

# From The Depths of the Shadows

**IRGC and Hacker Collectives Of  
The 12-Day War**





## Executive Summary

In June 2025, the 12-day conflict between Israel and Iran spilled into cyberspace, revealing not only a surge in offensive operations but a tangled network of threat actors and motivations. As air strikes crossed borders, a vast array of hacking groups—some linked with the Islamic Revolutionary Guard Corps (IRGC), others with less direct ties—began working to sway public opinion, disrupt businesses, and intimidate and undermine adversaries.

Through detailed analysis of hundreds of thousands of Telegram messages, this report explores how state-linked Iranian hackers, Iranian cyber proxies, and collectives of ideologically-aligned hacktivists supported Iran's broader war aims in a disruptive digital offensive.

This research offers a look inside the operational mechanics, motivations, and campaigns from Iranian cyber-operators, and details just how quickly they spun up campaigns to align with the kinetic conflict. From phishing infrastructure to propaganda coordination, this report covers the groups':

- Proactive reconnaissance
- Recruitment via Telegram
- Coordination with Lebanese and Iranian cyber brigades
- Discussions on punishing adversaries and collecting intelligence on them
- Cyber campaigns aimed at intimidating adversaries, defacement, and phishing
- Targeted operations to deliver malware to those sympathetic to Israel's cause
- Custom scripts and scanning for vulnerabilities
- Data theft and database dumping
- Sale of zero-days and other vulnerabilities

The report reveals a campaign from Imperial Kitten—also known as Tortoiseshell, Cuboid Sandstorm, and Yellow Liderc—that shows exactly how it adjusted its strategy to align with Iran's kinetic operations.

In examining messaging and cyber-operations from state-aligned and hacktivist groups, such as Fatimion Cyber Team, the Cyber Fattah team, the Cyber Islamic Resistance, and the Tunisian Maskers Cyber Force, we observe IRGC-aligned and hacktivist collectives exploit cyberspace for diverse strategic goals, including intelligence gathering, propaganda, and direct attacks on critical infrastructure and public entities.

# Table of Contents

Executive Summary	2
Chapter 1: Hacker Chatter Message Analysis	5
Introduction	5
Cyber Proxies	7
Fatimion Cyber Team	7
Cyber Fattah Team	8
Cyber Islamic Resistance	10
Tunisian Maskers Cyber Force	12
Chapter 2: State-Sponsored Activity: Imperial Kitten's conflict-themed phishing campaign	13
Tortoiseshell's conflict-themed phishing campaign	13
Timing the Operation	13
Typosquatting and Victim Selection	15
Chapter 3: Cyberdefense During Kinetic Conflict	16
Final Thoughts	16
A Web of Linked Activity	17
The Blend of Proxy and Volunteer	17
Symbolism and Tasking	18
Key Takeaways	19
Contact STRIKE for Incident Response	20

## Background

SecurityScorecard's STRIKE threat intelligence team conducted a comprehensive analysis of 250,000 messages from Iranian proxy and hacktivist chatter from over 178 active groups over the 12-day war, revealing exactly how state-linked Iranian hackers, Iranian cyber proxies, and ideologically aligned hacktivists supported Iran's broader war aims in a disruptive digital offensive. STRIKE also uncovered an IRGC-linked malware-laden phishing operation launched at the outset of the conflict, suggesting careful orchestration and planning aligned to the fighting.

The report presents a detailed account of the wide variety of groups that make up Iran's digital footsoldiers and probes how ideology, opportunism, hacking, and propaganda intersect with tasking and broader warfare.

Moving forward, it is clear that defenders must understand more than malware, tactics, techniques, and procedures (TTPs), and indicators of compromise (IOCs). Coordinated hacking campaigns include Telegram channels as a shared hub, social engineering hooks tied to kinetic conflict themes, and phishing domains spun up within hours of geopolitical shifts, suggesting deep integration between kinetic warfare and state-linked (or state-inspired) cyber-operations.





# Chapter 1: Hacker Chatter Message Analysis

## Introduction

Our analysis of the 178 groups active over the 12-day conflict pinpointed ten that were responsible for the bulk of the propaganda—each blending ideologically driven messaging with coordinated cyber-operations.

Rank	Channel	Total Messages
1	Al-Qassam Toast (Shark Attack Blood Bath)	46,311
2	Mundo Multipolar	45,996
3	📢 Freedom Tube	18,384
4	Komfortzone verlassen – selbst denken	12,163
5	Resistance Toast ▼	9,361
6	IRGC 🚩 نارادساپ یرب یاس هاپس	9,136
7	Piccola guerriera	6,641
8	Islamic Hacker Army group	5,286
9	sharp333	4,738
10	جبنم امس	3,884

If we break down the most active cyber-operation messaging channels, two clear clusters emerge. First, we have IRGC-aligned proxies—chiefly نارادساپ یرب یاس هاپس IRGC and هاپس هاریا یرب یاس—which, given their frequent use of IRGC insignia and direct references to Revolutionary Guard cyber brigades, we assess with moderate confidence are operated or sponsored by Iran’s cyber forces.

