# Telegram Hacktivist Activity Timeline of Iran - Israel & US War

Published: 2026-03-10 · Archived: 2026-04-05 13:06:50 UTC

From the first hours of Iran vs. Israel & US War: Operation Epic Fury, hacktivist groups mobilized faster than any state-sponsored actor could. What started as DDoS campaigns against Israeli government sites quickly expanded into a global coalition of pro-Iranian, pro-Palestinian, and Russian-aligned collectives hitting Gulf states, European targets, and US infrastructure.

This blog post tracks that activity day by day, since the first coalitions forming on March 1.

| 📅 Date | 🔎 Update |
|---|---|
| **March 25, 2026** | Handala Doxxes Former Mossad Chief, BD Anonymous ‘’Hits’’ Interpol, and Keymous Returns to Egypt |
| **March 24, 2026** | Alliance Fractures, Bounties, and a Kurdish Front Opens |
| **March 23, 2026** | Handala Publishes Power Grid Maps, NoName Reaches Denmark, and DieNet Tests Google |
| **March 22, 2026** | Keymous Reaches Egypt, a New Channel Geolocates Hotels, and the Lockheed Claim Gets a PoC |
| **March 21, 2026** | NoName Sweeps Romania for the Second Time, DieNet Claims 100 Attacks in a Day |
| **March 20, 2026** | Eid, Nowruz, and a Quiet Day With a Loud Claim |
| **March 19, 2026** | FBI Seizes Handala’s Domain, 313 Team Takes Down the Internet Archive, and the Coalition Keeps Expanding |
| **March 18, 2026** | Larijani Killed, Iran Retaliates, NoName Hits Israeli Insurers, INDOHAXSEC Drops 8.3 Million Records |
| **March 17, 2026** | Microsoft Services Targeted, South Korea Swept, Israeli Lawyers Doxxed, and the Coalition Expands |
| **March 14-16, 2026** | Golden Falcon Leak, MME Targeting, Syria Joins Both Sides, and the Cyber Front Enters Its Third Week |
| **March 13, 2026** | Cyber Islamic Resistance Targets Israeli Cybersecurity Firm, 313 Team Strikes UAE, Cyprus Becomes NoName’s Fixation |

| | |
|---|---|
| **March 12, 2026** | Handala Wipes Stryker, Keymous Sweeps the Gulf, and 313 Team Crosses into Europe |
| **March 11, 2026** | New Alliances, Kuwait Swept, and the Short Story of NetStrike |
| **March 10, 2026** | Critical Infrastructure in the Crosshairs as FSociety Issues 42-Hour Threat |
| **March 7-9, 2026** | New Supreme Leader, Wider Borders, Deeper Systems |
| **March 6, 2026** | Gulf Governments Under Siege, Iraqi Cyber Resistance Declares War on Kuwait |
| **March 5, 2026** | Two Wars, One Cyber Front, Data Breaches, New Recruits, and the Expanding Target Map |
| **March 4, 2026** | OT Intrusion Claims, Multi-Vector Escalation, and the Expanding Target Map |
| **March 3, 2026** | Pro-Russian Hackers Have Joined the Lobby, Critical Infrastructures Under Attack |
| **March 2, 2026** | Escalation Across Critical Infrastructure, Ransomware, and Coordinated Campaigns |
| **March 1, 2026** | Hacktivist Collectives & Alliances Emerging |

For the full threat intelligence feed, visit the Iran vs. Israel & US Cyber War 2026: Operation Epic Fury Threat Intelligence blog.

## March 25, 2026: Handala Doxxes Former Mossad Chief, BD Anonymous ‘’Hits” Interpol, and Keymous Returns to Egypt

Day 26 opened with Handala’s most personally targeted operation since the conflict began. While DDoS campaigns continued across Egypt and international organizations, the day’s defining moment was a hack-and-leak post naming a former intelligence chief and claiming 14 gigabytes of documents to prove it.

### Handala Targets Former Mossad Chief

On March 25, Handala published a post on its website titled “From Hunter to Hunted: Mossad’s Former Chief Falls into the Trap.” The post named him directly, published photographs of him at what appear to be public events, and claimed to have released 14 gigabytes of personal and confidential documents as a Proof of Concept.

Handala website post titled “From Hunter to Hunted” showing photographs of Tamir Pardo at public events alongside Handala branding and a download link for the alleged 14GB document release

The claim is unverified. No independent researcher has confirmed the authenticity of the files. Pardo is a public figure with a documented history of public appearances, and some of the photographs in the post appear to come from open sources. Handala’s documented pattern of inflating claims and combining real with exaggerated material makes independent verification essential before drawing any conclusions about the files’ contents.

What is clear is the intent. Following the FBI's seizure of its domain on March 19 and the DOJ's $10 million bounty on its members, Handala has consistently ''escalated'' rather than retreated. The $50 million counter-bounty on March 24, the power grid maps on March 23, and now the personal targeting of a named former intelligence official represent a deliberate escalation curve in the group's public posture.

### BD Anonymous Takes Aim at Interpol

BD Anonymous claimed a DDoS attack against interpol.int on March 25, publishing the target's IP address, port configuration, and ISP details showing Akamai Technologies as the host. The attack was timed to 10:40 UTC and framed explicitly around the ICC arrest warrant for Netanyahu, with the message telling global law enforcement to "open your eyes" and arrest war criminals.

BD Anonymous post showing an ICC-style "WANTED" poster of Netanyahu alongside attack details for interpol.int including IP, ports, and ISP information

Interpol is a neutral international organization with no role in the Iran conflict. Its targeting is symbolic, chosen for the message it sends rather than any operational value. The Akamai hosting makes a sustained outage unlikely, but the framing of the attack as a law enforcement accountability operation marks BD Anonymous as one of the more messaging-focused groups in the current coalition.

### Keymous Plus Returns to Egypt's Ministry of Interior

Keymous Plus published a Check-Host report on March 25 showing connection timeouts for Egypt's Ministry of Interior website across more than 20 global nodes, confirming the site was still down at time of posting. The operation was tagged under #Op_Epstein_Gulf and #Elite_Network.

Egypt has now been targeted across multiple days. Like other countries in the campaign's expansion phase, its inclusion appears to follow geographic sweep logic rather than any specific Egyptian political action that triggered the operation.

## March 24, 2026: Alliance Fractures, Bounties, and a Kurdish Front Opens

March 24 produced one of the most significant structural shifts of the conflict's cyber dimension. Two of the day's developments had nothing to do with DDoS claims or data leaks. They had to do with who was still in the coalition and who had left.

### Cyb3r Drag0nz Kurdish Breaks from CIR and Turns Against Iran

Cyb3r Drag0nz Kurdish had been a member of the Cyber Islamic Resistance coalition from the conflict's early days, participating in joint operations against Israeli and Gulf targets. On March 24, the group published a post mourning six Peshmerga fighters killed in Iranian strikes, naming each one and condemning the Iranian regime directly. The post called on the Kurdish diaspora to stand against Iran alongside Israel and the United States.

Cyb3r Drag0nz Kurdish post showing six named Peshmerga fighters with their photographs, Kurdish text, and condemnation of Iran

The departure has context. Early in the conflict, reports circulated that Kurdish forces in Iraq might be used by the US in operations against Iran. Around the same time, Cyb3r Drag0nz Kurdish had already begun distancing itself from CIR operations targeting Israel. The Iranian strikes on Peshmerga positions appear to have been the final trigger.

This is one of the conflict's clearest alliance fractures. A group that was operating against Israeli targets three weeks ago is now explicitly aligned against Iran. The reversal reflects the fact that Iran's missile and drone campaign has not been limited to Israel and Gulf states. Kurdish-controlled Iraq has also been struck, and Kurdish forces have taken casualties.

### Fynix Announces Operations Against Kurdish Targets

On the same day, Iran-aligned group Fynix announced it was beginning attacks on Kurdish government websites, organizations, and companies. The stated justification was "insults to the Islamic Republic of Iran by Kurdish cyber teams." The post was a direct mirror of the Cyb3r Drag0nz situation, confirming that the fracture between pro-Iranian actors and Kurdish groups had opened a new sub-front within the conflict's cyber dimension.

Fynix post announcing attacks on Kurdish governments, organizations, and companies in response to Kurdish cyber groups insulting Iran

### Handala Posts a $50 Million Bounty on Trump and Netanyahu

Handala published a statement on its website offering $50 million to any individual or group that eliminates Trump and Netanyahu, describing it as a direct response to the US DOJ's $10 million bounty on Handala members announced alongside the domain seizure. The post used Session as its communication channel and promised encrypted, anonymous payment.

Handala's reward post for Trump & Netenyahu on their website

The post is incitement. Its publication via an app and domain outside FBI jurisdiction reflects the group's adaptation following the March 19 seizure.

### Cyber Fattah Issues Reconnaissance Statement

Cyber Fattah published a statement announcing that planned attacks would follow after the group finished "collecting specific resources." The post warned that "all types of attacks" would be used and framed the operation in explicitly anti-Zionist terms. No technical activity was published alongside the statement.

## March 23, 2026: Handala Publishes Power Grid Maps, NoName Reaches Denmark, and DieNet Tests Google

On March 23, Handala published a nine-panel grid of detailed schematic maps on its website, each showing what appeared to be Israeli power plant and electrical grid infrastructure, including transmission lines, substations, and facility layouts. Each panel was watermarked with the Handala logo. A short URL linked to the full post on the Handala site.

Handala post showing nine schematic maps of Israeli power and electrical infrastructure, each panel watermarked with the Handala logo

This is qualitatively different from any previous Handala publication in this conflict cycle. Prior posts involved breach claims, doxxing of military personnel, and propaganda. This post is targeting intelligence against critical national infrastructure, specifically the kind of information that would be useful not for a DDoS campaign but for a kinetic or destructive cyber operation against power systems. Thus, does Handala's effort really effect the physical war?

### NoName057(16) Shifts to Denmark and Greenland

NoName057(16) opened a new front on March 23, targeting Denmark under #OpDenmark. The framing was explicit: the Danish Prime Minister had announced early elections for March 24, driven in part by her rising approval ratings amid Trump's threats to annex Greenland. NoName said it had decided to "join, but in our own way."

