INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-04 15:22 UTC

Iranian Cyberattacks Against Israel Triple Following U.S.-Israeli Military Offensive

THREAT CAMPAIGN | CRITICAL

SCC Item ID	SCC-CAM-2026-0619
Type	Threat Campaign
Severity	CRITICAL
Affected Products	Israel critical infrastructure, central government organizations, small and medium-sized businesses, and the general public
Published	2026-07-03
Discovery Source	Gemini

Executive Summary

Israel's National Cyber Directorate chief publicly reported a nearly threefold increase in Iranian-attributed cyberattacks targeting Israel in June 2026, with approximately 4,800 hostile cyber incidents recorded compared to approximately 1,600 in June 2025, according to a single official Israeli government statement. Targets span critical infrastructure, government organizations, and small and medium-sized businesses, with reported impacts including wiped computer systems at some affected companies. Organizations with operational or supply-chain ties to Israel, particularly in critical infrastructure sectors, face elevated risk of disruptive cyberattacks attributed to Iranian state-sponsored actors.

Technical Analysis

No CVE or CWE identifiers are associated with this campaign in the provided source material. The attack volume data originates from a single official statement by INCD chief Yossi Karadi and has not been independently corroborated by INCD advisories, CISA, or third-party threat intelligence firms as of the time of this writing. MITRE ATT&CK techniques associated with this campaign type include T1190 (Exploit Public-Facing Application), T1485 (Data Destruction), T1486 (Data Encrypted for Impact), and T1566 (Phishing). Reported impacts include data destruction (wiped systems), consistent with T1485 tradecraft previously attributed to Iranian-nexus state-sponsored actors. Specific malware families, infrastructure indicators, or exploitation pathways are not detailed in the available source material. Attribution is to Iranian state-sponsored actors per Israeli government statement; independent technical attribution has not been confirmed in provided sources.

Action Checklist

1. Step 1: Containment. Audit and restrict externally-exposed services, particularly public-facing applications susceptible to T1190; prioritize systems processing critical operational data. Reference NIST AC-17 (Remote Access) and AC-4 (Information Flow Enforcement) to enforce access restrictions on internet-facing assets. Implement or validate firewall rules per CIS 4.4 and CIS 4.5.
2. Step 2: Detection. Monitor for indicators consistent with data destruction (T1485) and ransomware-style encryption (T1486): sudden large-scale file deletion or overwrite events, anomalous volume shadow copy deletions, and mass encryption activity across endpoints. Audit inbound phishing campaigns (T1566) via email gateway logs. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). No specific IOCs are available in the provided source material.
3. Step 3: Eradication. No specific patch or exploitation vector is detailed in available sources. Apply principle of least privilege (NIST AC-6) and enforce MFA on all externally-exposed and administrative accounts (CIS 6.3-6.5) to limit lateral movement and initial access risk. Conduct a vulnerability scan of public-facing applications to identify and remediate T1190-class weaknesses.
4. Step 4: Recovery. Validate integrity of backup systems before restoration; confirm backups are offline or immutable and have not been targeted by destruction activity. Verify system file integrity per NIST SI-7 (Software, Firmware, and Information Integrity). Monitor restored systems for re-infection indicators. Reference NIST AU-9 (Protection of Audit Information) to ensure log integrity is preserved for post-incident review.
5. Step 5: Post-Incident. Conduct a review of data destruction response procedures. Assess gaps in backup isolation, network segmentation, and phishing controls. Map identified control gaps to NIST IR family controls. Implement multi-factor authentication (NIST IA-2) and credential rotation (NIST IA-4) where not already in place, particularly for privileged accounts and externally-exposed services.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to national CERT (CERT-IL), sector ISAC, and executive leadership if any of the following are confirmed: evidence of wiper or destructive payload execution on any host, compromise of backup infrastructure rendering recovery impossible, access to OT/ICS-adjacent systems in critical infrastructure environments, or PII/regulated data exfiltration triggering statutory breach notification obligations.
Recovery Notes	Given confirmed wiper activity in this campaign destroying systems at affected organizations, restoration must begin only after forensic imaging of all affected hosts and independent verification that backup stores were not themselves targeted or corrupted by the destructive payload. Restored systems should be monitored continuously for a minimum of 14 days using Sysmon and network flow analysis for re-infection indicators, as Iranian actors in this campaign period have demonstrated re-entry capability following incomplete eradication. Segment restored systems from production OT and critical data environments until a full clean-bill-of-health review is completed.

