts to reduce ATO impact from credential exposure events.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership and legal/compliance if your organization's employee or customer credentials confirmed on LeakBase; escalate to external IR firm if active ATO or unauthorized access detected during Steps 3–4 or if remediation capacity is insufficient for organization size.
Recovery Notes	After containment of active abuse (Steps 2–4), focus on hardening credential security posture (Steps 5–6) and validating MFA coverage before resuming normal operations. Conduct post-incident review against NIST 800-61r3 §3.4 to document lessons learned, document any organizational changes triggered by this event, and schedule 30-, 90-, and 180-day check-ins to validate sustained improvement in detection tuning and MFA enforcement.

Forensic Artifacts	Windows Event Log 4624 (Successful Logon) and 4625 (Failed Logon) with source IP, account SID, logon type, and timestamp | Windows Event Log 4720 (Account Created), 4722 (Account Enabled), 4723 (Password Changed), 4724 (Password Reset) for baseline and anomaly correlation | /var/log/auth.log and /var/log/secure (Linux SSH login records with source IP and timestamp) | Proxy/Firewall logs showing outbound HTTPS connections to SaaS domains and credential stuffing source IPs | DNS query logs (Windows Event Viewer DNS Analytics, ISC BIND querylog, firewall DNS request logs) for command-and-control and SaaS domain resolution | Identity Provider MFA enrollment and authentication logs (Office 365 Unified Audit Log, Okta System Log, Azure AD Sign-In Logs) | Application-specific audit logs: Office 365 Mailbox Audit, Salesforce LoginHistory, AWS CloudTrail, GitHub Audit Log, Slack workspace logs | File access logs (Windows Event ID 4656, 4663; Linux auditd) correlating account, timestamp, and resource access | Browser history and download cache from affected user endpoints (C:\Users*\AppData\Local\Microsoft\Windows\INetCache, ~/.cache/chromium, ~/.mozilla/firefox/)

Per-Action IR Details

Step 1 — Immediate: Submit your organization's domains and email address ranges to Have I Been Pwned (haveibeenpwned.com) and your identity threat monitoring vendor to identify credentials exposed via LeakBase or its source breaches.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase — tools and resources)

Controls: NIST 800-53 SI-4 (Information System Monitoring), CIS 6.1 (Establish an incident response process)

Compensating: Use free OSINT tools: query Shodan, GreyhatWarfare, and GitHub for your domain names in public breach datasets; use grep and custom Python scripts to cross-reference internal email lists against publicly available breach dumps from breachforums.is (via Tor or proxy); set up Google Alerts for your domain + 'breach' keywords.

Evidence: Capture baseline list of active corporate email addresses and domains before querying; document timestamp of HIBP and vendor API submissions; screenshot or export confirmation receipts showing domains submitted and response dates for chain of custody.

Step 2 — Immediate: Force password resets for any accounts identified as exposed; prioritize privileged accounts, service accounts, and accounts with access to financial or customer data.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2 (Containment), specifically credential revocation

Controls: NIST 800-53 IA-4 (Identifier Management), NIST 800-53 AC-2(1) (Account Management — privileged accounts), CIS 5.3 (Use MFA for all administrative access)

Compensating: Document exposed account list with UPN, last login date, and group memberships before reset; use PowerShell for bulk resets in Active Directory: `Get-ADUser -Filter {mail -eq $exposedEmail} | Set-ADAccountPassword -NewPassword (ConvertTo-SecureString -AsPlainText 'TempPassword123!' -Force) -Reset; Set-ADUser -ChangePasswordAtLogon $true`; for non-AD systems, export user lists, manually reset via CLI, and log each action with timestamp.

Evidence: Capture pre-reset password age (Get-ADUser -Properties PasswordLastSet); export security event logs (Event ID 4723 — password changed, 4724 — password reset); preserve AD change audit logs with change requester, timestamp, and affected accounts; screenshot or export password reset confirmation from identity provider; document any service account resets with dependent application impact assessments.