Verified targets included the Air Greenland Authorization Portal and Nuup Bussii, the public transport system in Nuuk, Greenland's capital. Both were confirmed via Check-Host. The Denmark operation is unrelated to the Iran conflict and reflects NoName's consistent pattern of using geopolitical news events as operational triggers for campaigns that serve Russian rather than Iranian objectives.

### Conquerors Electronic Army Hits Israeli Business Directory

Conquerors Electronic Army, operating under CIR, claimed a DDoS against t.co.il, an Israeli companies and services directory. Check-Host verification was published. The attack was attributed to Beamed.cc infrastructure.

### DieNet Tests Google's Defenses via Lamborghini

DieNet published a claim that it had bypassed Google LLC's hosting protection on the Lamborghini website, publishing a Check-Host verification link confirming the site was inaccessible. The post framed this as proof that Google's infrastructure is not adequate protection regardless of the scale of the host, stating that "it's a big lie" that powerful machines provide immunity.

The Lamborghini website has no connection to the Iran conflict. The targeting reflects DieNet's ongoing effort to demonstrate that its capabilities extend beyond government and military portals to commercially hosted civilian sites protected by major cloud providers.

## March 22, 2026: Keymous Reaches Egypt, a New Channel Geolocates Hotels, and the Lockheed Claim Gets a PoC

Keymous Plus continued its systematic country-by-country sweep under #Op_Epstein_Gulf, turning to Egypt on March 22. The group published verified downtime for six targets: the Egypt Government Portal, the Cabinet (Prime Minister's office), the Ministry of Interior, the Ministry of Finance, the Ministry of Petroleum, and the Ministry of Water Resources and Irrigation. All were confirmed via Check-Host links.

Keymous Plus post showing six Egyptian government targets verified down under #Op_Epstein_Gulf

Its targeting by Keymous Plus appears to be part of the operation's geographic expansion logic rather than a response to any specific Egyptian political position. The same pattern applied to Syria in the March 12 and 14 sweeps.

### Harvesting Time: A New Channel Geolocating Civilian Sites

A newly surfaced Telegram channel calling itself "Harvesting Time" published satellite imagery on March 22 with precise geolocations of two civilian hotel sites. The first post identified the King David Hotel in Jerusalem, Israel. The second identified the Erbil Rotana Hotel on Gulan Street in Erbil, Kurdistan, Iraq. Neither post contained a breach claim, data dump, or DDoS target list.

Harvesting Time channel post showing satellite imagery of the King David Hotel in Jerusalem with location label

Harvesting Time channel post showing aerial imagery of the Erbil Rotana Hotel with nighttime fire visible nearby and location identified as Gulan Street, Erbil, Kurdistan, Iraq

The Erbil post is more significant than it first appears. Erbil is in the Kurdistan Region of Iraq, which has been caught in the middle of the conflict. The lower image in the Erbil post shows what appears to be fire near the hotel, which may reflect the kinetic strikes on Erbil that occurred during this period.

Harvesting Time is a new actor with no prior track record. Its channel name in Arabic translates roughly to "It Is Their Time." The combination of civilian hotel targeting and Erbil's position in Kurdish-controlled territory gives the channel a distinct profile from the hotel geolocation posts seen from other groups.

### Cyber Fattah Publishes Lockheed PoC Forwarded from APT IRAN

On March 22, Cyber Fattah forwarded a post from APT IRAN claiming a Proof of Concept for the Lockheed Martin breach announced on March 20. The PoC post included a dark web .onion domain, IOC strings, and references to sample data via Telegram and qTox contact channels.

## March 21, 2026: NoName Sweeps Romania for the Second Time, DieNet Claims 100 Attacks in a Day

NoName057(16) had already targeted Romania's National Tax Agency on March 12 following the Romanian president's statements on US military base access. On March 21 the group returned with a far more comprehensive sweep, publishing two separate rounds of verified downtime across Romanian transport, government, legal, and industrial targets.

The first wave hit MOL Romania's oil division, TIM Rail Cargo SRL, Romanian Railways Authority, Bucharest Metro, the Chamber of Deputies, and Romanian Railways. The second wave, published shortly after, added the Supreme Court, the Supreme Court of Cassation, the Industrial Real Estate Management Agency, and a state plant for the construction and modernization of passenger and freight rail cars.

NoName057(16) first Romania wave showing Check-Host verified downtime for MOL Romania, TIM Rail Cargo, Romanian Railways Authority, Bucharest Metro, Chamber of Deputies

NoName057(16) second Romania wave showing Supreme Court, Supreme Court of Cassation, Industrial Real Estate Management Agency all verified down, courts closed by geo-restriction

Both courts were found to be closed by geo-restriction at time of verification, meaning NoName's Check-Host links showed the sites inaccessible but the closure may have been a pre-existing access restriction rather than the result of the attack. The group acknowledged this in its framing, calling it "continuing our journey around Romania."

Romania's consistent appearance as a target through March reflects the group's Operation Time of Retribution framework, which explicitly targets NATO-aligned European countries. Romania's specific role began with the president's statements on US military base access. It has since become a standing target.

### DieNet Reports 100+ Attacks in a Single Day Under #CanYouResist

DieNet, the DDoS infrastructure supplier and primary volume driver for the pro-Iranian coalition since day one, announced it had carried out more than 100 attacks against more than 50 Israeli websites in a single day as part of its #CanYouResist operation. Targets listed included El Al (Israel's national airline), the IDF's military news portal, Rafael defense contractor, Hotnet ISP, IsraelInternet, and SEM, a local web service provider. The network reported that some military websites and services remained down for longer periods than usual.

DieNet's role throughout the conflict has been less about individual named targets and more about sustained volume, providing the DDoS infrastructure that many smaller coalition groups rely on for their own claimed operations. A 100-attack single-day claim, even with typical inflation factored in, is consistent with its established operational tempo.

### RuskiNet Republishes 2025 Bank of Jerusalem Data

RuskiNet Group published what it described as Bank of Jerusalem data, noting the leak originated from a security vulnerability exploited in 2025 and was being republished for those who had missed it at the time. The post invited users to find the data at the linked address.

The re-publication of old leaks is a common tactic used to maintain pressure and media presence without the operational cost of a new breach. The data itself is not new. Its republication on March 21 is a visibility play timed to the conflict's ongoing coverage cycle.

## March 20, 2026: Eid, Nowruz, and a Quiet Day With a Loud Claim

March 20, 2026 was the first day of Eid al-Fitr and the Persian New Year Nowruz, a rare alignment of the two most significant holidays in the Islamic and Iranian calendars. Hacktivist activity dropped noticeably, as expected. Pro-Iranian groups that had been posting multiple operations daily went quiet or published symbolic messages rather than attack claims. The absence of coordinated DDoS sweeps and target lists was itself a data point.

APT IRAN used the relative quiet to publish a different kind of claim.

### APT IRAN Claims ICS Access at Kupferle Water Solutions

APT IRAN published a screenshot of what appeared to be an active HMI panel for a water treatment control system belonging to Kupferle Water Solutions, a company operating in Fenton, Missouri. The panel showed chlorine levels, temperature readings, a “Flushing in Progress” status, and a date stamp of March 10, 2026. The group claimed the device had been accessed, rebooted, and that a backup had been taken.

APT IRAN post showing water treatment HMI panel with active readings, chlorine and temperature levels visible, date 03-10-2026

If the screenshot is genuine, it shows a publicly exposed or weakly secured industrial control panel connected to a water treatment process. The claim is unverified. The ten-day gap between the alleged access date and the publication date is consistent with either delayed publication for propaganda purposes or a staged screenshot. No service disruption was reported. Water utilities have been a recurring target category for Iranian-linked actors in prior conflict cycles, making the claim pattern-consistent even if the specific incident is unconfirmed.

### The Lockheed Martin Claim: Treat With Skepticism

Also on March 20, a post attributed to APT IRAN circulated claiming the group had infiltrated Lockheed Martin’s infrastructure and exfiltrated 375 terabytes of data, including F-35 Block 4 documentation, future missile defense system architecture, Pentagon contracts through 2030, and personnel records for 63,000 current and former employees. The claim valued the stolen data at approximately $330 million and offered it for sale via ThreatMarket on a .onion domain.

The figures are implausible at face value, Lockheed Martin made no public statement, and no third-party researcher confirmed any indicators of compromise. Until verified evidence emerges, this should be treated as an unverified actor claim designed for media amplification.

*March 20 was otherwise the quietest day of the conflict’s third week on the cyber front. Iran and Israel continued trading strikes on Eid and Nowruz, with Kuwait’s Mina al-Ahmadi refinery hit by two waves of Iranian drones. The holiday did not stop the kinetic war.*

## March 19, 2026: FBI Seizes Handala’s Domain, 313 Team Takes Down the Internet Archive, and the Coalition Keeps Expanding

Day 20 of Operation Epic Fury brought one of the conflict’s clearest signals that the cyber front was drawing direct US government attention. The FBI seized Handala’s primary web domain, the group migrated and kept operating, and the day’s hacktivist activity continued at pace with the Internet Archive taken offline, South Korea targeted again, and a new Southeast Asian operation announced for the days ahead.

### The FBI Steps In: Handala’s Domain Seized

The most significant development of the day had nothing to do with a DDoS claim or a data leak. Visitors to handala-redwanted.to were met with a federal seizure banner, carrying the seals of the Department of Justice and the Federal Bureau of Investigation.

FBI seizure notice on handala-redwanted.to showing DOJ and FBI seals and the text “This Website Has Been Seized

The seizure notice stated the domain had been taken under a warrant from the US District Court for the District of Maryland, citing its use to conduct, facilitate, or support malicious cyber activities on behalf of, or in coordination with, a foreign state actor. The notice warned that individuals who knowingly assist with or attempt to restore seized infrastructure may face criminal prosecution, sanctions, or other legal action under US law.

