THREAT ANALYSIS

Recorded Future®

Insikt Group®

June 2, 2026

Iran Expands Handala Brand to Physical Threats

Iran's Ministry of Intelligence (MOIS) likely expanded its Handala brand to include personas focused on global physical threat activities, alongside personas for hacktivist and influence operations.

Insikt Group attributes three influence operations networks ("VIPEmployment," "MOISIran," and "Brave Israel") to MOIS, based on online overlaps with Handala Hack Team, a known MOIS persona.

During the Iran War, MOIS has leveraged its Handala brand to solicit physical, cyber, and influence operations targeting the US and Israel, as a form of asymmetric retaliation.

Executive Summary

Iran's Ministry of Intelligence (MOIS) has likely broadened the use of its "Handala" brand to encompass MOIS's external physical and influence operations targeting US and Israeli interests. Since the beginning of the Iran War, Insikt Group has observed significant overlaps in the online activities of Handala Hack Team, a newly created, Handala-branded persona referring to itself as the "Handala Popular Resistance Front" (HPRF), and three influence operations networks previously identified by Insikt Group. Based on frequent amplification and cross-posting of claims and content between Handala Hack Team and these four additional entities, we now attribute these groups to MOIS, with varying degrees of confidence.

The nexus between these personas and MOIS, as well as their multidomain tactics, techniques, and procedures (TTPs) and targeting, likely reflects how MOIS's external operations have shifted in response to the Iran War. Notably, the HPRF and the three influence operations networks all almost certainly share a modus operandi: their administrators solicit individuals to conduct physical attacks and espionage targeting US and Israeli entities, on behalf of Iranian intelligence agencies, for a financial reward. By encompassing these groups under the Handala brand, MOIS likely seeks to take advantage of Handala's global recognition to amplify its solicitation efforts.

MOIS's likely coordination of distinct cyber, physical, and influence personas under a single brand very likely amplifies physical and cyber threats to targeted individuals and facilities. Handala-linked physical threat actors could almost certainly leverage the recognition of the brand's hacktivist personas to recruit individuals to conduct targeted violent attacks, espionage, sabotage, or other physical threat activities. Shared resources, intelligence, and coordination efforts from a centralized source likely increase the impact of an attack. This very likely entails heightened risks for US and Israeli law enforcement, military, and intelligence agencies and their personnel, in addition to energy, transportation, and research organizations operating in the region.

Key Findings

- MOIS has likely expanded its use of the Handala brand, broadening its scope to include physical threat actor personas alongside existing hacktivist and influence operations networks.
- MOIS's expansion of its Handala brand includes a newly identified threat actor persona, Handala Popular Resistance Front (HPRF), which claims to be a network of physical threat actors associated with Handala Hack Team.
- In addition to the HPRF, Insikt Group assesses that three influence operations networks — "VIPEmployment", "MOISIRAN", and "Brave Israel" — are likely MOIS personas, due to cross-amplification of online content between these networks and Handala Hack Team, a known MOIS persona.
- Under the Handala brand, MOIS is almost certainly using HPRF, VIPEmployment, MOISIRAN, and Brave Israel for a common purpose: soliciting physical attacks, assassinations, espionage, and sabotage targeting personnel and assets associated with US and Israeli security services. While predominantly targeting Israel-based audiences, these activities have expanded their geographic scope as a result of the Iran War.
- Interactions between hacktivist and physical threat actor personas under the Handala brand likely enhance the reach and impact of MOIS's external operations, and could enable advanced targeting through cyber-enabled physical attacks and influence operations.

Table of Contents

Iran's Ministry of Intelligence's Use of Operational Personas

Historically, Iran's MOIS has organized its external cyber and influence operations using operational personas. MOIS-linked threat actor networks operate as "independent" hacktivist or media groups with distinct identities and targets but overlapping TTPs. MOIS almost certainly re-uses personas for multiple operations, adapting their online behavior, characteristics, and branding to MOIS's strategic objectives. As personas expand their reach and gain notoriety, MOIS creates new personas to support existing personas' growing operational requirements (including soliciting physical threats), thereby creating operational "brands."