Second, a diverse array of regional and ideological hacktivist collectives—including Palestinian-linked cells like Cyber Islamic Resistance and Cyber Fattah team, Afghanistan’s Fatimion cyber team, Tunisia’s Maskers Cyber Force, as well as pan-Islamic outfits such as Islamic Hacker Army group and sharp333—contribute additional DDoS campaigns, phishing operations, and data dumps under the banner of local grievance narratives.

Beyond Iran, this cyber conflict now spans multiple countries—Palestine, Afghanistan, Tunisia, Iraq and others—creating a resilient, multi-vector threat environment that complicates attribution and response.

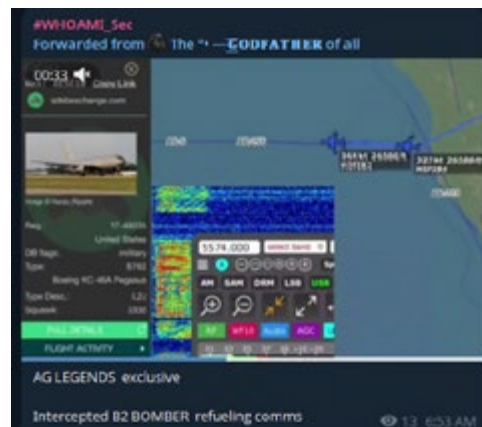
Rank	Channel	Total Messages
1	IRGC ناردساپ یرب یاس هاپس	9,136
2	Islamic Hacker Army group	5,286
3	sharp333	4,738
4	CyberActivism™	612
5	ناریا یرب یاس هاپس	361
6	Cyber Fattah team	248
7	Cyber Islamic resistance	242
8	ینورت کلالا نویم طاف قیرف – Fatimion cyber team	239
9	Chat Islamic Hacker Army	236
10	Tunisian Maskers Cyber Force	175

A number of cyber actors created a flurry of activity during the war. During the conflict, for instance, we observe SEPAHCYBERY, an IRGC-linked psychological warfare channel, engaged in psychological operations, such as issuing threats and boasting capabilities to strike Western targets. Overall, they posted approximately 9,000 posts between June 13-27. Their efforts appear aimed at promoting and amplifying attacks, while simultaneously promoting IRGC's cyber prowess and deterrence.

Other actors played a prominent role as well. AGLegends, an Iranian hacktivist group that is likely a collective of multiple affiliated entities, appeared to hint at advance knowledge of the B-2 bombers the United States used to launch the Midnight Hammer attack on Iran on June 22. It is not absolutely certain that they had advance knowledge, but they explicitly discussed B-2 refueling communications, which could suggest they were, by whatever means, expecting this development.

They have also conducted campaigns against Israeli defense entities and engaged in operations designed to disrupt internet connectivity in Israel.

This report is non-exhaustive and does not delve into every actor and each message, but the examples we examine are intended to shed light on the actors, tactics, and patterns shaping cyber conflict in one of the world's most volatile regions. Our team has verified a number of the claimed operations and defacements contained in the messaging in this report. However, the proxy actors appear to leverage bravado in their messaging at times, which could indicate they are trying to amplify their effects.



AGLegends' claim of intercepted communications

## Cyber Proxies

In this analysis we will focus on a few notable groups with a considerably high message volume during the course of the 12 day conflict. This analysis focuses on the proxy groups in alignment with Iran and anti-Israel and anti-Western narratives.

From these operations we observe that cyber offensives in this threat landscape are increasingly ideologically driven and woven together in coordinated ways, rather than disjointed and divided by geographies or languages. From this, STRIKE assesses that future kinetic warfare and clashes will ignite cyberattacks coordinated within global webs of ideologically aligned threat actors with shared aims.

This is a demonstration of the visibility of Telegram and how physical strikes are coordinated with cyber-operations and claims of cyberattacks. We see that as physical conflict leads to unimaginable carnage, there is a concurrent cyber war taking place alongside it as well.

## Fatimion Cyber Team

The Fatimion Cyber Team is a self-styled hacktivist group operating primarily via Telegram to announce and claim responsibility for disruptive cyber-operations across financial, governmental, and media targets in Iraq, Syria, the UAE, and Israel. Their public messaging emphasizes ideological motives—labeling certain officials and companies as “collaborators” or “legitimate targets”—and highlights both proactive reconnaissance (gathering personal data on “collaborators”) and offensive actions (website defacements or availability disruptions).

The Fatimion Cyber Team publicly operates under its self-assigned name on Telegram without any verifiable ties to established state cyber units. Its “Fatimion” label echoes the IRGC-aligned Fatemiyoun militia, hinting at ideological sympathy with pro-Iranian Shia networks. But there is no concrete evidence of Iranian state sponsorship or access to advanced tooling.

This leads us to assess it as a loosely organized, ideologically motivated hacktivist cell rather than a formal state-sponsored advanced persistent threat (APT) actor, with a low confidence rating due to the lack of corroborating technical forensics or intelligence.

