



IRAN-ISRAEL CONFLICT

Threat Landscape Report



Table of Contents

Executive Summary	3
Timeline	4
Geopolitical Risk Overview	7
Cyber Threat Landscape	8
Threat Actors	21
Disinformation and Influence Operations	26
Recommendations and Risk Forecast	31

Executive Summary

The conflict between Israel and Iran escalated over time, evolving from indirect proxy warfare into direct military confrontation by mid-2025. Key events in this escalation include:

- In June 2025, Israel launched Operation Rising Lion, conducting airstrikes on Iranian nuclear and military facilities.
- Iran responded with missile and drone attacks targeting major Israeli cities, though most attacks were intercepted.
- Israel carried out targeted assassinations, killing high-ranking Iranian officials, including Iran's intelligence chief and Quds Force commander Saeed Izadi.
- The United States intervened by conducting airstrikes against Iranian nuclear sites, increasing geopolitical tensions globally.

Throughout the conflict, cyber threats surged significantly, involving state-sponsored cyber groups, hacktivists, and various international actors:

- Israeli-linked Predatory Sparrow launched impactful cyberattacks, notably breaching Iran's Bank Sepah, leading to major disruptions.
- Iranian cyber groups, particularly Charming Kitten (APT35) executed targeted phishing campaigns against journalists, cybersecurity experts, and critical infrastructure sectors.
- Hactivist groups, including Mr. Hamza, Keymous, and Arabian Ghosts, frequently conducted Distributed Denial of Service (DDoS) attacks and spread propaganda targeting Israeli, U.S., and Middle Eastern entities.
- Telegram emerged as a key platform, recording over 600 unique cyberattack claims within a 15-day period during peak conflict activity.
- Dark Web activities surged, marked by increased data leaks targeting Israel and commercial cybercrime targeting Iran.

The escalation of direct conflict and cyber activities presents substantial strategic implications for stakeholders, including:

- Risks to critical infrastructure sectors such as energy, finance, telecommunications, and healthcare increased.
- Economic instability amplified by fluctuating oil markets and disruptions to maritime trade due to regional proxy activities.
- Significant spread of disinformation and AI-generated fake content aimed at civilian populations, intended to create fear, confusion, and societal instability.
- Urgent need for enhanced cybersecurity protocols, including strong monitoring systems, efficient response strategies, and effective public communication efforts to counter disinformation.

Timeline

Notable Political Events

Notable Cyber Events

JUNE 13



- Israel launches Operation Rising Lion: Massive airstrikes on Iranian nuclear/military sites.
- Iran responds with a large missile-drone barrage targeting Israel. Most are intercepted.
- Casualties on both sides, infrastructure disrupted.

- Iran-linked hackers launch **fake SMS alerts**, spoofing Israel's Home Front Command.
- Hacktivist groups begin **DDoS attacks** on Israeli government and media sites.
- Israeli cyber units likely disrupt Iranian air defense systems.

JUNE 14



- Iranian media reported two projectiles, followed by an explosion and a fire at Tehran's Mehrabad International Airport.

- Over **30 DDoS attacks** claimed by pro-Iran groups like **Mr. Hamza and Arabian Ghosts**.

JUNE 16



- Iran-linked groups spread **fake SMS and Telegram alerts** about gas leaks and evacuation orders.
- Messages include phishing links.
- Israeli authorities respond with counter-warnings.

JUNE 16-17



- Hostilities peak: Iran strikes Tel Aviv, Haifa, Jerusalem; Israel strikes back at extensive military and media targets within Iran. Civilian areas and hospitals were impacted.
- The IDF hit a building where several senior officials of Iran's intelligence organizations were staying, was targeted, killing Iran's intelligence chief and other key senior officials.
- The IAEA stated that Israeli attacks likely damaged the underground facilities in Natanz.

Timeline

Notable Political Events

Notable Cyber Events

JUNE 17



- The Washington Post confirmed four strikes in Tel Aviv. While the Mossad headquarters was not hit, Camp Moshe Dayan, home to Israel's Military Intelligence Directorate and Unit 8200, was directly targeted.

- **Predatory Sparrow** hacks **Bank Sepah**, claiming full data destruction.
- Customers report service outages and blocked accounts.
- Hacktivist attacks on Israeli targets continue.

JUNE 18



- Predatory Sparrow breaches **Nobitex**, burning **\$90M** in crypto.
- Source code partially leaked; exchange goes offline.
- **Iranian state TV (IRIB)** is briefly hijacked by Israel-linked hackers.
- Iran experiences a **nationwide internet blackout**.

JUNE 19



- A direct hit destroyed the IR-40 reactor building at Arak and nearby heavy water towers. The IAEA confirmed the reactor was inactive and held no nuclear material.

- Internet in Iran remains down.
- Iranian cyber teams likely purge compromised systems.
- Hacktivists continue defacements and DDoS attacks.

JUNE 20



- Iranian actors scan **Israeli home cameras** and IoT systems.
- Israeli cyber agency confirms the activity.

JUNE 21-22



- Defense Minister Israel Katz announced that the IDF had killed Quds Force commander Saeed Izadi.
- Iran confirmed the death of a tenth nuclear scientist.

- Low-level DDoS and propaganda continue.
- Attack counts are rising in hacktivist threat landscape.

Timeline

Notable Political Events

Notable Cyber Events

JUNE 22



- U.S. B-2 bombers and Tomahawks strike Fordow, Natanz, Isfahan nuclear sites. China, Russia, EU condemn.

JUNE 23



- Iran launches missiles fired at Al Udeid (Qatar) and at U.S. bases in Iraq. Mostly intercepted, no casualties.
- U.S. announces a ceasefire.

JUNE 23-24



- **Ceasefire begins.**
- Telegram channels quiet down but stay active.

JUNE 25-26



- Despite the truce, **DDoS attacks persist at lower levels**, mostly by Russian-aligned groups.

Geopolitical Risk Overview

Between October 2023 and June 2025, tensions between Israel and Iran escalated dramatically, shifting from years of proxy warfare to open, direct confrontation. Following the October 7 events, Iran's regional allies, including Hezbollah and the Houthis, opened multiple fronts against Israel. During the early stages, Tehran offered vocal support while steering clear of direct engagement.

A major turning point came in April 2024, when an Israeli strike on Iran's consular compound in Damascus killed several senior commanders of the Islamic Revolutionary Guard Corps (IRGC). In response, Iran launched its first direct attack on Israeli territory, deploying drones and missiles.

The conflict quickly widened. In Syria, Israeli airstrikes intensified against Iranian assets, while in Yemen, the Houthis escalated their involvement by launching long-range attacks on Israel including a drone strike on Tel Aviv in July 2024.

Beyond the battlefield, the crisis had far-reaching economic consequences. Oil markets became highly unstable, and Houthi attacks in the Red Sea severely disrupted maritime trade. Container traffic dropped significantly, with many routes forced to divert, driving up global shipping costs.

The standoff reached its peak in June 2025 with the launch of "Operation Rising Lion". This operation marked the first full-scale war between Israel and Iran since the beginning of the conflict. Israel carried out preemptive strikes targeting Iranian nuclear facilities, prompting Iran to retaliate with a barrage of ballistic missiles aimed at major Israeli cities.

Cyber Threat Landscape

Israel and Iran are prominent players in cyberspace with a track record of cyber operations against each other and other nations. Since the war began, state-sponsored hackers, hacktivists from both countries, and cyber actors from non-participant nations ranging from South Asia to Russia to across the Middle East have become active.

