INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-08 19:03 UTC

Iranian threat group used Chaos ransomware as a 'false flag,' researchers say

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0292
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Organizations targeted by MuddyWater, primarily in MENA region
Published	2026-05-07
Discovery Source	Gemini

Executive Summary

Iranian state-sponsored group MuddyWater deployed Chaos ransomware against targets in the Middle East and North Africa as a deception tactic, presenting ransom demands while conducting credential theft and espionage operations underneath. No files were encrypted; the ransomware branding was designed to mislead attribution and distract incident response teams from the actual intrusion objectives. Organizations in the MENA region face elevated risk of undetected long-term compromise, as responding to a ransomware narrative may cause security teams to miss the credential theft and persistence activity that represents the true damage.

Technical Analysis

MuddyWater (MITRE G0069, also tracked as TEMP.Zagros and Static Kitten) conducted an intrusion campaign deploying Chaos ransomware as a false flag. Despite rendering ransom notes to victims, no file encryption occurred. Actual objectives included credential harvesting (T1003), persistence via scheduled tasks (T1053) and service creation (T1543), and intelligence collection. Initial access was achieved via spearphishing (T1566) and valid account abuse (T1078). Masquerading (T1036) and the ransomware branding (T1486 used as deception rather than destructive payload) served to complicate attribution. A February 2026 campaign documented by The Hacker News extended MuddyWater's toolset with GhostFetch and CHARUSERAGENT against MENA targets. Relevant weaknesses include CWE-506 (embedded malicious code) and CWE-287 (improper authentication, consistent with credential abuse). No CVE is associated with this campaign; exploitation relied on tradecraft rather than a specific software vulnerability.

Action Checklist

1. Containment: If MuddyWater activity is suspected, isolate affected hosts from the network immediately and revoke active sessions for accounts present on those systems. Prioritize hosts where scheduled tasks or new services were created in the relevant timeframe. Do not treat this as a standard ransomware containment; assume credential theft has occurred and treat all credentials on affected hosts as compromised.
2. Detection: Hunt for Chaos ransomware artifacts (ransom note file creation, known Chaos hashes from available threat intelligence feeds) alongside credential access indicators: LSASS access events (Event ID 4656, 4663 on Windows), suspicious scheduled task creation (Event ID 4698), and new service installs (Event ID 7045). Look for CHARUSERAGENT and GhostFetch IOCs per The Hacker News February 2026 reporting. Cross-reference outbound connections against known MuddyWater C2 infrastructure documented in MITRE ATT&CK G0069. Flag any PowerShell or script execution originating from phishing email attachment chains.
3. Eradication: Remove all persistence mechanisms: audit and delete unauthorized scheduled tasks, services, and startup entries on affected hosts. Rotate all credentials present on compromised systems, including service accounts. Remove Chaos ransomware components and any identified MuddyWater tooling. Re-image hosts where deep persistence (e.g., kernel-level implants) cannot be ruled out.
4. Recovery: Before restoring operations, validate that no unauthorized accounts or backdoor credentials remain. Monitor for re-access attempts using previously stolen credentials against VPN, email, and remote access infrastructure. Confirm that no exfiltration channels (C2 callbacks, DNS tunneling, cloud storage uploads) remain active. Establish a 30-day enhanced monitoring window on previously affected systems and accounts.
5. Post-Incident: This campaign exploited the gap between ransomware response playbooks and espionage intrusion response. Conduct a tabletop exercise that incorporates false flag scenarios. Review whether your ransomware playbook includes credential theft and persistence hunting as parallel workstreams, not sequential steps. Assess email gateway controls against spearphishing (T1566) and review privileged account hygiene to reduce valid account abuse (T1078) exposure.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if any evidence of successful credential exfiltration is confirmed (Event ID 4648 showing lateral movement to privileged systems, or C2 callbacks containing encoded credential material), if affected systems process PII or PHI triggering breach notification obligations under applicable MENA or EU regulatory frameworks, or if the organization lacks the internal capability to perform memory forensics required to distinguish false flag ransomware artifacts from actual encryption activity.