The Fatimion Cyber Team’s intent is clearly ideological, driven by a desire to punish “collaborators” and those they deem normalizers of adversary regimes. We observe evidence of this behavior in their public threats and targeting of banks, media outlets, and government entities. Their capability appears moderate, with repeated success in defacing and disrupting public-facing websites but no indication of advanced, persistent access beyond DDoS and simple web exploits.

Their opportunity is high, given the permissive Telegram-centric propaganda environment in Iraq and Syria and the relatively weak cyber defenses of their chosen financial, governmental, and media targets.

## Cyber Fattah Team

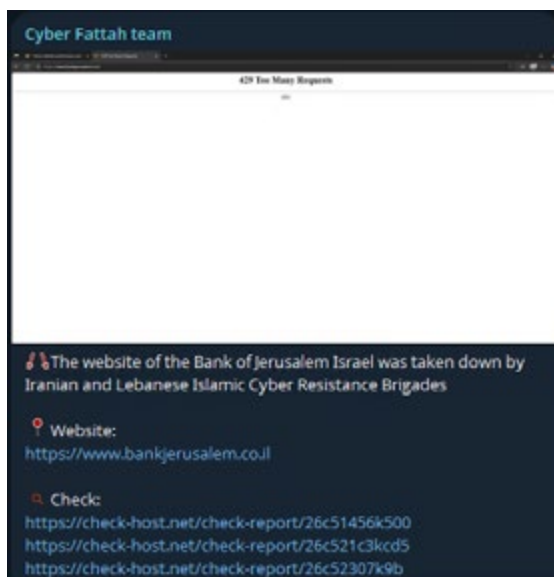
The Cyber Fattah team, which operates via the Telegram channel @fattah\_iriii, is an ideologically-motivated, state-aligned cyber resistance group that presents itself as part of a broader “Islamic Cyber Resistance” network. From March through June 2025, they have claimed multiple operations targeting Israeli and Gulf-region entities, including financial institutions, industrial websites, academic portals, and media outlets, primarily through web defacement, database exfiltration, and service disruptions.

One notable attack timed with the conflict includes their data dump of thousands of records from the Saudi Games, leaking Personally Identifiable Information (PII) and bank account information of some victims.

Their messaging typically emphasizes solidarity with Palestinian and Iranian “resistance” narratives, framing each operation as retaliation or preemptive deterrence against perceived adversaries. Cyber Fattah’s operations serve a clear strategic purpose: To project Iran-aligned cyber “warfare” in support of Palestinian causes and to intimidate adversaries through visible website defacements and data dumps.

They’ve demonstrated the technical chops to scan for vulnerable web applications, deploy custom web-shells and defacement scripts (notably their “Def.php” tool), and exfiltrate complete databases—evidenced by the May 26, 2025 Bank of Jerusalem breach. For instance, the Cyber Fattah team claims in a dump that they targeted Channel 13 News and several other small organizations in Israel during the 12-day conflict.

By focusing on small- to mid-sized news outlets, municipal media, and niche financial platforms with minimal cybersecurity defenses, they exploit low-barrier entry points (SQL injections, basic DDoS) to sustain a steady drumbeat of disruptive activity.



Cyber Fattah team alert



Cyber Fattah's messaging and claimed partnerships strongly point to Iran-aligned proxy activity: They publicly celebrate joint operations with "Lebanese and Iranian Islamic Cyber Resistance Brigades" and affiliated cells like Liwa Muhammad and the "Holy League" Cyber Cell, a coalition of hackers that target Israel, signaling coordinated state-aligned collaboration. The Holy League has demonstrated previous interest in other ideologically-driven cross-border operations, [claiming targeting of Ukraine](#) in May of 2025.

In one case during the 12-day war, they shared a collage labeled "Cyber Fattah team," showing senior Iranian military figures, such as Major General Gholam Ali Rashid, the country's highest-ranking military official Mohammad Bagheri, and Major General Hossein Salami, the head of the IRGC, each of whom were killed in the June clashes. The post's Persian caption declared the group the "People's Cyber Army of Iran" and vowed relentless attacks on adversary infrastructure. They closed with the hashtags #IRAN and #FATTAH.