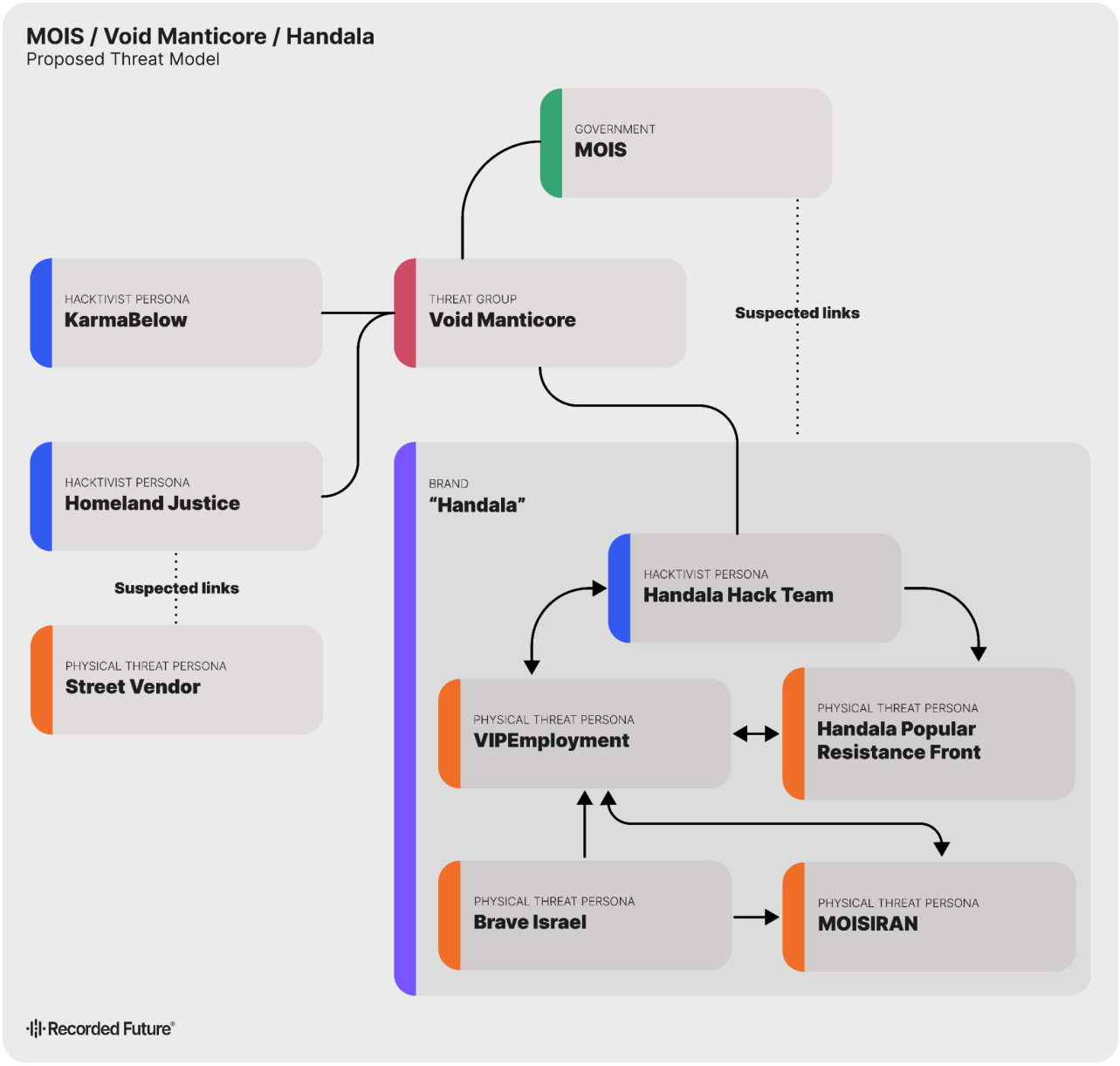


***Figure 1**: Overview of threat actor groups, brands, and personas linked to MOIS by Insikt Group (Source: Recorded Future)*

Void Manticore

Handala Hack Team has been attributed to Void Manticore (TAG-145, Red Sandstorm, Banished Kitten), a threat activity cluster linked to Iran's MOIS by researchers and the US Department of Justice. Handala Hack Team represents one of several personas that MOIS operates to target Israel, Iranian opposition groups, and increasingly the US. These personas — including KarmaBelow and Homeland Justice — are associated with Void Manticore and linked to MOIS's Counterterrorism Division, operating under Seyed Yahya Hosseini Panjaki, Deputy Minister of Intelligence for Israeli Affairs. Prior to his death in Israeli airstrikes in early March 2026, Panjaki headed MOIS's Directorate for Internal Security.

Between 2022 and 2025, Void Manticore personas frequently conducted hack-and-leak operations and wiper attacks, which it subsequently amplified by publicly leaking information from targeted organizations. Homeland Justice focuses on targeting Iranian opposition groups, and since 2022 has claimed responsibility for several cyberattacks on Albania, which hosts the exiled Iranian opposition group Mojahedin-e-Khalq (MEK). KarmaBelow has targeted the Israeli government, deploying destructive malware called the "BiBi wiper" (named after Israeli Prime Minister Benjamin "Bibi" Netanyahu). Handala Hack Team has emerged as the most prolific of the Void Manticore personas, claiming a broad range of operations targeting Israeli leadership, government agencies, security institutions, technology companies, and critical infrastructure, including Israel's nuclear facilities. It has also claimed cyberattacks on Iranian opposition outlet Iran International, which aligns with one of the IRGC and MOIS's priority targets for physical threat operations. Handala Hack Team has also claimed responsibility for hack-and-leak operations targeting US government personnel.

Personas linked to Void Manticore have previously claimed to be soliciting physical threat activities targeting Iranian opposition leaders. In 2024, Insikt Group identified a Telegram persona promoted on Homeland Justice's Telegram channel (*t[.]me/justice_homeland*) named "Shites Rruge" ("Street Vendor" in Albanian). The persona's Telegram channel (*t[.]me/@shitesirruges*) solicited threats against MEK leaders, promising $70,000 for injuring targets and between one and eight Bitcoin (approximately $65,000–$525,000) for "neutralizing" them (**Figure 2**, below). Other posts promised Bitcoin payments for taking videos while burning pictures of MEK politicians or throwing Molotov cocktails at MEK facilities in Durrës, Albania. Posts by the persona included hashtags like #HomelandJustice and asked recruits to email videos and Bitcoin wallet addresses to a Homeland Justice-affiliated email address, *HomelandJustice[@]airmail[.]cc*.

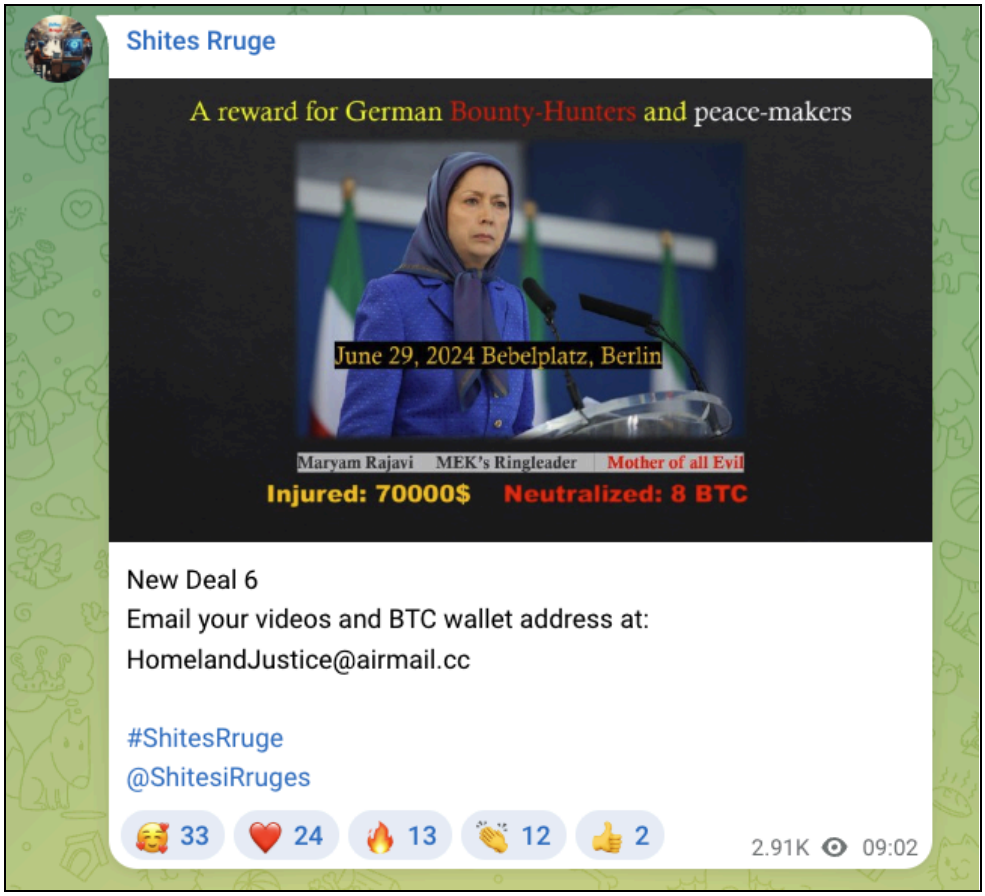


***Figure 2**: "Street Vendor" post soliciting physical threats against MEK leader Maryam Rajavi (Source: Recorded Future)*