Forensic Artifacts	Windows $UsnJrnl (NTFS change journal) on affected endpoints — captures mass file deletion and overwrite sequences characteristic of wiper execution; extract with Kroll Artifact Parser and Extractor (KAPE) or `fsutil usn readjournal C:` before reimaging | Volume Shadow Copy inventory and VSS service event logs (Windows Event ID 8193, 8194 in System log and vssadmin history) — Iranian destructive tooling in this campaign period consistently deletes shadow copies to prevent recovery; absence of expected snapshots is itself a forensic indicator | Windows Security Event Log Event ID 4688 process creation chains — reconstruct execution lineage of wiper or encryption binaries (parent process, command-line arguments, user context) from the intrusion window, particularly chains originating from email client or browser processes consistent with phishing initial access | Email gateway MTA delivery logs and any sandboxed attachment detonation reports — identify phishing lure documents, sender infrastructure, and payload delivery timeline consistent with the T1566 initial access vector reported in this campaign | Memory image (RAM) of any host suspected of active compromise prior to shutdown or reimaging — Iranian actors in this campaign have used in-memory loaders and credential-harvesting tools that leave no on-disk artifacts; RAM is the only recovery path for these indicators and is destroyed on host shutdown

Per-Action IR Details

Step 1: Containment — Audit and restrict externally-exposed services, particularly public-facing applications susceptible to T1190; prioritize systems processing critical operational data. Reference NIST AC-17 (Remote Access) and AC-4 (Information Flow Enforcement) to enforce access restrictions on internet-facing assets. Implement or validate firewall rules per CIS 4.4 and CIS 4.5.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run `netstat -ano` (Windows) or `ss -tulpn` (Linux) to enumerate all listening services and cross-reference against an expected baseline. Use `nmap -sV --open -p- ` from a trusted internal scanner to map externally exposed ports. Apply host-based firewall rules via `netsh advfirewall` (Windows) or `iptables`/`ufw` (Linux) to block non-essential inbound access. Disable or unpublish non-critical web-facing services immediately until validated.

Evidence: Before restricting or terminating any externally exposed service, capture: active TCP connection state via `Get-NetTCPConnection` (Windows) or `netstat -ano` output (preserve to file with timestamp); running process list via `tasklist /v` or `ps auxf`; active authenticated sessions from IIS logs (`%SystemDrive%\inetpub\logs\LogFiles\`) or Apache/Nginx access logs (typically `/var/log/apache2/access.log` or `/var/log/nginx/access.log`) including source IPs, URI stems, and HTTP response codes consistent with exploitation attempts (e.g., 200 responses to unusual POST requests targeting admin or upload endpoints); Windows Security Event Log Event ID 4624/4625 for recent remote logon successes and failures from external IPs. Acquire RAM image (e.g., via WinPmem or LiME) if any service process is suspected of in-memory implant activity, before any service restart or firewall rule change.

Step 2: Detection — Monitor for indicators consistent with data destruction (T1485) and ransomware-style encryption (T1486): sudden large-scale file deletion or overwrite events, anomalous volume shadow copy deletions, and mass encryption activity across endpoints. Audit inbound phishing campaigns (T1566) via email gateway logs. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). No specific IOCs are available in the provided source material.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config; watch for Event ID 23 (FileDelete) and Event ID 11 (FileCreate) with high-frequency bursts indicating mass file manipulation. Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on `vssadmin.exe delete shadows`, `wmic shadowcopy delete`, `cipher.exe /w`, `wbadmin delete`, or `bcdedit /set {default} recoveryenabled No` — all observed in Iranian-attributed destructive campaigns. For phishing detection without a SIEM, parse email gateway MTA logs (e.g., Postfix `/var/log/mail.log`, Exchange Message Tracking logs) for high-volume inbound delivery from new or spoofed domains using a bash one-liner: `grep 'from=' /var/log/mail.log | awk '{print $7}' | sort | uniq -c | sort -rn | head -20`. Use Sigma rule `proc_creation_win_vssadmin_delete_shadows` and `proc_creation_win_wbadmin_delete_backup` for offline log scanning with `sigmac`.