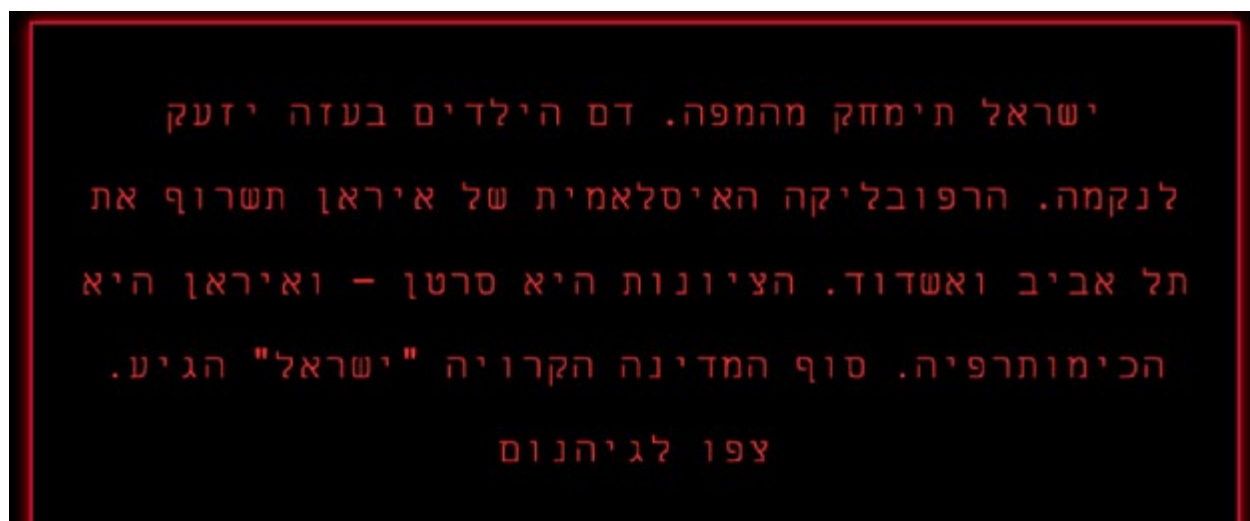
Their multilingual broadcasts in Arabic, Persian, and English and peppered with Qur'anic verses and Persian Gulf references suggest operators fluent in Farsi and Arabic, likely based in Iran or allied territories. Reinforcing this narrative, they consistently deploy hashtags such as #free\_palestine, #PersianGulf, and #iran, cementing their identity as an Iran-backed cyber resistance network.

## General TTPs

Cyber Fattah relies on a straightforward but effective toolkit: They scan for web vulnerabilities to inject custom defacement scripts (notably their "Def.php" endpoint) and overwrite site content, then pillage full databases. They often publish dumps via public links and sporadically launch rudimentary service disruptions against financial platforms as well.

After each hack, they amplify impact by mirroring defacements and data leaks on Zone-H, a cybercrime archive, ensuring broad visibility and bolstering their credibility within hacktivist circles.

For example, defacements stating "Hacked by Fattah" and a video and a Hebrew message placed on the home pages show the intent of the campaigns. The defacement proclaims in Hebrew that "Israel will be erased from the map" and that "the blood of the children in Gaza will cry out for revenge." It threatens that "the Islamic Republic of Iran will burn Tel Aviv and Ashdod," labels "Zionism as a cancer—and Iran as the chemotherapy," declares "the end of the state called 'Israel' has arrived," and warns viewers to "expect hell."



Page defacement message

## Cyber Islamic Resistance

“Cyber Islamic Resistance” (CIR) is a loosely organized, ideologically motivated hacktivist collective operating primarily via Telegram. Analysis of 242 CIR posts between March and June 2025 reveals a sustained campaign of website defacements, service disruptions, propaganda broadcasts, and morale messaging directed mainly at Israeli and Western targets. CIR self-identifies as an extension of Palestinian and Iran-aligned resistance (“[هلالارات](#) Brigade,” “Islamic Resistance of Iran Brigade”) and utilizes Telegram channels (e.g., [t.me/Mhwear98](#)) for command-and-control, victim disclosures, and recruitment.



CIR prominently brands itself as the “Cyber Islamic Resistance,” invoking Palestinian liberation imagery (“Free\_Palestine”) alongside Iranian revolutionary symbols and brigade names like “[هلالارات](#)” and “Islamic Resistance of Iran,” all communicated in Arabic with occasional Farsi and English overlays via Telegram channels such as [t.me/Mhwear98](#). Its reliance on Telegram for command-and-control and Zone-H mirror archives further reflects a regionally focused infrastructure.

Taken together, its self-identification, messaging style, and platform choices point to a likely Iran-aligned hacktivist proxy leveraging Palestinian narratives, though direct state sponsorship remains unconfirmed, yielding a moderate confidence assessment.

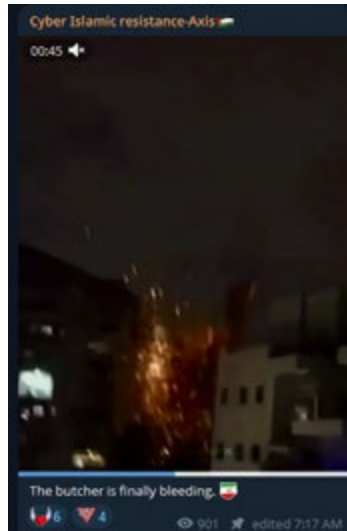
Cyber Islamic Resistance’s stated objective is to weaken Israeli resolve, portraying each cyber-attack as an act of solidarity with Palestinian resistance and, by implication, Iran. For example, on March 29, 2025, CIR posted:

”رمع وبأ”كعَمَس

#HolyLeague #FreePalestine  #OpIsrael ▼

This use of #FreePalestine  alongside #OpIsrael—coupled with the channel’s banner “Cyber Islamic Resistance ”—shows clear

interest in framing their operations as aligned with both Palestinian and Iranian causes.