Handala’s nameservers were redirected to ns1.fbi.seized.gov and ns2.fbi.seized.gov, a pattern consistent with previous FBI domain seizure operations. The group responded with characteristically defiant messaging, framing the seizure as proof of the enemy’s fear, and migrated to a new domain. The operation did not disrupt Handala’s Telegram activity, which continued uninterrupted.

The seizure matters less for its operational impact than for what it signals. It places Handala explicitly within the US government’s active enforcement posture, and formally connects the group’s infrastructure to the broader legal framework used against state-adjacent cyber actors. The US DOJ had previously placed a $10 million bounty on Handala members.

### 313 Team Takes Down the Internet Archive

313 Team, the Iraq-based CIR affiliate responsible for some of the conflict’s most consistent DDoS operations, turned its attention to archive.org on March 19. The group published a post confirming the attack was ongoing and that the Internet Archive remained offline at time of announcement, alongside a Check-Host verification link.

313 Team post showing archive.org displaying “Temporarily Offline” message with Check-Host verification link

The Internet Archive is not a military or government target. It is a civilian digital library hosting hundreds of billions of web pages, books, audio, and video. Its targeting reflects the coalition’s continued expansion beyond operationally meaningful infrastructure toward anything associated with the United States or the broader Western internet ecosystem.

### BD Anonymous Hits South Korea’s Ministry of National Defence

BD Anonymous, the Bangladeshi group that had previously swept South Korean targets alongside Hider_Nex under #OpSouthKorea, returned on March 19 with a direct claim against mnd.go.kr, the official website of South Korea’s Ministry of National Defence, publishing two Check-Host verification links and a DownDetector confirmation.

BD Anonymous post showing Operation South Korea branding alongside mnd.go.kr showing “This site can’t be reached” error

The stated grievance was that the South Korean government had not raised its voice for Palestine and was blindly supporting the US-Israel coalition. South Korea has no direct military involvement in the Iran conflict. Its repeated appearance on target lists across multiple groups reflects a pattern of expanding the definition of legitimate targets to include any US-aligned democracy, regardless of its actual role in the conflict.

### Conquerors Electronic Army Hits Israeli Business Directory

Conquerors Electronic Army, operating under the CIR umbrella, claimed a DDoS against t.co.il, an Israeli companies and services directory, with Check-Host verification and the attack attributed to Beamed.cc. The operation was tagged under the Battle of the Great Confrontation framing used consistently by CIR groups throughout the conflict.

### #OpsShadowStrike: A New Campaign Announced for After Eid

A Malaysia-based channel published an announcement for #OpsShadowStrike, declaring the operation would launch after Eid al-Fitr. The post, written in both Malay and English, stated the operation's targets would be countries allied with Israel.

OpsShadowStrike announcement post showing campaign branding and the tagline "One Attack, a Thousand Effects. Targeting countries allied with IsraHell

The announcement was mobilization rather than active operations. It is notable primarily as evidence that new groups continue to form and announce intent even three weeks into the conflict, with the post-Eid timing suggesting the group was explicitly planning around the religious calendar.

## March 18, 2026: Larijani Killed, Iran Retaliates, NoName Hits Israeli Insurers, INDOHAXSEC Drops 8.3 Million Records

D+19 opened with the most significant leadership decapitation since the war's opening day. Iran confirmed the killing of Ali Larijani, secretary of the Supreme National Security Council and the highest-ranking Iranian official killed since Khamenei's assassination on February 28.Israel also confirmed the killing of Basij commander Gholamreza Soleimani, his deputy, and the IRGC's Aerospace Force chief in the same operation. Iran's IRGC said its missiles struck more than 100 military and security targets inside Israel in retaliation.On the cyber front, the day's activity reflected the coalition's continued expansion into new target categories with little slowdown in tempo.

### NoName057(16) Sweeps Israeli Insurance Sector

On March 18, NoName057(16) published a verified sweep of Israeli insurance and defense-adjacent companies under #OpIsrael, hitting Gahat Systems Ltd, Shlomo Insurance Company, Shomera Insurance Company, Harel Insurance Company, Igudbit Insurance Association, and Hachshara Insurance Company. Check-Host verification links confirmed downtime across all targets. Gahat Systems, which specializes in firefighting, rescue, and tactical defense technology, was highlighted as the anchor target. Hachshara was noted as closed by geo-restriction at time of reporting.

NoName057(16) post showing downtime for six Israeli insurance and defense-technology targets

### INDOHAXSEC Leaks 8.3 Million Israeli Voter Records

INDOHAXSEC published what it described as 8.3 million Israeli residents' records taken from general election results, framing the leak as support for Palestine and Iran. The dataset allegedly contains 1,618 files across 116 folders, with an original size of 2GB compressed to 617MB, hosted via Anonymous File Upload. Data fields include names, addresses, emails, phone numbers, geolocation, national ID numbers, and voter registration details.

INDOHAXSEC post showing alleged 8.3 million Israeli citizen data leak from general election results

### Cyber Islamic Resistance Claims Breach of Logit E.D

Cyber Islamic Resistance published a video claim of breaching Logit E.D, an Israeli company, on March 17, framing the operation as part of the ongoing Battle of the Great Confrontation. The post referenced the Yemeni Islamic Resistance and was published under #Cyber_Islamic_Resistance_Axis. Server access was claimed. Unverified.

Cyber Islamic Resistance Telegram post claiming breach of Logit E.D with 58.1MB video proof

### APT IRAN Issues Starlink Warning, Threatens VPN Sellers

APT IRAN published a warning to Iranian Starlink device users, claiming the tool had been compromised by Israeli intelligence to track precise locations of users inside Iran. The group warned users to stop using the devices, claiming Israeli forces were using Starlink terminal data to locate and target individuals. In follow-up posts, the group threatened to expose VPN sellers and their customer networks operating inside Iran, naming them as collaborators. The posts signal an active counter-surveillance and intimidation operation targeting Iranians using circumvention tools, consistent with MOIS-linked activity patterns.

APT IRAN Telegram post -auto translated- warning Starlink users in Iran of Israeli intelligence tracking

## March 17, 2026: Microsoft Services Targeted, South Korea Swept, Israeli Lawyers Doxxed, and the Coalition Expands

*Our Week 2 Threat Assessment Report is now available. Check it for a summary of both weeks' developments.*

The conflict's third week opened with a notable change in targeting scope. The coalition's focus shifted away from regional governments toward global technology infrastructure, with Microsoft's cloud services drawn into the crossfire for the first time. Simultaneously, two groups expanded their geographic footprint to corners of the world with no obvious connection to the Iran-Israel conflict, South Korea and Egypt, signaling that the #Op_Epstein_Gulf and allied campaigns are no longer bounded by the Middle East.

### 313 Team and Anti-Zionist Cyber Group Take Aim at Microsoft

On March 17, two groups operating under the Cyber Islamic Resistance umbrella launched coordinated DDoS claims against Microsoft's core cloud services: office.com, m365.cloud.microsoft, and copilot.cloud.microsoft. Check-Host verification links confirmed gateway timeouts and Azure Front Door errors across multiple nodes, affecting Microsoft 365, Outlook, and Copilot.

313 Team, Anti-Zionist Cyber Group, and Keymous Plus posts showing Microsoft downtime and Check-Host verification links

An emerging group, Anti-Zionist Cyber Group framed Microsoft Store as a global target, stating intentions to continue targeting US companies over Trump's military actions. 313 Team published the Check-Host links. The two groups are both CIR-affiliated but operated this campaign independently from Keymous Plus, which simultaneously claimed disruption of the same Microsoft 365 infrastructure.

### Keymous Plus Takes Down Telecom Egypt

Under #Op_Epstein_Gulf, Keymous Plus claimed disruption of Telecom Egypt (te.eg), the country's primary telephone operator. Egypt's inclusion in the operation is the first time the campaign has reached North Africa, extending a sweep that began in the Gulf and has now touched Syria, Romania, and Egypt within a single week.

Keymous Plus post showing te.eg downtime confirmation

### Hider_Nex Opens a New Front in South Korea

In the most geographically ambitious operation of the day, Hider_Nex launched a sweep of South Korean government infrastructure under #OpSouthKorea, publishing Check-Host verified downtime for more than 15 domains.

Hider_Nex posts showing Check-Host verification for 15+ South Korean government domains

South Korea has no direct role in the Iran-Israel conflict. Its appearance on the target list follows the same logic seen in the Romania and Cyprus attacks. Hider_Nex tagged the operation #Justice and #DDoS with no specific stated grievance against Seoul.

### 29,300 Records Israeli Lawyers Database

NetStrike, the group that appeared for a single day on March 11, published what it described as a database of 29,300 Israeli lawyers under #OpIsrael, allegedly including names, addresses, emails, phone numbers, firm affiliations, geolocation data, and website details. The claim is unverified.

29,300 Records Israeli Lawyers Database

If the data is genuine, it represents a significant doxxing operation targeting a civilian professional class rather than government or military infrastructure.

## March 14–16, 2026: Golden Falcon Leak, MME Targeting, Syria Joins Both Sides, and the Cyber Front Enters Its Third Week

D+14 through D+16 brought a shift in tone. The raw volume of the first two weeks, hundreds of DDoS claims, sweeping coalition announcements, and daily country-wide operations, gave way to something more deliberate. Fewer groups, more targeted claims, and a growing emphasis on intelligence value over disruption volume. The conflict's cyber front was maturing.

## Golden Falcon: A Military Satellite Site Surfaces Online

One of the more operationally significant posts of the period came from an account identifying itself as Golden Falcon, which published what appeared to be satellite imagery of a military facility inside Israel, labeling it “a military satellite site.” The image showed an aerial view of a compound with large satellite dishes, runways, and associated infrastructure in a desert setting.

Golden Falcon Telegram post showing aerial satellite imagery of Israeli military compound with coordinates

The post carried no wiper claim, no data dump, and no DDoS target list. It was pure targeting intelligence, the kind of post designed not to disrupt, but to locate, identify, and mark. Whether the imagery was sourced from open satellite services or exfiltrated from a compromised network, the effect is the same: a potential military installation publicly geolocated and circulated across Telegram channels followed by thousands of users. This type of activity represents a quieter but more consequential form of cyber-enabled warfare than the DDoS pile-ons dominating the first two weeks.

