INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 17:21 UTC

Iran Multi-Actor Cyber Campaign Following Military Operations [SCC-2026-0005]

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0003
Type	Threat Campaign
Severity	HIGH
Published	20260304

Executive Summary

Following escalating military operations in the region during early March 2026, multiple Iran-linked and Iran-adjacent threat actors activated coordinated cyber operations targeting organizations perceived as aligned with U.S. or Israeli interests. The campaign spans DDoS disruption, malicious mobile applications for intelligence collection, and Sicarii ransomware, which has a confirmed no-decryption defect meaning payment does not result in data recovery. Organizations with Middle East operations or government/defense relationships face the highest exposure.

Technical Analysis

Following escalating regional military operations in early March 2026, multiple Iran-linked and Iran-adjacent threat actors activated coordinated cyber operations against organizations perceived as aligned with U.S. or Israeli interests. Three distinct threat vectors have been confirmed:nn1. DDoS Operations: Large-scale volumetric attacks targeting government, financial, and media organizations. Attribution to Iran-affiliated hacktivist networks (medium confidence). TTPs: T1498 (Network Denial of Service).nn2. Malicious Mobile Applications: Trojanized apps distributed via unofficial channels targeting Android users, collecting location data, contacts, and communications. Assessed as intelligence collection operation. TTPs: T1204.002 (User Execution: Malicious File), T1430 (Location Tracking).nn3. Sicarii Ransomware: A financially motivated ransomware group operating in parallel with the campaign. Critical characteristic: Sicarii has a confirmed no-decryption defect, payment does not result in decryption. This is documented in incident response reports from this campaign window. TTPs: T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery).nnThe three vectors serve different objectives (disruption, collection, financial) suggesting coordination between distinct actor clusters under a shared operational directive.

Action Checklist

1. 1. Activate or verify DDoS protection service is active with current upstream escalation contacts
2. 2. Issue employee advisory: elevated social engineering and malicious app risk, do not download apps from unofficial sources
3. 3. Review MDM app inventory for unauthorized or sideloaded Android applications on enrolled devices
4. 4. For organizations with Middle East operations or government/defense relationships: brief leadership on elevated campaign risk and activate enhanced monitoring posture
5. 5. Hunt for indicators of Sicarii ransomware precursor activity: unusual volume shadow copy deletion (vssadmin delete shadows), rapid file enumeration across network shares, lateral movement from a single compromised workstation
6. 6. If ransomware incident occurs during this campaign window: do NOT pay, Sicarii has a confirmed no-decryption defect. Engage IR immediately and prioritize backup recovery.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm immediately upon confirmed ransomware execution or sustained DDoS attack exceeding 5 Gbps, or if lateral movement/VSS deletion is confirmed on more than one workstation.
Recovery Notes	Post-containment: verify all backups are unencrypted and isolated from production network during restoration. Patch all identified compromise vectors (vulnerable apps, weak credentials, unpatched systems). Conduct full network rescan for lateral movement artifacts and persistence mechanisms (scheduled tasks, registry run keys, startup folders). Brief employees on what compromise occurred (transparent communication reduces secondary attacks). Re-enable normal monitoring thresholds 7 days after last confirmed indicator of compromise.
Forensic Artifacts	Windows Event ID 4688 (Process Creation) with focus on vssadmin.exe, wmic.exe, psexec.exe, net.exe, cmd.exe, powershell.exe commands | Windows Event ID 3389 (RDP session reconnection) and Security Event ID 4624 (successful logon) with unusual source IPs or timestamps | Windows Event ID 5145 (network share object access) showing high-frequency enumeration from single source | Volume Shadow Copy (VSS) deletion logs and Registry hive (SYSTEM, SOFTWARE) for persistence indicators and last execution timestamps | Filesystem timeline (mtime/atime/ctime) of encrypted files, ransom note, and file extension pattern correlation to Sicarii variant

Per-Action IR Details

1. Activate or verify DDoS protection service is active with current upstream escalation contacts

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase)

Controls: NIST SC-7 (boundary protection), CIS 12.6.1 (DDoS mitigation)

Compensating: If no DDoS service: configure rate-limiting on edge routers (Cisco, Juniper native ACLs), enable GeoIP filtering to block traffic from sanctioned regions, document ISP upstream contact and escalation procedure in runbook with response SLA. Test failover to backup ISP if available.