Recovery Notes	Do not restore any affected host from backup without first validating the backup predates the earliest identified MuddyWater access event — given the group's documented long-dwell espionage objectives (MITRE ATT&CK G0069), assume the intrusion predates the Chaos ransomware deployment by weeks to months, meaning recent backups may contain persistence mechanisms. Enforce MFA on all externally-accessible services (VPN, email, remote desktop) before restoring network connectivity, as stolen credentials are the primary re-entry vector for MuddyWater follow-on operations. Maintain enhanced monitoring via Sysmon, Windows Security Event Log alerting on Event ID 4648 and 4698, and DNS query logging for a minimum of 30 days post-recovery, with particular attention to the compromised account list being used against any infrastructure not yet identified as affected.
Forensic Artifacts	Windows Security Event Log (Security.evtx) — Event ID 4656 and 4663 (LSASS handle requests indicating credential dumping), Event ID 4698 (scheduled task creation used by MuddyWater for persistence), and Event ID 4648 (explicit credential logon indicating lateral movement using stolen credentials from the compromised host) | Memory image of affected hosts captured pre-isolation — MuddyWater implants including PowGoop loader, Canopy/Starwhale backdoor, and PhonyC2 or GhostFetch components will reside in process memory and are the primary forensic artifact for identifying the espionage toolchain operating beneath the Chaos ransomware false flag | Chaos ransomware ransom note files and any files with the Chaos-characteristic 'AAAAA' extension appended — critically, the absence of corresponding encrypted file content (files renamed but not encrypted) is itself a false flag indicator that must be documented as evidence of the deception tactic | PowerShell ScriptBlock logs (Microsoft-Windows-PowerShell/Operational, Event ID 4104) — MuddyWater consistently uses PowerShell-based download cradles and obfuscated execution for tool delivery (MITRE ATT&CK G0069, T1059.001); these logs capture the decoded script content even when invocation used obfuscation | DNS resolver query logs and Sysmon Event ID 22 (DNS Query) — GhostFetch and MuddyWater C2 infrastructure identified in MITRE ATT&CK G0069 communicates via DNS-based channels; query logs will reveal C2 domain lookups that persist as evidence of active beaconing even after the Chaos ransomware artifacts have been removed

Per-Action IR Details

Containment — If MuddyWater activity is suspected, isolate affected hosts from the network immediately and revoke active sessions for accounts present on those systems. Prioritize hosts where scheduled tasks or new services were created in the relevant timeframe. Do not treat this as a standard ransomware containment; assume credential theft has occurred and treat all credentials on affected hosts as compromised.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Use 'netsh advfirewall firewall add rule name=ISOLATE dir=in action=block' and 'netsh advfirewall firewall add rule name=ISOLATE dir=out action=block' on affected Windows hosts to achieve network isolation without enterprise NAC. Run 'query session /server:' and 'logoff ' to terminate active RDP sessions. Use 'net user /active:no' to immediately disable accounts identified on compromised hosts. For service account rotation without a PAM tool, script password resets via 'Set-ADAccountPassword' in PowerShell across all identified accounts simultaneously.

Evidence: Before isolating, capture a full memory image using Magnet RAM Capture or WinPmem — MuddyWater tooling including credential-harvesting implants and C2 beaconing agents will reside in memory and will not survive isolation or reboot. Snapshot Windows Security Event Log (Security.evtx) and System Event Log (System.evtx) from the affected host before network cutoff, preserving Event ID 4698 (scheduled task creation), Event ID 7045 (new service installed), Event ID 4624/4625 (logon success/failure), and Event ID 4648 (explicit credential use). Export the

scheduled tasks registry hive at HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks and HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree before any eradication steps touch persistence mechanisms.

Detection — Hunt for Chaos ransomware artifacts (ransom note file creation, known Chaos hashes where available from Rapid7 advisory) alongside credential access indicators: LSASS access events (Event ID 4656, 4663 on Windows), suspicious scheduled task creation (Event ID 4698), and new service installs (Event ID 7045). Look for CHARUSERAGENT and GhostFetch IOCs per The Hacker News February 2026 reporting. Cross-reference outbound connections against known MuddyWater C2 infrastructure documented in MITRE ATT&CK G0069. Flag any PowerShell or script execution originating from phishing email attachment chains.

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 AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity's config (github.com/SwiftOnSecurity/sysmon-config) to capture Event ID 1 (Process Creation), Event ID 3 (Network Connection), Event ID 10 (ProcessAccess targeting lsass.exe), and Event ID 11 (FileCreate for ransom note drops). Use the following PowerShell one-liner to hunt scheduled task anomalies created in a specific timeframe: 'Get-ScheduledTask | Where-Object {$_.Date -gt (Get-Date).AddDays(-30)} | Select TaskName, TaskPath, Date | Export-CSV suspicious_tasks.csv'. Write a YARA rule targeting the Chaos ransom note string patterns (e.g., 'AAAAA' extension marker and hardcoded ransom note text) and scan all hosts using YARA standalone binary. Use Wireshark or tcpdump with a BPF filter for known MuddyWater C2 IP ranges from MITRE ATT&CK G0069 to detect active beaconing before full isolation.

