INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-30 19:06 UTC

Iranian APT 'Screening Serpens' Deploys Six New RAT Variants Targeting US, Israel, and UAE

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0385
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Organizations in defense, aerospace, technology, and critical infrastructure sectors in the United States, Israel, and United Arab Emirates
Published	2026-05-30
Discovery Source	Gemini

Executive Summary

Iranian APT group Screening Serpens (also tracked as UNC1549 and Smoke Sandstorm) has deployed six new remote access Trojans in an active espionage campaign targeting defense, aerospace, technology, and critical infrastructure organizations in the United States, Israel, and the United Arab Emirates. The campaign uses job-themed spearphishing and cloud-based command-and-control infrastructure, consistent with this actor's established tradecraft. Organizations in targeted sectors face elevated risk of long-term network compromise, intellectual property theft, and theft of military operational data and personnel records.

Technical Analysis

Attribution source: Palo Alto Networks Unit 42, with pending primary report publication (as of configuration date 2026-03-04; secondary corroboration from industry threat advisories and reporting). The campaign is attributed to Screening Serpens, which overlaps with UNC1549, Smoke Sandstorm, and the Iranian Dream Job cluster. Tradecraft aligns with prior UNC1549 activity: job-themed spearphishing lures (T1566.001), use of legitimate cloud services for C2 (T1102), ingress tool transfer (T1105), and command execution via scripting interpreters (T1059). Masquerading (T1036) and obfuscation (T1027) are used to evade detection. Valid account abuse (T1078) and standard application layer protocols for C2 (T1071.001) round out the observed technique set. Six new RAT variants were reportedly deployed February through April 2026. Specific variant names, capabilities, persistence mechanisms, and C2 infrastructure are not confirmed from available raw data; Unit 42 primary report verification is pending. Prior UNC1549 tooling includes MINIBIKE and MINIBUS backdoors. No CVE or CWE identifiers apply to this campaign-level item. CVSS base score of 8.1 reflects assessed campaign severity,

not a specific vulnerability. Confidence in actor attribution: medium, pending confirmation from Palo Alto Networks Unit 42 primary report publication. Confidence in six-variant claim: low-to-medium pending primary report verification.