"Handala" Persona and Handala Hack Team

The Handala persona first emerged in a Telegram channel for the Handala Hack Team established on December 18, 2023, following the outbreak of the Israel–Hamas war in Gaza. "Handala" refers to an iconic character created by Palestinian political cartoonist Naji al-Ali in 1969: a 10-year-old boy whose back is always turned, symbolizing rejection of foreign-imposed solutions to the Israeli-Palestinian conflict. The use of the Handala name and image signals the group's ideological alignment with and support of Palestinian resistance, portraying itself as an independent hacktivist group taking action against Israel as retaliation for Israeli military actions in Gaza. Between 2023 and 2025, Handala almost certainly used pro-Palestinian symbolism and "axis of resistance" narratives as cover for its operations, preserving plausible deniability while executing strategic operations. That approach has since shifted: MOIS has now overtly deployed its Handala brand to amplify the psychological impact of those operations, with Iranian media openly describing it as a "strategic front of the Axis of Resistance" in the US–Iran conflict.[1]

[1] *tehrantimes[.]com/news/526282/Handala-s-digital-storm-topples-US-Israeli-cyber-supremacy*

Figure 3: *Handala Hack Team's logo reflects an iconic pro-Palestinian cartoon character (Source: Check Point)*

Since late 2023, Handala Hack Team's claimed operations have centered on the "hack-and-leak" model targeting Israeli government officials, security organizations, and companies. Claimed leaks have included alleged personal photos and contact lists of Israeli senior government leaders, data from Israel's Soreq and Dimona nuclear facilities, identities of Mossad agents, Israeli police databases, and companies' sensitive customer information, internal communications, blueprints, and proprietary data. Handala Hack Team's public releases, which amplify the exposure of stolen data alongside political messaging, are hallmarks of the persona's tradecraft. Handala Hack Team has also deployed ransomware, though its operations are almost certainly aimed at sowing chaos in audiences targeted by the attack and creating a sense of vulnerability, rather than collecting an extortion payment.

Handala Hack Team's role in Iran's asymmetric retaliation against the US and Israel, the high-profile nature of its targets, and significant, widespread media coverage of its activities during the Iran War have almost certainly granted Handala Hack Team a level of global media recognition that is uncharacteristic of most modern hacktivist groups. Since the beginning of the Iran War, Handala Hack Team's claimed cyber operations against US targets have surged. Targets have included US medical device maker Stryker, county government infrastructure, FBI director Kash Patel, and US Marine Corps personnel. Handala Hack Team is now "the main face" of Iranian state-sponsored hacktivist activity, and its modus operandi — combining destructive attacks with the publication of details from its victims — enables Iran to "combine deniability with psychological impact."

Handala Pivots to Physical Threats

Iran's MOIS has likely expanded the Handala brand to include distinct threat actor personas focused on physical threat activities. The inclusion of new personas in the existing Handala brand likely seeks to leverage Handala Hack Team's global recognition to advertise and amplify a broader set of MOIS-affiliated personas for influence and intimidation.

Insikt Group has attributed four personas to MOIS and its Handala brand. Two of these personas (VIPEmployment and Brave Israel) were previously identified by Insikt Group, but unattributed; two are newly identified:

- **The Handala Popular Resistance Front (HPRF)** is a purported network of physical threat actors in Israel that has claimed responsibility for physical attacks against Israeli government officials on behalf of Iran's intelligence services.
- **VIPEmployment** is an online network engaging in coordinated inauthentic behavior (CIB) that solicits proxies outside Iran to conduct attacks against US and Israeli interests for financial rewards.
- **MOISIRAN** is a Telegram persona posting claimed surveillance footage of Israeli intelligence and military personnel. MOISIRAN also advertises links to VIPEmployment infrastructure. This persona likely serves to amplify physical threat activities on social media.
- **Brave Israel** is a largely inactive Telegram persona that claimed responsibility for physical threat activities in Tel Aviv in December 2024. A Telegram account linked to Brave Israel now advertises links to VIPEmployment. This persona likely served as an early-stage prototype for recruiting and amplifying proxy threat activities before being repurposed to amplify VIPEmployment bots. Insikt Group assesses that Brave Israel is a likely predecessor of MOISIRAN and is likely operated by the same threat actors.

Handala Popular Resistance Front Claims Attacks in Israel

Iran's MOIS is likely applying the "Handala" brand to assets in Israel tasked with carrying out physical attacks against Israeli government agencies. On April 26, 2026, a group referring to itself as the "Handala Popular Resistance Front" (HPRF) claimed responsibility for an arson targeting an Israeli law enforcement official's vehicle. Beginning on April 21, 2026, online accounts attributed to Handala Hack Team have alleged that its "operational units" in Israel were conducting physical threat activities targeting Israeli law enforcement, intelligence, and military officials.

Insikt Group assesses the HPRF persona as likely attributable to MOIS. Not only does it use the same brand name as Handala Hack Team — which is almost certainly attributable to MOIS — but its TTPs almost certainly mirror those of other MOIS physical threat operations in Israel. Moreover, HPRF's online activity significantly overlaps with other online networks that we assess are almost certainly or very likely tied to MOIS personas, including the Handala Hack Team and VIPEmployment personas' frequent amplification of HPRF's claims.

According to data in the Recorded Future Intelligence Operations Platform, the first mention of the HPRF was in an April 26 now-deleted post from the Telegram account Handala Partisan (*t[.]me/HANDALA_PARTISAN*), which claimed the HPRF conducted a "secret field operation" within Israel in which they lit a car on fire. The post stated that the car — likely a late-2000s or early-2010s silver Ford Focus — belonged to a Shin Bet "senior officer" working on Iran-related issues. (Shin Bet is Israel's domestic security and counterintelligence authority.) The account further claimed that "Handala agents" were conducting "dozens of large-scale field operations" in "the very heart of enemy-controlled areas." Two videos attached to the post, depicting an individual dousing a car very likely located in Israel with a flammable liquid and setting it on fire, contain links to a Handala Hack Team website (*handala-hack[.]ps*) and a Telegram bot account almost certainly connected to VIPEmployment (*t[.]me/VIPEmployment02Bot*). The post's text also contains a link to this bot.

***Figure 4**: Video depicting HPRF-claimed vehicle arson, overlaid with Handala Hack Team and VIPEmployment contact information (Source: Telegram)*

If its claims are accurate, the claimed arson on April 26 would represent the first physical attack overtly claimed by a persona using the Handala name. Although an April 29, 2026, DarkOwl assessment covering the April 26 Telegram post claimed it "announced a rebrand" of Handala Hack Team to the HPRF, this framing is very likely inaccurate. On April 28, Handala Hack Team issued a statement claiming responsibility for the doxing of US forces stationed in the Middle East, which references "Handala Hack Team," not "HPRF," as the responsible persona. This very likely indicates that they are distinct personas.

Despite their mutual use of the "Handala" brand name, it is also unlikely that HPRF is a "branch" of the Handala Hack Team persona. Instead, these are two separate personas operating under MOIS's existing "Handala" brand. HPRF is a persona almost certainly designed to conduct and publicize physical threat activities; Handala Hack Team almost exclusively conducts and amplifies cyber threat activities. The two threat streams very likely require different sets of personnel, infrastructure, knowledge, skills, and abilities. In addition, HPRF claims that most of its assets are based within Israel, while Handala Hack Team very likely operates from Iran.

