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

Global Law Enforcement Disruption: Operations Synergia III, Red Card, and LeakBase Seizure Across 72 Countries

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0014
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	No specific vendor products; impersonated infrastructure targeting casinos, banks, government portals, and payment service platforms; cybercrime forum LeakBase (142,000 members)
Published	2026-03-13

Executive Summary

A coordinated international law enforcement campaign spanning 72 countries sinkholed 45,000 malicious IP addresses, arrested nearly 400 suspects, seized 212 devices, and shut down the LeakBase credential marketplace serving 142,000 members. Financial institutions, government portals, casinos, and payment platforms were the primary targets of the impersonated infrastructure. The immediate disruption is significant, but displaced threat actors and orphaned command-and-control nodes historically resurface under new identities within weeks; security teams should expect a short-term spike in reconnaissance and rebranded phishing campaigns.

Technical Analysis

Operations Synergia III and Red Card dismantled phishing infrastructure and malware C2 nodes operating across 72 countries, with law enforcement sinkholing 45,000 IPs previously used for command-and-control communications (T1071.001, T1071) and drive-by compromise delivery (T1189). Threat actors employed domain acquisition (T1583.001, T1583) and compromised legitimate accounts (T1586, T1078) to stage phishing lures (T1566, T1566.002) impersonating banks, casinos, government portals, and payment platforms. Targeted phishing for credential harvesting (T1598) and email collection (T1114) were observed alongside session cookie theft (T1539) and content injection (T1659). Remote access tooling (T1219) supported post-compromise persistence. The LeakBase forum seizure removes a primary redistribution point for stolen credentials and breach data; 142,000 member records are now in law enforcement custody, creating follow-on exposure risk for

actors who registered with traceable identities. No CVEs are associated with this campaign. Relevant CWEs: CWE-940 (improper verification of source of communication channel), CWE-345 (insufficient verification of data authenticity), CWE-200 (exposure of sensitive information). No vendor patches are applicable; the threat is infrastructure and social-engineering based. Source quality is T3 (BleepingComputer reporting); authoritative confirmation from Interpol or FBI press releases should be sought before citing figures in formal reporting.

Action Checklist

1. Step 1, Immediate: Pull and block any threat intelligence feeds referencing the 45,000 sinkholed IPs; cross-reference against your firewall and proxy deny-lists and add confirmed malicious entries. Monitor sinkholed IP ranges for any internal hosts attempting outbound connections, which would indicate active C2 beaconing.
2. Step 2, Detection: Search email gateway and proxy logs for phishing lures impersonating financial institutions, government portals, and payment platforms (T1566, T1566.002). Query SIEM for T1071.001 patterns: unusual HTTP/HTTPS POST traffic to newly registered or low-reputation domains, especially from workstations outside expected communication baselines.
3. Step 3, Assessment: Audit privileged and service accounts for signs of compromise (T1078, T1586); review authentication logs for anomalous login times, geolocations, or credential reuse patterns. Inventory any credential sets potentially exposed via LeakBase by cross-referencing corporate email domains against known breach notification services (e.g., Have I Been Pwned, SpyCloud if licensed).
4. Step 4, Communication: Brief the CISO and relevant stakeholders on displacement risk: disrupted actors may reappear under new infrastructure within weeks. If your organization operates in financial services, government contracting, or payment processing, elevate awareness to fraud and customer-facing teams about expected rebranded phishing waves.
5. Step 5, Long-term: Initiate a threat hunt hypothesis around C2 beaconing to orphaned infrastructure that has not yet been sinkholed (T1071, T1219). Update phishing simulation and awareness training content to reflect current impersonation themes. Review and tighten email authentication controls (SPF, DKIM, DMARC) and enforce phishing-resistant MFA on all externally accessible applications. Establish a recurring review cycle for credential exposure monitoring given the ongoing LeakBase member data investigation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to external IR firm or FBI field office if any internal host is confirmed connecting to sinkholed IPs (active C2 beaconing), if authentication logs reveal compromise of privileged accounts, or if organizational credentials appear in LeakBase breach inventory with evidence of exploitation.