Message of Iranian aligned narrative

From March through June 2025, CIR publicly claimed 17 successful defacements and service disruptions, always accompanied by archive screenshots for propaganda.

During the 12-day conflict, for instance, the group claimed to hack the Hadassah Ein Kerem Hospital in Israel.

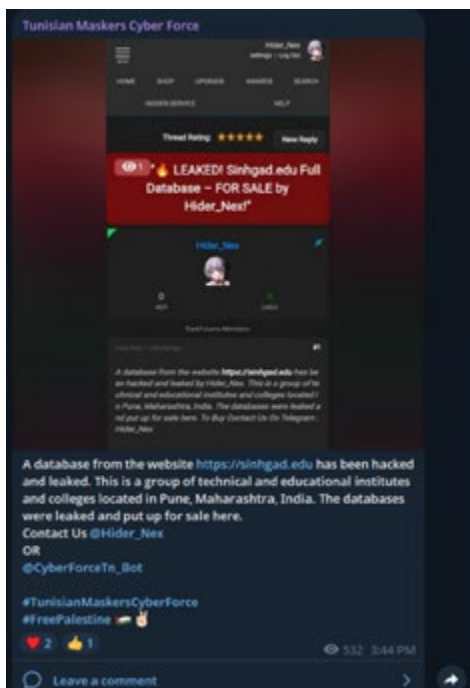


CIR hacking claim

CIR broadcasts every operation via an open Telegram channel—sharing “classified” scripts (often linking to public GitHub repos)—and deliberately times high-profile outages to follow Israeli or U.S. military actions, though they seldom detail the specific vulnerabilities they exploit.

## Tunisian Maskers Cyber Force

Tunisian Maskers Cyber Force (TMCf) is a self-described cyber-activist collective that surfaced on Telegram in May 2025. Across 149 distinct messages between 9 May and 13 July 2025, TMCf has claimed responsibility for multiple website defacements, data exfiltration operations, and the sale of zero-day vulnerabilities. Their communications mix Arabic, English, and occasional French, suggesting a primarily Tunisian core with outreach to global audiences.



Example of database dump

They leverage Telegram as their primary broadcast and C2 channel, posting proof-of-concept screenshots, database dumps, and links to paste sites where stolen data can be accessed.

Tunisian Maskers Cyber Force is a non-state, ideologically and financially motivated hacktivist group that primarily broadcasts in Arabic with occasional English via Telegram channels (such as t.me/CyberforceTn) and public paste sites. Despite their activity against government and commercial targets, there are no clear ties to state intelligence, as their messaging emphasizes public “exposés” and the sale of vulnerabilities rather than advancing geopolitical objectives. We see this in its notes, such as: “This government website hacked by Tunisian Maskers Cyber Force” (May 26, 2025) and their solicitation “Who wants to buy a vulnerability in a Cypriot Ministry website?” (May 28, 2025).

As IRGC-linked cyber operators and ideologically-aligned hacker collectives back Iran in the conflict, TMCf stands out as a notable new player. Its appearance underscores a broader trend of hacking teams forming loose collectives around regime goals based and ideological alignment, driven by shared ideology rather than formal command structure.



## Chapter 2: State-Sponsored Activity

### Tortoiseshell's conflict-themed phishing campaign

Also known as Cuboid Sandstorm, Yellow Liderc, and Tortoiseshell, Imperial Kitten is an Iranian state-sponsored cyber threat actor with strong ties to the IRGC. This group is known for its persistent and adaptive targeting of organizations across various sectors, including defense, government, and technology, primarily in the Middle East and North America. This malicious threat actor frequently leverages sophisticated social engineering, spear-phishing campaigns, and custom malware to achieve intelligence collection and disruption objectives.

Only a few days after the conflict between the two nations flared, the actor began purchasing domain names from NameCheap that revolve around themes of the conflict, such as `nowsupportisrael[.]com`, `supportisraelfunding[.]com` or `stoprirannukes[.]com`. The actor then purchased a few virtual servers to host their domain.

### Timing the Operation

The threat actor used these VPSs alongside the Evilginx phishing framework, to lure Hebrew speaking victims with petition forms offering support for Israel while focusing on the October 7th attack, when Hamas attacked Israel in 2023.

While uncovering this activity, we detected a shift in the threat actors' tactics that was timed with the eruption of the 12-Day conflict in 2025. In particular, the actor began using conflict-themed domain names for phishing campaigns.

Prior to the conflict's eruption on June 13th, Tortoiseshell had already been using certain VPSs from which they performed phishing attacks, including domains with names such as `wioccteam[.]net`, `mixanalyzer[.]com`, as well as the `nobelform[.]com` domain and subdomains. State-sponsored and financially-motivated threat actors notoriously use vague and neutral names for malicious infrastructure.

