INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 14:02 UTC

Iran-Nexus APT Operations Persist and Expand Despite Kinetic Conflict: GreenGolf Targets Critical Infrastructure with Rust-Based Malware

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0252
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Aviation, energy, maritime, and finance sector systems globally; 12,000+ internet-exposed systems across critical infrastructure verticals; US water utilities
Published	2026-05-01T00:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Iran-nexus threat actor GreenGolf, assessed with medium-high confidence as overlapping with MuddyWater/Boggy Serpens, is actively targeting critical infrastructure sectors including energy, aviation, maritime, and finance with newly developed Rust-based malware (LampoRAT and BlackBeard) and exploitation of five unspecified CVEs. Intelligence from Recorded Future assesses any apparent reduction in Iranian cyber activity as a temporary regrouping phase, not a strategic stand-down. Organizations in affected sectors face risk of operational disruption, data theft, and per US government warnings, physical disruption to water and energy infrastructure.

Technical Analysis

GreenGolf (assessed with medium-high confidence as overlapping with MuddyWater/Boggy Serpens) has deployed two novel malware families written in Rust: LampoRAT and BlackBeard (designated by source; no public IOCs released as of report date). Rust-based tooling complicates static analysis and signature-based detection due to the language's unique binary structure and lack of standard runtime artifacts. Five CVEs are being actively exploited across the campaign; specific CVE identifiers were not included in source data and are not fabricated here. Contact Recorded Future or monitor CISA advisories for CVE identifiers expected to be disclosed. Exploitation activity maps to five CWE classes: OS command injection (CWE-78), SQL injection (CWE-89), improper authentication (CWE-287), missing authentication for critical functions (CWE-306), and deserialization of untrusted data (CWE-502). MITRE ATT&CK techniques observed across the campaign

include external remote service exploitation (T1190), valid account abuse (T1078), external remote services (T1133), command-and-control over standard application protocols (T1071, T1071.001, T1071.002), obfuscated files (T1027), data archival (T1560), defense evasion via indicator removal (T1562), web shell deployment (T1505), lateral movement via remote services (T1021), and data encrypted for impact (T1486). Internet-exposed systems across energy, aviation, maritime, and finance verticals represent the primary attack surface. Patch status for the five exploited CVEs cannot be confirmed without specific CVE identifiers; organizations should treat all five CWE classes as active exposure vectors requiring immediate review.