Evidence: This step is analytical and does not alter live system state. Collect and preserve before any containment action: Windows Volume Shadow Copy inventory via `vssadmin list shadows` (timestamp and count); Windows Security Event Log Event IDs 7045 (new service installed — common dropper behavior), 4688 (process creation chains from email clients or browsers), and 1102 (audit log cleared — a hallmark of Iranian destructive playbooks); Sysmon Event ID 3 (network connections) from mail client processes; email gateway quarantine logs and any attachment hashes submitted to VirusTotal; file system change journals (`$UsnJrnl`) from endpoints for bulk deletion forensics; memory-resident malware indicators from a RAM image if a host is behaving anomalously prior to visible destruction.

Step 3: Eradication — No specific patch or configuration remediation is identified in the provided source material, as attack vectors are not detailed. Apply principle of least privilege per NIST AC-6 and CIS 5.4 to limit lateral movement potential. Enforce MFA on all externally-exposed and administrative accounts per CIS 6.3, CIS 6.4, and CIS 6.5.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Audit privileged group membership via `net localgroup administrators` and `Get-ADGroupMember 'Domain Admins'`; remove any accounts not explicitly authorized. Rotate all service account and administrative passwords immediately using a scripted approach (e.g., PowerShell `Set-ADAccountPassword`). For MFA on externally-exposed systems without enterprise tooling, implement Duo Security free tier or enable Windows Hello for Business; for Linux SSH, enforce TOTP via `libpam-google-authenticator`. Disable all unused remote access protocols (RDP on non-admin hosts, Telnet, default SNMP community strings) via `netsh advfirewall` or `iptables` drop rules.

Evidence: Before rotating credentials or modifying account privileges — actions that destroy authentication state evidence — capture: Windows Security Event Log Event ID 4672 (Special Logon/privileged account use) and 4648 (explicit credential use) to identify accounts used during the intrusion window; active session tokens and Kerberos ticket cache via `klist` on potentially compromised hosts; LSASS memory dump (using ProcDump: `procdump -ma lsass.exe lsass.dmp`) if credential harvesting is suspected, as Iranian actors in this campaign period have used credential-theft tooling to enable lateral movement before triggering destructive payloads; domain controller Security Event Log for Event ID 4768/4769 (Kerberos TGT/TGS requests) from anomalous sources in the intrusion timeframe.

Step 4: Recovery — Validate integrity of backup systems before restoration; confirm backups are offline or immutable and have not been targeted by destruction activity. Verify system file integrity per D3-SFA (System File Analysis). Monitor restored systems for re-infection indicators. Reference NIST AU-9 (Protection of Audit Information) to ensure log integrity is preserved for post-incident review.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 3.4 (Enforce Data Retention)

Compensating: Before restoring from backup, verify backup file hashes against catalog baselines (use `sha256sum` or `Get-FileHash`) to confirm the backup itself was not corrupted or encrypted by destructive malware that propagated

to backup-connected storage. Run `sfc /scannow` (Windows) or `rpm -Va` / `debsums -c` (Linux) on restored systems to validate OS file integrity against known-good checksums. Deploy ClamAV with updated signatures on restored hosts and perform a full scan before reconnecting to production networks. Monitor restored systems for 72 hours minimum using Sysmon, watching for recurrence of destruction-precursor behaviors (shadow copy deletion, bulk file operations, unusual outbound connections) that would indicate persistence survived the restore.