DieNet



DIE NET

New War Started, And We Will Support Iran.


Israeli Radio Live services will be under massive attack from us now. Let the fun begin.

Новая война началась, и мы поддержим Иран. Израильские радиостанции теперь будут подвергаться массовой атаке с нашей стороны. Пусть начнется веселье.

جنگ جدیدی آغاز شده است و ما از ایران حمایت خواهیم کرد. ایستگاه‌های رادیویی اسرائیل اکنون مورد حمله گسترده از جانب ما قرار خواهند گرفت. بگذارید خوش بگذرد.

#DieNet #Iran
#CyberWar

Garuna Ops 

Forwarded from  **Garuna Ops** 



GARUNA
OPS
WE SUPPORT THE WAY YOU ARE

We Stand with Israel!

We are garuna ops, alive and relentless. Open your eyes to Israel's cause, or we'll make you see with our cyber blades.

We're watching closely.... 

#wesupportisrael #fuckiran #fuckislam

Middle East and North Africa

The MEA region naturally stands out as the primary threat zone. Both Iran and Israel have strong operational footprints in the region, and their state-linked groups and proxies frequently operate across these borders.

The UAE, Jordan, and Saudi Arabia have been named repeatedly in attack claims, mostly for allegedly supporting Israeli goals. Many attacks focus on telecom, government, and critical infrastructure.



Translation: "The UAE Ministry of Defense website has been taken down due to its support for the Zionist entity and in response to the handover of commander Issam Buwaydhani to the French court."

DDoS attack targeting UAE .gov domain

Note: Egypt is also a key target of recent hacktivist activity, though mainly in the context of the Palestine issue.

United States

The U.S. has been a **consistent secondary target**. Not only governmental or military organizations targeted, civilian infrastructure like healthcare and telecommunications, has seen the most exposure in these leaks.



10 minutes ago


SELLING [USA] 1 MILLION HEALTH CARE PATIENT DATA



HEALTH CARE PATIENT DATA

holaaa, we sell health care patient data from the USA with a total of more than 1 million data, this data is from various regions in the USA for complete details please check below..

SYLHET GANG-SG



We attacked Spectrum causing Disruption in the landlines Internet and Signal All Over America

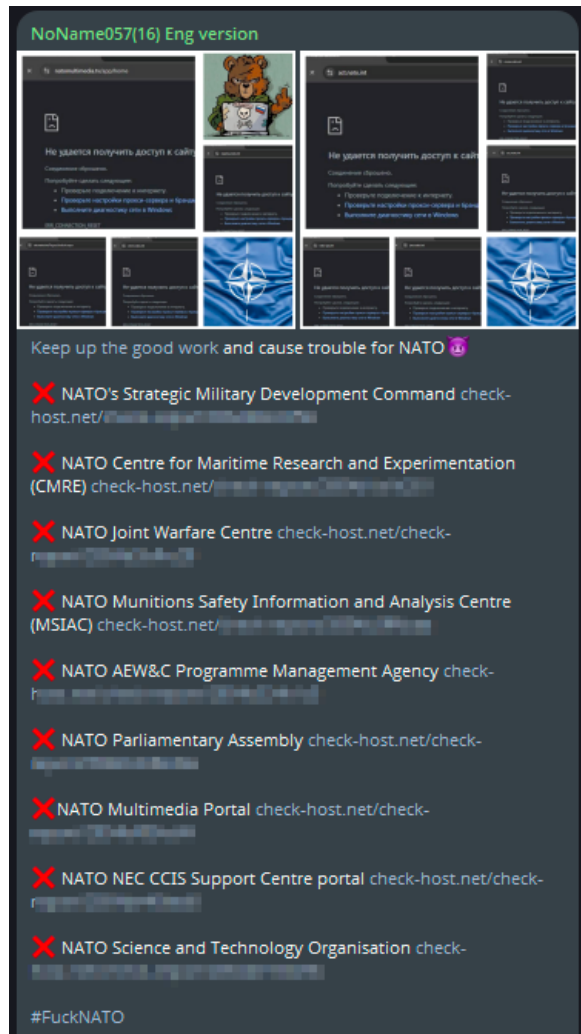
The attack was initiated half an hours ago
In retaliation to American Aggression on Iran.

We will continue to support Iran
in every terms possible

In several Telegram channels and Dark Web posts, attackers frame these actions as **"retaliation"** for American involvement.

Europe

While Europe has not been a primary battleground in this conflict, some industries with defense or aerospace ties to Israel have become indirect targets. European companies involved in arms expos, tech transfers, or trade events have been mentioned in Telegram posts and forums.

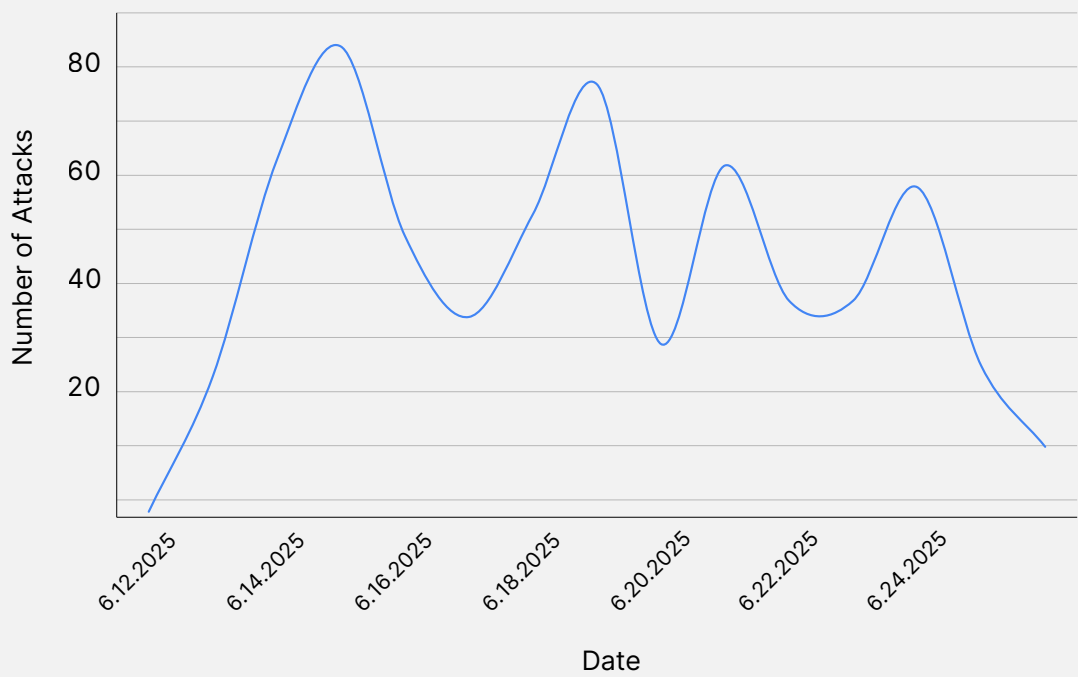


While not primary targets for the Israel-Iran cyber conflict, European countries are currently attracting hacktivist activity, partly due to tensions from the Russia-Ukraine war.