Action Checklist

1. Containment: Audit all internet-exposed systems in energy, aviation, maritime, and finance environments for the five active CWE classes (CWE-78, CWE-89, CWE-287, CWE-306, CWE-502). Temporarily restrict or firewall any externally reachable service that cannot be confirmed as patched or mitigated. Once Recorded Future releases specific CVE identifiers, cross-reference against your asset inventory and prioritize patches for matching products. Prioritize OT/ICS-adjacent and water sector systems given reported physical disruption intent.
2. Detection: Hunt for LampoRAT and BlackBeard indicators: look for Rust binary artifacts (absence of standard C runtime imports, unusual section entropy), anomalous outbound C2 traffic on standard protocols (HTTP/S, DNS per T1071.001/T1071.002), unexpected web shell artifacts (T1505), and new or modified scheduled tasks or services consistent with persistence. Review authentication logs for valid account abuse (T1078) and external remote service access (T1133). Cross-reference endpoint and network telemetry against MITRE techniques T1190, T1036, T1082, T1016, T1105, T1057, and T1498.
3. Eradication: Until specific CVE identifiers are released by Recorded Future or a government advisory, apply vendor patches addressing any known OS command injection, SQL injection, authentication bypass, and deserialization vulnerabilities in all externally facing systems within affected verticals. Remove identified web shells (T1505). Revoke and rotate all credentials associated with any systems showing signs of valid account compromise (T1078).
4. Recovery: Validate that all externally facing services have authentication enforced on critical functions (CWE-306 remediation confirmed). Confirm no residual web shells or implants via EDR and file integrity monitoring. Restore from verified clean backups for any system where LampoRAT or BlackBeard execution is confirmed. Monitor C2 egress paths for 30 days post-remediation.
5. Post-Incident: Conduct a control gap review against NIST SP 800-53 SI-3 (malicious code protection), SI-7 (software and information integrity), and AC-17 (remote access). Document whether the five CWE classes were covered in your last vulnerability scan cycle. Update detection rules and threat intel feeds to track GreenGolf/MuddyWater/Boggy Serpens indicator releases. Revisit your OT/ICS network segmentation posture given the stated physical disruption objective.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISA (via report.cisa.gov) and sector-specific ISAC immediately upon confirmed LampoRAT or BlackBeard execution on any OT/ICS-adjacent system, any evidence of lateral movement from IT to OT network segments, confirmed exploitation of any of the five CWE classes in water, energy, or aviation environments, or discovery of web shells with estimated dwell time exceeding 72 hours — all of which meet CIRCIA reportable incident thresholds and indicate active GreenGolf campaign intrusion with physical disruption potential.
Recovery Notes	Prior to restoring any system where LampoRAT or BlackBeard execution is confirmed, rebuild from a verified clean OS image rather than attempting in-place remediation — Rust-based malware can achieve deep persistence via service installation (T1543) or scheduled tasks (T1053) that survive partial cleanup. Maintain enhanced monitoring on all previously compromised hosts and internet-facing systems for a minimum of 30 days, specifically watching for re-emergence of Rust binary execution from web server process trees, anomalous outbound DNS queries to newly registered domains (GreenGolf C2 infrastructure rotation pattern consistent with MuddyWater operational history), and any unauthenticated access attempts against functions that were previously CWE-306 vulnerable. Given Recorded Future's assessment that reduced Iranian cyber activity represents regrouping rather than stand-down, treat the 30-day post-remediation window as an elevated-threat period and retain the enhanced logging posture established during the incident.
Forensic Artifacts	Rust binary artifacts on disk: PE files in web-accessible directories or system paths with near-empty import tables (absence of MSVCRT/VCRUNTIME imports), PE section entropy >7.2, and embedded Rust runtime strings (e.g., 'rust_begin_unwind', '__rust_alloc', 'panicked at') — primary forensic signature for LampoRAT and BlackBeard on compromised systems | Web server access logs (Apache /var/log/apache2/access.log, Nginx /var/log/nginx/access.log, IIS C:\inetpub\logs\LogFiles\W3SVC**.log) showing URI patterns consistent with CWE-78 exploitation (encoded shell metacharacters %3B %7C %60 in GET/POST parameters) and CWE-89 exploitation (SQL keywords UNION SELECT, OR 1=1, stacked queries with semicolons in parameter fields) during the initial intrusion window | Windows Security Event Log entries: Event ID 4688 (Process Creation with command line logging enabled) showing cmd.exe or powershell.exe spawned by w3wp.exe, httpd.exe, or tomcat processes (T1190 → T1059 execution chain); Event ID 4698/4702 (Scheduled Task Created/Modified) and Event ID 7045 (New Service Installed) for GreenGolf persistence mechanisms (T1053, T1543); Event IDs 4624/4648 for T1078 valid account abuse | Network captures and DNS resolver query logs showing C2 beaconing patterns: regular-interval HTTPS POST requests to non-categorized or newly registered domains (BlackBeard HTTP C2 per T1071.001), high-frequency DNS queries with encoded subdomains consistent with DNS tunneling (LampoRAT DNS C2 per T1071.002), and any outbound connections to port 443 from processes that do not normally generate external traffic (IIS worker process, Java application server) | File system timeline artifacts from web root directories: newly created or modified PHP, ASPX, or JSP files with timestamps correlating to exploitation events in web server access logs (T1505 web shell deployment), combined with inode change times differing from modification times (indicating timestamp manipulation via T1070.006), and file hashes cross-referenced against known MuddyWater/GreenGolf web shell variants documented in prior CISA and Recorded Future advisories

Per-Action IR Details

Containment — Audit all internet-exposed systems in energy, aviation, maritime, and finance environments for the five active CWE classes (CWE-78, CWE-89, CWE-287, CWE-306, CWE-502). Temporarily restrict or firewall any externally reachable service that cannot be confirmed as patched or mitigated. Prioritize OT/ICS-adjacent and water sector systems given reported physical disruption intent.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 12.2 — Establish and Maintain a Secure Network Architecture (IG2/IG3)