Step 3 — Detection: Review authentication logs for credential stuffing indicators — high-volume failed logins, logins from anomalous geographies or ASNs, and successful logins preceded by repeated failures — correlated with T1110.004.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis), specifically anomaly detection

Controls: NIST 800-53 AU-2 (Audit Events — login events), NIST 800-53 SI-4(1) (Information System Monitoring — monitoring for brute force), CIS 8.5 (Log user access and changes)

Compensating: Export Windows security event logs (Event ID 4625 — failed login, 4624 — successful login) and application logs to CSV; use grep and awk to identify patterns: `grep '4625' security.log | awk -F, '{print $NF}' | sort | uniq -c | sort -rn` to count failures per account; correlate with geolocation via IP lookup (MaxMind GeoIP2 free tier or ip2location.com free dataset); identify source IPs with `grep '4624' security.log | grep -v '127.0.0.1' | awk '{print $NF}' | sort | uniq` and cross-reference against known corporate VPN/office IPs.

Evidence: Export raw Windows Event Logs 4624 and 4625 in EVTX format with full timestamps; preserve source IP, account name, logon type (3=network), workstation name, and failure reason; extract firewall/proxy logs showing connection attempts from same source IPs; capture DNS query logs to identify command-and-control or credential stuffing tool domains; preserve any IDS/IPS alerts (Suricata, Snort rules for T1110.004).

Step 4 — Detection: Hunt for T1078 and T1078.004 abuse: successful authentications outside normal working hours, impossible travel events, and first-time access to sensitive resources from accounts that have not recently been used.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis — behavioral anomalies)

Controls: NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), NIST 800-53 SI-4(4) (Information System Monitoring — inbound anomaly detection), CIS 8.2 (Collect audit logs)

Compensating: Query auth logs for successful logins (Event ID 4624 logon type 3 or 10) outside 06:00–22:00 UTC for your region; extract IP geolocation and compare travel distance to prior login location using MaxMind GeoIP2 (free 8K queries/month) — flag logins >900km apart in <1 hour; use `last -f /var/log/wtmp` on Linux to identify first-time source IPs per account; correlate successful logins with file access logs to identify new resource access from dormant accounts (Event ID 4660 — object deleted, 4656 — object opened).

Evidence: Preserve Event ID 4624 (successful login) with source IP, timestamp, account SID, logon type, and workstation name; capture Event ID 4720 (account created) and 4722 (account enabled) to establish baseline activity windows; extract /var/log/auth.log (SSH login records) with timestamp and source IP; preserve DNS query logs to identify domains accessed post-login; capture file access logs (Event ID 4656, 4663) correlating account and timestamp; document baseline geographic profile for each account (typical login locations and hours).

Step 5 — Assessment: Audit MFA coverage across all externally accessible services; accounts lacking MFA are the primary downstream risk vector from credential marketplace operations. Map gaps against CWE-308.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation — security architecture assessment)

Controls: NIST 800-53 IA-2(1) (Authentication — MFA for privileged accounts), NIST 800-53 IA-2(3) (Authentication — MFA for remote access), CIS 5.3 (Use MFA for all administrative access), CIS 5.4 (Use MFA for all remote access)

Compensating: Manually audit each SaaS application (Office 365, Okta, Salesforce, Slack, GitHub, AWS, Azure) for MFA settings; export user lists from Active Directory/identity provider with MFA status (`Get-MsolUser -All | Select UserPrincipalName, StrongAuthenticationMethods | Export-Csv mfa_audit.csv`); create spreadsheet mapping service → user → MFA enabled/disabled; identify gaps by cross-referencing with group membership (privileged groups should be 100% MFA-enabled); use CWE-308 (Use of Single-Factor Authentication) mapping to document compensating controls (IP whitelisting, conditional access rules, VPN-only access).

Evidence: Export MFA enrollment status reports from each SaaS platform (Office 365, Okta, identity provider); capture conditional access policies and MFA enforcement rules; preserve any exemptions or legacy accounts with documented business justification; document baseline MFA status by department/role; preserve screenshots of disabled MFA accounts and change logs if available.