The screenshot shows a phishing form in Hebrew. The title is "לעולם לא עוד: עכשיו" (Never Again: Now). The form includes the following fields and options:

- 1. שם (Name): A text input field.
- 2. כתובת דואר אלקטרוני (Email Address): A text input field.
- 3. מס' טלפון (Phone Number): A text input field.
- 4. האם אתם תומכים ב? (Do you support?) - A radio button selection for "כן" (Yes), "לא" (No), and "אני לא יודע" (I don't know).
- 5. האם אתם רוצים להצטרף ל? (Do you want to join?) - A radio button selection for "כן" (Yes) and "לא" (No).
- 6. כתובת (Address): A text input field.
- 7. האם אתם רוצים לקבל מידע נוסף? (Do you want to receive more information?) - A radio button selection for "כן" (Yes), "לא" (No), and "אני לא יודע" (I don't know).

After June 13, 2025, however, the threat actor changed their approach and began purchasing domains with themes tied to the conflict in a very matter-of-fact way. The domains were oriented explicitly in support of Israel, in what appeared to be an attempt to target those empathetic to the Israeli side. This shift in phishing demonstrates the evergrowing threat of a methodical social engineering campaign, which is not only well-crafted and motivated, but timely as well.

**Domain list:**

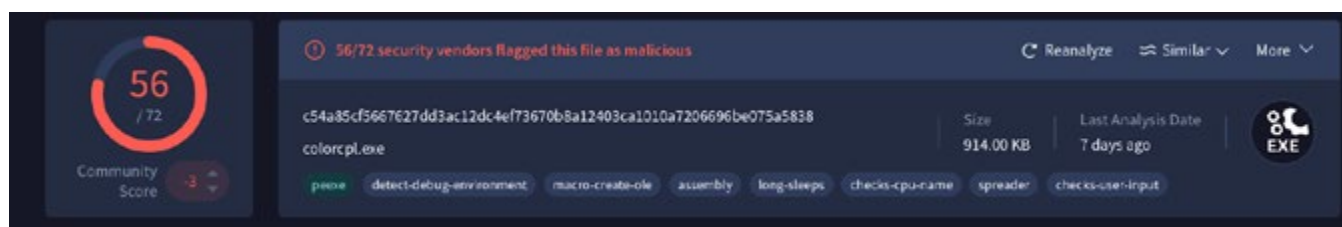
1. stoppirannukes[.]com
2. nowsupportisrael[.]com
3. mixanalyzer[.]com
4. wioccteam[.]net
5. supportisraelfunding[.]com
6. stopviolenceagainstchildren[.]com
7. stopholocaust[.]com



## Typosquatting and Victim Selection

Based on netflow data, we were able to track an upstream management VPS from which the actor established SSH connections to their VPSs. The upstream VPS using IP 69.30.198[.]236, resolved to the following domain at the time of the activity: info-vi.nobelform[.]com. The main domain of this website seems to be typosquatting the domain of NobleForms[.]com, which belongs to an Oregon-based company providing automation services for estate planning.

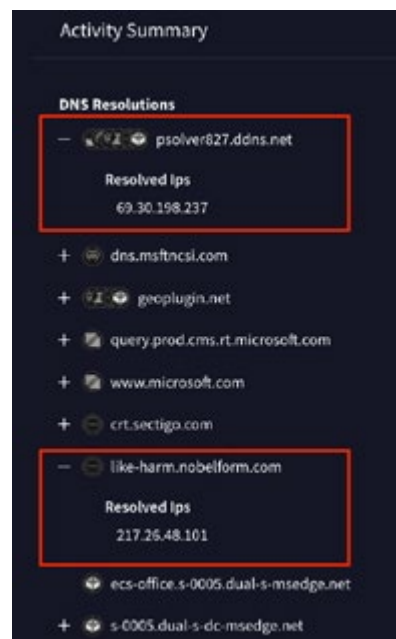
The hijacked domain had a set of subdomain operations under it, each hosted separately on the same C-class IPs as the VPS on 69.30.198[.]236. Another sibling subdomain, like-harm[.]nobelform[.]com, was observed hard-coded in a sample of the RemCosRAT malware, a commercially available remote access tool, commonly abused by hackers and threat actors for espionage operations.



The payload was using like-harm[.]nobelform[.]com as its secondary C2 domain, along with psolver827[.]ddns[.]net.

We assess that access and information collected in the first observable part of this campaign enables the actor to compile a list of potential targets. From this point forward, we assess that the threat actor makes decisions about graduating the victim to the next stage, at which point the threat actor deploys malware, such as RemCosRAT, against the targets.

In all, the campaign indicates a well-crafted, multi-stage intelligence operation, complete with phishing for targets and malware deployment.



TK - imagery on the process of the domains, the mitm Evilginx,

## Chapter 3: Cyberdefense During Kinetic Conflict

This report can present key insights for defenders operating in the context of kinetic conflict. As air strikes cross borders, cyber proxies and hacktivists launch increasingly coordinated campaigns complete with reconnaissance, recruitment, defacement, data theft, data dumps, phishing, and malware delivery.

Many of the threat actors analyzed in this research appear to select their messaging and victims based on their symbolic value rather than their strategic effect, in many cases relying on cyber-operations as an act of solidarity with Palestinian resistance. Several of the operators choose targets with minimal cybersecurity defenses.