Telegram Threats

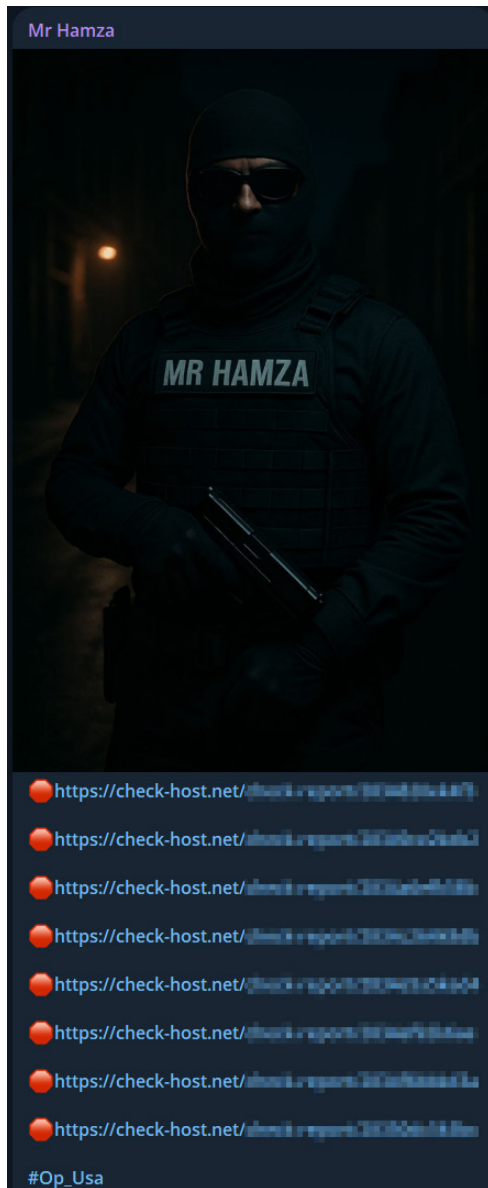
Telegram served as a central hub for cyber activity during the reporting period. We identified over **600** distinct cyberattack claims across more than 100 Telegram channels in **15 days**, based on **thousands** of messages.

Number of Attack Claims



Only unique claims with at least one piece of proof, even if weak, were counted. Duplicate posts, forwarded messages, and recycled claims were excluded.

The number of daily claims peaked on **June 15**, with over **80 distinct attack claims** in a single day. The activity rose and fell in waves every few days, many spikes came just hours after missile strikes.

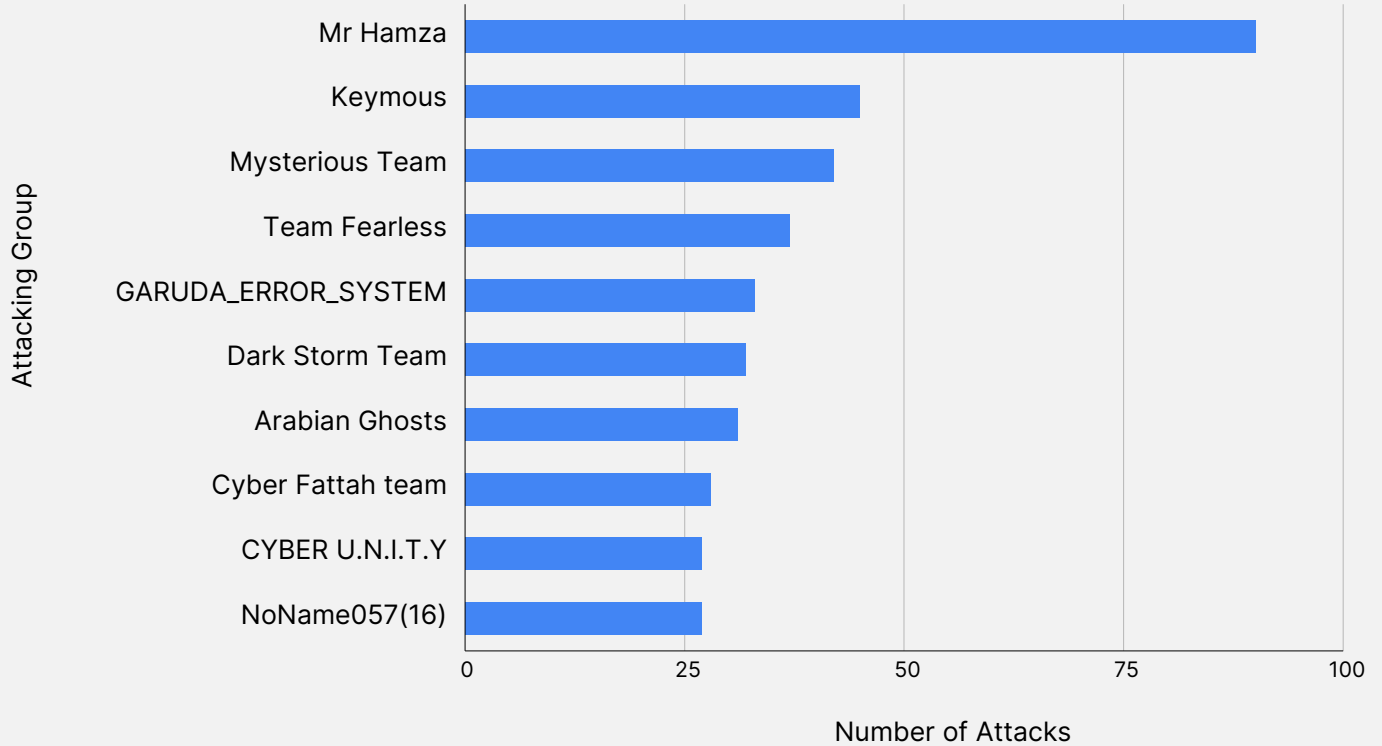


DDoS attacks targeting U.S. organizations

Mr Hamza is the leading group in DDoS attacks but also sells DDoS tools.

A wide range of hacktivist groups used Telegram to report attacks, but most of the activity came from a handful of dominant actors.