Evidence: Capture baseline DDoS service configuration (rules, thresholds, logging level) and current upstream contact list before activation. Record NetFlow/sFlow baseline during non-attack period for comparison. Screenshot DDoS service status dashboard and verify logging is writing to syslog or SIEM.

2. Issue employee advisory: elevated social engineering and malicious app risk, do not download apps from unofficial sources

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (awareness and training)

Controls: NIST AT-2 (security awareness and training), CIS 17.7 (phishing and social engineering)

Compensating: Teams without formal comms infrastructure: use email distribution list + chat system notice (Slack, Teams, email) signed by CISO or IR lead. Include: (a) indicator — 'Do not download [specific app names if known]', (b) safe behavior — 'Apps only from official app store with MDM enrollment', (c) reporting — 'Report suspicious apps to [email/ticket system]'. Document timestamp and distribution list in incident log.

Evidence: Archive the advisory text (email headers, timestamp, recipients) in incident folder. Capture employee acknowledgment logs if platform supports read receipts. If phishing emails are observed, preserve full headers and body for forensic correlation to campaign actors.

3. Review MDM app inventory for unauthorized or sideloaded Android applications on enrolled devices

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (detection and analysis)

Controls: NIST SI-7 (software, firmware, and information integrity), CIS 10.1 (mobile device inventory)

Compensating: Without MDM: query Android devices via ADB (Android Debug Bridge) over USB on management workstation. Run 'adb shell pm list packages -3' to enumerate third-party apps; compare against approved list. Export device inventory via manual survey (device name, Android version, installed apps) to CSV. For enterprises, use free tier of Google Play Console to verify app signatures of suspicious packages against known malicious app hashes.

Evidence: Export MDM app inventory report with device ID, app name, app version, installation source (Play Store vs. sideloaded), and installation timestamp. If possible, capture APK file hash (SHA-256) of suspicious apps for malware analysis. Preserve MDM audit logs showing app installation events for 90 days prior to advisory issuance.

4. For organizations with Middle East operations or government/defense relationships: brief leadership on elevated campaign risk and activate enhanced monitoring posture

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation and management approval)

Controls: NIST IR-1 (incident response policy), CIS 19.1 (incident response planning)

Compensating: Document risk briefing in writing (email or memo) with: (a) threat summary (Iran-linked actors, DDoS + malware + ransomware), (b) your org's exposure (Middle East ops, defense/government ties), (c) required actions (enhanced monitoring, IR activation, contact escalation), (d) decision point (approve or defer monitoring uplift). Distribute to C-level and department heads; retain signed approval in incident folder.

Evidence: Preserve briefing slides or memo with approval date/signature. Establish baseline for 'enhanced monitoring': define which logs, sensors, or alerts will be elevated (e.g., all outbound DNS to suspicious domains, all RDP/SSH logins, all file share access). Document baseline alert volume and threshold for escalation before uplift begins.

5. Hunt for indicators of Sicarii ransomware precursor activity: unusual volume shadow copy deletion (vssadmin delete shadows), rapid file enumeration across network shares, lateral movement from a single compromised workstation

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (analysis techniques and tools)

Controls: NIST AU-12 (audit generation), CIS 8.5 (endpoint detection and response)

Compensating: No EDR/SIEM: (1) VSS deletion — Enable Windows Event Log 'System' and audit process creation (Audit Policy > Detailed Tracking > Process Creation). Hunt for 'vssadmin.exe delete shadows' in Event ID 4688 (Process Create); export to CSV with timestamp, user, command line. (2) File enumeration — Enable network share audit (Share Properties > Auditing > Object Access). Look for Event ID 5145 with high frequency from single source IP.