Compensating: Run Shodan CLI or Censys to enumerate your own internet-exposed attack surface: `shodan search 'org:"YourOrg" port:80,443,8080,22,23,3389,502,102' --fields ip_str,port,product`. For each exposed service, check vendor advisories against CWE-78 (OS command injection), CWE-89 (SQLi), CWE-287 (authentication bypass), CWE-306 (missing auth on critical function), and CWE-502 (unsafe deserialization). Block inbound access at the perimeter firewall using iptables or Windows Firewall with Advanced Security (`netsh advfirewall firewall add rule name='GreenGolf-Block' dir=in action=block remoteip=`) for any service that cannot be confirmed patched. For OT/ICS segments, enforce a deny-all inbound rule at the IT/OT boundary switch and confirm via `netstat -an` or `ss -tulpn` that no PLC management interfaces (Modbus TCP/502, S7 TCP/102) are reachable from internet-facing VLANs.

Evidence: Before restricting services, capture full netflow or pcap from internet-facing interfaces using `tcpdump -i eth0 -w /evidence/greengolf_prefirewall_$(date +%F).pcap` to preserve pre-containment C2 traffic patterns. Pull current connection tables (`ss -tulpn > /evidence/active_connections_$(date +%F).txt`) and running process list (`ps auxf > /evidence/process_snapshot_$(date +%F).txt`) from each exposed system. Capture web server access logs (Apache: `/var/log/apache2/access.log`; Nginx: `/var/log/nginx/access.log`; IIS: `C:\inetpub\logs\LogFiles\W3SVC*\*.log`) — GreenGolf exploitation of CWE-78/89 would show URI-encoded shell metacharacters (`%3B`, `%7C`, `%60`), stacked SQL statements, or abnormal POST bodies in these logs. For authentication-facing services, export Windows Security Event Log (Event ID 4625: failed logon, Event ID 4624: successful logon, Event ID 4648: explicit credential use) from all internet-exposed hosts prior to firewall rule changes.

Detection — Hunt for LampoRAT and BlackBeard indicators: look for Rust binary artifacts (absence of standard C runtime imports, unusual section entropy), anomalous outbound C2 traffic on standard protocols (HTTP/S, DNS per T1071.001/T1071.002), unexpected web shell artifacts (T1505), and new or modified scheduled tasks or services consistent with persistence. Review authentication logs for valid account abuse (T1078) and external remote service access (T1133). Cross-reference endpoint and network telemetry against MITRE techniques T1190, T1036, T1082, T1016, T1105, T1057, and T1498.

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), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a hardened config (SwiftOnSecurity or olafhartong/sysmon-modular) to capture Event ID 1 (Process Create), Event ID 3 (Network Connect), Event ID 7 (Image Load), and Event ID 11 (File Create). To detect Rust-compiled LampoRAT/BlackBeard binaries lacking standard MSVC C-runtime imports, run: `dumpbin /imports | findstr -v KERNEL32 MSVCRT` — a near-empty import table on a large binary is a strong Rust indicator. Calculate PE section entropy with `python3 -c "import pefile, math; pe=pefile.PE(''); [print(s.Name, s.get_entropy()) for s in pe.sections]"` — packed or obfuscated Rust malware typically shows entropy >7.2 in `.text` or custom sections. Write YARA rules matching Rust-specific signatures (e.g., `rust_alloc`, `__rust_begin_short_backtrace` strings) and scan with `yara -r rules/rust_rat.yar /proc/*/exe 2>/dev/null`. For C2 over DNS (T1071.002), run `zeek` or parse Sysmon Event ID 22 (DNS Query) logs for high-frequency queries to newly registered or algorithmically generated domains. For web shells (T1505), scan web roots with `find /var/www -name '*.php' -newer /var/www/html/index.php -exec grep -l 'eval\|base64_decode\|system\|passthru\|shell_exec' {} \;`. Hunt T1078 abuse by querying Windows Security Event Log: `Get-WinEvent -FilterHashtable @{LogName='Security';Id=4624} | Where-Object {$_.Properties[8].Value -eq 10 -or $_.Properties[8].Value -eq 3} | Export-Csv logins.csv` (logon types 10=RemoteInteractive, 3=Network).