Top 10 Hacktivist Groups



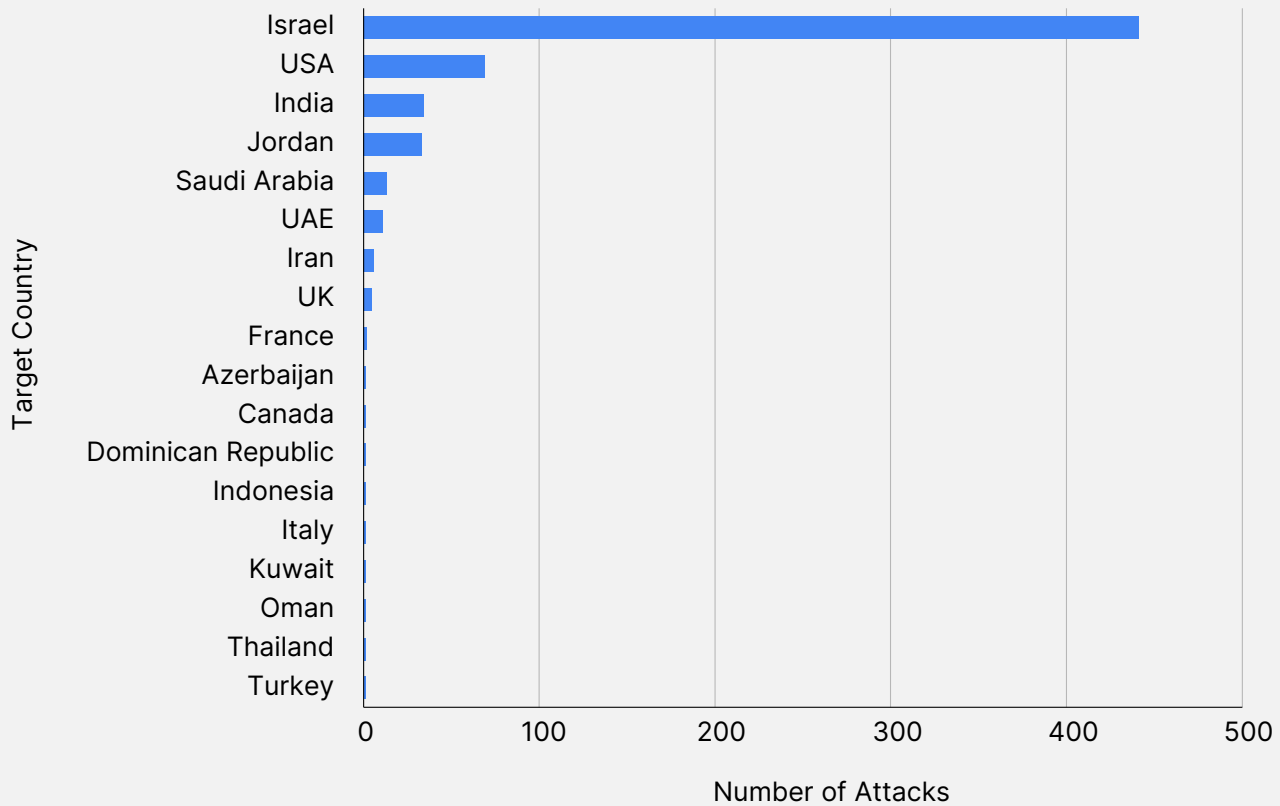
Each recorded claim includes some form of proof and was filtered to remove duplicates or forwards.

Across 100+ Telegram channels with self-claimed hacktivist titles, there are approximately 50 groups that claimed attacks.

Many hacktivist channels express support without taking action, often just forwarding messages from others.

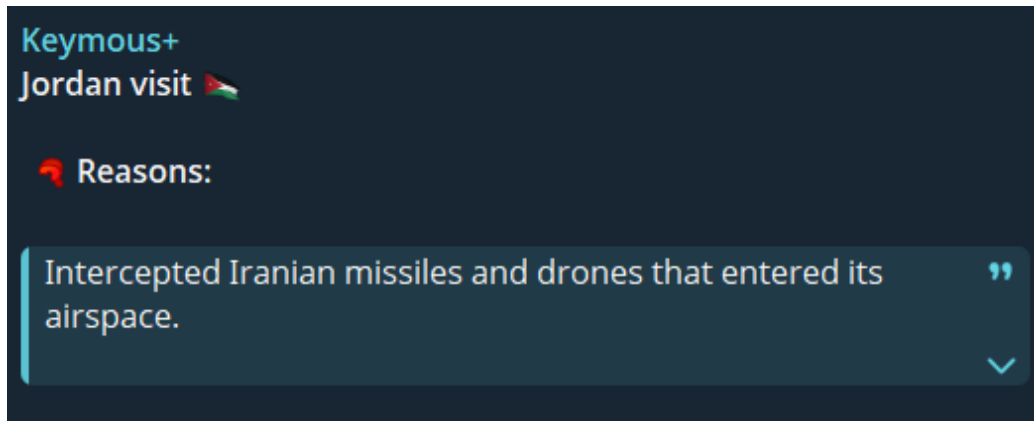
Israel was the most targeted country with **441 attack claims**, making up **+70%** of all recorded activity.

Number of Attacks by Target Country



The country count includes only activities linked directly to the Iran-Israel conflict. Countries like Egypt, Thailand, Japan, Italy, Germany, and Vietnam were targeted due to current geopolitical issues and are not included here.

Israel was followed by the **U.S. (69)**, **India (34)**, **Jordan (33)**, **Saudi Arabia (13)**, and the **UAE (11)**.



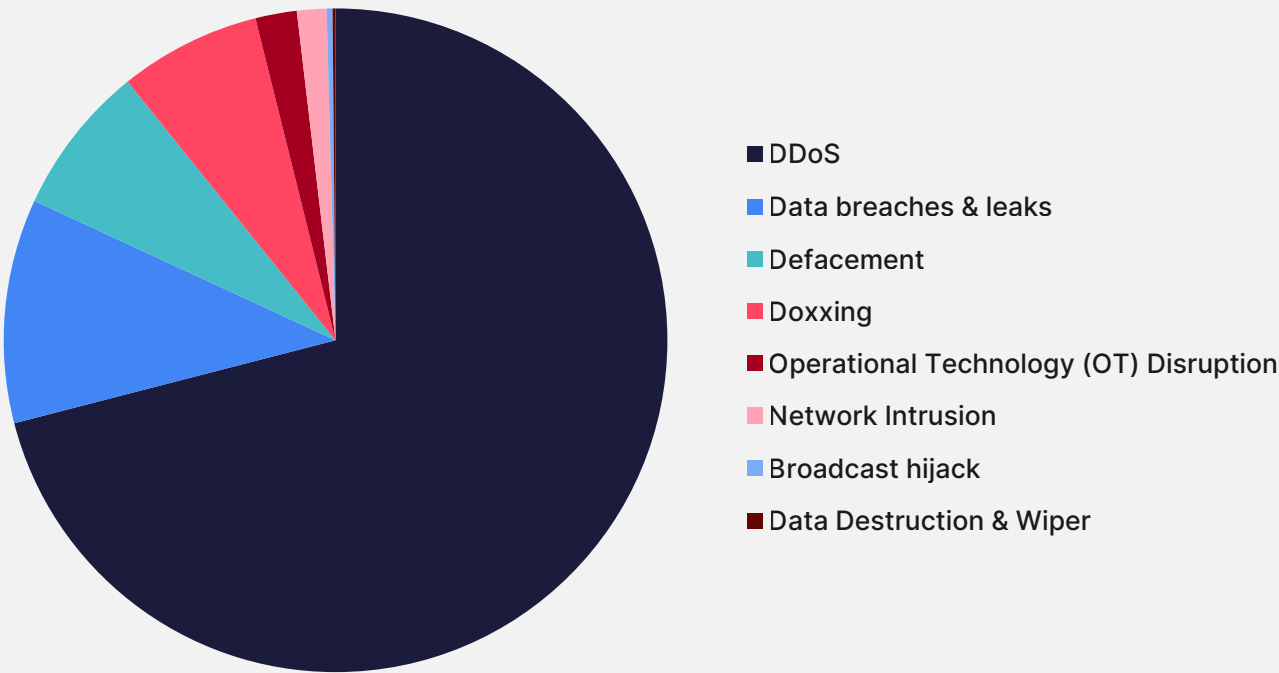
Why are various MEA countries being targeted? The claimed reason is their “support” for Israeli goals.