## Keymous Plus Turns to Syria — Every Major Ministry Down

On March 14, Keymous Plus extended its #Op_Epstein_Gulf sweep to Syria, publishing a verified target list that included the Presidency of the Syrian Arab Republic, the Syrian Parliament, the Ministry of Foreign Affairs and Expatriates, the Ministry of Social Affairs and Labor, the Ministry of Transport, the Ministry of Information, the Ministry of Agriculture and Agrarian Reform, and the Ministry of Defense..

Keymous Plus Telegram post showing Check-Host verification of Syrian government domains

Syria’s inclusion is notable for two reasons. First, Syria had only recently re-entered the international fold following the fall of the Assad government. Second, this marks the second time in the current conflict that Damascus has been targeted after its initial appearance in the March 12 Gulf sweep, suggesting Keymous Plus has designated it a standing target rather than an opportunistic one.

## Free Hacker Claims MME/PGW Telecom Infrastructure Attack in Israel

Mad Ghost, forwarding a post from the Free Hacker channel, claimed a successful attack against MME/PGW devices belonging to Israeli mobile network operators. The group published IP addresses for four affected systems belonging to Cyberpower Ltd, LB Annatel Ltd, and Welcome Mobile Ltd, describing them as the core Mobility Management Entity infrastructure handling session control and movement in Israel’s 4G network.

Mad Ghost Telegram post listing four Israeli mobile operator IP addresses with GTP-C protocol details and port numbers

If accurate, an MME/PGW disruption would affect how subscribers connect to mobile data services rather than cutting voice calls entirely, but would degrade network performance across the affected operator’s user base. The post included technical detail including GTP-C protocol, UDP port 2123, and TCP/SCTP port 3868, giving the claim more specificity than typical DDoS announcements. Unverified but technically coherent.

## Anonymous Syria Hackers Runs #Op_Iran Against Iranian Educational Institution

On March 14, Anonymous Syria Hackers published what it described as a 3.2GB data leak from an Iranian educational institution linked to Khamenei loyalists, framing the operation under #Op_Iran. The published material allegedly included full personal details of staff and government specialists: names, fathers' names, national ID numbers, dates of birth, scanned certificates, and personal photos. Screenshots showed a file archive with hundreds of entries and official Iranian certificates overlaid with group branding.

Anonymous Syria Hackers post showing file archive and Iranian certificate overlaid with group branding under #Op_Iran

The group has been operating consistently on the pro-Israel side of the conflict throughout the period, targeting Iranian propaganda infrastructure and IRGC-linked channels. This marks its most data-heavy operation to date and its first confirmed targeting of an Iranian civilian educational institution.

## March 13, 2026: Cyber Islamic Resistance Targets Israeli Cybersecurity Firm, 313 Team Strikes UAE, Cyprus Becomes NoName's Fixation

March 13 brought one of the heaviest kinetic escalations yet. Israel launched a new extensive wave of strikes on Tehran, Kuwait's airport was hit, and Iran's new Supreme Leader Mojtaba Khamenei issued his first public statement vowing to keep the Strait of Hormuz closed. Iran's President Pezeshkian outlined three conditions for ending the war: recognition of Tehran's rights, reparations, and international guarantees against future aggression. A US KC-135 refueling aircraft went down in western Iraq, France confirmed its first casualty of the conflict, and six vessels were struck in the Gulf in two days. The IEA described the oil supply disruption as the largest in history. On the cyber front, the day's activity pushed further into new territory, with a cybersecurity firm becoming a target and the UAE absorbing its heaviest single-day hacktivist pressure of the conflict.

### NoName057(16) Has a Thing for Cyprus

NoName057(16) published two more rounds of DDoS claims against Cyprus, continuing what has become one of the most sustained single-country campaigns of the conflict. Targets across both posts included Nicosia city authorization portal, Limassol city, Paphos City, Payment of Bills e-Paphos, Morphou Town, Politis newspaper, Alithia news portal, Register of Insurance Companies, Organization of Local Government of Limassol, Authorization Portal, Ayia Napa city, and the EAC Cyprus Electricity Authority. Several targets had implemented geo-based access restrictions in an attempt to limit impact, which the group acknowledged and framed as a failed evasion attempt, publishing check-host links showing the sites remained inaccessible. The campaign continues under #FuckEastwood and #TimeOfRetribution, tied to Ukraine-related grievances rather than the Iran theater directly.

NoName057(16) continues #OpCyprus with Check-Host verified DDoS claims across Cypriot municipal, media, and infrastructure targets, noting Cyprus attempted geo-based access restrictions in response

### Cyber Islamic Resistance Claims Breach of Israeli Cybersecurity Firm MEGINIM DATA SERVICES

Cyber Islamic Resistance, the Iraqi-Syrian joint collective operating under the broader Cyber Islamic Resistance Axis, claimed a breach of MEGINIM DATA SERVICES, an Israeli cybersecurity company. The group published three sequential batches of alleged exfiltrated data, describing the operation as part of the “Great Battle” framework. Screenshots showed what appeared to be file directories, spreadsheets, and database exports from the company’s servers. Targeting a cybersecurity firm rather than a civilian or government entity carries clear symbolic intent: the group is deliberately attempting to undermine confidence in Israeli defensive cyber capabilities. No independent verification of the breach has been established.

Cyber Islamic Resistance publishes alleged data from Israeli cybersecurity firm MEGINIM DATA SERVICES across three sequential posts, framing the operation as part of the “Great Battle”

### 313 Team Turns to the UAE, Hitting 20 Government Domains Across Abu Dhabi and Dubai

313 Team published a coordinated DDoS campaign against 20 UAE government servers spanning Abu Dhabi and Dubai, conducted in partnership with the elitestress.st stress testing platform. Targets included the Abu Dhabi Digital Authority, Economic Development Council, Social Support Authority, Agriculture and Food Safety Authority, Civil Defence Authority, Abu Dhabi Municipality and its e-Portal, Urban Planning and Public Transport Department, Building and Real Estate Services e-Portal, Department of Community Development, National Anti-Piracy UAE, Dubai Public Prosecution Portal and Services e-Portal, and the UAE Government Empowerment Department. The operation marks the group’s most concentrated focus on UAE infrastructure since the conflict began.

313 Team publishes a coordinated DDoS target list covering 20 UAE government servers across Abu Dhabi and Dubai, conducted in partnership with elitestress.st

### INDOHAXSEC Claims Data Breach of Israeli Online Shopping Platform

INDOHAXSEC claimed a data breach against P1000 (p1000.co.il), an Israeli online shopping platform, publishing samples of alleged customer records -only 2 person- including identity numbers, email addresses, names, phone numbers, delivery addresses, and passwords across two posts. The group continues its pattern of selecting Israeli civilian and commercial targets for maximum public visibility rather than operational impact.

INDOHAXSEC claims breach of Israeli e-commerce platform P1000 by publishing 2 customer records including identity documents, contact details, and credentials

## March 12, 2026: Handala Wipes Stryker, Keymous Sweeps the Gulf, and 313 Team Crosses into Europe

The most significant incident of the day sits well outside the usual DDoS noise. Handala, the MOIS-linked group, claimed a destructive wiper attack against a global medical technology company with real, confirmed operational impact.

Simultaneously, Keymous Plus published the broadest single-day target list of the conflict, sweeping across six Arab countries in one operation. And 313 Team extended the conflict’s geographic reach into Europe for the first time, targeting Romania directly over its government’s public statements.

## Handala Claims Wiper Attack on Stryker via Microsoft Intune

Handala claimed a mass data-wiping attack against Stryker, a global medical technology company with 56,000 employees across 61 countries. The group alleged it erased data from more than 200,000 systems, servers, and mobile devices across Stryker's offices in 79 countries. News reports from Ireland, Stryker's largest hub outside the US, confirmed more than 5,000 workers were sent home. A voicemail at Stryker's Michigan headquarters stated the company was "experiencing a building emergency."

According to a source cited by KrebsOnSecurity, the attack appears to have been carried out by abusing Microsoft Intune, a cloud-based device management platform, to issue remote wipe commands across all enrolled devices. Employees on Reddit confirmed they were urgently instructed to uninstall Intune. The Irish Examiner reported that staff were communicating via WhatsApp, that anything connected to the network was down, and that personal phones with Microsoft Outlook installed had also been wiped.

Handala framed the attack as **retaliation for a February 28 missile strike on an Iranian school** that killed at least 175 people, most of them children. The group labeled Stryker a "Zionist-rooted corporation," referencing its 2019 acquisition of Israeli company OrthoSpace.

Handala's Telegram post claiming a mass wiper attack against Stryker across 79 countries

## Handala Also Claims Verifone Breach — Company Denies It

Separately, Handala claimed on March 11 to have breached Verifone's systems in Israel. Verifone responded, stating it had "found no evidence of any incident related to this claim and has no service disruption to our clients" after monitoring its systems following the allegations. The denial was shared by breach researcher Dissent Doe via LinkedIn.

## Keymous Plus Targets Six Arab Countries, 50+ DDoS Attacks

Keymous Plus published its most expansive operation of the conflict under #Op_Epstein_Gulf, targeting government ministries across Bahrain, Kuwait, Jordan, Qatar, Syria, and the UAE with Check-Host verified DDoS claims in a single coordinated post. Targets spanned nearly every major ministry in each country, including Interior, Finance, Foreign Affairs, Justice, Transport, and Economy, alongside the Qatar Central Bank and the UAE Government Official Portal. Syria's addition to the target list is notable, marking the first time the group has explicitly included Damascus in a Gulf-focused operation, suggesting the campaign is expanding beyond US-allied Gulf states toward the broader regional order.