While typical characterizations of “cyberwarfare” can evoke offensive cyber-operations that devolve into physical effects, this research on the Twelve Day War shows that cyber-operations during conflict can also result in sustained disruption, intimidation, data leaks, and phishing lures.

Overlapping targets, shared narratives, and similar timing between these groups can blur the line between proxy and independent action as well, which can complicate intelligence assessments.

As hacking campaigns tied to kinetic conflict evolve so too must defense. Defense against offensive cyber-operations and reconnaissance during times of great turmoil must not only include historical threat actor behavior, but also real-time monitoring and analysis of campaigns and hacker chatter in order to keep threats at bay.

Key recommendations include emphasizing employee awareness to the dangers of phishing and social engineering at times of conflict and asking your security vendors to assess whether your organization might fall within the scope of a targeted campaign.

## Final Thoughts

The 12-day conflict between Israel and Iran extended beyond conventional warfare into a complex cyber landscape. This report, based on analysis of 250,000 Telegram messages from 178 active groups, offers strategic insights into the roles of cyber proxies and regional hacktivists operating on Iran’s behalf. These groups amplified narratives and coordinated cyber-operations against perceived adversaries, highlighting a multi-vector threat environment encompassing state-sponsored campaigns and opportunistic hacktivist activities.

In concert, the hacker chatter and activity that emerged during the 12-day conflict can appear sweeping, chaotic, or even disparate. But upon a closer examination, key patterns—and at times, coordination—emerge, showing a great amount of tailoring, precision, and targeted alignment between hundreds of Iranian-tied threat actors.



Our analysis reveals a detailed map of operations that were fast, targeted, and ideologically charged. In many cases, the threat groups appear to have coordinated their operations with agility and deep alignment.

The mosaic of threat activity that emerges appears to be emblematic of a broader trend in Iranian cyber-operations, which the U.S. intelligence community has alluded to in its unclassified 2025 [Annual Threat Assessment](#): Iran's guidance on cyber-operations has incentivized threat groups to become more intense in developing cyberattack capabilities.

## A Web of Linked Activity

We observe three main categories of threat actors on this digital front, each of which is growing increasingly interlinked:

1. First, we observe a layer of hacktivists, which are aligned with the IRGC but which appear to lack clear tasking.
2. Next, we observe a cluster of hackers that are more aligned with IRGC and state-backed priorities.
3. At the top, we find outright state-sponsored hackers.

IRGC-aligned proxies, which are likely operated or sponsored by Iran's cyber forces, combine sophisticated operational capabilities with direct ideological alignment with the Revolutionary Guard. Their high message volumes and consistent use of IRGC insignia underscore their strategic importance in Iran's cyber arsenal, suggesting a more organized and centrally controlled operation. Their activities involve targeted disruptions and intelligence gathering, reflecting a strategic approach to cyber warfare.

In another turn, a diverse array of regional and ideological hacktivist collectives includes cells like the Cyber Islamic Resistance (CIR) and Cyber Fattah Team, Fatimion cyber team, Tunisia's Maskers Cyber Force (TMCF), and Iran-aligned groups such as Islamic Hacker Army group and sharp333. These groups contribute to the broader cyber conflict through a range of ideologically-driven disruptive activities.

Their operations are often framed under local grievance narratives, creating a resilient and geographically dispersed threat. These groups, while aligned with the general cause, often operate with less direct oversight and exhibit more opportunistic behavior.

## The Blend of Proxy and Volunteer

The involvement of actors from multiple countries and groups within the region can significantly complicate attribution and response efforts. Some appear to operate with tasking closely aligned with the IRGC, while others act based on ideological fervor or opportunism, complicating attribution and muddying the response calculus for defenders.

Understanding the difference between state-sponsored and opportunistic groups is crucial for making sense of increasingly complex and interlinked cyber and kinetic conflicts.

- Even as distinctions emerge between threat groups, our analysis of the myriad operations suggests that cyber offensives in this threat landscape are increasingly ideologically driven and woven together in coordinated ways, rather than entirely disjointed or erratic.
- Taken together, STRIKE assesses that kinetic activities will likely continue to trigger tasking or inspire action that leads to disruptive cyber campaigns, each coordinated in a global web of ideologically aligned threat actors.

Each group appears aimed at intimidating adversaries, weakening Israeli morale, and amplifying Iran-aligned cyber “warfare” in support of Palestinian causes. Many state-aligned groups have focused efforts on defacement, disruption, and data-theft, each aimed at intimidating adversaries, weakening Israeli morale, and amplifying Iran-aligned cyber “warfare” in support of Palestinian causes.

We also observed some IRGC-inspired groups opting to target financial, governmental, and media targets, driven by ideological intent to punish "collaborators." Gathering intelligence and conducting offensive operations was a focus for several hacktivist and state-aligned groups alike.

## Symbolism and Tasking

Many of the threat actors appear to select their messaging and victims based on their symbolic value rather than their strategic effect, in many cases relying on cyber-operations as an act of solidarity with Palestinian resistance. But symbolic attacks can still lead to real disruption.

From data theft and data dumps to SQL injection operations and DDoS campaigns, both the structured proxies aligned with the IRGC and the looser constellation of regional hacktivist groups participated in coordinated activity against a set of overlapping targets.