Step 6 — Assessment: Inventory third-party SaaS applications where employees use corporate email addresses as usernames; these are high-value ATO targets if credentials were traded on LeakBase.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation — IT inventory and asset management)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), NIST 800-53 SA-3 (System Development Life Cycle), CIS 1.1 (Establish a detailed inventory of all hardware assets)

Compensating: Query Active Directory for 'lastLogonTimestamp' and 'distinguishedName' to identify all corporate email accounts; use Shodan queries (`org:company.com`) and Google dorking (`site:*.saas-provider.com @company.com`) to discover registered SaaS applications; analyze proxy/firewall logs for outbound HTTPS connections to known SaaS domains (use free SaaS list from securitytrails.com or curated lists); interview department heads and IT staff to identify non-standard SaaS tools; use WHOIS and SSL certificate searches to find domains registered to your company email.

Evidence: Export corporate email list with creation date and last-used timestamps; preserve list of all active SaaS subscriptions (subscription management system, expense reports, SSO logs); capture proxy/firewall logs showing HTTPS connections to SaaS domains over last 90 days; extract DNS query logs for SaaS domain resolutions; document approval status for each SaaS application (approved vs. shadow IT); preserve account creation timestamps in each SaaS platform.

Step 7 — Communication: Notify affected users whose credentials were confirmed exposed; provide clear password reset instructions and guidance on recognizing phishing follow-on attempts.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities — communication and public disclosure)

Controls: NIST 800-53 IR-4(9) (Incident Handling — incident-related information sharing), CIS 6.5 (Establish a process for incident post-mortem)

Compensating: Create email template with: account exposure confirmation, step-by-step password reset instructions (with screenshots), MFA enrollment link, phishing indicators (urgency, requests for password confirmation, suspicious sender domains), and security helpdesk contact; send via authenticated organizational email channel (not auto-mailer); use secure delivery method (identity provider notification system, intranet portal) rather than mass email blast; document delivery with recipient list, send timestamp, and bounce rate; follow up with users who did not reset passwords within 48 hours via secondary channel (phone, manager escalation).

Evidence: Preserve email template and all communications sent; document recipient list with delivery timestamps and bounce information; log all password reset requests and completions (Event ID 4724); capture helpdesk tickets from users reporting phishing attempts or reset issues; preserve any phishing emails reported by users (full headers, envelope-from, SPF/DKIM/DMARC status); document user acknowledgment (read receipts, portal login confirmations).

Step 8 — Long-term: Implement or validate continuous credential monitoring against dark web and breach corpus feeds to reduce mean time to detection for future exposures.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities — lessons learned and prevention)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 RA-5 (Vulnerability Scanning), CIS 6.2 (Establish a logging and alerting policy)

Compensating: Subscribe to free breach notification services (Have I Been Pwned API, SecurityTrails, Abuse.ch); use open-source tools (theHarvester, recon-ng, SpiderFoot) to monitor public mentions of your organization and employee email addresses in pastebin, GitHub, and forums; set up Google Alerts and feed aggregators (IFTTT) to flag mentions of your domains on dark web forum archives and breach corpus indexes (BreachForums, LeakBase successor platforms); manually query breach databases (breachforums.is, darkleaks, etc.) via Tor browser monthly; use WHOIS history monitoring to detect domain registration anomalies (domaintools.com free tier).

Evidence: Document baseline credential exposure status (pre-monitoring snapshot); preserve all breach notification receipts and alerts with timestamps; maintain log of monitoring tool queries and results; capture screenshots of dark web forum queries and results; document any new exposures detected and response timeline; preserve links to breach corpus entries mentioning your organization for forensic correlation.