Keymous Plus publishes Check-Host verified DDoS claims against six Arab countries in a single post under #Op_Epstein_Gulf

## NoName057(16) Extends #OpCyprus with 14 Additional Targets

NoName057(16) returned to Cyprus with a new wave under #OpCyprus, adding 14 verified targets to its previous list. New targets included the Register of Insurance Companies, Organization of Local Government of Limassol, JCC Payment Systems, Authorization Audit Office, Cyprus Statistics Service, Cyprus Government Portal, Live

Buses OSYPA, EAC portal of the Cyprus Electricity Authority, Supreme Court of Cyprus, Ministry of Justice, and Cyprus Ports Authority.

NoName057(16) extends #OpCyprus with a new wave of verified DDoS claims against Cypriot government, financial, and infrastructure targets

### 313 Team Hits Romania Over Base Access Statement

313 Team targeted Romania's National Tax Agency (anaf.ro), one of the most frequently visited government websites in the country, in direct response to the Romanian president's statements allowing the US to use Romanian bases to strike Iran. The group framed the attack explicitly as retaliation, shut the site down completely for one hour, and provided a Check-Host verification link. The operation marks the first confirmed European government target hit by an Iraq-based group in this conflict cycle, and signals that public political statements by European leaders are now being treated as sufficient justification for targeting.

313 Team shuts down Romania's National Tax Agency for one hour, citing the Romanian president's statements on US military base access

## March 11, 2026: New Alliances, Kuwait Swept, and the Short Story of NetStrike

The day's activity was driven less by new capabilities and more by new relationships. A Tunisian group entered the coalition with a formal alliance declaration, immediately put it to work against Kuwait, and the pattern of short-lived groups materializing, claiming attacks, and going quiet continued with NetStrike.

### Hider_Nex Forms Alliance with NoName057(16), Immediately Targets Kuwait

Hider_Nex, a **Tunisian-flagged** group new to this conflict, announced a formal alliance with pro-Russian NoName057(16) under the banner "Together nothing can stop us." Within the same hour, the group launched its most coordinated operation so far under #OpKuwait, publishing **DDoS claims against 18 Kuwaiti government domains** with Check-Host verification links for each. Targets included the Ministry of Defense, Ministry of Foreign Affairs, Ministry of Health, Ministry of Education, Ministry of Finance, the national electricity and water authority, the civil registration authority PACI, the national news agency KUNA, and Burgan Bank. The breadth of the target list, spanning defense, civil services, finance, and public infrastructure in a single post, mirrors the multi-sector sweep pattern established by 313 Team against Kuwait on March 6.

Hider_Nex announces formal alliance with NoName057(16)

### Moroccon Black Cyber Army Claims DDoS on Israeli Bank

Moroccon Black Cyber Army claimed a DDoS attack against Discount Bank, one of Israel's largest financial institutions based in Tel Aviv, framing it as a strike against the "Zionist economy." A Check-Host link accompanied the post. The site was temporarily unreachable during the claimed window. The disruption was real but limited, a brief outage rather than the breach the group's language implied.

Disruption against Discount Bank under #OpIsrael

### NetStrike: A Complete Hacktivist Arc in One Day

NetStrike ran through the full hacktivist lifecycle in a matter of hours. Channel created, alliance declared with Keymous+, DDoS claim published against Galey Israel, a Hebrew-language radio station serving central and northern Israel, Check-Host link posted, and activity stopped. The operational impact was minimal. The pattern, however, is consistent with dozens of short-lived groups that have emerged since March 1: the conflict is functioning as a recruitment and visibility event, pulling in actors who contribute to aggregate volume even when individual impact is low.

NetStrike announces alliance with Keymous+

NetStrike claims DDoS disruption against Galey Israel, a Hebrew-language radio station based in Jerusalem

### INDOHAXSEC Defacement Hits US Corporate Target

INDOHAXSEC claimed a defacement of CareerLab America, a career consulting firm based in Denver, Colorado, serving major corporations including Coca-Cola, AT&T, and KPMG. The group replaced the homepage with its own branding. The target has no direct government or military connection, continuing the pattern of Southeast Asian pro-Iranian aligned groups selecting symbolic US civilian targets for visibility rather than operational impact.

INDOHAXSEC claims defacement of CareerLab America

## March 10, 2026: Critical Infrastructure in the Crosshairs as FSociety Issues 42-Hour Threat

Team Fearless continued its #OpIsrael campaign, claiming DDoS disruption against four Israeli targets: a digital marketing and online advertising firm, Alon Israel Oil Company, Goldtec Technologies (an advanced defense firm), and Amarel Ltd., an industrial and technology services company. Check-Host verification links accompanied each claim. The inclusion of a defense-adjacent and an energy company alongside commercial targets suggests the group is deliberately mixing sector coverage rather than focusing on a single vertical.

Team Fearless claims DDoS disruption against Israeli energy, defense, and commercial targets under #OpIsrael

### NoName057(16) Hits Israeli Critical Infrastructure and Continues Cyprus Campaign

NoName057(16) published a fresh round of Israeli targets under #OpIsrael, claiming disruption of Bezeq (Israel’s primary telecom provider), Mekorot (the national water supply company), Kavim (a major bus operator), and E.M.I.T. Aviation, an Israeli UAV systems company. Check-Host links were provided for each. The combination of telecom, water, public transit, and defense-adjacent targets in a single post reflects the group’s consistent pattern of targeting operationally significant infrastructure rather than symbolic web assets.

NoName057(16) claims disruption of Bezeq, Mekorot, Kavim, and E.M.I.T. Aviation under #OpIsrael

In a separate post, NoName057(16) claimed ongoing DDoS attacks against Cyprus under the #OpCyprus banner, hitting the Office of the Republic of Cyprus, Limassol Airport Express, the OSYPA live bus tracking system, and

the EAC portal of the Cyprus Electricity Authority. The group tagged the campaign with #FuckEastwood and #TimeOfRetribution alongside #OpCyprus, reinforcing that this is treated as a distinct operational theater from their Israeli targeting, tied to their Ukraine conflict grievances rather than the Iran theater.

NoName057(16) continues its #OpCyprus campaign

### FSociety Threatens 42-Hour Operation Against Israel and the US

A Telegram channel operating under the FSociety banner published a threat declaring that within 42 hours the group would “destroy Israel and the Israeli alliance.” The Russian-language post calls on followers to join the channel, share the message, and launch cyberattacks against Israel and the US. The statement frames America as an aggressor attacking Iran without justification and condemns those cooperating with it. At this stage the post is mobilization and threat signaling with no technical evidence of active operations, but FSociety has a history of capitalizing on high-profile conflict moments for recruitment and visibility.

Translation: “Within the next 42 hours we will destroy Israel and the Israeli alliance, and everyone who supports us, join our channel to receive the latest news and share this message with friends and strangers. We hate this society and this world. We hate such animals as America and some fools, because they are involved in the killing of people etc. Israel kills people. America attacks Iran without reason. We condemn America and those who cooperate with it. Everyone cooperates with us. Join us and start cyberattacks on Israel and America!”

## March 7–9, 2026: New Supreme Leader, Wider Borders, Deeper Systems

*Our Week 1 Threat Assessment Report is now available. Check it for a summary of last week’s developments.*

The first week of the conflict generated **368** tracked cyber incidents across a dozen countries, with Israel absorbing **184** of them, followed by Kuwait **(53)** and Jordan **(41)**. Government infrastructure was the single most targeted sector with 84 claims, trailed by financial services, defense, aviation, and education. DieNet led all groups in volume with 59 claimed operations, followed by Keymous Plus **(51)** and 313 Team **(42)**. Attack volume peaked on March 2 with **77 daily claims** before stabilizing at 52–63 per day through the end of the week.

The second week opened with a kinetic development that will shape the cyber domain going forward: **Mojtaba Khamenei** was elected Supreme Leader, succeeding his father. Senior figures, including Ghalibaf, Larijani, and Pezeshkian, pledged allegiance. A new leadership consolidating power under IRGC influence is likely to accelerate rather than temper state-directed cyber operations, particularly as the regime seeks to project continuity and strength. Against that backdrop, the three days covered here show the hacktivist front pushing into new geographies, deeper into OT systems, and for the first time consistently targeting non-Middle Eastern soil.

### OT Claims Intensify: Hotels, Universities, Banks, and Water Systems

The most operationally significant claims of the period came from three separate groups, all asserting control over physical infrastructure rather than just web-facing services.

Cyber Islamic Resistance published a coordinated claim against Prima Park Hotel in Tel Aviv, alleging electricity and water cutoffs alongside exfiltration of customer data. The same post claimed access to Technion’s administrative network and Haifa’s main electrical line, framing the operation as retaliation for 165 students killed

in Iran. A separate post from the group published a grid of screenshots showing alleged access to multiple ICS and SCADA systems simultaneously — building management panels, pipeline schematics, and process automation dashboards — described as a “first wave” with more to follow.

Cyber Islamic Resistance shares alleged SCADA grid screenshots

APT Iran published screenshots of live solar PV monitoring dashboards for Bank al Etihad in Jordan, claiming backdoor access to the bank’s energy control systems. The same post alleged breach of the Aqaba Special Economic Zone (ASEZA) and ISAR Engineering through legacy FileManager vulnerabilities, with full read/write access to energy dashboards visible in the screenshots.

APT Iran -has a verified but thwarted ICS attack claim- shares the alleged Bank al Etihad OT dashboard screenshot

NoName057(16)’s DDoSia Project published what it described as full access to an Israeli industrial pump control HMI with a Hebrew-language interface, claiming real-time control of pumps, valves, alarms, and the ability to switch between automatic and manual modes. The post stated volunteers “disabled an important part of Israel’s critical infrastructure in a couple of minutes.” As with almost all OT claims in this conflict, independent verification has not been established — but the consistency of Hebrew-language interface screenshots across multiple groups over multiple days suggests at minimum a coordinated effort to identify and probe exposed Israeli ICS assets.

NoName057(16) alleged water pump HMI screenshot

### Geographic Expansion: Cyprus, the United Kingdom, and Saudi Arabia

Team Fearless published Check-Host verified DDoS claims against five Saudi Arabian government portals: the Saudi Embassy website, Ministry of Interior, Ministry of Commerce, Ministry of Health, and the National Digital Government Information Portal.

Team Fearless Saudi Arabia target list

Cyber Islamic Resistance and 313 Team jointly claimed defacement of the Saudi University of Business and Technology (UBT), replacing the homepage with group branding.