Keymous' DDoS attacks targeting various organizations in Jordan

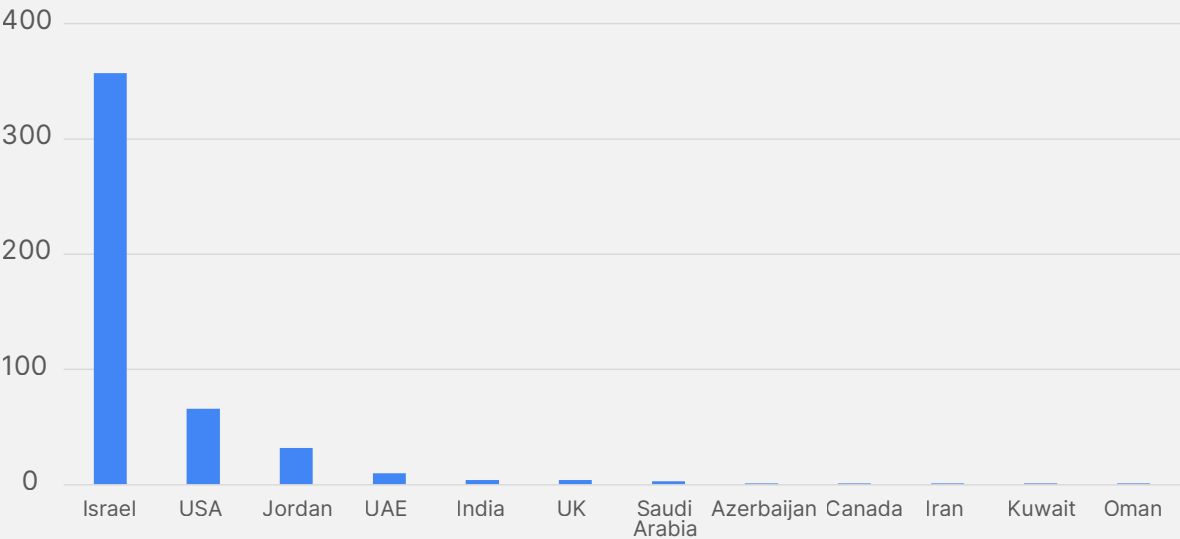
The majority of attacks claimed on Telegram were DDoS attacks, followed by data breaches, leaks, defacements, doxxing, broadcast hijacking, OT disruption, and network intrusions.

Distribution of Attack Types



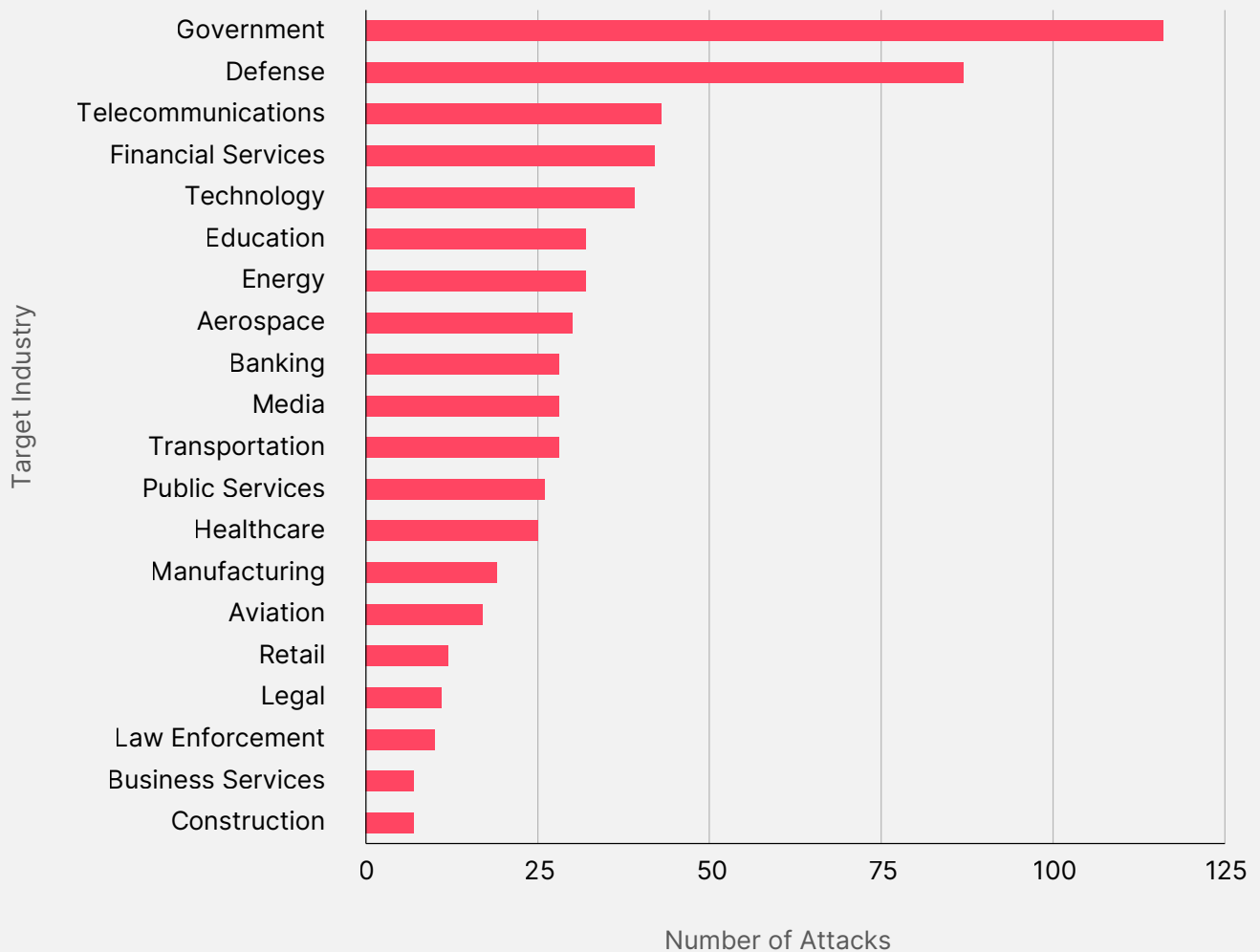
Israel was the main target of DDoS attacks, with 357 claims, making up 74% of all DDoS activity.