Step 9 — Long-term: Enforce passwordless or phishing-resistant MFA (FIDO2/passkeys) for all privileged and externally accessible accounts to reduce ATO impact from credential exposure events.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities — improvements and prevention)

Controls: NIST 800-53 IA-2(1) (Authentication — MFA for privileged accounts), NIST 800-53 IA-5(1)(12) (Authentication Mechanisms — phishing-resistant authentication), CIS 5.3 (Use MFA for all administrative access), CIS 5.5 (Use MFA for all email)

Compensating: For organizations without enterprise MFA platforms: provision free or low-cost FIDO2 keys (YubiKey 5 Series ~$45/unit, or SoloKeys open-source ~$70); deploy Windows Hello for Business (passwordless sign-in, built into Windows 10+, free); use OS-native passkey support (Windows 11 Passkey Support, macOS/iOS iCloud Keychain, Android Passkey Manager); for legacy remote access (VPN), implement FIDO2 via OpenVPN plugins or open-source authenticators (Yubico Yubihsm, privacyIDEA); enforce passwordless-only access to privileged accounts via conditional access policies (Azure AD, Okta, Ping Identity free trials offer limited policies); document exceptions and require management sign-off.

Evidence: Document baseline privileged account authentication methods and risk assessment; preserve MFA enrollment records (FIDO2 device registration, passkey setup); capture conditional access policy logs showing authentication method enforcement; preserve audit logs of privileged access attempts (failed passwordless attempts, forced MFA re-enrollment); document baseline and post-implementation unauthorized access attempts; preserve any user feedback or technical issues during rollout for post-incident review.

Detection Guidance

No platform-specific IOCs (IPs, domains, hashes) have been publicly attributed to LeakBase infrastructure at this time per available T1 sources. Detection focus should be on downstream abuse of credentials that transited the platform. Key log sources: identity provider authentication logs (Azure AD, Okta, Ping), VPN access logs, and SaaS application access logs. Behavioral indicators: (1) Credential stuffing, spike in HTTP 401/403 responses against login endpoints, especially from rotating IP ranges or known residential proxy ASNs; (2) Valid account abuse, successful logins from IPs flagged in threat intel feeds, impossible travel alerts, or logins during off-hours for accounts that never previously exhibited that pattern; (3) Session hijacking (T1539), session tokens used from a different IP or user agent than the originating login within the same session. Query recommendation (generic SIEM): correlate successful authentication events where the source IP appears in commercial threat intel feeds AND the account has not authenticated from that geography in the prior 30 days. For Splunk users, the ESCU 'Credential Stuffing' and 'Brute Force' analytic stories are relevant starting points. No confirmed IOCs are available for LeakBase infrastructure from T1 sources; treat any claimed IOC sets from non-T1 sources with caution until corroborated.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`leakbase[.]io`	Primary LeakBase platform domain — defanged. Block at DNS and proxy layers to prevent internal hosts from resolving or connecting. Treat historical traffic to this domain as an indicator of potential insider involvement or compromised host. Source: Europol/DOJ press releases (T1).	HIGH

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft
- **T1110.004** — Credential Stuffing
- **T1078.004** — Cloud Accounts
- **T1539** — Steal Web Session Cookie
- **T1586.001** — Social Media Accounts
- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts
- **T1589.001** — Credentials
- **T1586.002** — Email Accounts
- **T1650** — Acquire Access

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

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

HIPAA-SECURITY

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

CIS-V8

- **5.2**
- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1110.004	Credential Stuffing	Credential-Access

Technique ID	Technique Name	Tactic
T1078.004	Cloud Accounts	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1586.001	Social Media Accounts	Resource-Development
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1589.001	Credentials	Reconnaissance
T1586.002	Email Accounts	Resource-Development
T1650	Acquire Access	Resource-Development

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/leakbase-admin-arrested-in-russia...	T3
United States Leads Dismantlement of One of the World's Largest ...	https://www.justice.gov/opa/pr/united-states-leads-dismantlement-on...	T1
Major data leak forum dismantled in global action against ... - Europol	https://www.europol.europa.eu/media-press/newsroom/news/major-data-...	T1
Could You Be Affected by the LeakBase Cybercrime Forum Seizure ...	https://www.cloaked.com/post/could-you-be-affected-by-the-leakbase-...	T3
LeakBase Cybercrime Forum Shut Down, Suspects Arrested	https://www.securityweek.com/leakbase-cybercrime-forum-shut-down-su...	T3

Generated 2026-03-29 18:39 UTC by TJS Security Command Center