Action Checklist

1. Step 1: Containment, Identify and isolate endpoints in defense, aerospace, technology, and critical infrastructure business units that have received unsolicited job-offer communications via email or LinkedIn-equivalent platforms since February 2026. Block or monitor (depending on operational dependencies) known UNC1549-associated cloud C2 providers (Microsoft OneDrive, Dropbox, and similar platforms used as C2 relay points per prior UNC1549 reporting) at egress, with escalation criteria and business continuity validation before implementation. Apply NIST AC-4 (Information Flow Enforcement) to restrict outbound connections from high-risk endpoints to unapproved cloud storage destinations.
2. Step 2: Detection, Search email gateways and endpoint logs for job-themed lure documents (T1566.001) targeting employees in cleared, engineering, or executive roles. Query EDR telemetry for scripting interpreter execution (T1059) originating from document viewers or browser processes. Hunt for outbound connections to cloud hosting infrastructure (T1102) from systems that do not have a business need for those services. Review AU-6 (Audit Record Review) findings for anomalous after-hours access patterns and lateral movement indicators. Apply CIS 8.2 (Collect Audit Logs) verification; confirm logging is active across email, endpoint, and network egress tiers.
3. Step 3: Eradication, For confirmed compromised hosts, terminate identified RAT processes and remove persistence mechanisms (startup entries, scheduled tasks, registry run keys) per incident response playbook. Rotate all credentials for accounts active on compromised systems per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Revoke and reissue any API keys or service account tokens present on affected endpoints. Block identified C2 domains and IPs at perimeter once Unit 42 IOC list is confirmed from primary report.
4. Step 4: Recovery, Validate clean state via EDR full-disk scan and network traffic baseline comparison before returning systems to production. Monitor reinstated systems for 30 days with elevated logging verbosity per AU-12 (Audit Record Generation). Confirm MFA is enforced on all externally exposed applications and VPN access per CIS 6.3 and CIS 6.4 before restoring remote access. Verify no residual scheduled tasks, WMI subscriptions, or service entries remain from pre-remediation state.
5. Step 5: Post-Incident Review and Continuous Improvement, Review spearphishing awareness training currency for employees in targeted roles (cleared personnel, recruiters, engineers) per NIST AT controls. Assess whether cloud egress monitoring and DLP policies adequately cover UNC1549's known C2 abuse of legitimate cloud platforms. Map gaps to CIS 7.1 (Vulnerability Management Process) and update threat model to reflect Iranian state-sponsored targeting of your sector. Submit indicators to CISA and relevant ISACs to support community-wide detection.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and government liaison (DSS/DCSA if defense contractor, CISA if critical infrastructure) immediately upon confirmation of any successful RAT installation, credential access, or data staging activity — active Iranian state-sponsored espionage targeting cleared personnel or controlled unclassified information (CUI) triggers mandatory reporting obligations under DFARS 252.204-7012, CMMC, and applicable sector-specific regulations.
Recovery Notes	Before returning any compromised system to production, verify that all six RAT variant process signatures are absent via YARA scan, all cloud-storage-based C2 communication paths are blocked or monitored at egress, and all credentials authenticated on the system since February 2026 have been rotated — UNC1549 is known to harvest credentials for follow-on operations separate from the initial RAT implant. Maintain elevated Sysmon logging and DNS query capture for a minimum of 30 days post-recovery, with weekly Autoruns diff comparisons against the clean baseline, as this actor has demonstrated multi-stage persistence resilience in prior campaigns against defense and aerospace targets. Any recurrence of outbound API calls to OneDrive or Dropbox from non-browser processes during the monitoring window should be treated as a new incident, not a remediation failure.
Forensic Artifacts	Cloud C2 API beaconing records: Zeek or proxy logs showing periodic HTTP/S POST requests from non-browser processes to api.onedrive.com, api.dropbox.com, or content.dropboxapi.com — UNC1549 RAT variants use legitimate cloud storage APIs as C2 relay points, producing a distinctive regular-interval beaconing pattern distinguishable from normal Office 365 or OneDrive sync client traffic by process context and User-Agent string. | Spearphishing lure delivery artifacts: Email gateway message trace logs and attachment hashes for job-themed messages targeting cleared personnel, engineers, or executive roles since February 2026; file system artifacts in user Downloads and %TEMP% directories including LNK, MSIX, ISO, or PDF files with hashes matchable against Unit 42 and Mandiant IOC releases for this Screening Serpens campaign. | RAT persistence mechanism artifacts: Registry exports of HKCU and HKLM Run/RunOnce keys, schtasks /query /xml full output, and WMI EventFilter/EventConsumer subscription inventory — UNC1549 RAT variants have used scheduled tasks with encoded PowerShell payloads and registry run keys pointing to %APPDATA% or %TEMP% staging directories as primary persistence mechanisms. | Credential access indicators: Windows Security Event ID 4648 (Logon with explicit credentials) and 4624 Type 3 (Network logon) records from compromised hosts in the period following initial RAT execution — UNC1549 conducts credential harvesting alongside RAT implantation, and lateral movement attempts using harvested credentials will appear as network logons from the compromised host to other internal systems. | Process execution chain evidence: Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connection) logs showing the full execution chain from lure document opener (Word, Acrobat, Edge) through scripting interpreter invocation (PowerShell, WScript, cmd.exe) to the RAT process establishing its first outbound connection to cloud C2 infrastructure — this chain is the primary forensic evidence tying the initial spearphish to the confirmed compromise.

Per-Action IR Details

Step 1: Containment — Identify and isolate endpoints in defense, aerospace, technology, and critical infrastructure business units that have received unsolicited job-offer communications via email or LinkedIn-equivalent platforms since February 2026. Block known UNC1549-associated cloud C2 providers (Microsoft OneDrive, Dropbox, and similar platforms used as C2 relay points per prior UNC1549 reporting) at egress if operationally feasible, pending scoping. Apply NIST AC-4 (Information Flow Enforcement) to restrict outbound connections from high-risk endpoints to unapproved cloud storage destinations.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On endpoints without EDR: run `netstat -ano` to identify active outbound connections to OneDrive (*.sharepoint.com, onedrive.live.com) and Dropbox (*.dropbox.com, *.dropboxstatic.com) and cross-reference PIDs against running processes via `tasklist /v`. Block egress with Windows Firewall using `netsh advfirewall firewall add rule name='Block UNC1549 C2 Cloud' dir=out action=block remotehost=*.onedrive.com,*.dropbox.com` (enumerate full IP ranges via nslookup). On Linux hosts use `iptables -A OUTPUT -d -j DROP`. For network-layer blocking without a next-gen firewall, push DNS sinkholes for known UNC1549 cloud relay domains via your internal DNS server (bind or Windows DNS RPZ).