Distribution of DDoS Attacks by Target Country



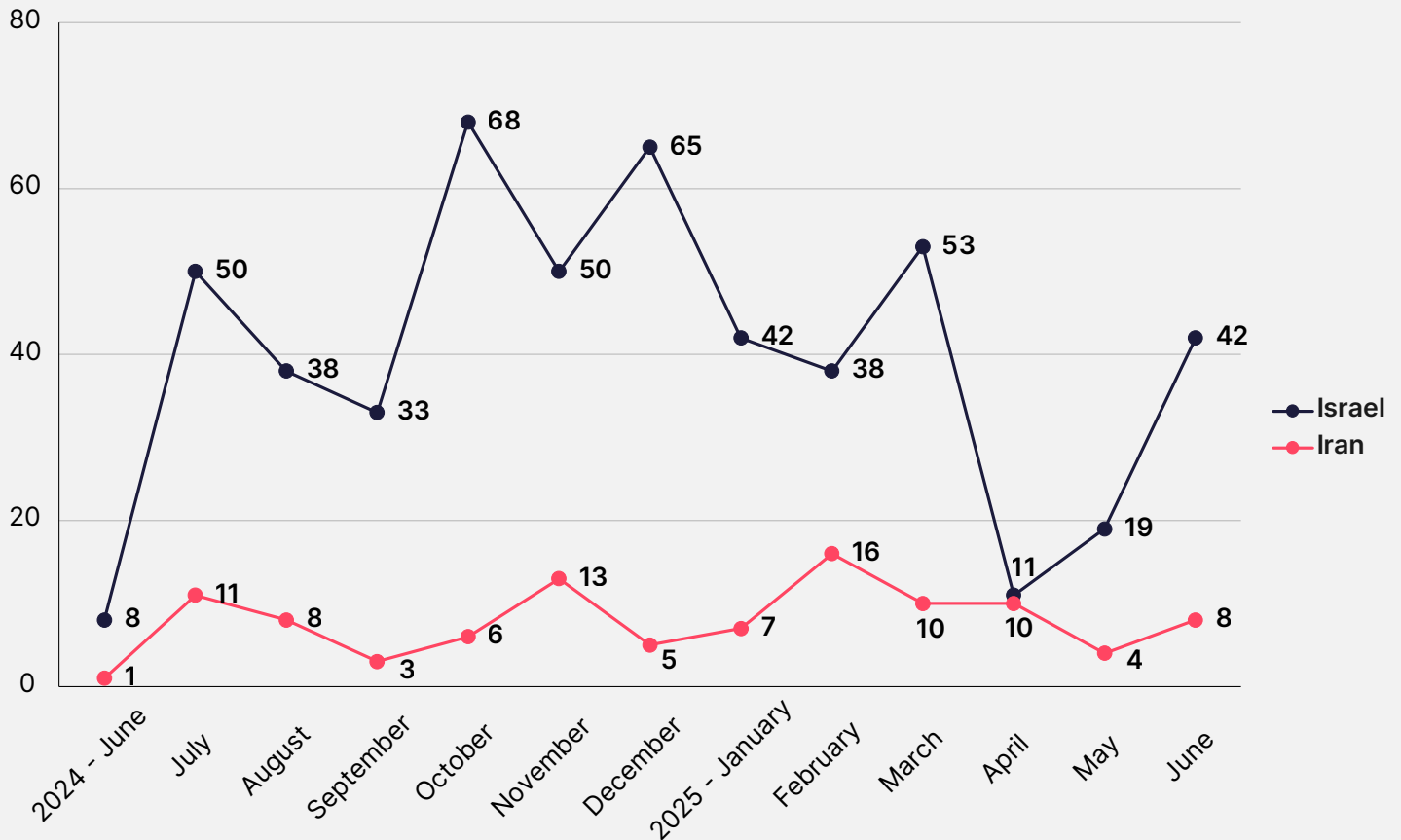
The most targeted industries were Governmental Organizations (116), Defense&Military (87), Telecommunications (43), Financial Services (42), and Technology (39). Other affected sectors included Energy, Education, Aerospace, Banking, Media, Transportation, Healthcare, and Public Services, among others.

Top 20 Industries Targeted



Dark Web Threats

Dark Web Posts Targeted Israel and Iran



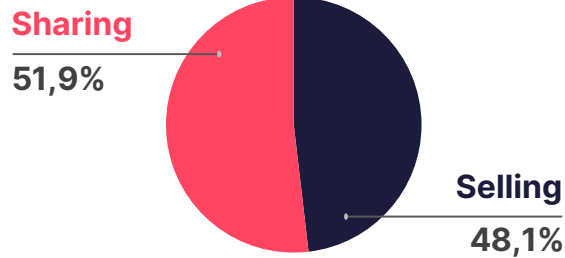
Following the June 2025 military escalation between Israel and Iran, Dark Web activity targeting both countries increased. Israel saw a sharp rise in posts, with 42 in June, double the May count. Notably, 51.9% of these posts involved data sharing, and 67.7% focused on databases, indicating a surge in politically motivated exposure.

In contrast, 80% of posts targeting Iran were commercial in nature, with 100% involving data sales, suggesting profit-driven cybercriminal interest.

Dark Web Post Categories / Post Type

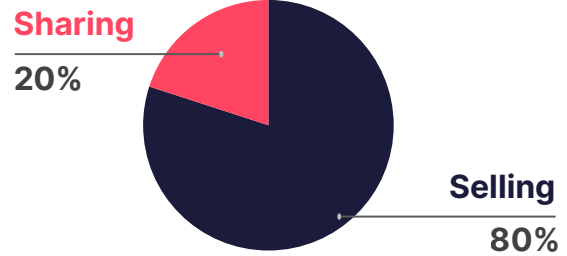
Israel

Dark Web Post Categories After 13th of June

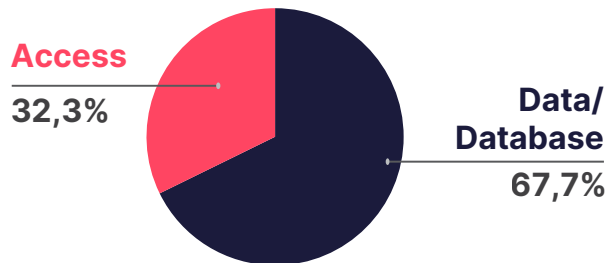


Iran

Dark Web Post Categories After 13th of June



Dark Web Post Types After 13th of June



Dark Web Post Types After 13th of June



Is Your Organization Exposed on the Dark Web?
Get your **free report** now and stay ahead of cyber threats:
[SOCradar's Free Dark Web Report](#)

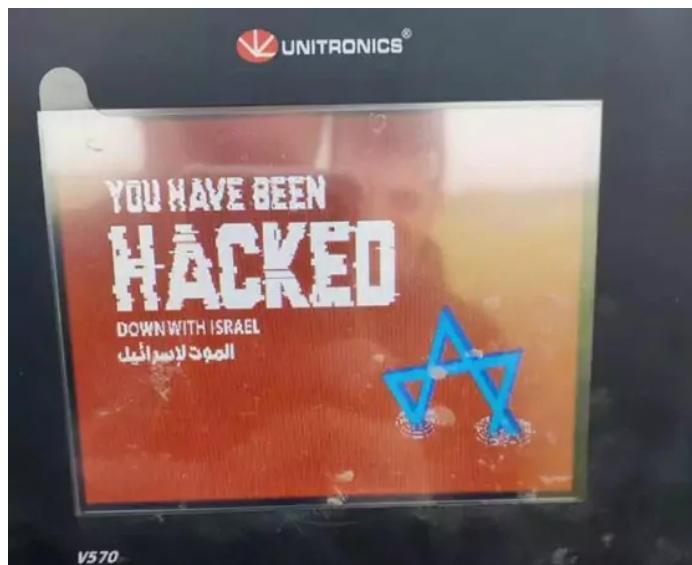


Threat Actors

The conflict involves a wide array of actors. On one side are Iran's cyber forces (mostly IRGC-linked) and allied hacktivists; on the other side Israeli state cyber units and pro-Israel hackers.

Iranian Cyber Capabilities and Operations

Iran has long invested heavily in asymmetric cyber capabilities. Its Revolutionary Guard cyber units (and other intelligence-linked teams) are capable of sophisticated attacks on industrial and civilian infrastructure. U.S. officials note Iran has repeatedly targeted water systems, pipelines, power grids and other critical systems in past campaigns.



Defaced Unitronics product by [Cyber Av3ngers](#)

In the current conflict, however, Iran's response has been relatively low-profile, contrary to the physical warfare.

A recorded APT group activity was AI-Powered phishing attacks.

APT35, also known as Charming Kitten, **carried out** a spear-phishing campaign targeting Israeli journalists, cybersecurity experts, and computer science professors. The group posed as assistants to tech executives or researchers, contacting victims through email and WhatsApp, and directing them to fake Gmail login or Google Meet pages.

APT35





APT35, also known as Charming Kitten, Phosphorus, and other aliases, is an Iranian state-sponsored cyber-espionage group active. The group is known for its cyber espionage operations targeting government entities, political activists, journalists, and organizations in critical sectors.