Evidence: Before bringing any restored system online, confirm that forensic images of the wiped or compromised systems were taken prior to reimaging (bit-for-bit image via `dd` or FTK Imager); verify that Windows Event Logs, Sysmon logs, IIS/web server access logs, and email gateway logs from the incident window are preserved on a write-protected or isolated log server — consistent with NIST AU-9 requirements — since Iranian destructive actors have specifically targeted log stores to impede forensics. Confirm backup storage access logs show no unauthorized access events in the 30 days preceding the incident, as this campaign has involved pre-positioning prior to triggering destruction.

Step 5: Post-Incident — Conduct a review of data destruction response procedures. Assess gaps in backup isolation, network segmentation, and phishing controls. Map identified control gaps to NIST IR family controls. Implement D3-MFA (Multi-factor Authentication) and D3-CRO (Credential Rotation) where not already in place, particularly for privileged accounts and externally-exposed services.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 6.2 (Establish an Access Revoking Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a structured lessons-learned session within 5 business days of recovery using a tabletop template modeled on CISA's Post-Incident Review guidance. Document specifically: which externally exposed services were the initial attack surface, how long the threat actor had access before detection (dwell time), and whether backup isolation failed. Use the findings to write or update a data-destruction-specific runbook covering vssadmin/wbadmin abuse, mass file deletion detection thresholds, and out-of-band backup verification steps. Share sanitized IOCs and TTPs with the Israeli CERT (CERT-IL) or your sector ISAC to support collective defense given the campaign's national-scale targeting.

Evidence: Preserve and archive for post-incident review: all Windows Event Logs (Security, System, Application, Sysmon) from affected hosts covering at least 90 days prior to incident declaration; network flow data (NetFlow/IPFIX) or firewall connection logs showing initial access and lateral movement; email gateway logs documenting phishing delivery attempts and any payload downloads; memory images and disk forensic images of destroyed or compromised systems; a timeline artifact (e.g., log2timeline/plaso output) reconstructing the full attack chain from initial access through destructive payload execution, which is essential given Iranian actors in this campaign have used multi-stage intrusions with significant dwell time before triggering wipers.

Detection Guidance

Specific IOCs (IP addresses, domains, file hashes) are not available in the provided source material. Detection should focus on behavioral indicators consistent with the associated MITRE techniques. For T1485 (Data Destruction): alert on mass file deletion events, Volume Shadow Copy deletion (Windows Event ID 524 or vssadmin commands), and sudden disk write anomalies across multiple endpoints. For T1486 (Data Encrypted for Impact): monitor for rapid file extension changes, high-volume encryption activity, and ransom note file creation. For T1566 (Phishing): review email gateway logs for spoofed sender domains, malicious attachment types, and link-click events to newly registered or low-reputation domains. For T1190 (Exploit Public-Facing Application): monitor web application logs for anomalous request patterns, unexpected error spikes, and authentication bypass attempts. Enable and review logging across all critical systems per NIST AU-2 (Event Logging) and AU-3 (Content of Audit Records). No vendor-specific detection rules or SIEM query templates are

supported by the provided source material.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1485** — Data Destruction
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access

Technique ID	Technique Name	Tactic
T1485	Data Destruction	Impact
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
ISAC advisory highlights cyber and physical risks to critical ...	https://industrialcyber.co/industrial-cyber-attacks/isac-advisory-h...	T2
Small and Medium Businesses - CISA	https://www.cisa.gov/audiences/small-and-medium-businesses	T1
Israel-US Binational Industrial R&D Foundation to Invest $3.85M in ...	https://www.darkreading.com/cybersecurity-operations/israel-us-bina...	T2
[PDF] Critical Infrastructure Small & Medium-Sized Businesses (SMBs)	https://ustelecom.org/wp-content/uploads/2021/03/USTelecom-2021-Cyb...	T3
National Cyber Strategy: Issues for Discussion - jstor	https://www.jstor.org/stable/resrep61283	T3

Generated 2026-07-04 15:22 UTC by TJS Security Command Center