It is likely that MOIS applied the existing Handala brand to assets and recruits within Israel to constitute the HPRF as a distinct persona. The inclusion of the HPRF persona under the Handala brand likely boosts the notoriety of both Handala Hack Team and the HPRF. This behavior is likely a hallmark of MOIS cyber-enabled threat activity, which frequently uses hacktivist brands and related personas and constantly adapts them with new infrastructure, entities, and TTPs in alignment with geopolitical trends. In this case, through mutual use of the Handala brand, the HPRF very likely intends to gain credibility by association with Handala Hack Team, which has an established reputation as a hacktivist threat; Handala Hack Team very likely intends to promote HPRF's claims of association to gain credibility as a multifaceted threat actor group with multiple divisions and subgroups. Both of these factors also very likely benefit MOIS, which can use the perceived credibility of the Handala brand writ large to attract recruits for physical threat operations targeting Israel.

VIPEmployment Infrastructure Very Likely Tied to Handala Persona

The Iran-linked intelligence recruitment network VIPEmployment, previously identified by Insikt Group in August 2025, is very likely a persona within MOIS's Handala brand. Insikt Group's attribution is based on the activity of three almost certain VIPEmployment Telegram channels (*t[.]me/Ir_intel_voice*, *t[.]me/ir_intel_voice_ar,* and *t[.]me/ir_intel_voice_ar_dis*, henceforth referred to as the "Intel Voice" channels), which share VIPEmployment's stated objective of soliciting Israel-based individuals to carry out attacks and espionage inside the country on behalf of Iran's intelligence services. As with previously observed VIPEmployment infrastructure, the three Intel Voice channels frequently post links to a Telegram bot using variations of the name "VIPEmployment", claim to represent "Iran's intelligence service," and state their intent as "recruiting high-paid agents in a completely secure and professional environment with 24/7 monitoring and support."

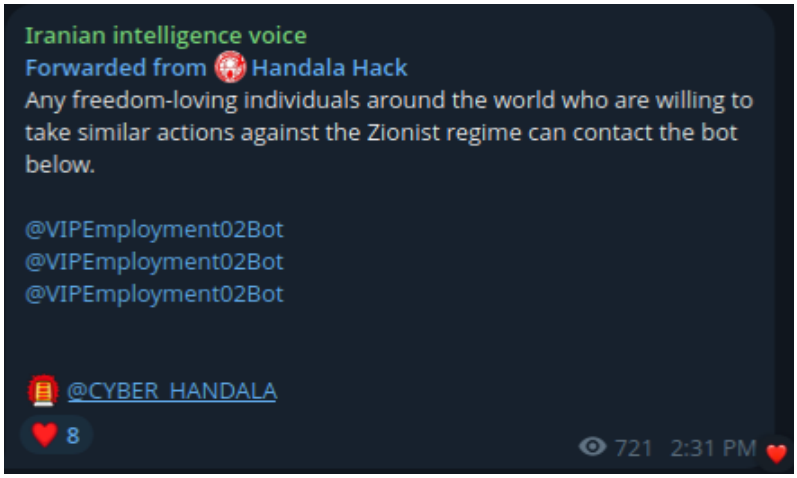


***Figure 5**: April 21, 2026 Handala Hack Team post advertising VIPEmployment's Telegram bot (Source: Telegram)*

The degree and frequency of interactions between the Intel Voice Telegram channels and Handala infrastructure very likely suggest that the three Intel Voice channels are part of the overarching Handala brand, and that VIPEmployment is also attributable to MOIS. Unlike previously identified VIPEmployment channels, the English- and Arabic-language Intel Voice channels — bearing the usernames "Iranian intelligence voice" and "صوت المخابرات الإيرانية" (Iranian intelligence voice) respectively — have frequently reposted or amplified content originally posted to Handala Hack Team or HPRF Telegram channels. For instance:

Date	Channel	Information
2026-04-26	English and Arabic Intel Voice	Repost of HPRF claim from Handala Partisan Telegram channel to have conducted an arson targeting a Shin Bet officer
2026-04-21	English and Arabic Intel Voice	Repost of claim from a Handala Hack Team Telegram channel (*t[.]me/CYBER_HANDALA*) to have surveilled "one of the highest-ranking officials of the Zionist regime's security apparatus"
2026-04-21	English and Arabic Intel Voice	Repost of solicitation from a Handala Hack Team Telegram channel (*t[.]me/CYBER_HANDALA*) asking "any freedom-loving individuals around the world who are willing to take similar actions against the Zionist regime" to "contact the bot below." The post contained three links to the VIPEmployment Telegram bot (@VIPEmployment02Bot)
2026-04-21	English and Arabic Intel Voice	Repost of a statement from a Handala Hack Team Telegram channel (*t[.]me/CYBER_HANDALA*) that "Handala does not need to publicize all of its actions; it acts in a way that preserves the strategic interests of the Resistance Front. When the time is right, we will make our actions known."

Date	Channel	Information
2026-04-14	Arabic Intel Voice	Repost of a poll from a Handala Hacking Team Telegram channel (*t[.]me/handala_intel)* titled "What do you think of the new head of Mossad after he saw the surprises from Iranian intelligence?" (شو رأيكم بالرئيس الجديد للموساد بعد ما شاف مفاجآت المخابرات الإيرانية؟

***Table 1**: Amplification of Handala Hack Team content by Intel Voice accounts in April 2026 (Source: Telegram)*

Conversely, known Handala Hack Team and HPRF accounts have also frequently reposted content from the Intel Voice channels, or provided links to the VIPEmployment Telegram bot:

Date	Account	Information
2026-04-26	t[.]me/CYBER_HANDALA	Post soliciting individuals who "seek true security and a different future." The post links to a VIPEmployment bot (@VIPEmployment02Bot) and the Handala Partisan Telegram channel
2026-04-22	@HPRRed	Post soliciting "freedom-loving individuals around the world who are willing to take similar actions against the Zionist regime" to contact a VIPEmployment bot (@VIPEmployment02Bot)
2026-04-21	t[.]me/CYBER_HANDALA	Post soliciting "freedom-loving individuals around the world who are willing to take similar actions against the Zionist regime" to contact a VIPEmployment bot (@VIPEmployment02Bot)
2026-04-14	t[.]me/HANDALA_INTEL	Post linking to a VIPEmployment bot (@VIPEmployment01Bot)
2026-04-14	t[.]me/HANDALA_INTEL	Post soliciting "resident[s] of the occupied territories" to "join us through the Telegram bot below and play a role in shaping a better future for your children." The post links to a VIPEmployment bot (@VIPEmployment01Bot) and the English Intel Voice channel.