A more covert player also shifted tactics in line with the conflict as it progressed. Tortoiseshell or Imperial Kitten, a known Iranian state-linked threat actor, adopted conflict-themed phishing lures and stood up campaign infrastructure almost immediately after kinetic operations began.

It showed a marked shift from its operations before the 12-Day conflict began. This campaign suggests the threat actor, notorious for its sophisticated social engineering and custom malware, has planning or tasking cycles that respond quickly to conflict flashpoints, which can inform defenders as future conflict unfolds.

# Key Takeaways

Based on our findings, several key takeaways emerge:

1. **Cyber Warfare:** The Israel-Iran conflict underscores a critical shift in modern warfare: Cyber-operations are no longer secondary but fundamental to geopolitical disputes. State-sponsored actors and aligned proxies exploit cyberspace for diverse strategic goals, including intelligence gathering, propaganda, and direct attacks on critical infrastructure and public entities. This evolving landscape demands a comprehensive understanding of conflict that fully integrates both kinetic and cyber dimensions.

This is particularly evident in Russia's war in Ukraine, where [Russian APTs](#) targeted Ukrainian power plants and critical infrastructure to pave the way for kinetic battles. Previous SecurityScorecard research has indicated this trend: Russian-linked hackers unleashed the [Zhadnost botnet](#) against Ukrainian government and financial websites in advance of—and during—Russia's invasion of Ukraine.

Similarly, in the India-Pakistan border clashes earlier this year, Pakistan coordinated its state-sponsored and [hactivist groups](#) to align cyber efforts against India.

Ultimately, cyber warfare has, yet again, emerged as an indispensable and integrated component of contemporary international conflict.

2. **The Rise of Hybrid Threat Actors and Complicated Attribution:** The report highlights the blurred lines between state-sponsored and independent hactivist groups. While some proxies show clear ties to state entities like the IRGC, others operate with varying degrees of autonomy, driven by ideological or even financial motives. This creates a multi-vector threat environment where attribution becomes increasingly challenging.

The diverse geographic origins and varying levels of sophistication among these groups demand a nuanced approach to threat intelligence and defense. Understanding the distinct motivations and capabilities of each group, rather than simply lumping them together as threats from Iran, is crucial for effective counter-measures.

Our research consistently demonstrates how strong ideological motivations drive cyber-operations. Whether it's "Islamic Cyber Resistance" narratives, "Free\_Palestine" slogans, or anti-Western sentiments, these ideological underpinnings provide the impetus for attacks and shape targeting decisions. The sustained nature of these campaigns suggests that these actors are not merely opportunistic but are committed to their objectives, making them persistent threats globally, not just regionally.

This results in a broader understanding of the mosaic of ideologically-driven operators that contribute to offensive hacking campaigns across borders, rather than dividing or confining them to certain geographies. Global networks of ideologically-aligned hacking groups with shared aims are now proliferating and coordinating across borders.

- 3. Telegram's Role as a Centralized Hub for Cyber-Operations:** Telegram has emerged as a critical platform for coordination, propaganda dissemination, and command-and-control for both state-aligned proxies and hacktivist collectives.

Its perceived anonymity and broad reach make it an attractive medium for these groups to organize, share information, claim responsibility for attacks, and even recruit new members.

Monitoring and understanding the activity on such platforms is essential for anticipating and responding to cyber threats originating from these networks.

- 4. Low-Barrier Entry Points and Opportunistic Exploitation:** Many of the observed cyber-operations, particularly those of hacktivist groups, rely on straightforward but effective tactics such as web defacements, basic DDoS attacks, and exploitation of common web vulnerabilities (such as SQL injection campaigns). This indicates that even with limited technical sophistication, these groups can achieve significant disruptive impacts, especially against targets with weaker cybersecurity defenses.

This underscores the importance of basic cyber hygiene, patch management, and robust security practices for organizations, regardless of their perceived risk level. Sophisticated hackers can conduct damaging operations—but so too can hackers with far less advanced tools and technical acumen.

- 5. The Interplay of Ideology and Strategic Objectives:** Contemporary social engineering campaigns continue to leverage current events and human psychology to their advantage. In the cases examined, the threat actors weaponize human curiosity and empathy, often evoking themes of conflict, war, and geopolitical tensions to elicit strong emotional responses.

This emotional manipulation is designed to bypass victims' usual judgment and critical thinking, making them more susceptible to phishing attempts, malware delivery, and other malicious activities. Understanding these evolving psychological tactics is crucial for developing effective awareness campaigns and defense mechanisms.

## Contact STRIKE for Incident Response

SecurityScorecard's STRIKE Team has access to one of the world's largest databases of cybersecurity signals, dedicated to identifying threats that evade conventional defenses. With proactive risk management and a rapid response approach, SecurityScorecard offers companies protection against third-party risks and the ability to counter active threats like those tied to Iran. Discover how SecurityScorecard and its STRIKE Team can strengthen your enterprise's security.

For STRIKE media inquiries, contact us [here](#).