Evidence: Before isolating, capture: (1) Full memory dump of suspect endpoint using WinPmem or `procdump -ma` targeting any process with an established connection to OneDrive/Dropbox API endpoints — UNC1549 RAT variants stage payloads and receive tasking via cloud storage APIs, so the RAT process will hold decryption keys and C2 session state in memory. (2) `netstat -ano` output with timestamps showing established outbound sessions to cloud relay IPs. (3) Browser or Office process handles — UNC1549 lures have used weaponized MSIX or LNK files delivered via job-themed PDFs, so capture open file handles via `handle.exe -p ` before termination. (4) Prefetch files from `C:\Windows\Prefetch\` for any processes that executed from %TEMP%, %APPDATA%, or user Downloads directories within the spearphishing window.

Step 2: Detection — Search email gateways and endpoint logs for job-themed lure documents (T1566.001) targeting employees in cleared, engineering, or executive roles. Query EDR telemetry for scripting interpreter execution (T1059) originating from document viewers or browser processes. Hunt for outbound connections to cloud hosting infrastructure (T1102) from systems that do not have a business need for those services. Review AU-6 (Audit Record Review) findings for anomalous after-hours access patterns and lateral movement indicators. Apply CIS 8.2 (Collect Audit Logs) verification — confirm logging is active across email, endpoint, and network egress tiers.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM: (1) Deploy Sysmon with SwiftOnSecurity config and filter Event ID 3 (Network Connection) for destination hostnames matching `*onedrive*`, `*dropbox*`, `*sharepoint*`, `*github*` from parent processes of Word, Acrobat, or Edge/Chrome (UNC1549 delivery chain). (2) Use Sigma rule `proc_creation_win_susp_shell_spawn_from_office.yml` converted to native Windows Event Log queries: query Windows Security Log Event ID 4688 (Process Creation) for `cmd.exe`, `powershell.exe`, or `wscript.exe` where `ParentProcessName` matches `WINWORD.EXE`, `AcroRd32.exe`, or `msedge.exe`. (3) For email hunting without a gateway search tool: use PowerShell `Search-Mailbox` or `Get-MessageTrace` (Exchange Online) filtering on subject keywords: 'opportunity', 'position', 'recruiter', 'cleared', 'defense contractor', 'aerospace' with attachments containing `.pdf`, `.lnk`, `.msix`, or `.iso` extensions since February 2026. (4) Use Zeek or Wireshark capture on egress to flag HTTP/S POST requests to `api.onedrive.com` or `api.dropbox.com` from workstations — UNC1549 RATs poll cloud APIs for tasking, producing periodic beaconing intervals detectable as regular outbound POST cadence.

Evidence: Collect before analysis concludes: (1) Email gateway/Exchange message trace logs showing sender domain, attachment hash, and recipient for all job-themed emails since February 2026 — UNC1549 spearphishing uses lookalike domains mimicking defense recruiters and LinkedIn notifications, so extract full headers including `Reply-To` and `Return-Path`. (2) Sysmon Event ID 11 (File Create) and Event ID 15 (FileCreateStreamHash) from user Downloads and %TEMP% directories — MSIX and LNK lures create identifiable file streams. (3) Windows Security Event ID 4688 process creation tree showing any child processes spawned by document viewer processes. (4) DNS query logs from internal resolver or endpoint (Sysmon Event ID 22) for cloud relay domains contacted by non-browser processes — RAT beaconing to OneDrive will appear as repeated DNS queries to `*.sharepoint.com`

from unexpected process contexts. (5) MITRE ATT&CK T1102 (Web Service C2) artifact: HTTP User-Agent strings in proxy or Zeek logs from RAT processes — UNC1549 RAT variants have used custom or spoofed User-Agent strings distinguishable from legitimate Office 365 client traffic.

Step 3: Eradication — For confirmed compromised hosts, terminate identified RAT processes and remove persistence mechanisms (startup entries, scheduled tasks, registry run keys) per incident response playbook. Rotate all credentials for accounts active on compromised systems per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Revoke and reissue any API keys or service account tokens present on affected endpoints. Block identified C2 domains and IPs at perimeter once Unit 42 IOC list is confirmed from primary report.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST CM-7 (Least Functionality), NIST SI-3 (Malware Protection), NIST SI-2 (Flaw Remediation), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise EDR for process termination and persistence removal: (1) Use Autoruns (Sysinternals) to enumerate and compare all persistence locations — `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, Task Scheduler (`schtasks /query /fo LIST /v`), and WMI subscriptions (`Get-WMIObject -Namespace root\subscription -Class __EventFilter`) — against a known-clean baseline. (2) UNC1549 RAT variants have been documented using scheduled tasks and registry run keys for persistence; export current state with `reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run C:\evidence\run_keys_.reg` before deletion. (3) Rotate credentials using AD `Set-ADAccountPassword` for all accounts that authenticated to the compromised host since February 2026 (pull from Security Event ID 4624 logon records). (4) For cloud token revocation: use Azure AD `Revoke-AzureADUserAllRefreshToken` and invalidate any OneDrive OAuth tokens the RAT may have harvested or abused as its C2 transport layer.

