INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-19 06:44 UTC

INTERPOL Operation Ramz Dismantles MENA Phishing-as-a-Service Infrastructure: 53 Servers Seized, 200+ Arrested

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0335
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	No specific software products affected; infrastructure targets included phishing servers, malware distribution servers, and a PhaaS platform operating across 13 MENA countries. Private sector partners: Kaspersky, Group-IB, Shadowserver Foundation, Team Cymru, TrendAI.
Published	2026-05-18T18:15:30
Discovery Source	Rss

Executive Summary

INTERPOL's Operation Ramz dismantled cybercriminal infrastructure across 13 Middle East and North Africa countries, resulting in 200+ arrests and seizure of 53 servers supporting phishing, malware distribution, and investment fraud operations. A Phishing-as-a-Service platform in Algeria was taken down, lowering the barrier for regional threat actors to launch credential-harvesting campaigns against global targets. Organizations with customers, partners, or operations in MENA face reduced near-term phishing risk from these specific operators, though successor infrastructure is likely.

Technical Analysis

Operation Ramz targeted interconnected cybercriminal infrastructure across 13 MENA countries. Disrupted infrastructure included a PhaaS platform (Algeria), malware distribution servers, and investment fraud operations with a coerced-labor component (Jordan). Nearly 8,000 intelligence packages were recovered from seized equipment; 3,867 victims confirmed. MITRE techniques observed span infrastructure acquisition (T1583.003, Virtual Private Server, T1583.006, Web Services, T1584, Compromise Infrastructure), account abuse (T1585, Establish Accounts, T1586, Compromise Accounts, T1078, Valid Accounts), phishing delivery (T1566, Phishing, T1566.002, Spearphishing Link, T1598, Spearphishing for Information), C2 communication (T1071, Application Layer Protocol, T1071.001, Web Protocols), and credential harvesting (T1056, Input

Capture). Financial extortion (T1657) rounds out the confirmed technique set. CWE-20 (Improper Input Validation) and CWE-287 (Improper Authentication) reflect the weakness classes targeted by phishing and credential-abuse TTPs. No CVE identifiers are associated; this is an infrastructure disruption operation, not a software vulnerability. Technical details of the PhaaS platform, tooling, pricing, customer base, are not available in current reporting. Private sector partners: Kaspersky, Group-IB, Shadowserver Foundation, Team Cymru. Source: Bleeping Computer / INTERPOL (confidence HIGH for operational facts).

Action Checklist

1. Containment, Review and block known-bad infrastructure: cross-reference your threat intel platform and email security gateway against IOCs published by Shadowserver Foundation (shadowserver.org/news-insights) and Team Cymru (team-cymru.com/news) following Operation Ramz; apply blocks at DNS, proxy, and email layers. No specific IP/domain list is available in current reporting. Monitor partner feeds weekly for 30 days following the operation; apply blocks within 24 hours of publication.
2. Detection, Hunt for PhaaS-linked phishing patterns in email logs: search for messages with spoofed sender domains, credential-harvesting redirect chains, and login-page lookalikes targeting your user base. Query SIEM for T1566 and T1056 indicators: unexpected authentication attempts (T1078), web protocol C2 beaconing (T1071.001), and anomalous account creation (T1585/T1586). Pull Kaspersky and Group-IB threat intel feeds for MENA-linked campaign signatures if licensed.
3. Eradication, Reset credentials for any accounts flagged during detection hunting. Revoke sessions for accounts showing anomalous authentication patterns. Audit externally registered domains that could be used in typosquatting campaigns against your brand, file takedown requests for confirmed lookalikes.
4. Recovery, Validate email security gateway, DNS RPZ, and proxy blocklists reflect updated IOCs as partner organizations release them post-seizure. Confirm MFA enforcement on all externally accessible applications. Monitor for resumed activity from successor infrastructure, PhaaS ecosystems often reconstitute within weeks of takedowns.
5. Post-Incident, Review phishing simulation results and user reporting rates; this operation confirms PhaaS lowers the cost of targeted phishing. Assess whether your anti-phishing controls (DMARC enforcement, MFA coverage, proxy filtering) are tuned for PhaaS-pattern campaigns. Map control gaps to NIST CSF DE.CM-7 (monitoring for unauthorized activity) and PR.AC-3 (remote access management).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if detection hunting confirms any accounts successfully authenticated via PhaaS-harvested credentials, as this constitutes a confirmed breach triggering regulatory notification obligations under GDPR, CCPA, or applicable MENA data protection laws depending on the affected user population.