(3) Lateral movement — Check Windows Event ID 4688 (process create) and 3389 (RDP) for parent process cmd.exe or powershell.exe spawning network tools (psexec, wmic, net use). Create hunt query/report run weekly during campaign window.

Evidence: Preserve Windows Event Logs (System, Security, Application) for 90 days minimum (configure log retention before hunt begins). Capture network share access logs and SMB connection logs if available. Document exact timestamps, usernames, source IPs, and command lines for any VSS deletion, share enumeration, or lateral movement commands. If found, isolate system immediately and preserve forensic image.

6. If ransomware incident occurs during this campaign window: do NOT pay, Sicarii has a confirmed no-decryption defect. Engage IR immediately and prioritize backup recovery.

NIST Phase: Containment | Recovery

Reference: NIST 800-61r3 §3.3 (containment), §3.4 (eradication), §3.5 (recovery)

Controls: NIST IR-4 (incident handling), IR-6 (incident reporting), CIS 11.3 (data recovery capability)

Compensating: Incident response without external firm: (1) Containment — Isolate affected device(s) from network immediately (unplug Ethernet, disable WiFi). DO NOT restart or shut down yet; preserve RAM for memory dump. (2) Evidence — Capture forensic image of affected drive using write-blocker and free tool (Guacamole DDRescue, FTK Imager Lite, or dd on Linux). (3) Recovery — Wipe affected device(s) and restore from verified clean backup dated before first signs of compromise. Test backup integrity before restoring (verify file checksums, sample-open documents). Document timeline and decision not to pay in incident log. Notify law enforcement (FBI IC3, CISA) per org policy.

Evidence: Preserve disk image, memory dump (if possible), file system timeline (mtime/atime/ctime), Registry hives (if Windows), Prefetch files, MFT (Master File Table), and event logs from moment of detection. Document exact encryption file extension and ransom note content for threat intelligence correlation. Capture network traffic (pcap) during and before encryption onset if SIEM or IDS captures available.

Detection Guidance

DDoS: Monitor for abnormal inbound traffic spikes at the network perimeter. Verify DDoS protection service is active and has current contact information for escalation.nnMobile: Flag any corporate-enrolled Android devices that have sideloaded applications outside approved channels. Review MDM app inventory for unknown or unverified applications.nnSicarii Ransomware Precursor: Look for mass volume shadow copy deletion (vssadmin delete shadows), rapid sequential file access across network shares, and unauthorized RDP or SMB lateral movement in a short window.

Indicators of Compromise

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\Temp\*.exe`	Iranian threat actors frequently drop payloads and tools in Windows Temp directory for staging, particularly when executed by suspicious parent processes (cmd.exe, powershell.exe, or Office applications) or when filenames match known malware families; legitimate software rarely executes unsigned binaries from Temp with obfuscated names, so look for process creation events with Temp-sourced executables lacking proper code signatures, unusual parent-child process chains, and execution patterns occurring outside normal software installation windows.	MEDIUM
FILE_PATH	`C:\ProgramData\*.dll`	Suspicious .dll files in C:\ProgramData\ are indicative of post-exploitation persistence when they are unsigned, lack legitimate vendor provenance, or are spawned by non-system processes (cmd.exe, powershell.exe, rundll32.exe); legitimate software rarely uses unsigned DLLs in this shared directory, and EDR should flag unsigned binaries in ProgramData combined with execution from rundll32 or registry run key references as high-confidence indicators of MuddyWater and APT33 loader deployment.	MEDIUM
FILE_PATH	`C:\Users\Public\*.ps1`	PowerShell scripts dropped in public directories used for lateral movement and execution by Iranian actors	MEDIUM
REGISTRY_KEY	`HKCU\Software\Microsoft\Windows\CurrentVersion\Run\*`	Persistence mechanism used by Iranian APT groups including MuddyWater and APT35 for maintaining access	HIGH
REGISTRY_KEY	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\*`	Used by Iranian actors for persistence and defense evasion via debugger hijacking	MEDIUM
REGISTRY_KEY	`HKCU\Software\Microsoft\Office\*\Excel\Security\AccessVBOM`	Modified to enable macro execution, associated with Iranian spearphishing campaigns using malicious Office documents	MEDIUM
URL	`https://*/upload.php`	Common C2 exfiltration endpoint pattern observed in Iranian-linked webshell and RAT campaigns	MEDIUM