Recovery Notes	After containment, conduct a full 30-day threat hunt for orphaned C2 infrastructure that re-emerges post-sinkhole using ATT&CK patterns for T1071 (Application Layer Protocol Usage) and T1219 (Remote Access Software). Implement continuous credential exposure monitoring tied to incident response runbooks — treat new LeakBase data releases as recurring threat intelligence inputs. Schedule post-incident review (IR-3) at 30, 60, and 90 days to track threat actor re-emergence patterns and validate compensating controls effectiveness.
Forensic Artifacts	Windows Event Logs: Event ID 4624 (logon), 4625 (logon failure), 4688 (process creation), 4720-4722 (account creation/modification), 4738 (user account modification) — focus on privileged accounts and service accounts from 90 days pre-incident | Proxy/Firewall logs: Full traffic flows including source IP, destination IP, port, protocol, HTTP method, URL, user agent, referer, request/response size, and timestamps — critical for T1071.001 and C2 identification | Email gateway logs: SMTP headers (envelope from/to, DKIM/SPF/DMARC results, originating IP), email body (HTML and text), attachment metadata (file hash, type, size), and any sandbox verdicts — essential for T1566 phishing attribution | DNS query logs: All external DNS resolutions for 90 days, including timestamp, source IP, query domain, response IP, and TTL — identifies beaconing patterns to newly registered domains | Authentication/IAM logs: AD logon events, password reset events, MFA enrollment timestamps, password changes (Event ID 4724, 4725), account lockouts (Event ID 4740), and service account usage patterns | Network flow data: NetFlow/sFlow exports or full PCAP captures from network taps, focusing on long-duration connections, unusual port combinations, and traffic to low-reputation ASNs — supports C2 hunting and beaconing identification

Per-Action IR Details

Step 1, Immediate: Pull and block any threat intelligence feeds referencing the 45,000 sinkholed IPs; cross-reference against your firewall and proxy deny-lists and add confirmed malicious entries. Monitor sinkholed IP ranges for any internal hosts attempting outbound connections, which would indicate active C2 beaconing.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation: tools and resources) and §2.2 (mitigation: blocking malicious infrastructure)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AC-4 (Information Flow Enforcement), CIS 6.2 (Boundary Defense)

Compensating: Download the 45,000 sinkholed IP list from CISA or partner law enforcement advisories; import into open-source pfSense or iptables rules on edge routers. Use grep to cross-reference against existing deny-list files: `grep -f sinkholed_ips.txt firewall_denies.txt`. Monitor DNS queries to sinkholed ranges using tcpdump (`tcpdump -i any 'dst net '`) and log to syslog for manual review.

Evidence: Before blocking: capture 72 hours of full network flow data (NetFlow, sFlow, or tcpdump) to establish baseline C2 communication patterns. Document firewall rule change logs and proxy access logs (timestamp, source IP, destination, port, protocol, user agent) for any connections to the 45,000 IPs pre-block. Export firewall state tables and active connection logs.

Step 2, Detection: Search email gateway and proxy logs for phishing lures impersonating financial institutions, government portals, and payment platforms (T1566, T1566.002). Query SIEM for T1071.001 patterns: unusual HTTP/HTTPS POST traffic to newly registered or low-reputation domains, especially from workstations outside expected communication baselines.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (analysis: log aggregation and review) and §3.2.4 (attack pattern recognition)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), CIS 8.2 (Email Gateway Filtering)

Compensating: Export email gateway logs (Microsoft Exchange, Postfix, or Exim) to CSV; search for sender domains matching known impersonation targets using regex patterns (e.g., 'financial-bank.com', 'gov-payroll.net'). For proxy logs, use AWK/grep to identify POST requests: `awk '$7 ~ /^POST/ && $9 !~ /^(10\.0|172\.16|192\.168)/ {print}' proxy.log`. Cross-reference domain registrant data against WHOIS history to identify newly registered domains (<30 days old).

Evidence: Preserve unmodified email headers (SMTP relay path, authentication results, originating IP), email body (HTML source and text), and attachment metadata (hash, file type, size). Capture proxy request/response pairs: full URL, HTTP headers (User-Agent, Referer, Authorization), request body, response status, and destination IP resolution at request time. Document any URL shortener redirects by expanding before log capture.