CIR and 313 Team UBT defacement

NoName057(16) expanded its geographic scope to Cyprus, claiming DDoS disruption of six targets: the Authorization Audit Office, Hellenic Bank portal, Central Bank, Public Transport Cyprus, Cyprus Chamber of Commerce, and the CY Login national digital identity system. The group’s justification was explicit — Cyprus hosts Swarmly, the manufacturer of H-10 Poseidon drones supporting Ukrainian artillery.

NoName057(16) Cyprus DDoS

The framing ties the Cyprus campaign directly to the group’s Ukraine conflict grievances, not the Iran theater, illustrating how pro-Russian actors are using the current moment to pursue **parallel agendas under a single operational umbrella.**

The same group also claimed live surveillance access to Anglia Indoor Karting in Ipswich, UK, publishing real-time CCTV footage from inside the facility. Its high possibility that hacktivist groups are trying to show how they can also gather ‘’intelligence,’’ significantly more targeting of CCTV cameras observed during this conflict period.

NoName057(16)’s UK CCTV hijack claim

### Cyber Isnaad Front Sustains Its Leak Campaign

Allegedly IRGC-aligned, Cyber Isnaad Front, continued publishing material from its claimed breach of telecom and fuel logistics infrastructure — 160+ data centers allegedly compromised and 5TB exfiltrated from a national fuel logistics provider. The group’s sustained publication cadence across multiple days, regardless of verification status, functions as an information operation in its own right: maintaining narrative pressure and forcing defenders to allocate resources to triage claims of uncertain authenticity.

### What the Pattern Shows

Taken together, the March 7–9 activity reflects three converging trends. First, OT and ICS claims are becoming routine across multiple groups simultaneously, normalizing the targeting of physical infrastructure in ways that will outlast this specific conflict.

Second, the geographic perimeter is no longer just the Middle East. Cyprus and the UK are active targets, with distinct justifications from different actor clusters.

Third, the election of a new Supreme Leader introduces a variable that could either consolidate and professionalize Iran’s cyber posture or trigger a surge in proxy activity as groups attempt to demonstrate loyalty to the new leadership.

## March 6, 2026: Gulf Governments Under Siege, Iraqi Cyber Resistance Declares War on Kuwait

The hacktivist front keeps expanding, but the more significant development today sits beneath it. Upcoming findings confirming that MuddyWater, an Iranian state-sponsored group operating under the Ministry of Intelligence and Security, had already planted backdoors inside a U.S. bank, airport, defense-adjacent software company, and NGOs in the U.S. and Canada before the first strike of Operation Epic Fury.

The group’s Israeli operation appears to have been the primary target, with a new implant named Dindoor deployed across its networks alongside a second Python-based backdoor called Fakeset. Jordan’s National Cybersecurity Center also officially confirmed it **thwarted an Iranian attack on its wheat silo management system**, the first government-confirmed foiled OT intrusion of this conflict, lending **credibility to the APT Iran claims** covered in our **March 4 update.**

The surface noise is loud. The quieter activity underneath it may be the part that matters more.

### RuskiNet Brings #OpIsrael to Israeli Industry

One of the less known actors, RuskiNet Group posts daily DDoS attacks. Their latest Check-Host verification links targeting turpaz.co.il, the website of Turpaz Industries, a TASE-listed Israeli manufacturer operating across food, beverage, pharma, and cosmetics sectors. Before/after availability snapshots confirm a disruption window. As primary government and financial sites harden behind DDoS mitigation, groups are pivoting toward publicly traded industrial companies where uptime carries reputational and investor consequences.

RuskiNet targets Turpaz Industries under #OpIsrael

## DieNet Strikes Qatar Through Amazon's Network

DieNet Media post framed the Qatar campaign as retaliation for Qatari state media blacking out coverage of Iranian strikes on U.S. bases within its borders. Nine government sites were listed as targets: Ministry of Interior, Hukoomi (Qatar's eGovernment platform), Ministry of Labor, Central Municipal Council, General Authority of Customs, Ministry of Transportation, and Ministry of Education. The framing of Qatar as complicit in US-aligned information suppression signals that the Gulf escalation is politically motivated, not opportunistic.

DieNet's API bot posts real-time disruption of Qatar's open data portal via Amazon's IP network, a routing choice that signals capability beyond basic stresser tooling

DieNet Media's full Qatar target list spans nine government domains across customs, transport, labor, and eGovernment infrastructure, framed explicitly as retaliation for media censorship

### A British Charity Site in Conquerors Electronic Army Propaganda

A Conquerors Electronic Army propaganda poster, styled under the "Wa'd al-Akhira" banner with militant imagery and Quranic verse, references a UK-registered charity (est. 2008) described as collecting donations to fund civil society projects inside Israel, including psychological care and emergency relief. Whether the site was targeted, breached, or merely cited in an influence operation is not confirmed, but a Check-Host link in the same post suggests a disruption attempt accompanied the claim.

Conquerors Electronic Army embeds a British-registered charity link under their operational banner. The Check-Host stub in the same post implies a disruption attempt, not just an information operation.

### 313 Team Declares a Comprehensive Assault on Kuwait

The Islamic Cyber Resistance in Iraq, 313 Team, claimed targeting of 26 Kuwaiti government IP domains, alleging the national e-government portal was offline for over 18 hours. Named targets span Kuwait's entire public administration: Ministry of Defense, Kuwait Credit Bank, National Guard, Ministry of Electricity, the Army, Public Authority for Civil Information, Ministry of Health, Central Agency for Information Technology, Public Authority for Manpower, Public Works, Public Authority for Youth, the Government Performance Monitoring Agency, and the Civil Service Commission, among others. Kuwait has already been the single most targeted nation in this conflict cycle. The 313 Team's sweep, if even partially confirmed, represents the most coordinated single-group assault on any Gulf government's digital infrastructure so far.

313 Team's full Kuwait target list, 15 named government institutions spanning defense, civil information, and communications, claimed alongside an 18-plus hour shutdown of the national e-government portal

# March 5, 2026: Two Wars, One Cyber Front, Data Breaches, New Recruits, and the Expanding Target Map

Iran's hackers stay quiet behind a near-total blackout, but the groups filling the void are no longer just Middle East players. Pro-Iranian hacktivists and Russian-aligned collectives are running DDoS attacks, data leaks, and infrastructure probes across the US, Israel, and the Gulf — and now India and Pakistan are appearing in the target map too, suggesting the fallout from two separate regional conflicts is beginning to blur into a single cyber theater. CISA, the agency meant to hold the line, is understaffed and mid-reshuffle. The wars are still distinct on the ground. In cyberspace, the boundaries are dissolving.

## Cyber Jihad Movement Calls for Global Cyber Campaign

A propaganda poster circulated online under the banner **Cyber Jihad Movement**. The message calls on supporters to join a global cyber campaign described as "Cyber Jihad." The statement urges participants to conduct cyber disruptions against government institutions, financial systems, and public agencies connected to the United States, Israel, "Arab governments," Pakistan, and India.

Cyber Jihad Movement propaganda message calling for global cyber participation

The statement explicitly declares the group's entry into what it describes as the **Iranian–American war** and the conflict environment in the **Afghanistan–Pakistan region**. The group claims it will provide cyber assistance to militant actors associated with the Taliban and the Islamic Emirate of Afghanistan.

At this stage, the announcement appears primarily ideological and mobilization-focused. No concrete technical evidence of attacks attributed to this specific group has surfaced yet.

## Data Leaks and Credential Breaches: Israel and Iran Both Targeted

The hack-and-leak front intensified on March 5, with groups on both sides of the conflict claiming database access and credential dumps.

**Anonymous Syria Hackers** escalated their #OP_IRAN campaign by claiming a breach of an Iranian e-commerce platform, alleging access to PayPal login credentials, usernames, personal email addresses, and bcrypt-encrypted passwords.

Anonymous Syria Hackers claims breach of Iranian e-commerce site, posting PayPal credentials to BreachForums under #OP_IRAN

The data was posted to BreachForums with instructions requiring users to comment on the post to unlock the download link.

The leaked dataset was posted on BreachForums, gated behind a comment-to-unlock mechanic

On the other side, **Keymous** claimed a far more sensitive breach: the Israeli Ministry of Education's internal "Education Institutions Portal" — a backend system used exclusively by school administrators and teachers to manage student records, class lists, teacher employment data, and Bagrut (matriculation) exam records. The group

alleged access to over 300,000 rows of data. This is not a public-facing website. If confirmed, it represents a meaningful intrusion into national education infrastructure.

Keymous claims 300,000+ records from Israel's Ministry of Education internal portal, including student and teacher data

## DDoS Campaigns Continue Against Israeli Government and Financial Infrastructure

Disruption operations against Israeli targets remained active, with multiple groups publishing Check-Host verification links as proof of impact.

**DarkStorm Team** claimed coordinated DDoS attacks against seven Israeli targets under the #OpIsrael banner, listing MAX (a financial services platform offering credit cards and loans), the Prime Minister's Office, Ministry of Foreign Affairs, Ministry of Finance, Ministry of Justice, the Israel Security Agency, and the intelligence agency. The breadth of the target list — spanning financial, governmental, and intelligence infrastructure in a single campaign — reflects the group's continued ambition to hit symbolic high-value targets simultaneously.

DarkStorm Team claims DDoS across seven Israeli targets, including the PM's Office and intelligence agency

**Team Fearless** published a similar multi-target DDoS claim hitting the Israeli Tax Authority, the official IDF website, Sony Pictures Israel, a civic government engagement platform, a transit technology company, and the Oron Group. The inclusion of Sony Pictures is notable — it suggests target selection is broadening beyond pure government and military infrastructure toward commercial entities with Israeli presence.

Team Fearless claims DDoS hits on IDF site, Israeli Tax Authority, Sony Pictures Israel, and others

## New Entrants and Internal Tensions

**Server Killers**, a Russian-linked group, officially announced it has entered the conflict, citing the US-Israel strikes as justification. The announcement continues the pattern observed since March 3, when pro-Russian actors began formally joining the pro-Iran hacktivist coalition. The cyber front is no longer regional — it is drawing in actors with their own grievances against the US-Israel.