Type	Value	Context	Confidence
URL	`https://*/panel/index.php`	C2 panel URL pattern associated with Iranian threat actor infrastructure	MEDIUM
FILE_PATH	`C:\Windows\System32\Tasks\*`	Scheduled tasks created by Iranian APT groups for persistence, often mimicking legitimate Windows task names	HIGH
FILE_PATH	`%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\*.lnk`	LNK file persistence mechanism used by MuddyWater and related Iranian threat clusters	MEDIUM
FILE_PATH	`C:\Windows\SysWOW64\*.dat`	Encoded payload storage location used by Iranian actors to evade detection	MEDIUM
FILE_PATH	`\\*\ADMIN$\*.exe`	SMB-based lateral movement path used during Iranian military-targeted intrusion campaigns	MEDIUM
FILE_PATH	`C:\Windows\System32\wbem\mofcomp.exe`	WMI-based persistence technique abused by Iranian actors for fileless persistence via MOF files; suspicious when mofcomp.exe is spawned by Office macros, scripts (powershell.exe, cscript.exe, wscript.exe), or from temp/download directories rather than legitimate WMI compilation tasks, and differs from legitimate use where mofcomp.exe is rarely invoked directly by end-user processes or scheduled tasks without administrator oversight. Hunt for mofcomp.exe process execution with parent processes excluding wmiprvse.exe or svchost.exe, command-line arguments referencing .mof files in user-writable paths, and correlate with WMI Event Consumer creation events in Windows Event Log (Event ID 5861).	MEDIUM
FILE_PATH	`%TEMP%\~*.tmp`	Temporary file staging pattern associated with Iranian dropper and loader activity	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1498** — Network Denial of Service
- **T1486** — Data Encrypted for Impact
- **T1204.002** — Malicious File
- **T1490** — Inhibit System Recovery

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1498	Network Denial of Service	Impact
T1486	Data Encrypted for Impact	Impact
T1204.002	Malicious File	Execution
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
CISA Advisory AA22-320A - Iranian Government-Sponsored APT Actors Compromise Federal Network	https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a	T1
CISA Advisory AA21-321A - Iranian Government-Sponsored Cyber Actors	https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a	T1
CISA Advisory AA23-320A - Scattered Spider Threat Actor	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a	T1

Source	URL	Tier
Microsoft Threat Intelligence - MERCURY and DEV-1084 Iran Linked Actors	https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-an...	T1
CISA Iran Cyber Threat Overview and Advisories	https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-sta...	T1
Mandiant APT33 Profile - Iranian Cyber Espionage	https://www.mandiant.com/resources/apt33-insights-into-iranian-cybe...	T3
MITRE ATT&CK - MuddyWater (G0069)	https://attack.mitre.org/groups/G0069/	T3
MITRE ATT&CK - APT33 (G0064)	https://attack.mitre.org/groups/G0064/	T3
MITRE ATT&CK - APT35 (G0059)	https://attack.mitre.org/groups/G0059/	T3
NSA/CISA Joint Advisory - Iranian State Actors Conduct Cyber Operations Against Defense	https://media.defense.gov/2022/Sep/12/2003091798/-1/-1/0/CSA_IRGC_A...	T1
Crowdstrike 2023 Global Threat Report - Iranian Nexus Threat Actors	https://www.crowdstrike.com/global-threat-report/	T3
Recorded Future - Iranian Threat Actor Targeting of Military Organizations	https://www.recordedfuture.com/research/iranian-cyber-operations	T3

Generated 2026-03-29 17:21 UTC by TJS Security Command Center