Step 3, Assessment: Audit privileged and service accounts for signs of compromise (T1078, T1586); review authentication logs for anomalous login times, geolocations, or credential reuse patterns. Inventory any credential sets potentially exposed via LeakBase by cross-referencing corporate email domains against known breach notification services (e.g., Have I Been Pwned, SpyCloud if licensed).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.5 (profile abnormalities) and §4.1 (eradication: account and credential analysis)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Control / Privileged Access), NIST 800-53 IA-4 (Identifier Management), CIS 5.2 (Account Privilege Management), CIS 6.5 (Credential Access Protections)

Compensating: Export authentication logs (Windows Event ID 4624 for logons, 4625 for failures; Linux /var/log/auth.log; application logs) to CSV. Use free OSINT tools to check corporate domain against Have I Been Pwned API (script available on GitHub: 'hibp-domain-checker'). Create a manual spreadsheet of privileged accounts (domain admins, service accounts) and correlate against login IP geolocation using free MaxMind GeoIP2 Lite database; flag logins from unexpected regions or after hours. Query AD lastLogon and pwdLastSet attributes using `Get-ADUser -Filter * -Properties lastLogon,pwdLastSet | Export-CSV`.

Evidence: Capture full authentication audit logs (90 days minimum) with timestamps, user account, source IP, logon type, and result. Export AD account attributes: lastLogon, pwdLastSet, accountExpires, userAccountControl flags. If SIEM available, preserve raw login events in original format. Document all password reset events (Event ID 4724) and account modifications (Event ID 4738) for privileged accounts in the 90-day window. Save Have I Been Pwned breach results and enrollment dates if available.

Step 4, Communication: Brief the CISO and relevant stakeholders on displacement risk: disrupted actors may reappear under new infrastructure within weeks. If your organization operates in financial services, government contracting, or payment processing, elevate awareness to fraud and customer-facing teams about expected rebranded phishing waves.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3.1 (preparation: tools and communication); §3.1 (detection: alerts and thresholds)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-2 (Incident Response Training), CIS 17.1 (Incident Response Program)

Compensating: Document threat actor displacement timelines from public CISA advisories and VirusTotal retroactive detections to project re-emergence window (typically 2-4 weeks). Create a one-page briefing template with: (1) original threat actor infrastructure summary, (2) law enforcement disruptive actions, (3) expected threat actor pivot patterns from ATT&CK, (4) organization-specific risk vectors (financial sector = phishing, payment platforms = C2 exfiltration). Schedule standing 15-minute daily calls between IR team, CISO, and customer-facing stakeholders during the 30-day post-disruption window.

Evidence: Preserve CISA advisories, Interpol communications, and public law enforcement statements as briefing reference material. Document current organizational threat surface: externally facing applications, payment processing touchpoints, brand-impersonation attack surface. Maintain attendance logs and timestamp of stakeholder briefings for compliance documentation (IR-2 training verification).

Step 5, Long-term: Initiate a threat hunt hypothesis around C2 beaconing to orphaned infrastructure that has not yet been sinkholed (T1071, T1219). Update phishing simulation and awareness training content to reflect current impersonation themes. Review and tighten email authentication controls (SPF, DKIM, DMARC) and enforce phishing-resistant MFA on all externally accessible applications. Establish a recurring review cycle for credential exposure monitoring given the ongoing LeakBase member data investigation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §4.2 (post-incident analysis and lessons learned); NIST 800-53 IA-5 (Authentication); SI-4 (Continuous Monitoring)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-5 (Authenticator Management), NIST 800-53 SC-7 (Boundary Protection), CIS 6.3 (Email Authentication), CIS 6.4 (Phishing and Spearphishing), CIS 5.7 (MFA Enforcement)

Compensating: C2 Hunt: Query proxy/firewall logs for POST traffic to newly registered domains (WHOIS age 7.0 indicates potential encoded C2). Use Zeek or Suricata IDS with free rulesets to flag long-duration connections to low-reputation ASNs. Email Auth: Deploy free DMARC analyzer (easydmarc.com or dmarcian free tier) to audit SPF/DKIM coverage; manually edit DNS records to enforce DMARC reject policy in stages. MFA: Enforce passwordless sign-in (Windows Hello for Business, FIDO2) on all VPN and cloud portals using built-in OS capabilities (no licensing required). Credential Monitoring: Subscribe to free tier credential databases (Dehashed API community version, Google's password checkup plugin) and run monthly manual audits against employee lists.