Recovery Notes	Post-containment, maintain an active monitoring window of at least 90 days for MENA-region ASN traffic in email, DNS, and proxy logs, given that PhaaS ecosystems historically reconstitute within 4–8 weeks of law enforcement takedowns using modified infrastructure. Verify DMARC policy is set to `p=reject` (not `p=quarantine`) and that SPF records do not include overly permissive `+all` or `?all` mechanisms, as PhaaS operators targeting your brand will exploit lookalike domains that DMARC does not protect against — proxy and DNS RPZ filtering are the primary compensating controls. Confirm that all post-eradication credential resets were followed by forced MFA re-enrollment, not just password changes, since PhaaS-harvested session cookies can survive password resets if active sessions were not explicitly revoked.
Forensic Artifacts	Email gateway delivery logs with full MIME headers (Received chain, Authentication-Results, DKIM-Signature, Return-Path, X-Originating-IP) for the 30-day window preceding Operation Ramz public disclosure — PhaaS platforms reuse header templates producing detectable fingerprints across campaign waves | DNS resolver query logs (Windows DNS Debug Log or BIND query log) filtered for queries to domains registered within 60 days, particularly those matching typosquats of your organization name or key partners — newly registered short-lived domains are the primary PhaaS infrastructure pattern | Windows Security Event Log Event IDs 4624 (Type 3 network logon), 4625 (failed logon), and 4648 (explicit credential use) from externally-facing systems, filtered to source IPs in MENA-region ASN ranges as mapped by Team Cymru IP-to-ASN data | Mailbox inbox rule audit logs (Exchange `Get-InboxRule` output or M365 Unified Audit Log operation `New-InboxRule`) for any accounts flagged during hunting — PhaaS post-compromise playbooks commonly auto-forward harvested mailbox content to attacker-controlled addresses | Proxy or web gateway logs showing HTTP 301/302 redirect chains to login-page lookalikes, specifically multi-hop redirects through link-shortening or open-redirect URLs (a PhaaS delivery technique to bypass URL reputation filters) ending at pages mimicking Microsoft 365, banking portals, or government services

Per-Action IR Details

Containment — Review and block known-bad infrastructure: cross-reference your threat intel platform and email security gateway against IOCs published by Shadowserver Foundation (shadowserver.org/news-insights) and Team Cymru (team-cymru.com/news) following Operation Ramz; apply blocks at DNS, proxy, and email layers. No specific IP/domain list is available in current reporting — monitor partner feeds for post-operation IOC releases.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), CIS 9.2 (Use DNS Filtering Services), CIS 9.3 (Maintain and Enforce Network-Based URL Filters)

Compensating: Without an enterprise TIP, use the free Shadowserver and Team Cymru daily feed exports (both publish structured IOC reports post-operation). Ingest domains and IPs into a Pi-hole or pfBlockerNG DNS sinkhole for DNS-layer blocking. For email, use a Postfix header_checks or milter rule to reject or quarantine messages with From: domains matching the published PhaaS lookalike patterns. Script the feed pull with a cron job: `curl -s https://dl.shadowserver.org/reports/ | grep 'ramz\|phishing' > /tmp/ramz_iocs.txt && pihole -b < /tmp/ramz_iocs.txt`. Apply proxy ACL blocks via Squid using a domain blacklist file refreshed daily.

Evidence: Before applying blocks, snapshot your DNS resolver query logs (Windows DNS Debug Log or `/var/log/named/query.log` on BIND) and email gateway delivery logs (MTA queue logs, message-tracking logs) to preserve pre-block visibility. Capture any existing SMTP envelope headers showing Return-Path mismatches or X-Originating-IP fields pointing to MENA-region ASNs associated with Operation Ramz infrastructure. Export proxy logs filtered to HTTP 200/301/302 responses to domains registered within 30 days (newly registered domains are a

PhaaS hallmark). This baseline confirms whether any Operation Ramz infrastructure already reached your environment before you applied blocks.

Detection — Hunt for PhaaS-linked phishing patterns in email logs: search for messages with spoofed sender domains, credential-harvesting redirect chains, and login-page lookalikes targeting your user base. Query SIEM for T1566 and T1056 indicators: unexpected authentication attempts (T1078), web protocol C2 beaconing (T1071.001), and anomalous account creation (T1585/T1586). Pull Kaspersky and Group-IB threat intel feeds for MENA-linked campaign signatures if licensed.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 10.1 (Deploy and Maintain Anti-Malware Software)

Compensating: Without a SIEM, run the following targeted queries manually. For email: parse MTA logs with `grep -E '(DMARC=fail|SPF=fail|DKIM=fail)' /var/log/maillog | awk '{print $7}' | sort | uniq -c | sort -rn` to surface failing authentication at volume — PhaaS campaigns generate bulk spoofed sender failures. For authentication anomalies (T1078): query Windows Security Event Log for Event ID 4648 (explicit credential use) and Event ID 4625 (failed logon) from external IPs using PowerShell: `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4648,4625} | Where-Object {$_.Message -match 'LogonType.*3'} | Select TimeCreated, Message | Export-Csv auth_anomalies.csv`. For redirect chain detection: use Wireshark or Zeek to capture and filter HTTP 301/302 chains where the final destination domain age is under 60 days (correlates with PhaaS infrastructure spin-up patterns). Deploy the free Sigma rule `phishing_T1566_suspicious_redirect.yml` from SigmaHQ if log forwarding is available.