Evidence: The critical forensic distinction for this campaign is that Chaos ransomware artifacts (ransom note files, renamed file extensions) will be present WITHOUT corresponding encrypted file content — this asymmetry is itself a false flag indicator. Collect Windows Prefetch files from C:\Windows\Prefetch\ for any MuddyWater-associated executables (historically: PowGoop, Canopy/Starwhale, PhonyC2 components) to establish execution timeline. Pull PowerShell ScriptBlock logging from Microsoft-Windows-PowerShell/Operational event log (Event ID 4104) for obfuscated download cradles consistent with MuddyWater's documented TTPs (MITRE ATT&CK G0069, T1059.001). Capture DNS query logs from the local DNS resolver or endpoint (via Sysmon Event ID 22) to identify C2 domains associated with GhostFetch callbacks. Examine email gateway logs and Outlook attachment cache (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Outlook\) for the phishing delivery vector, preserving original email headers for sender attribution.

Eradication — Remove all persistence mechanisms: audit and delete unauthorized scheduled tasks, services, and startup entries on affected hosts. Rotate all credentials present on compromised systems, including service accounts. Remove Chaos ransomware components and any identified MuddyWater tooling. Re-image hosts where deep persistence (e.g., kernel-level implants) cannot be ruled out.

NIST Phase: Eradication

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Use 'schtasks /query /fo LIST /v > all_tasks.txt' to enumerate all scheduled tasks and diff against a known-good baseline; delete unauthorized entries with 'schtasks /delete /tn /f'. Run 'sc query type= all state= all > all_services.txt' and cross-reference against your software inventory for unauthorized services, removing with 'sc delete '. For credential rotation without an enterprise PAM solution, use a PowerShell script to bulk-reset all Active Directory accounts that authenticated to the compromised host within the incident window, extracting the list via 'Get-ADComputer | Get-ADObject -Properties LastLogonDate'. Scan all hosts with ClamAV using an updated signature database targeting known MuddyWater tool hashes before declaring eradication complete. Do not skip re-imaging for hosts where Sysmon Event ID 10 showed lsass.exe access — credential material is fully compromised on those systems regardless of tooling removal.

Evidence: Before removing any persistence, export the full HKLM\SYSTEM\CurrentControlSet\Services registry hive and HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run hives to document the pre-eradication state for forensic continuity. Preserve copies of all identified MuddyWater tooling (PowGoop loader DLLs, any identified PhonyC2 or GhostFetch binaries) in a password-protected forensic container with SHA-256 hashes recorded — these are intelligence artifacts for threat sharing (MITRE ATT&CK G0069 enrichment) and should not be destroyed. Capture the Windows registry AutoRun locations including HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon (Userinit, Shell values) which MuddyWater has historically abused for persistence alongside scheduled tasks.

Recovery — Before restoring operations, validate that no unauthorized accounts or backdoor credentials remain. Monitor for re-access attempts using previously stolen credentials against VPN, email, and remote access infrastructure. Confirm that no exfiltration channels (C2 callbacks, DNS tunneling, cloud storage uploads) remain active. Establish a 30-day enhanced monitoring window on previously affected systems and accounts.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Run 'Get-ADUser -Filter * -Properties LastLogonDate, PasswordLastSet, Enabled | Where-Object {$_.Enabled -eq $true} | Export-CSV accounts_audit.csv' to enumerate all active accounts and cross-reference against your pre-incident account inventory to identify any backdoor accounts created by MuddyWater during the intrusion. Use osquery with the query 'SELECT username, uid, gid, directory, shell FROM users WHERE uid > 500 AND username NOT IN ()' on Linux/macOS assets to detect unauthorized local accounts. Configure Sysmon Event ID 3 (Network Connection) filters for outbound DNS over non-standard ports (DNS tunneling) and known cloud storage endpoints (OneDrive, Dropbox API endpoints) used as exfil channels — MuddyWater has historically leveraged legitimate cloud services for C2 (MITRE ATT&CK G0069, T1567). Enforce MFA immediately on VPN and email access using available identity provider controls before restoring network connectivity to recovered hosts.

Evidence: Before declaring recovery complete, pull VPN authentication logs and email gateway logs for the 30 days prior to incident discovery and search for logons using the compromised account list — MuddyWater credential theft operations may have established access patterns prior to the Chaos ransomware deployment that constitutes the actual intrusion dwell time. Query DNS resolver logs for any domains matching MuddyWater-associated naming conventions or newly registered domains (less than 30 days old) that received queries from affected hosts during the incident window, as DNS-based C2 may persist through eradication if the implant was not fully identified. Document all artifacts collected throughout the incident in a structured timeline before closing the incident record, per NIST IR-5 (Incident Monitoring) requirements.