Country of Origin: Iran

Motivation:

Cyber Espionage

Target Countries:

United States, Israel, Middle Eastern and European nations

Target Sectors:

Government, Defense, Media, Telecommunications, Education

Attack Type:

Phishing, Credential Theft, Malware Deployment

-TTPs-

Phishing:

T1566

Application Layer Protocol:

T1071

Credential Dumping:

T1003

Dark Web Profile: APT35

Historically, Iran-linked APT groups have targeted a wide range of sectors across the region and beyond. **APT42** has focused on espionage, credential harvesting, and intelligence gathering against civil society, healthcare, education, and media sectors in over 15 countries.

APT34 (OilRig) has primarily targeted government, energy, telecom, and finance sectors using spear-phishing and custom malware.



OilRig (APT34)



OilRig, also known as APT34, is an Iranian cyber espionage group active since at least 2014. The group primarily targets organizations in the Middle East, leveraging spear-phishing campaigns and custom malware.

Country of Origin: Iran 	
Motivation:	Espionage
Target Countries:	Middle Eastern nations, United States, EU
Target Sectors:	Financial, Energy, Telecommunications, Government, and Defense
Attack Type:	Malware, Spear Phishing, Credential Harvesting

-TTPs-

Spear Phishing Attachment:
T1193

Application Layer Protocol:
T1071

Command and Scripting Interpreter:
T1059

Dark Web Profile: OilRig APT34

Other IRGC-linked units such as [MuddyWater](#), [Storm-842 \(Void Manticore\)](#), and the propaganda-driven [Cyber Avengers](#) have engaged in destructive campaigns including ransomware, wipers, and defacements, mainly against Israeli and regional infrastructure.

Israeli Cyber Capabilities and Operations

The principal known Israeli-linked hacking group active in this conflict is Predatory Sparrow (Gonjeshke Darande). While it publicly styles itself as a private collective, multiple reports tie it closely to the Israeli military intelligence apparatus.

Predatory Sparrow claimed responsibility for hacking Iran's state-owned Bank Sepah, causing major service outages and disrupting access to accounts and cards. Known for past attacks on Iran's steel, rail, and fuel infrastructure, the group is widely believed to be linked to Israeli cyber units.

After the IRGC's "Bank Sepah" comes the turn of **Nobitex**

WARNING!

In 24 hours, we will release **Nobitex's** source code and internal information from their internal network.
Any assets that remain there after that point will be at risk!


The **Nobitex** exchange is at the heart of the regime's efforts to finance terror worldwide, as well as being the regime's favorite sanctions violation tool. **We, "Gonjeshke Darande", conducted cyberattacks against Nobitex.**

Nobitex doesn't even pretend to abide by sanctions. In fact, it publicly instructs users on how to use its infrastructure to bypass sanctions.

The regime's dependence on **Nobitex** is evident from the fact that working at **Nobitex** is considered valid military service, as it is considered vital to the regime's efforts.

These cyberattacks are the result of **Nobitex** being a key regime tool for financing terrorism and violating sanctions. Associating with regime terror financing and sanction violation infrastructure puts your assets at risk.

Take action before it's too late!



Reflections of the Israel-Iran Conflict on the Cyber World

A day later, it also breached Nobitex, Iran's top crypto exchange, accusing it of aiding terrorism and sanctions evasion. The group threatened to leak internal data, and investigators confirmed around **\$90 million** in crypto was stolen.

Hacktivist Groups

Active groups from both parties:

Mr Hamza – 90
Keymous – 45
Mysterious Team – 42
Team Fearless – 37
GARUDA_ERROR_SYSTEM – 33
Dark Storm Team – 32
Arabian Ghosts – 31
Cyber Fattah team – 28
NoName057(16) – 27
CYBER U.N.I.T.Y – 27
Elite Squad – 26
Server Killers – 24
Octo Dark Cyber Squad – 22
LulzSec_Black – 20
Moroccan Black Cyber Army – 20
Handala Hack – 19
Cyber Islamic resistance – 18

Inteid – 18
Akatsuki Cyber Team – 16
GhostSec – 12
The Godfather of all – 10
Yemen Cyber army – 9
Anonymous Guys – 9
DieNet – 8
TwoNet – 7
RootSec – 5
Sons of Anarchy – 5
Fredens of Security – 4
Z-ALLIANCE – 3
EvilMorocco – 3
Tunisian Maskers Cyber Force – 3
SYLHET GANG-SG – 2
RipperSec – 2
Coup Team – 2

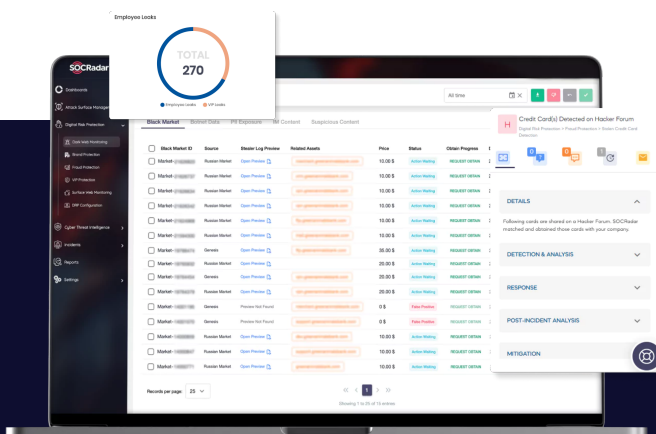
GC Kul – 2
RedEyes – 2
Predatory Sparrow / Gonjeshke
Darande – 2
Lulzsec Black – 2
Unit Nine – 2
WeRedEvils – 2
177 Members Team – 2
313 Team – 2
Anonymous Syria Hackers – 1
BD Anonymous – 1
ZeroDayX – 1
Ghostnet-X – 1
Vendetta Mafia – 1
Blackswamp – 1
FAD Team – 1
Assasins – 1

Hacktivist groups from Muslim-majority South Asian countries, Arab groups, and Russian collectives are actively targeting Israel and its allies. In contrast, only a small number of attacks, mainly from Israeli sources or rare allied actors like two Syrian groups, have been directed at Iran. On the Israeli side, there are fewer groups, but their operations have had a much greater impact beyond hacktivism.

SOCRadar's Advanced Dark Web Monitoring

provides Kenyan organizations with critical insights into hidden threats targeting their sectors, including Retail Trade, finance, and Insurance, which have faced significant risks over the past year. With real-time tracking of underground chatter and sensitive data exposure, SOCRadar enables proactive defense against Dark Web threats.

Activate your [free demo today](#) to safeguard your organization's most valuable assets.



**SOCRadar's Advanced
Dark Web Monitoring**

Disinformation and Influence Operations

Key Narratives and Target Audiences

During the June 2025 conflict, a surge of AI-generated and fake news content spread across digital platforms. These narratives were crafted to manipulate perception, fuel fear, and increase confusion during a volatile period. Leveraging generative AI tools, various actors rapidly produced and distributed false content to shape public sentiment and distort reality.

Key Narratives

1. **“Israel is Under Massive Attack”**
 AI-generated images and false reports depicted widespread destruction and the collapse of Israeli defenses. These stories aimed to trigger panic, damage morale, and create an exaggerated sense of crisis.
2. **“Iran Will Annihilate Israel”**
 Content in this narrative inflated Iran’s military capabilities and portrayed imminent retaliation or overwhelming force.
3. **“Iran is the Dominant Regional Power”**
 Disinformation framed Iran as decisively winning, using fake battlefield maps, victory statements, and statistical fabrications to enhance its perceived strength.