Evidence: Capture Sysmon Event ID 1 logs showing parent-child process trees for any web server process (w3wp.exe, httpd, nginx) spawning cmd.exe, powershell.exe, or sh — this is the primary execution artifact for CWE-78 (OS command injection) exploitation by GreenGolf (MITRE T1190, T1059). Preserve memory images from any

suspected host using WinPmem or LiME before remediation: `winpmem_mini_x64.exe /o C:\evidence\mem.img` — LampoRAT and BlackBeard in-memory artifacts (heap strings, Rust runtime symbols, socket handles) will not survive reboot. Export all DNS query logs from the resolver (Windows DNS debug log: `%SystemRoot%\system32\dns\dns.log`; BIND: `/var/log/named/query.log`) covering 72 hours pre-detection for C2 beaconing pattern analysis. Pull scheduled task XML exports (`schtasks /query /fo XML /v > tasks.xml`) and Windows service registry hive (`reg export HKLM\SYSTEM\CurrentControlSet\Services services.reg`) to baseline GreenGolf persistence via T1053 and T1543. Collect authentication event exports (Event IDs 4624, 4625, 4648, 4768, 4769) from all domain controllers and internet-facing systems for T1078/T1133 correlation.

Eradication — Until specific CVE identifiers are released by Recorded Future or a government advisory, apply vendor patches addressing any known OS command injection, SQL injection, authentication bypass, and deserialization vulnerabilities in all externally facing systems within affected verticals. Remove identified web shells (T1505). Revoke and rotate all credentials associated with any systems showing signs of valid account compromise (T1078).

NIST Phase: Eradication

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

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: For web shell removal (T1505): enumerate all files in web roots modified in the last 30 days (`find /var/www -mtime -30 -type f | xargs grep -l 'eval\|base64_decode\|system\|assert' > /evidence/suspected_shells.txt`) and compare against a known-good file manifest or version-controlled deployment baseline. Remove confirmed shells and replace with verified originals from source control or vendor distribution package (validate checksums: `sha256sum -c vendor_manifest.sha256`). For credential revocation tied to T1078 abuse: force password reset for all accounts with logon activity on compromised hosts (`net user /domain` to check last logon; in AD: `Set-ADUser -Identity -ChangePasswordAtLogon $true`), revoke all active sessions, and invalidate Kerberos tickets (`klist purge` on endpoints; reset KRBTGT account password twice in AD if domain-level compromise is suspected). For CWE-502 (deserialization) in Java-based services, deploy the ysoserial gadget-chain blocklist via JVM property `-Djava.security.properties=deser_block.policy` as a compensating control until patching is complete. Scan for LampoRAT/BlackBeard persistence artifacts using ClamAV with a custom signature database updated to include Rust-binary heuristics (`clamscan -r --detect-pua=yes /var/www /opt /usr/local/bin`).

Evidence: Before removing web shells, preserve full copies with metadata intact: `cp -a /var/www/html/shell.php /evidence/webshell_$(date +%F)/` and record inode timestamps (`stat /var/www/html/shell.php`) — GreenGolf-deployed web shells will have creation timestamps correlating to the initial CWE-78/89 exploitation window visible in web server access logs. Hash all removed artifacts (`sha256sum /evidence/webshell_*`) for chain-of-custody documentation per NIST IR-5 (Incident Monitoring). Before credential rotation, export a full Active Directory logon audit from domain controllers covering Event IDs 4768 (Kerberos TGT request), 4769 (Kerberos service ticket request), and 4776 (NTLM credential validation) — these will show lateral movement paths from initially compromised internet-facing hosts. Capture the full patch state of affected systems pre-remediation (`wmic qfe list full /format:csv > /evidence/patches_prerem.csv` on Windows; `rpm -qa > /evidence/rpm_prerem.txt` on RHEL/CentOS) to document the vulnerability window for regulatory reporting.