***Table 2**: Amplification of VIPEmployment content by Handala accounts in April 2026 (Source: Telegram, Social Media)*

Insikt Group has previously observed VIPEmployment using Telegram bots to solicit individuals around the world to conduct physical attacks on Iran's behalf. Since 2024, VIPEmployment has used accounts across multiple social media and messaging platforms — almost certainly engaging in CIB — to recruit individuals in dozens of countries around the world to conduct espionage and physical attacks against US- and Israel-linked targets. Posts containing links to VIPEmployment Telegram bots, which purport to represent Iranian intelligence agencies' preferred conduit for communications with overseas assets, are almost certain indicators of VIPEmployment activity.

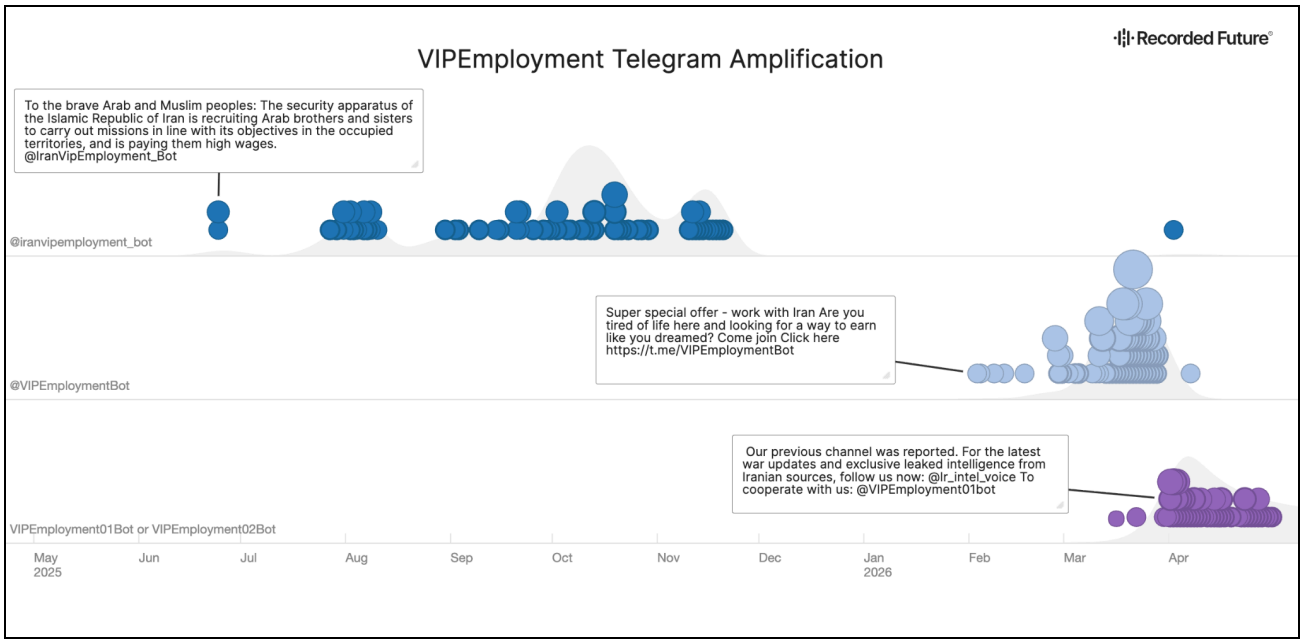


***Figure 6**: CIB amplification on Telegram promoting VIPEmployment bots (Source: Recorded Future)*

Broader interactions between VIPEmployment and other Handala-branded personas likely indicate that VIPEmployment is also attributable to MOIS. VIPEmployment targeting activity almost certainly aligns with Iran's external operations footprint before and after Operation Epic Fury. In an initial phase of VIPEmployment activity — taking place between August 2024 and the beginning of Operation Epic Fury in late February 2026 — a network of Telegram channels with Hebrew alphabet usernames, almost certainly engaging in CIB, posted several hundred links to VIPEmployment Telegram bots in Hebrew-language Telegram channels almost certainly directed toward Israeli audiences. Solicitations directed Israelis, particularly individuals seeking job opportunities and Haredi (ultra-orthodox) Jews disaffected by Israeli government policies, to contact the bot, typically promising significant financial rewards for cooperation with Iranian intelligence. In August 2025, Israeli law enforcement arrested two individuals from Holon, Israel, on suspicion of committing "security offenses involving contact with Iranian intelligence agents." One of the individuals was reportedly in contact with "individuals linked to VIPemployment" and "received payments in cryptocurrency."

Beginning in February 2026 after the start of Operations Epic Fury and Roaring Lion, VIPEmployment accounts began broadening the geographic aperture of their solicitations, posting links to the VIPEmployment bots in multiple types of Telegram group chats, including chats advertising job opportunities in Europe, Gulf Cooperation Council (GCC) countries, Australia, and other countries; group chats for university students; "buy/sell" groups in Mexico and Latin America; and Telegram channels and group chats focusing on political issues in English-speaking countries. Posts alongside these solicitations used English and Arabic, not Hebrew, and cited political issues— such as the Israel–Hamas conflict, the release of legal documents connected to Jeffrey Epstein, and Operation Epic Fury — as motivators to cooperate with Iran's intelligence agencies.

From English-language posts, the ultimate intent of Iranian intelligence solicitation through VIPEmployment bots is unclear without directly engaging the bot. Nevertheless, several Arabic-language posts advertising the bot have explicitly stated that Iranian intelligence intends to solicit physical threat actors around the world to attack US and Israeli interests (see **Table 3**).