Evidence: Preserve 180 days of proxy/firewall full-content logs (PCAP or flow export) to support retrospective C2 hunting queries. Export email authentication configuration (SPF records, DKIM selectors, DMARC policy) before and after policy changes for compliance audit trail. Document MFA implementation rollout: enrollment timestamp, user, device type, authenticator method, fallback authentication method. Maintain a historical log of credential exposure findings and remediation dates for post-incident lessons learned (IR-3 requirements).

Detection Guidance

Focus detection on three areas: outbound C2 activity, inbound phishing, and credential anomalies. For C2: query firewall and proxy logs for outbound connections to IPs in threat intelligence feeds linked to Synergia III or Red Card; flag any internal host initiating connections to sinkholed address ranges. For phishing: review email gateway quarantine for messages containing lookalike domains mimicking financial, government, or payment brands; look for newly registered domains (less than 30 days old) in URL click-through logs. For credential anomalies: alert on authentication events from IP addresses not associated with the user's normal geography or device; flag accounts with multiple failed logins followed by a success (potential credential stuffing using LeakBase data). MITRE technique pivot points for SIEM rule development: T1071.001 (web protocol C2 beaconing, look for regular interval POST requests to low-prevalence external domains), T1189 (drive-by compromise, browser process spawning unusual child processes), T1539 (session cookie theft, unexpected session reuse from new IP without re-authentication). No specific IOCs have been publicly released with verified hashes or domain lists as of the available sourcing; monitor Interpol and FBI official channels for published indicator sets.

Indicators of Compromise

Type	Value	Context	Confidence
IP	`45000-ip-range-sinkholed`	Law enforcement sinkholed 45,000 IPs associated with Synergia III and Red Card C2 and phishing infrastructure. Specific IP list not publicly released in available sources; obtain from Interpol, FBI, or vetted threat intelligence feeds. Internal hosts attempting outbound connections to these ranges require immediate investigation.	LOW

Framework Mappings

MITRE-ATTACK

- **T1598** — Phishing for Information
- **T1583.001** — Domains
- **T1071.001** — Web Protocols
- **T1189** — Drive-by Compromise
- **T1078** — Valid Accounts
- **T1566.002** — Spearphishing Link
- **T1594** — Search Victim-Owned Websites
- **T1534** — Internal Spearphishing
- **T1114** — Email Collection
- **T1586** — Compromise Accounts
- **T1071** — Application Layer Protocol
- **T1583** — Acquire Infrastructure
- **T1539** — Steal Web Session Cookie
- **T1659** — Content Injection
- **T1566** — Phishing
- **T1219** — Remote Access Tools

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
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection

- **CA-7** — Continuous Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **2.5**
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

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

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1598	Phishing for Information	Reconnaissance
T1583.001	Domains	Resource-Development
T1071.001	Web Protocols	Command-And-Control
T1189	Drive-by Compromise	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1566.002	Spearphishing Link	Initial-Access
T1594	Search Victim-Owned Websites	Reconnaissance
T1534	Internal Spearphishing	Lateral-Movement
T1114	Email Collection	Collection
T1586	Compromise Accounts	Resource-Development

Technique ID	Technique Name	Tactic
T1071	Application Layer Protocol	Command-And-Control
T1583	Acquire Infrastructure	Resource-Development
T1539	Steal Web Session Cookie	Credential-Access
T1659	Content Injection	Initial-Access
T1566	Phishing	Initial-Access
T1219	Remote Access Tools	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/police-sinkholes-45-...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/police-sinkholes-45-...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/police-arrests-300-s...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/fbi-seizes-leakbase-...	T3
Cyber Criminals Target Vendor Portals Belonging to U.S. ...	https://www.cisecurity.org/insights/white-papers/cyber-criminals-ta...	T3

Generated 2026-03-29 18:40 UTC by TJS Security Command Center