Pro-Russian Server Killers officially joins the conflict, citing US-Israel strikes as justification

**DieNet** issued a rare public statement addressing the Gulf populations directly, clarifying that their targeting is directed at governments — not people — framing Gulf states as instruments of American regional power. What is more telling is their admission that the decision to target Gulf governments came after significant internal disagreement within the team. Public fractures like this are uncommon and worth monitoring.

DieNet addresses Gulf populations directly, admitting internal disagreement over the decision to target Gulf governments

## Academic and Media Infrastructure in the Crosshairs

**Cyber Islamic Resistance**, operating in coordination with FADTEAM in Iraq, claimed to have breached **WeLearn**, an Israeli academic platform, accessing its user database alongside series and episode content tables.

The post was dedicated to Khamenei and framed explicitly as retaliatory. Targeting academic platforms mirrors a broader trend: as hardened government targets prove more resilient, groups are shifting toward softer institutional infrastructure — universities, media, and education systems — where defenses are typically weaker.

Cyber Islamic Resistance claims breach of Israeli academic platform WeLearn, coordinated with FADTEAM

## March 4, 2026: OT Intrusion Claims, Multi-Vector Escalation, and the Expanding Target Map

The hacktivist landscape continued to intensify on March 4. Three trends stand out: a shift toward claimed OT and ICS intrusions, DieNet's expansion into Jordanian civilian infrastructure, and new water infrastructure claims by Z-Pentest Alliance against Israeli targets.

### DieNet Expands Its Jordan Campaign to Civilian and Utility Sectors

DieNet Network, previously observed targeting Kuwaiti government domains, has now declared Jordanian cyberspace its primary target. The group issued a preemptive warning urging Jordanian website administrators to take their sites offline before an imminent attack wave. The message was paired with satellite imagery of Jordan outlined in red, a visual format designed to amplify psychological pressure.

DieNet's ''warning'' post, shared in their Telegram channel

Claimed activity on March 4 included the disruption of a university-linked radio stream, with CheckHost results shared as proof of outage. The group's automated Telegram bot published real-time attack notifications.

Automated DDoS attack claim by DieNet API

DieNet is targeting a streaming service in Jordan

In a separate post, also forwarded through SYLHET GANG-SG, DieNet claimed access to employee account data from the Jordanian Electricity Distribution Company, including payroll records, national ID numbers, and HR data. The breadth of data fields listed suggests either a genuine credential-level compromise or access to a previously stolen dataset being repackaged for narrative effect.

DieNet's Telegram post, claiming employee account access and PII data

### APT Iran Claims OT-Level Intrusion into Jordanian Grain Storage

The most significant claims on March 4 come from a Telegram channel operating under the **APT Iran** banner, alleging deep intrusion into the Jordan Silos Company, a state-linked grain storage entity. The claim describes a phishing-enabled initial access operation roughly one month prior, followed by internal reconnaissance and alleged access to silo control systems governing temperature, humidity, weighing, and solar power infrastructure.

The alleged attack that is announced through the APT Iran Telegram channel

The actor claims to have gradually raised temperatures in northern silos to degrade stored wheat without triggering alarms, manipulated weighing software to underreport actual weight by 10%, and disabled solar inverters to force

reliance on limited diesel backup power. A solar PV monitoring dashboard was published alongside the claim, showing zero active power output, though this could reflect normal overnight readings rather than attacker-induced disruption.

**Warning**: These claims require significant caution. The level of narrative detail is high enough to be either genuine or deliberately crafted for psychological effect. Independent verification has not been confirmed. If any portion of the OT access claim is genuine, it would represent a meaningful escalation beyond DDoS into operationally relevant critical infrastructure interference.

### Z-Pentest Alliance Claims Access to Israeli Water Infrastructure

The pro-Russian Z-Pentest Alliance published a claim asserting full access to a pump control and water supply management system in Israel. The post was accompanied by what appears to be a screenshot of an HMI panel showing Hebrew-language controls for water pressure, flow rate, supply meters, and pump operating hours. The group claims the ability to switch equipment on and off, change settings, and trigger emergency processes.

Z-Pentest Alliance’s Telegram post, Russian threat groups are dividing their attention between Ukraine and Israel

The screenshot shows controls consistent with a real water management interface, but attribution to a specific Israeli operator has not been confirmed. The claim may reflect access to a test or decommissioned system. Regardless, the targeting intent is clear and consistent with prior OT-focused campaigns by groups like Cyber Av3ngers, which have historically targeted water infrastructure across the region.

### Conquerors Electronic Army Sustains Multi-Sector DDoS Campaign Against Israel

Operating under the **“Wa’d al-Akhira”** operational banner, Conquerors Electronic Army claimed five separate attacks against Israeli targets within a 12-hour window on March 4. Sectors hit across the campaign included civil emergency alerting, financial services, media, industrial, and healthcare. Each claim referenced CheckHost proof-of-disruption links and rented stresser infrastructure. The targeting of a civil alert system is the most operationally sensitive claim, though no independent confirmation of sustained impact has been established.

### NoName057(16) Targets The Jerusalem Post

Pro-Russian collective NoName057(16) claimed DDoS disruption of an Israeli internet service provider and a major Israeli news outlet on March 4, noting that both targets had moved behind DDoS mitigation stubs. The group framed the mitigation as the defender “hiding” rather than a successful defense, a rhetorical move designed to maintain narrative momentum even when attacks are blocked.

NoName’s Telegram post, the group is dividing its current attention between Germany and Israel

NoName’s re-engagement with Israeli targets confirms that pro-Russian groups are joining the cyber activity in support of Iran, a trend we flagged a day before.

### Broader Context: The OT Threshold Is Being Tested

Taken together, the March 4 activity marks a shift in claims being made. Groups are moving from DDoS against web assets toward alleged access to operational technology systems in food storage, water supply, and energy infrastructure. Whether the OT claims reflect genuine intrusions or elaborate information operations, the intent to signal capability against physical infrastructure is deliberate.

Despite the various claims, we haven't spotted any major Iranian APT activity. The gap between hacktivist claims and verified impacts remains wide. But the normalization of OT-targeting rhetoric across pro-Iranian, pro-Palestinian, and pro-Russian actor clusters is itself a meaningful intelligence signal. Organizations operating water, energy, food supply, and government infrastructure in Israel, Jordan, and the broader Gulf region should treat the current environment as an elevated risk regardless of claim verification status.

## March 3, 2026: Pro-Russian Hackers Have Joined the Lobby, Critical Infrastructures Under Attack

The current wave of cyber activity reflects expansion rather than escalation. Compared to the previous 12-day war cycle, the number of active hacktivist groups remains noticeably lower. However, operations have widened geographically, especially toward Gulf states perceived as politically aligned with Israel or the United States.

Another important visibility factor is Iran's restricted internet environment. With domestic connectivity heavily limited, direct activity from inside Iran is less observable. Instead, most visible operations originate from pro-Iranian actors outside Iran, particularly in Southeast Asia, Pakistan, the broader Middle East, and Shia-aligned communities abroad. This creates an ecosystem that is decentralized and narrative-driven rather than centrally coordinated at scale.

At the same time, Russian-affiliated hacktivist clusters appear to divide their operational focus between Europe and the Middle East. This signals structured targeting priorities instead of spontaneous mobilization. Below are the highlights of the last day:

### Further Expansion into the Gulf

Keymous is declaring daily targets, Kuwait, Jordan, and lastly Saudi Arabia

Kuwait, Jordan, and Saudi Arabia, respectively, emerged as declared "visit" targets under a themed campaign branding of the group Keymous, followed by public sector disruption claims against multiple ministries, including Interior, Finance, Education, Oil, and the central government portal.

Keymous' alleged DDoS targets inside Kuwait

Screenshots shared via Telegram show connection timeouts across international nodes using public uptime testing services. Similar validation methods were used in claims against Oman's government portal.

DieNet is one of the first hacktivist groups to target Oman

### Targets Inside Israel

Israeli banking institutions named as targets in coordinated DDoS claims. Financial institutions remain high-value symbolic assets due to public sensitivity and media amplification potential.

DarkStorm's Telegram post, targeting Israeli financial institutions

Short-lived service disruptions can create an outsized psychological impact even when technical damage remains limited. The repeated use of third-party uptime validation links suggests a standardized campaign method rather than independent intrusion activity.

Hacktivists are gathering under the #OpIsrael hashtag

## Large Scale Critical Infrastructure Narratives

Some actors escalated rhetoric by claiming full control over Israeli and US military government systems, including defense manufacturers. These statements included language about shutting down systems and burning networks.

Moroccan hacktivist claims ‘’complete control over all systems’’ with a DDoS attack(!)

However, no technical evidence supports such claims. The proof material again points toward availability testing rather than internal compromise.

Another narrative involves the alleged targeting of Israeli healthcare infrastructure, including one of the country's largest health service providers. Shared imagery included CCTV-style screenshots branded with ideological logos.

“In the great Battle of the Promised Conquest and the latest war, the Mujahideen carried out a raid on Clalit Health Services facilities (Hebrew: שירותי בריאות כללית), which is considered the largest health fund in the occupied territories.”

Healthcare targeting claims raises psychological stakes. However, no validated evidence confirms operational compromise.

In another claim, an IRGC-affiliated Telegram channel with more than 526,000 subscribers shared a post claiming a large-scale cyber operation against Israeli communication networks.

The message alleges penetration of over 160 data centers and disruption of internal systems across multiple locations. No technical evidence accompanies the claim, and the post appears primarily narrative-driven, aimed at signaling scale and projecting impact rather than demonstrating verifiable compromise.

“Large-scale cyber attack against the communication networks of the Zionist regime / Penetration into 160 data centers”

## Data Leak Operation

Several channels distributed links to files labeled as Israeli military databases or intelligence personnel lists. File names reference Mossad agents and military datasets.