Evidence: Collect email headers (full MIME source including Received chain, Authentication-Results, DKIM-Signature, and X-Mailer fields) from any messages flagged as suspicious — PhaaS platforms often reuse header templates across campaigns, producing detectable fingerprints. Capture browser history or proxy logs showing credential-harvesting redirect chains: look for multi-hop redirects ending at login-page lookalikes with URL patterns matching legitimate services (e.g., `/login`, `/signin`, `/verify`) on newly registered domains. Pull Windows Security Event Log Event ID 4624 (successful logon) for Type 3 (network) logons from IPs in MENA-region ASN ranges (ASN data from Team Cymru's IP-to-ASN mapping service). Document any O365/Azure AD or Okta conditional access policy trigger events showing sign-ins from unexpected geographies concurrent with the Operation Ramz campaign window.

Eradication — Reset credentials for any accounts flagged during detection hunting. Revoke sessions for accounts showing anomalous authentication patterns. Audit externally registered domains that could be used in typosquatting campaigns against your brand — file takedown requests for confirmed lookalikes.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential reset at scale without an IAM platform: use PowerShell `Set-ADAccountPassword` with `-Reset` for flagged AD accounts and force re-logon with `Set-ADUser -ChangePasswordAtLogon $true`. For session revocation without an enterprise IdP: on Windows, run `quser` to identify active sessions, then `logoff ` to terminate. For typosquatting discovery without a commercial brand-monitoring tool, use the free `dnstwist` utility (`pip install dnstwist && dnstwist --registered yourdomain.com -o csv > lookalikes.csv`) to enumerate permutations of your brand domain and cross-check registrations against WHOIS for recent registration dates. File UDRP or registrar abuse complaints for confirmed PhaaS-linked lookalikes using the registrar's abuse contact (findable via `whois` output).

Evidence: Before resetting credentials, preserve the full authentication audit trail: export Azure AD sign-in logs or Active Directory Security Event Log (Event IDs 4624, 4625, 4768, 4776) for all flagged accounts covering the full suspected compromise window. Capture any forwarding rules or inbox rules created on compromised mailboxes (a common PhaaS post-compromise step to harvest ongoing communications) — in Exchange/O365 query via `Get-InboxRule -Mailbox ` or the Microsoft 365 compliance portal. Document the specific lookalike domains discovered during the typosquatting audit with WHOIS registration timestamps so post-incident reporting can correlate

brand-targeting activity to the Operation Ramz campaign timeline.

Recovery — Validate email security gateway, DNS RPZ, and proxy blocklists reflect updated IOCs as partner organizations release them post-seizure. Confirm MFA enforcement on all externally accessible applications. Monitor for resumed activity from successor infrastructure — PhaaS ecosystems often reconstitute within weeks of takedowns.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST IA-3 (Device Identification and Authentication), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Validate DNS RPZ coverage without enterprise tooling by running `dig @ ` for a sample of known-bad domains — a sinkhole response (NXDOMAIN or RFC5735 address) confirms the block is active. For MFA gap discovery without an IAM dashboard: query Active Directory for accounts with `DoesNotRequirePreAuth` or `PasswordNeverExpires` flags set (`Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties *`), which identify Kerberoastable accounts that a PhaaS threat actor with harvested credentials would target first. Set a 90-day monitoring window specifically for MENA-region ASN traffic in your proxy and email logs — historical precedent from similar PhaaS takedowns (e.g., BulletProofLink) shows successor infrastructure emerges within 4–8 weeks, often reusing modified versions of the original phishing kit templates.

Evidence: During recovery validation, preserve blocklist audit logs (timestamped exports of DNS RPZ zone files, proxy ACL configs, and email gateway rule sets) to create a documented chain of control changes for post-incident review. Capture a baseline of authentication log volume (successful MFA challenges per day, failed MFA per day) immediately after enforcement changes so that anomalous post-recovery spikes — indicating successor PhaaS campaigns probing newly MFA-enforced accounts — are detectable against a known-good baseline. Archive the Shadowserver and Team Cymru IOC feed versions applied during this operation with their retrieval timestamps, since IOC lists will be updated as the investigation matures and you need to track which version was applied when.