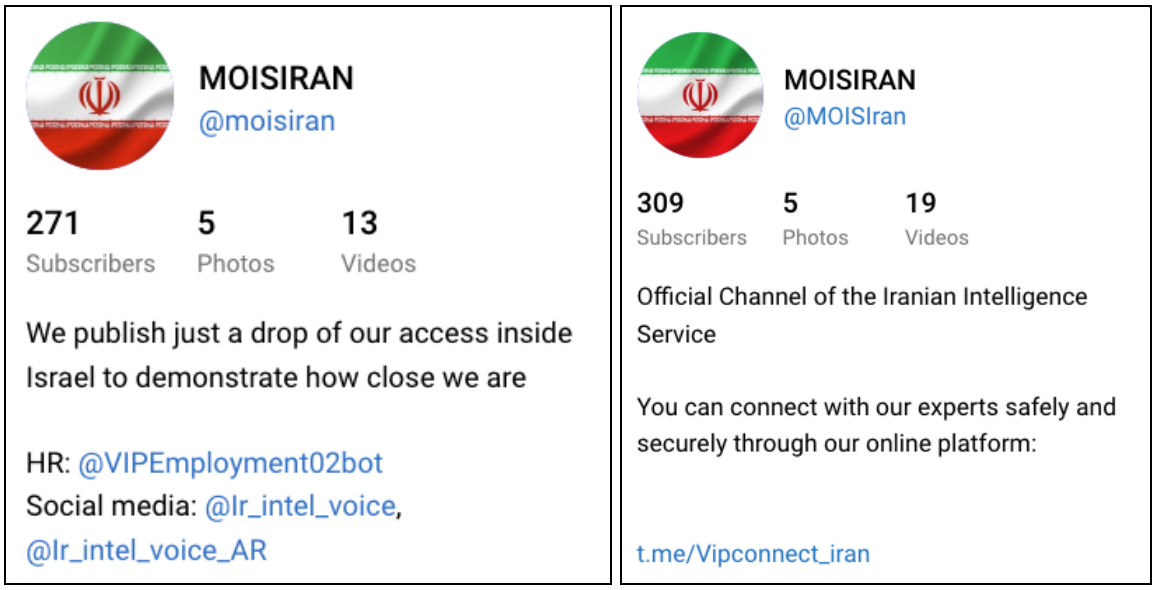
Arabic	English
نداء عاجل للتعاون من الأمة الإسلامية الشجاعة في فلسطين، ولبنان، والمملكة العربية السعودية، والإمارات العربية المتحدة، والبحرين، والعراق، والكويت، وسوريا، وتركيا، وباكستان، ودول أخرى	An urgent call for cooperation from the courageous Muslim Ummah in Palestine, Lebanon, Saudi Arabia, the United Arab Emirates, Bahrain, Iraq, Kuwait, Syria, Turkey, Pakistan, and other countries
🔻 🔻 يجب استهداف جميع المصالح والأفراد المرتبطين بالنظام الصهيوني وأمريكا و عملائهم في منطقتنا و مناطق أخرى من العالم، وستحصلون منا على أجر حسن	🔻 🔻 All interests and individuals associated with the Zionist regime, America, and their agents in our region and other parts of the world must be targeted, and you will receive a good reward from us.
◀إليكم بعض الأشياء التي يمكنكم القيام بها:	◀Here are some things you can do:
1️⃣قتل جنود ومواطني الحكومة الأمريكية الإجرامية أينما وجدتهم	1. Kill soldiers and citizens of the criminal American government wherever you find them.
2️⃣اغتيال تجار المرتبطين بشركات صهيونية وأمريكية	2. Assassinate businessmen associated with Zionist and American companies.
3️⃣حرق وتدمير جزئي أو كلي لمباني القنصلية أو مساكن الأمريكيين والصهاينة	3. Burn and partially or completely destroy consulate buildings or residences of Americans and Zionists.
4️⃣ارسال إحداثيات مواقع أفراد وضباط العدو مع الوثائق	4. Send the coordinates of enemy personnel and officers along with documents.
5️⃣كتابة الشعارات وحرق علم العدو	5. Write slogans and burn the enemy flag.
6️⃣استهداف المنشآت التابعة للعدو، بما في ذلك المعدات وخطوط نقل الغاز	6. Target enemy facilities, including equipment and gas pipelines.
اغتنمو الفرصة و تفضلوا بزيارة بوت تيليجرام الخاص بمخابرات الإيرانية: @vipemploymentbot	Take advantage of this opportunity and visit the Telegram bot of the Iranian intelligence service: @vipemploymentbot

***Table 3**: March 3, 2026, post in "مناقشات اخبار الياامون 🖤🔥" Telegram channel (Source: Recorded Future)*

MOISIRAN Likely Another Persona Amplifying Physical Activities

Insikt Group identified a Telegram persona named "MOISIRAN" (*t[.]me/moisiran,* almost certainly in reference to Iran's MOIS) created on April 20, 2026. The MOISIRAN persona has made multiple claims of having surveilled Israeli military and intelligence personnel. This includes targets with claimed affiliations to Shin Bet; Mossad, which is Israel's foreign intelligence agency; and Unit 8200, the Israel Defense Forces' foremost signals intelligence unit; as well as an Israeli nuclear scientist. The channel also claims to have successfully recruited an Israeli police officer, who allegedly shared "traffic patterns and sensitive intelligence" about a police facility with the channel's administrators.

Insikt Group assesses that this persona is likely also operating under the Handala brand and broader MOIS activity cluster. The Telegram channel listed VIPEmployment's Telegram bot as "HR", and two VIPEmployment-linked "Intel Voice" Telegram channels (*t[.]me/Ir_intel_voice* and *t[.]me/ir_intel_voice_ar*) as "Social Media." The Telegram channel's operators have also repeatedly linked to VIPEmployment accounts and used #Handala to amplify their messaging. Around May 10, 2026, MOISIRAN changed its description and posts to link to Telegram account @vipconnect_iran from "VIPEmployment"-themed accounts.[2] Less than an hour after a May 10, 2026, post by MOISIRAN first linking to the new Telegram account, a new "Intel Voice" channel (*t[.]me/ir_intel_voice_ar_dis*) forwarded MOISIRAN's post, suggesting continued bidirectional amplification between the two channels.[3]



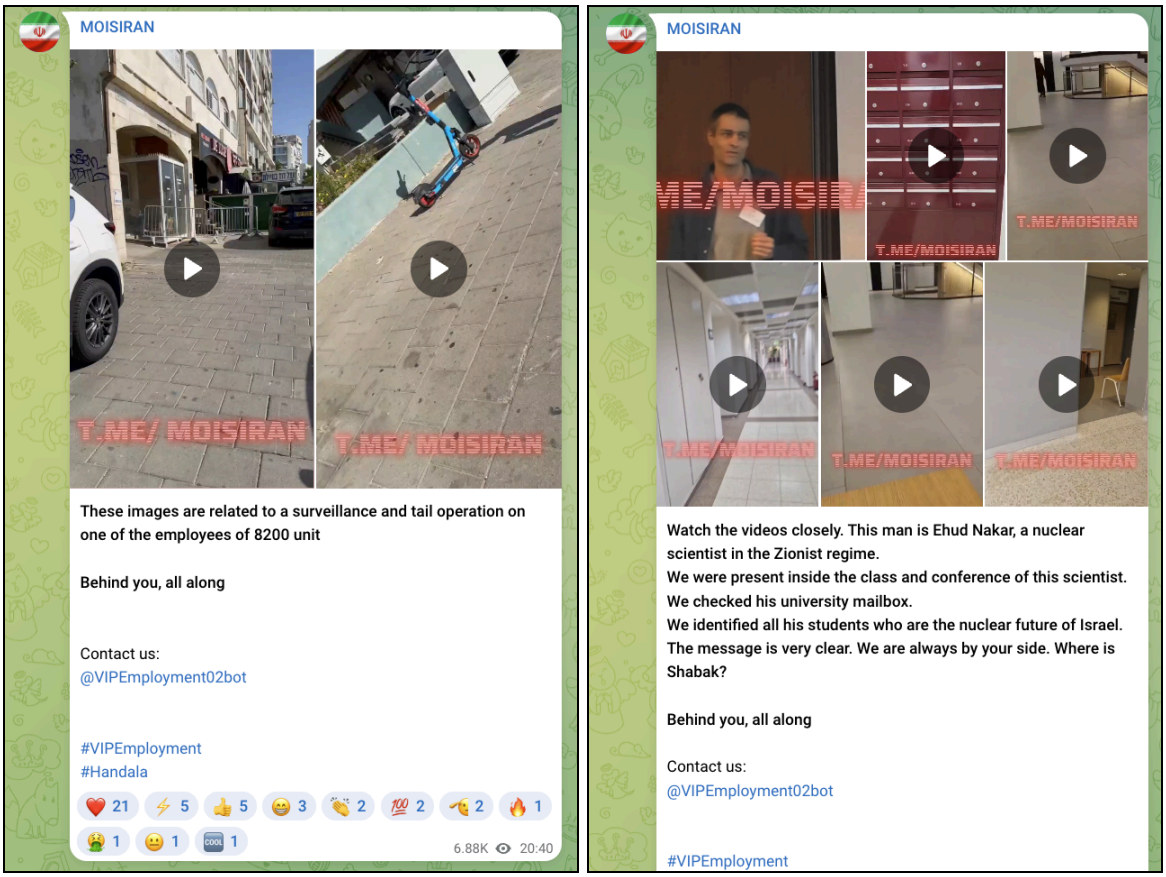
***Figures 7 and 8**: Screenshot of MOISIRAN's Telegram channel in April (left) and May 2026 (right) (Source: Telegram[4])*