Recovery — Validate that all externally facing services have authentication enforced on critical functions (CWE-306 remediation confirmed). Confirm no residual web shells or implants via EDR and file integrity monitoring. Restore from verified clean backups for any system where LampoRAT or BlackBeard execution is confirmed. Monitor C2 egress paths for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-4 (System Monitoring), NIST AC-17 (Remote Access), CIS 7.2 (Establish and Maintain a

Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Validate CWE-306 remediation by running an unauthenticated curl probe against all critical function endpoints: `curl -sk -o /dev/null -w '%{http_code}' https:///api/critical-function` — any 200 response without an Authorization header confirms CWE-306 is unresolved. For file integrity monitoring without EDR, deploy AIDE (Advanced Intrusion Detection Environment): initialize a baseline post-recovery (`aide --init && mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db`) and schedule daily checks (`aide --check > /var/log/aide_check_$(date +%F).log`). For C2 egress monitoring over 30 days, configure Zeek or run continuous `tcpdump -i eth0 -w /evidence/egress_%Y%m%d.pcap -G 86400` and parse daily for connections to new external IPs on ports 80/443/53 from previously compromised hosts. Validate backup integrity before restoration: `sha256sum backup.tar.gz` vs. stored hash at backup creation time; restore to isolated VLAN, run YARA scan for Rust-binary artifacts, then promote to production.

Evidence: Before restoring from backup, take a final forensic image of the compromised system disk (`dd if=/dev/sda of=/evidence/compromised_disk_$(hostname)_$(date +%F).img bs=512 conv=noerror,sync`) and preserve Sysmon and Windows Event logs to an offline archive — LampoRAT execution artifacts (process creation chains, network connections, file writes) in these logs are the primary evidence for post-incident analysis and any regulatory notification. During the 30-day C2 monitoring window, specifically watch for Rust binary re-execution events (Sysmon Event ID 1 for processes with Rust-characteristic command-line patterns), anomalous HTTPS beaconing with consistent jitter intervals (BlackBeard C2 characteristic), and any re-emergence of web shell files at previously compromised web root paths. Document system restore timestamps and backup provenance (backup creation date, hash, storage location) in the incident record per NIST IR-5 (Incident Monitoring) requirements.

Post-Incident — Conduct a control gap review against NIST SP 800-53 SI-3 (malicious code protection), SI-7 (software and information integrity), and AC-17 (remote access). Document whether the five CWE classes were covered in your last vulnerability scan cycle. Update detection rules and threat intel feeds to track GreenGolf/MuddyWater/Boggy Serpens indicator releases. Revisit your OT/ICS network segmentation posture given the stated physical disruption objective.

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-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AC-17 (Remote Access), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For the control gap review without a GRC platform: build a spreadsheet mapping each of the five CWE classes to your last Nessus/OpenVAS scan plugin IDs — CWE-78 maps to Nessus plugin families 'CGI abuses' and 'Web Servers'; CWE-89 to 'Databases' and 'CGI abuses'; CWE-287/306 to 'Misc.' and authentication-check plugins; CWE-502 to 'Java' and deserialization-specific checks. Document any coverage gaps as open risk items with owner and target remediation date. For threat intel feed updates tracking GreenGolf/MuddyWater/Boggy Serpens: subscribe to CISA's free Known Exploited Vulnerabilities (KEV) RSS feed, configure OpenCTI or MISP with Recorded Future's free community feed, and write Sigma rules for LampoRAT/BlackBeard behavioral TTPs (Rust binary execution from web server parent, DNS C2 beaconing, scheduled task creation by IIS worker process). For OT/ICS segmentation review: run a Nmap scan from the IT network targeting known OT protocol ports (`nmap -sS -p 102,502,20000,44818,47808 `) — any response confirms an IT/OT boundary gap that GreenGolf's physical disruption objective would exploit. Reference ICS-CERT advisories and CISA's Cross-Sector Cybersecurity Performance Goals for water and energy sector segmentation baselines.