Target Audiences

Our assessment indicates that these disinformation efforts were not aimed at the armed forces or decision-makers of either side, despite the military themes present in many narratives. The style, distribution channels, and language used suggest a clear focus on civilian populations, particularly those most likely to be influenced by emotionally charged content and real-time social media engagement.

The overarching goal appears to be psychological impact at the civilian level by using fear, uncertainty, and disinformation to influence public discourse and destabilize societal cohesion.

AI-Generated Content and Deepfakes



The above image is from a widely circulated post purported to depict an F-35 jet allegedly downed in the Iranian desert. However, indicators of AI-generated manipulation were apparent. Civilians appeared disproportionately sized compared to nearby vehicles, and the surrounding sand lacked any visible signs of impact.



One video depicted a continuous convoy of trucks transporting ballistic missiles from a mountainside facility. But when you look closer, you can clearly see indicators of AI-generated content. Rocks within the footage exhibiting unnatural movement and noticeable distortion in both the missiles and the vehicles transporting them.



Another image that circulated widely was claimed to show a downed American B-2 bomber within Iranian territory. However, analysis reveals several indicators consistent with AI-generated content.

Notably, an emergency responder visible in the lower-left corner appears to merge unnaturally with the background. Additionally, the aircraft shown appears largely intact, which is inconsistent with the level of destruction typically expected in such a scenario.

Iran Stop The War, We Are Sorry
Zionists are on Street and Apologising IRAN 🇮🇷
But it's too late "Revenge will be taken " 😞
[#iran](#) [#israel](#) [#iranisraelwar](#)



A video circulating online allegedly depicting Israeli citizens staging a protest to stop the war is AI generated content.

Visual inconsistencies such as distorted facial features, spelling errors on placards, and the presence of a "Veo" watermark shows synthetic creation.



An official account affiliated with the Israeli army shared a video titled “RAW FOOTAGE: Iran launched multiple ballistic missiles towards Israel in the past hours.”

The video includes text stating “Israel is under attack” and features a sequence of clips showing missiles being launched and striking various targets.

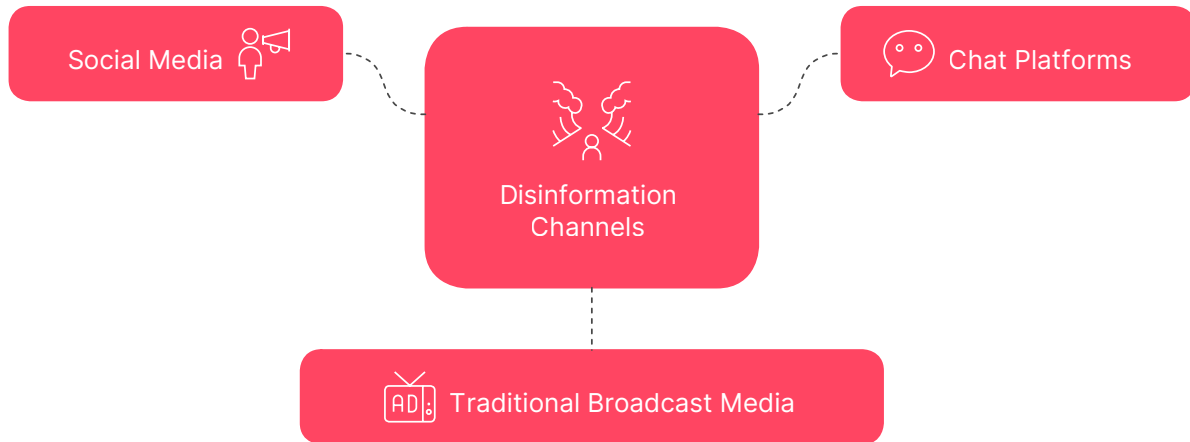
However, the content is not related to recent events. As highlighted by Community Notes, the opening clip in the sequence was originally published in 2024.

The image on the right is from a video falsely claiming to show damage to Tel Aviv. The video was shared on Instagram by a Pakistan-based user, showed crumbling buildings and was captioned, “A glimpse of Tel Aviv, the Zionist war-mongers’ capital.” The video also included Arabic-language text labeling the location as “Tel Aviv.”

Another similar clip, posted on Facebook with Thai-language text stating, “This is not AI, this is the real Tel Aviv airport”.



Channels of Dissemination



Disinformation related to the June 2025 Iran-Israel conflict was primarily spread through social media and messaging platforms, each serving different functions in the overall information campaign.

Although traditional broadcast media have played a role in this conflict's information landscape, they have been used to reinforce state-approved narratives. These channels serve more as amplifiers of official messages than as vectors for reaching bigger audiences.

Social Media

The main driver of reach and amplification. False content, often AI-generated, was widely shared to reinforce existing narratives and create a sense of community around them. In some cases, misleading information originated from state-affiliated sources (e.g., the IDF or Iranian media) and was later promoted across platforms to boost visibility and influence public perception.

Chat Platforms (e.g., Telegram)

Used to circulate disinformation within closed, targeted audiences, particularly ideological or regional communities. While effective for niche engagement, their overall impact was more limited due to platform structure and restricted discoverability.

Recommendations and Risk Forecast

The recent cyber activity between Israel and Iran shows how quickly geopolitical conflict can spill over into cyberspace. The following recommendations are based on the tactics observed during and after the June 2025 events. This section outlines practical steps organizations can take to strengthen their defenses, reduce risk, and prepare for similar threats in the near future.

Technical Controls (Detection, Prevention, Response):

Organizations should strengthen technical controls through the following actions:

- Establish comprehensive monitoring systems across all networks and regularly update threat intelligence feeds.
- Quickly apply software patches, review firewall rules, and disable unnecessary open ports.
- Regularly test incident response plans focusing specifically on ransomware, wipers, and DDoS attacks.
- Maintain offline backups to ensure recovery in the event of destructive cyber incidents.

Cyber Hygiene and Security Posture Enhancements:

To improve cyber hygiene, organizations should:

- Conduct regular cybersecurity awareness training, particularly around recognizing phishing attacks.
- Enforce multi-factor authentication (MFA) across all critical systems.
- Regularly review and update access controls to sensitive information.
- Ensure continuous monitoring and logging of network activity to quickly detect and respond to breaches.

Public Communication and Disinformation Countermeasures:

Organizations must actively counter disinformation by:

- Preparing swift verification and communication strategies to clarify misleading content.
- Coordinating messaging clearly and consistently during cyber incidents.
- Monitoring social media platforms for impersonation, fake accounts, and misinformation campaigns.
- Providing transparent and factual updates to maintain public trust and counteract misinformation.

Projected Cyber Threat Trends:

Based on recent activities, organizations should prepare for these ongoing and emerging threats:

- Hacktivist activities such as DDoS attacks, website defacements, and information leaks targeting public and private sectors.
- Targeting of organizations perceived as allied or indirectly involved in the regional conflict, including international banks and diplomatic entities.
- AI-driven disinformation, phishing campaigns, and manipulated digital content designed to mislead or extract sensitive information.

Conclusion

The cyber dimension of the Israel–Iran conflict shows signs of slowing down. However the organizations, especially those with exposure to the region, need to assume that digital operations may be disrupted, even if they are not directly involved in the conflict.

By focusing on the basics and preparing for the types of threats we've already seen, most organizations can reduce their exposure and respond more effectively in the event of a cyber incident.



Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.