Evidence: Capture before eradication actions: (1) Full registry export of Run/RunOnce keys and `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved` — UNC1549 RATs have used these for persistence alongside scheduled tasks. (2) `schtasks /query /xml` full export — document any tasks with actions pointing to %APPDATA%, %TEMP%, or encoded PowerShell commands, which are characteristic of this actor's RAT deployment. (3) WMI subscription inventory via `wmic /namespace:\\root\subscription PATH __EventFilter get *` — document any subscriptions referencing PowerShell or scripting engines, as UNC1549 has leveraged WMI for persistence in prior campaigns. (4) Shadow copy and VSS snapshot status — capture before eradication in case rollback evidence is needed. (5) Full list of OAuth tokens and app registrations accessible from the compromised endpoint, specifically any tokens scoped to OneDrive or SharePoint that the RAT process may have inherited from the logged-on user's browser session.

Step 4: Recovery — Validate clean state via EDR full-disk scan and network traffic baseline comparison before returning systems to production. Monitor reinstated systems for 30 days with elevated logging verbosity per AU-12 (Audit Record Generation). Confirm MFA is enforced on all externally exposed applications and VPN access per CIS 6.3 and CIS 6.4 before restoring remote access. Verify no residual scheduled tasks, WMI subscriptions, or service entries remain from pre-remediation state.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST CP-10 (System Recovery and Reconstitution), NIST SI-3 (Malware Protection), NIST IA-5 (Authenticator Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Without enterprise EDR for clean-state validation: (1) Run YARA rules against full disk targeting known UNC1549/Smoke Sandstorm RAT signatures — cross-reference Mandiant and Unit 42 public YARA releases for this actor. Use `yara -r C:\` and log all hits before releasing the system. (2) Capture a Sysmon baseline for the first

72 hours post-reimaging: any recurrence of Sysmon Event ID 3 network connections to cloud storage APIs from non-browser processes indicates reinfection or a second implant missed during eradication. (3) Validate scheduled tasks and WMI subscriptions again 7 days post-recovery using the same Autoruns export compared via `fc` or `diff` against the post-eradication snapshot — UNC1549 has demonstrated persistence resilience in prior campaigns. (4) For MFA enforcement validation without a commercial IAM dashboard: use Azure AD Sign-In Logs (`Get-AzureADAuditSignInLogs`) to confirm no successful authentications to VPN or externally-exposed apps occurred without MFA claim in the token.

Evidence: Document during recovery for post-incident use: (1) Pre- and post-eradication Autoruns exports in XML format for diff comparison — serves as evidence of successful persistence removal. (2) Network egress baseline: capture 72 hours of DNS query logs and NetFlow/Zeek connection logs post-recovery to establish a clean outbound communication profile; any resumption of periodic POST requests to OneDrive or Dropbox APIs indicates missed implant. (3) Windows Security Event ID 4624/4625 logon success and failure records for the 30-day monitoring window — UNC1549 has conducted credential harvesting alongside RAT deployment, so watch for reuse of compromised credentials from unexpected source IPs. (4) Azure AD Conditional Access and Sign-In logs confirming MFA enforcement is functioning on all accounts restored to these systems.

Step 5: Post-Incident — Review spearphishing awareness training currency for employees in targeted roles (cleared personnel, recruiters, engineers) per NIST AT controls. Assess whether cloud egress monitoring and DLP policies adequately cover UNC1549's known C2 abuse of legitimate cloud platforms. Map gaps to CIS 7.1 (Vulnerability Management Process) and update threat model to reflect Iranian state-sponsored targeting of your sector. Submit indicators to CISA and relevant ISACs to submit indicators to CISA and relevant ISACs to support community-wide detection.