Evidence: Compile the complete incident timeline from all preserved evidence sources (web server access logs, Sysmon Event ID 1/3/7/11, Windows Security Event Log, DNS query logs, netflow/pcap) into a unified chronology mapping GreenGolf's kill chain: initial exploitation (T1190) → web shell deployment (T1505) → discovery (T1082, T1016, T1057) → C2 establishment (T1071.001/T1071.002) → persistence (T1053/T1543) → potential lateral movement toward OT (T1133, T1078). This timeline is the primary artifact for lessons-learned review and is required documentation under NIST IR-8 (Incident Response Plan) for plan updates. Retain all evidence per your documented retention schedule (NIST AU-11 — Audit Record Retention) with chain-of-custody records, as GreenGolf operations against critical infrastructure may trigger CISA reporting obligations under CIRCIA or sector-specific requirements

(NRC for nuclear, TSA for pipeline/aviation, EPA for water).

Detection Guidance

Prioritize the following detection approaches given Rust-based malware and the MITRE technique set attributed to this campaign. (1) Binary analysis: Rust binaries lack standard C runtime imports and produce distinct PE/ELF section structures with elevated entropy; flag executables matching this profile that appear in unexpected directories or are newly written post-exploitation. (2) Network: Alert on outbound HTTP/S and DNS traffic from OT-adjacent or critical infrastructure systems to unrecognized external hosts (T1071.001, T1071.002). Flag large or compressed outbound transfers consistent with T1560 archiving. (3) Authentication: Correlate failed and successful logins against unusual source IPs or times on externally facing systems (T1078, T1133). Alert on authentication attempts to services that should have no external access. (4) Endpoint: Hunt for new processes spawned from web server or application service accounts (T1505 web shell indicator). Review for command interpreter execution (T1059) from non-standard parent processes. (5) Vulnerability surface: Run authenticated scans against all internet-exposed systems for CWE-78, CWE-89, CWE-287, CWE-306, and CWE-502 class vulnerabilities. Specific CVE identifiers have not been publicly confirmed in the available source data; monitor Recorded Future and CISA for CVE disclosure and update detection rules accordingly.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`[not available — specific LampoRAT/BlackBeard hashes not included in source data]`	LampoRAT and BlackBeard Rust-based malware families attributed to GreenGolf; monitor Recorded Future and CISA for hash releases	LOW

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1036** — Masquerading
- **T1078** — Valid Accounts
- **T1027** — Obfuscated Files or Information
- **T1486** — Data Encrypted for Impact
- **T1082** — System Information Discovery
- **T1071** — Application Layer Protocol
- **T1071.001** — Web Protocols
- **T1016** — System Network Configuration Discovery
- **T1190** — Exploit Public-Facing Application
- **T1105** — Ingress Tool Transfer
- **T1560** — Archive Collected Data

- **T1562** — Impair Defenses
- **T1505** — Server Software Component
- **T1021** — Remote Services
- **T1059** — Command and Scripting Interpreter
- **T1071.002** — File Transfer Protocols
- **T1498** — Network Denial of Service
- **T1057** — Process Discovery

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **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
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software

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

ISO-27001-2022

- **A.8.28** — Secure coding

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

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1036	Masquerading	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1082	System Information Discovery	Discovery
T1071	Application Layer Protocol	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1016	System Network Configuration Discovery	Discovery
T1190	Exploit Public-Facing Application	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1560	Archive Collected Data	Collection
T1562	Impair Defenses	Defense-Evasion
T1505	Server Software Component	Persistence
T1021	Remote Services	Lateral-Movement

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1071.002	File Transfer Protocols	Command-And-Control
T1498	Network Denial of Service	Impact
T1057	Process Discovery	Discovery

Sources

Source	URL	Tier
Recorded Future	https://www.recordedfuture.com/blog/the-iran-war-what-you-need-to-know	T3
	https://www.recordedfuture.com/blog/the-iran-war-what-you-need-to-know	T3
	https://www.nytimes.com/2026/04/16/us/politics/iran-war-hacking-cyb...	T2
	https://www.washingtonpost.com/opinions/2026/04/10/iran-water-hacks/	T2
U.S. Warns of Cyberattacks Tied to Iran on Water and Energy Systems	https://www.nytimes.com/2026/04/07/world/middleeast/us-cyberattacks...	T2

Generated 2026-05-01 14:02 UTC by TJS Security Command Center