Post-Incident — Review phishing simulation results and user reporting rates; this operation confirms PhaaS lowers the cost of targeted phishing. Assess whether your anti-phishing controls (DMARC enforcement, MFA coverage, proxy filtering) are tuned for PhaaS-pattern campaigns. Map control gaps to NIST CSF DE.CM-7 (monitoring for unauthorized activity) and PR.AC-3 (remote access management).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a formal GRC platform for control gap mapping, build a simple spreadsheet mapping your current DMARC policy (`p=reject` vs `p=quarantine` vs `p=none` — check via `dig TXT _dmarc.yourdomain.com`), MFA coverage percentage (derived from the AD query above), and proxy filter hit rates against the PhaaS attack chain steps. Use the free MXToolbox DMARC report aggregator to pull DMARC aggregate (RUA) reports and identify domains from which your brand is being spoofed — this directly surfaces active PhaaS abuse of your domain identity. Schedule a tabletop exercise scenario modeled on Operation Ramz: a PhaaS-enabled actor targeting your MENA-region partners or customers with credential-harvesting pages that bypass DMARC by using lookalike domains (not your actual domain), which is the primary PhaaS evasion technique against DMARC-protected organizations.

Evidence: For the lessons-learned record, compile: (1) the full timeline of IOC publication by Shadowserver and Team Cymru versus when your blocks were applied — the gap quantifies your detection latency for external-feed-dependent controls; (2) user-reported phishing ticket volume during the Operation Ramz campaign window correlated against your phishing simulation click rates, which together measure real-world susceptibility to PhaaS-quality lure quality; (3) DMARC aggregate report data for the 90 days preceding the operation, showing how many spoofed emails using your domain identity were intercepted externally before reaching your users — this establishes whether PhaaS operators were already targeting your brand identity prior to the seizure.

Detection Guidance

No confirmed IOCs are publicly attributed to Operation Ramz in current reporting. Detection posture should focus on behavioral indicators aligned to the confirmed MITRE technique set. In email security logs: look for credential-harvesting redirect URLs, lookalike sender domains targeting your industry, and spearphishing links (T1566.002) using URL shorteners or web service infrastructure (T1583.006). In authentication logs: flag impossible-travel logins, credential stuffing patterns, and new account creation followed by rapid privilege use (T1078, T1585). In proxy/DNS logs: identify beaconing patterns over HTTP/S to newly registered domains (T1071.001). In endpoint logs: monitor for input capture behavior (T1056), keyloggers, form grabbers, browser credential access. Subscribe to Shadowserver Foundation and Team Cymru post-operation IOC releases; Group-IB and Kaspersky feeds may publish MENA-linked PhaaS indicators as the investigation develops. MITRE ATT&CK Navigator layers for T1566, T1583, T1584, T1078, and T1071 provide detection coverage guidance.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not available`	No specific IOCs from Operation Ramz have been published in current reporting. Monitor Shadowserver Foundation, Team Cymru, Group-IB, and Kaspersky feeds for post-operation releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1584** — Compromise Infrastructure
- **T1071.001** — Web Protocols
- **T1583.003** — Virtual Private Server
- **T1585** — Establish Accounts
- **T1657** — Financial Theft
- **T1566.002** — Spearphishing Link
- **T1056** — Input Capture
- **T1566** — Phishing
- **T1583.006** — Web Services
- **T1598** — Phishing for Information
- **T1071** — Application Layer Protocol
- **T1586** — Compromise Accounts
- **T1078** — Valid Accounts

NIST-800-53R5

- **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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-10** — Information Input Validation
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.5.34** — Privacy and protection of personal information

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)(5)(i)** — Security Awareness and Training

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1584	Compromise Infrastructure	Resource-Development

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1583.003	Virtual Private Server	Resource-Development
T1585	Establish Accounts	Resource-Development
T1657	Financial Theft	Impact
T1566.002	Spearphishing Link	Initial-Access
T1056	Input Capture	Collection
T1566	Phishing	Initial-Access
T1583.006	Web Services	Resource-Development
T1598	Phishing for Information	Reconnaissance
T1071	Application Layer Protocol	Command-And-Control
T1586	Compromise Accounts	Resource-Development
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/interpol-operation-r...	T3
News & Insights | The Shadowserver Foundation	https://www.shadowserver.org/news-insights/	T3
Team Cymru Cyber Security News and Threat Intelligence Updates	https://www.team-cymru.com/news	T3
APT and financial attacks on industrial organizations in Q4 2025	https://ics-cert.kaspersky.com/publications/apt-and-financial-attac...	T3
Latest Cyber Threat Trends | Group-IB Blog	https://www.group-ib.com/blog/	T3

Generated 2026-05-19 06:44 UTC by TJS Security Command Center