While Insikt Group was unable to definitively substantiate MOISIRAN's claims, footage and screenshots posted by the persona appear to be authentic and align with intimidation tactics previously claimed by

[2] *t[.]me/moisiran/46*
[3] *t[.]me/ir_intel_voice_ar_dis/196*
[4] *t[.]me/moisiran*

Handala Hack Team, such as allegedly leaving a bouquet of roses in the car of Israeli nuclear scientist Dr. Isaac Gertz in November 2025.

On April 22, 2026, the MOISIRAN Telegram channel posted two videos (**Figures 9 and 10, below)** claiming to depict a "surveillance and tail operation on one of the employees of 8200 unit" using hashtags #VIPEmployment and #Handala in addition to prompting channel members to "contact us" using @VIPEmployment02bot, the same Telegram bot promoted in the "Intel Voice" channels.[5] On April 23, 2026, the channel posted five videos and one picture claiming to be footage of a surveillance operation targeting Israeli nuclear scientist Ehud Nakar at Tel Aviv University facilities (**Figure 10, below**).[6]

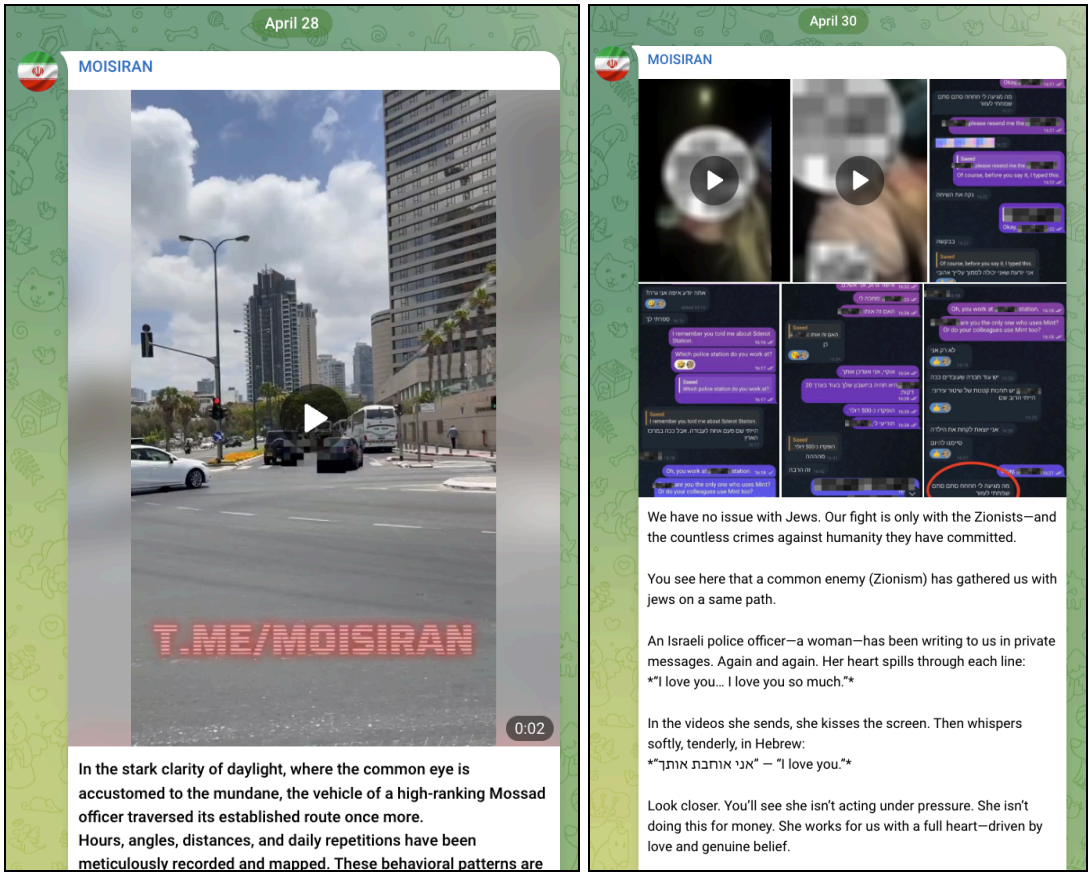


***Figures 9 and 10**: Videos posted by MOISIRAN on April 22 (left) and April 23 (right), 2026 (Source: Recorded Future)*

On April 28, 2026, MOISIRAN posted a video (**Figure 11**) claiming to depict surveillance of a "high-ranking Mossad officer" in Tel Aviv with similar hashtags and a link to @VIPEmployment02bot.[7] On April 30, MOISIRAN posted two videos and four screenshots of Telegram direct messages claiming that the account (named "Saeed") was corresponding with an Israeli police officer, stating that "This

[5] t[.]me/moisiran/7
[6] t[.]me/MOISIran/25
[7] t[.]me/MOISIran/33

brave woman, deep inside the Israeli police system, shares traffic patterns and sensitive intelligence with us—carefully, loyally."[8]