Post-Incident — This campaign exploited the gap between ransomware response playbooks and espionage intrusion response. Conduct a tabletop exercise that incorporates false flag scenarios. Review whether your ransomware playbook includes credential theft and persistence hunting as parallel workstreams, not sequential steps. Assess email gateway controls against spearphishing (T1566) and review privileged account hygiene to reduce valid account abuse (T1078) exposure.

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 IR-3 (Incident Response Testing), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Structure the tabletop exercise around a concrete MuddyWater scenario: the initial alert is a Chaos ransomware ransom note, but the inject at the 45-minute mark reveals lsass.exe access events and outbound C2 beaconing that predates the ransom note by 72 hours — teams must pivot from ransomware containment to espionage

intrusion response mid-exercise. Use the MITRE ATT&CK Navigator (attack.mitre.org/groups/G0069/) to build a MuddyWater-specific technique heatmap for the tabletop and for updating detection rules. Review email gateway quarantine logs for spearphishing indicators (T1566.001 — Spearphishing Attachment) specifically filtering for Office document attachments with macro-enabled content (.xlsm, .docm) from external senders targeting leadership or IT staff. Use the Sigma rule repository (github.com/SigmaHQ/sigma) to identify and deploy community rules mapped to MuddyWater TTPs including scheduled task creation and LSASS access patterns.

Evidence: The lessons-learned review must document the specific timeline gap between initial Chaos ransomware artifact creation and the earliest detected MuddyWater credential access event — this delta represents the actual dwell time the false flag operation was designed to obscure and is the primary metric for evaluating detection capability improvement. Preserve the complete incident artifact package (memory images, log exports, malware samples, network captures, timeline) per NIST AU-11 (Audit Record Retention) requirements and submit IOCs (CHARUSERAGENT, GhostFetch hashes, C2 infrastructure) to CISA and relevant ISACs to contribute to collective defense against MuddyWater operations targeting MENA-region organizations.

Detection Guidance

Prioritize behavioral detection over hash-based indicators given MuddyWater's documented tooling updates. Key signals: (1) Ransom note file creation without corresponding file encryption activity, flag any ransomware note drop where volume shadow copy deletion or mass file renaming did not occur. (2) LSASS credential access: Windows Event IDs 4656 and 4663 targeting lsass.exe, or Sysmon Event ID 10 with TargetImage lsass.exe. (3) Scheduled task creation (Event ID 4698) or new service installation (Event ID 7045) from unusual parent processes or user contexts. (4) Spearphishing delivery chains: email gateway logs for attachments executing scripts or spawning PowerShell. (5) Outbound C2 traffic patterns consistent with MuddyWater infrastructure, reference MITRE ATT&CK G0069 for documented C2 domains and IPs, supplemented by February 2026 GhostFetch and CHARUSERAGENT IOCs from The Hacker News reporting. (6) CHARUSERAGENT-specific: hunt for anomalous HTTP user-agent strings in proxy logs documented in the February 2026 threat intelligence reporting. SIEM rule recommendation: correlate ransomware note file creation with absence of mass file modification events within the same host and timeframe as a high-confidence false flag indicator.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See MITRE ATT&CK G0069 for documented MuddyWater C2 infrastructure`	MuddyWater command and control domains — reference ATT&CK G0069 for current list; specific campaign IOCs for GhostFetch and CHARUSERAGENT available in The Hacker News February 2026 reporting	MEDIUM
HASH	`Not published in available sources at time of configuration`	Chaos ransomware sample hashes from this campaign not confirmed in available T3 sources; request from Rapid7 directly via their advisory	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1003** — OS Credential Dumping
- **T1486** — Data Encrypted for Impact
- **T1053** — Scheduled Task/Job
- **T1036** — Masquerading
- **T1543** — Create or Modify System Process
- **T1566** — Phishing

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

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
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1003	OS Credential Dumping	Credential-Access
T1486	Data Encrypted for Impact	Impact
T1053	Scheduled Task/Job	Execution
T1036	Masquerading	Defense-Evasion
T1543	Create or Modify System Process	Persistence
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
gemini	https://www.scmagazine.com/news/ransomware/iranian-threat-group-use...	T3
MuddyWater Targets MENA Organizations with GhostFetch, CHAR ...	https://thehackernews.com/2026/02/muddywater-targets-mena-organizat...	T3
Is Your Organization Safe from MuddyWater's Attacks? - Vectra AI	https://www.vectra.ai/modern-attack/threat-actors/muddywater	T3
Iranian APT Intrusion Masquerades as Chaos Ransomware Attack	https://www.securityweek.com/iranian-apt-intrusion-masquerades-as-c...	T3
MuddyWater - MITRE ATT&CK®	https://attack.mitre.org/groups/G0069/	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 2026-05-08 19:03 UTC by TJS Security Command Center