NIST Phase: Post Incident

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

Controls: NIST AT-2 (Literacy Training and Awareness), NIST AT-3 (Role-Based Training), NIST IR-3 (Incident Response Testing), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST PM-16 (Threat Awareness Program), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a formal threat intelligence platform: (1) Submit confirmed IOCs (domains, IPs, file hashes, email sender domains) directly to CISA via the online reporting portal (cisa.gov/report) and to the relevant ISAC — DIBNet for defense industrial base, A-ISAC for aerospace — using their standard IOC submission templates. (2) Create YARA and Sigma rules from confirmed RAT artifacts (file paths, scheduled task names, registry key values, User-Agent strings) and publish to your sector ISAC's sharing channel or to open repositories (GitHub, VirusTotal) to enable community detection. (3) Build a Screening Serpens / UNC1549 threat profile card for your security awareness program: include real examples of job-themed lure themes documented in this campaign (recruiter impersonation, defense contractor job postings), the specific employee roles targeted (cleared personnel, engineers, executives), and the delivery vectors (email attachments, LinkedIn-equivalent platforms) so training is scenario-specific rather than generic phishing awareness. (4) Document DLP policy gaps for cloud egress (OneDrive, Dropbox, SharePoint) — if your DLP cannot inspect or block API-level data exfiltration over legitimate cloud storage protocols, log this as an open risk item with a remediation timeline tied to CIS 7.2.

Evidence: Preserve for lessons learned and regulatory reporting: (1) Full timeline reconstruction from email gateway logs, endpoint Sysmon logs, and network egress logs showing initial lure delivery through C2 establishment — this is required for any CMMC or DoD contractual incident reporting obligations. (2) All confirmed IOCs with first-seen and last-seen timestamps, mapped to MITRE ATT&CK techniques (T1566.001 Spearphishing Attachment, T1059 Command and Scripting Interpreter, T1102 Web Service C2) — formatted for STIX/TAXII sharing with CISA and ISACs. (3) Training records for targeted employee roles prior to the incident — establishes awareness program gap for regulatory and audit purposes. (4) DLP and cloud egress policy documentation as-of the incident date — required to assess whether the UNC1549 cloud C2 technique would have been detectable or blocked under existing controls, and to justify control improvement investments.

Detection Guidance

Detection should focus on three behavioral pillars consistent with UNC1549 tradecraft. First, email-layer detection: flag inbound messages containing job offer language, recruiter impersonation, or aerospace and defense position titles, particularly those with document attachments or links to cloud storage (T1566.001). Second, endpoint behavioral detection: alert on scripting interpreter processes (PowerShell, cmd.exe, wscript.exe) spawned by document viewer or browser parent processes (T1059); flag obfuscated script execution (T1027) and masquerading file extensions (T1036). Third, network-layer detection: alert on non-browser processes initiating HTTPS connections to OneDrive, Dropbox, Google Drive, or similar platforms (T1102, T1071.001); flag large or periodic outbound data transfers to cloud storage endpoints from workstations in sensitive business units (T1105). Specific IOC hashes, domains, and IPs for the six new RAT variants are not yet confirmed from available data. Subscribe to Palo Alto Networks Unit 42 Threat Intelligence feed or check their publications page weekly for release of the primary campaign report containing IOC hashes, domains, and IPs. Apply D3-SFA (System File Analysis) to review startup configuration entries and scheduled tasks on endpoints in targeted sectors. Cross-reference endpoint telemetry against AU-6 (Audit Record Review) findings for accounts exhibiting access patterns inconsistent with job function.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not confirmed from available data`	Unit 42 primary report IOC list for six new RAT variants not yet verified from raw data provided; monitor Unit 42 Threat Intelligence portal for published indicators	LOW

Framework Mappings

MITRE-ATTACK

- **T1036** — Masquerading
- **T1027** — Obfuscated Files or Information
- **T1102** — Web Service
- **T1105** — Ingress Tool Transfer
- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts
- **T1566.001** — Spearphishing Attachment
- **T1071.001** — Web Protocols

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring

- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **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
- **SI-8** — Spam Protection

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1036	Masquerading	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1102	Web Service	Command-And-Control
T1105	Ingress Tool Transfer	Command-And-Control
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access
T1071.001	Web Protocols	Command-And-Control

Sources

Source	URL	Tier
Iran-linked hackers target key US, allied sectors with sophisticated ...	https://www.cybersecuritydive.com/news/iran-cyberattacks-espionage-...	T3
Iran-linked hackers targeted US, Israel and UAE, Palo Alto Networks ...	https://www.yahoo.com/news/world/articles/iran-linked-hackers-targe...	T3
Check Point tracks Iranian password-spraying waves targeting ...	https://industrialcyber.co/threats-attacks/check-point-tracks-irani...	T3
Week 5 Threat Advisory on Iran-Israel-US Conflict - SISA	https://www.sisainfosec.com/blogs/week-5-threat-advisory-on-iran-is...	T3
US mission warns of threats to Jewish, Israeli communities in UAE	https://www.reuters.com/world/middle-east/us-mission-warns-threats-...	T2

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 2026-05-30 19:06 UTC by TJS Security Command Center