Liwaamohammad's Telegram channel, sharing alleged data leaks

At this stage, authenticity remains unverified. In previous cycles, similar file naming tactics served propaganda purposes without substantiated data exposure. Verification requires forensic validation before drawing conclusions.

## March 2, 2026: Escalation Across Critical Infrastructure, Ransomware, and Coordinated Campaigns

On the third day of the conflict, multiple actors escalated operations toward critical infrastructure across Israel and the Gulf states. Below we curated the highlights of the day:

Cyber Islamic Resistance and affiliated channels shared imagery allegedly showing access to industrial control environments, including PLC controller interfaces and energy monitoring dashboards. One screenshot references a VeroPoint PLC controller system. Another shows what appears to be a live energy production interface with operational data visualization.

Cyber Islamic Resistance’s alleged attack on PLC controllers

Accompanying claims state that attackers accessed internal networks of energy-related facilities and manipulated operational parameters. The messaging suggests prolonged access before disclosure. While independent validation is pending, the emphasis on energy systems marks a shift from public-facing website disruption toward OT/ICS-themed targeting.

APT IRAN claims it infiltrated Jordan’s critical infrastructure, maintained access for over a month, and manipulated power plant control systems, alleging up to a 75% reduction in electricity output.

In parallel, DieNet-affiliated messaging published a structured list of government, airport, financial, telecom, and utility targets across Qatar, Bahrain, the UAE, Kuwait, and Saudi Arabia. Specific references include ministries, airports, banks, and electricity and water authorities.

Targets of the DDoS attacks shared by the group “DieNet”

Check-host screenshots indicate connection timeouts consistent with DDoS activity against government and aviation infrastructure domains. Critical infrastructure is now being explicitly framed as the operational focus.

### Ransomware Activity

An Israeli-linked entity, ramet-trom.co.il, appeared on a ransomware disclosure blog associated with INC Ransomware. The listing claims approximately 1 terabyte of exfiltrated data, including blueprints and contracts.

INC Ransomware’s alleged disclosures, listing an Israeli company, were claimed as a ‘’political’’ attack rather than financial.

### Website Defacements

Cyber Islamic Resistance and Cyb3r Drag0nz Team claimed defacements of Israeli websites.

Defacement attack by Cyb3r Drag0nz

Defacement pages displayed coordinated branding and a unified coalition banner referencing multiple aligned groups, including 313 Team, Moroccan Black Cyber Army, and others.

Defacement attack by Cyb3r Drag0nz #2

Messaging emphasizes collective mobilization under a shared “electronic operations room.” The branding indicates cross-group coordination rather than isolated defacement incidents.

## Leaks and Reconnaissance Announcements

Anonghost published a file labeled “120K_USA_NetBlock.txt” claiming ownership or scanning of large U.S. IP ranges. The shared screenshot shows active scanning activity across 72.x.x.x address ranges.

AnonGhost’s reconnaissance sharings

The content appears to reflect reconnaissance or port scanning rather than confirmed compromise. However, the scale and framing signal intent toward U.S.-based network mapping.

Separately, groups using DieNet’s DDoS tools announce systematic attacks across Middle Eastern entities. It is possible to say that DieNet will provide the arsenal for many small hacktivist groups during this conflict.

Mad Ghost’s DDoS announcement

DieNet’s messaging expands the perceived conflict zone to **Cyprus**, citing the presence of British military bases as a strategic trigger point. Notably, this narrative circulated even before public reporting that the UK had granted permissions related to U.S. operations, suggesting that Cyprus was already being framed as a legitimate target within aligned cyber channels.

Given Cyprus’ role as a host to British bases, escalation toward it was foreseeable. Today’s reported Iranian drone impact on the island further reinforces that Cyprus is no longer peripheral to the conflict dynamic.

DieNet is targeting Cyprus due to British Bases

The overlap between kinetic activity and cyber threat signaling increases the likelihood of sustained targeting against Cypriot government, aviation, or infrastructure assets. The conflict perimeter is visibly widening beyond Israel and the Gulf, and Cyprus is now positioned within that expanding operational geography.

## Resurrected Threat Actors

Day 3 also shows signs of reactivation among previously known collectives. Several groups that had remained dormant or low-visibility in recent months are now resurfacing with renewed messaging and operational signaling.

**Team Fearless** announced its return, framing the current conflict as a renewed mission. While no technical proof accompanied the statement, the tone and branding signal intent to re-enter the operational landscape.

Pro-Palestine group Team Fearless’ Telegram post

**CyberAv3ngers** and **Al Toufan** channels have also shown signs of renewed activity. Even where direct attack claims are limited, signaling behavior, messaging frequency, and cross-channel amplification indicate preparation or coordination phases.

**Handala** is already highly active, with defacement activity and explicit threats directed at Israel's fuel and energy sector. The group's messaging focuses on strategic infrastructure rather than symbolic web assets, aligning with the broader shift toward critical industry targeting.

Handala claims compromise of an i24 News administrative interface

Collectively, this pattern reflects a widening mobilization cycle. Dormant or semi-active groups are repositioning themselves within the conflict narrative, increasing the likelihood of coordinated or parallel operations in the coming days.

## March 1, 2026: Hacktivist Collectives & Alliances Emerging

A collective operating under the name **Cyber Islamic Resistance** has announced the formation of a joint "Electronic Operations Room" and the launch of a general cyber mobilization campaign. The group publicly called for cyber warfare participants to join through an official contact channel and stated that multiple previously known hacktivist teams have formally joined the initiative.

Cyber Islamic Resistance's Telegram announcement

In subsequent messages, affiliated teams declared their integration into the operations room and claimed the start of coordinated attacks against Israeli websites. The campaign is framed as a unified electronic front under the broader "Islamic Resistance Axis" narrative.

The RipperSec team joins the axis

The Cyb3rDrag0nzz team joins the axis

The messaging indicates consolidation of several hacktivist entities under a single umbrella brand, followed by the initiation of coordinated disruptive cyber activity.

Alleged proof-of-access screenshots shared by the "Cyber Islamic Resistance" collective, showing a compromised network device management interface and ACL configuration panel, presented as evidence of intrusion into Israeli infrastructure.

### Current #1 Targets are Gulf Countries

The "313 Team," operating under the Islamic Cyber Resistance in Iraq banner, claimed responsibility for a disruptive attack against the official portal of the Jordanian government (jordan.gov.jo), alleging full website disablement. The group shared an SSL error screenshot as proof of impact and referenced third-party uptime verification links.

Alleged DDoS attack targeting Jordan's .gov domain

In a subsequent statement, the group expanded its threat posture, declaring that “the hand of revenge will reach the servers” of multiple states, explicitly naming Jordan, Saudi Arabia, the UAE, and Kuwait, alongside Israel and the United States.

313 Team declaring their targets

This marks a clear geographic broadening of declared targets from Israel-centric disruption toward Gulf state government infrastructure, signaling potential escalation across regional public sector domains.

Nation of Saviors claims breach of Saudi engineering firm Baran Company, alleging 21 GB of data exfiltration and announcing intent to release private data publicly.

## Targeting Will Expand Toward Israel and the United States

While Gulf government portals were initial targets, recent activity suggests that operations are expanding toward Israeli and U.S. entities.

Moroccan Black Cyber Army claimed a large-scale cyberattack against TCS Communications in Tel Aviv, alleging disruption of communication and server services. The group shared third-party uptime verification links to support its claim. Targeting a telecommunications provider indicates an intent to affect service-layer infrastructure rather than isolated web assets.

Moroccan Black Cyber Army’s Telegram post, claiming a DDoS attack

Keymous Plus published a mobilization statement calling for intelligence gathering, alliances, and operational coordination in the context of the current conflict. Although no technical evidence was provided, the messaging emphasized reconnaissance and collaboration, suggesting preparatory activity that could precede data exposure or intrusion attempts against Israeli and U.S.-linked organizations.

Keymous’ mobilization announcement

Nation of Saviors released alleged personal data linked to a U.S. military-related entity, including contact details and IP information. The post framed the exposure as retaliation.

A doxxing post by Nation of Saviors in their Telegram channel

The scope of activity is broadening, with Israel and the United States naturally positioned as central targets in both disruption and exposure campaigns.

## DDoS Will Remain the Primary Attack Vector

Distributed Denial of Service activity continues to emerge as the most frequently used technique across the current escalation. Recent posts from multiple collectives reinforce that service disruption, rather than deep network compromise, remains the dominant operational approach.

Nation of Saviors claimed the takedown of Israel’s Ministry of Education portal, sharing third-party check-host screenshots indicating connection failures and a reported 503 server error. The group stated the site would remain

down for an extended period, framing the action as a sustained disruption.

Alleged DDoS attack by Nation of Saviors targeting Israeli governmental domains

Similarly, posts forwarded by SYLHET GANG-SG and related channels promoted ongoing “DieNet network” attacks targeting Kuwaiti government domains. The shared material included automated check-host results showing connection timeouts across multiple nodes, consistent with volumetric or application-layer DDoS activity.

DieNet network notice indicating ongoing DDoS activity against Kuwaiti governmental domains

These examples align with patterns observed earlier in the escalation, where DDoS attacks were repeatedly used to generate visible service outages and public proof-of-impact screenshots. The technique offers rapid deployment, high visibility, and a low technical threshold compared to more complex intrusion or destructive operations.

Automated DieNet DDoS alert claiming active targeting of the Kuwaiti Airport website

DDoS remains the preferred method for achieving immediate disruption, media amplification, and psychological impact across both government and infrastructure-related targets.

## Conclusion

The hacktivist front of this conflict showed how quickly a regional war can become a global cyber mobilization. DDoS remained the dominant method, but the more significant shift was the steady normalization of OT targeting, with groups across multiple coalitions claiming access to water, energy, and food infrastructure regardless of whether those claims held up to scrutiny. The rhetoric alone carries operational weight. As a new Supreme Leader consolidates power in Tehran, both state-directed and proxy cyber activity are likely to intensify rather than wind down.

For continued coverage, verified incident data, and deeper threat intelligence, follow SOCRadar’s full analysis at socradar.io/blog/cyber-reflections-us-israel-iran-war.

---