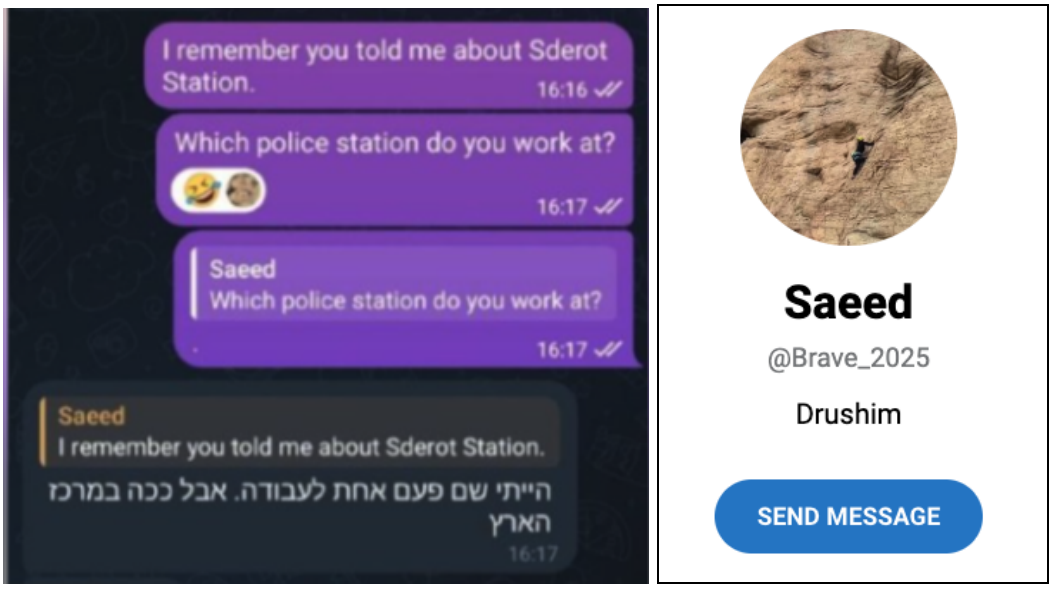


***Figures 11 and 12**: Videos posted by MOISIRAN on April 28–30, 2026 (Source: Telegram[9])*

Insikt Group assesses that MOISIRAN likely shares operators with Brave Israel and likely coordinates with Intel Voice channels tied to VIPEmployment. MOISIRAN's April 30 post detailing purported text messages with an Israeli police officer (**Figure 13**) shows the interlocutor quoting the screenshotter's message, displaying the quoted account's name as "Saeed." As of May 2026, the Telegram account @Brave_2025 — which Insikt Group previously attributed to Brave Israel — displays the name "Saeed" (**Figure 14**) with a description reading "Drushim" (דרושים, or "jobs" in Hebrew).

MOISIRAN, @Brave_2025, and the "Intel Voice" channels have also conducted coordinated amplification of MOISIRAN's content. On April 24, 2026, MOISIRAN posted a generic recruitment message at 17:25 GMT. Eleven minutes later, at 17:36 GMT, @Brave_2025 forwarded the message to another Telegram channel, *t[.]me/israel1chat*. At 17:53 GMT, the VIPEmployment Telegram account @Ir_intel_voice forwarded the exact same message to *t[.]me/ir_intel_voice*.

[8] *t[.]me/MOISIran/34*
[9] *t[.]me/MOISIran/33; t[.]me/MOISIran/34*



***Figures 13 and 14**: Screenshot posted by MOISIRAN on April 30, 2026 (left) and Brave_2025's Telegram profile (right) (Source: Telegram[10])*

Brave Israel Likely Prototype For Recruitment

Insikt Group assesses with high confidence that another persona historically involved in soliciting physical threat activities in Israel, "Brave Israel," is likely also part of the broader MOIS-linked cluster. After directly soliciting Israeli citizens to commit acts of vandalism in December 2024, Brave Israel operators shuttered the persona's main Telegram channel, sporadically solicited further activities in 2025, and pivoted to promoting Handala Hack Team, VIPEmployment, and MOISIRAN in 2026.

***Figure 15:** Brave Israel's Telegram profile picture (Source: Telegram[11])*

In December 2024, Insikt Group identified an inauthentic persona named "Brave Israel" operating a Telegram channel (*t[.]me/brave_il*) attempting to solicit individuals in Israel to conduct physical threat activities for financial rewards, including posting anti-government messages, graffiti, and burning cars. On several occasions, the channel's operators, using the Telegram account @Braveil, directed users to

[10] *t[.]me/MOISIran/34; archive[.]is/CLKQA*
[11] *t[.]me/brave_il*

the Telegram account @Brave_2025, also named "Morya Applee." In May 2024, the account @Braveil made several Telegram posts in Persian on cryptocurrency-related channels.

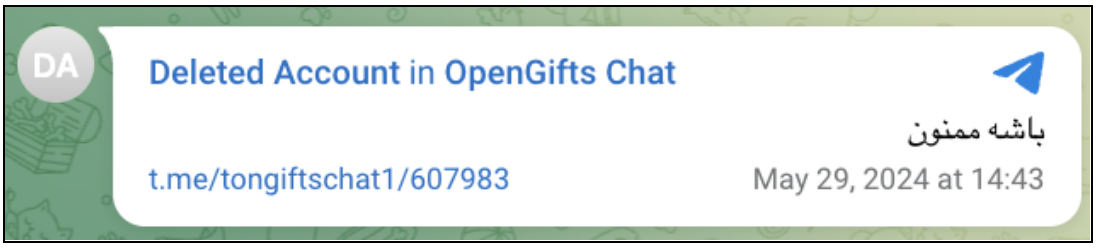


***Figure 16**: Telegram message by the now-deleted "Braveil" Telegram account (Source: Telegram[12])*

In December 2024, Brave Israel's Telegram channel offered $100 for sending an image of holding a piece of paper with text on it, $40 for "one graffiti," and $1,000 to burn a car, which is described as "a unique and exciting experience."[13] [14] [15] This pattern of low-level physical threat activity reflects techniques reportedly used by MOIS to recruit Israelis, described by a Shin Bet official as using a "spray-and-pray approach, which seeks to develop a handful of high-quality recruits by making low-stakes investments in many others."

***Figures 17, 18, and 19:** Screenshots of posts on the Telegram account Brave Israel providing examples of actions to receive a monetary reward (Source: t[.]me/brave_il)*

Based on open-source intelligence and geolocation techniques, Insikt Group assesses that some of the photos posted on *t[.]me/brave_il* were likely taken in Tel Aviv during the afternoon hours of December 2024. Three of the photos posted on December 12, 2024, were likely taken by an individual located in three different locations along Katzenelson Street in Tel Aviv (Katzenelson St 64, 115, and 158).[16]

[12] *t[.]me/tongiftschat1/607983*
[13] *t[.]me/brave_il/10*
[14] *t[.]me/brave_il/23*
[15] *t[.]me/brave_il/27*
[16] *t[.]me/brave_il/10*

Brave Israel's Telegram channel (*t[.]me/brave_il*) stopped operating after December 22, 2024. However, the Telegram account @Brave_2025 remained active, for example, posting a message on October 7, 2025, stating "I'm looking for a driver to deliver packages for me." On February 17, 2026, the account posted, "Looking for a job with high and fast income? Payment in dollars after each task. Suitable for brave and discreet people. Details in private."[17] The account began promoting VIPEmploymentBot on March 14, 2026, the Intel Voice's Telegram channel on March 16, 2026, the #Handala hashtag on April 22, 2026, and MOISIRAN content on April 22, 2026.

Mitigations

Despite its expansion to other threat vectors, the largest risk to most public and private sector organizations from personas in Iran's Handala brand very likely remains Handala Hack Team hack-and-leak and wiper attacks. Handala's access to breached personal information or company data can very likely enhance the impact of physical and influence operations by enabling pre-attack intelligence-gathering, surveillance, and coordinated promotion of Handala's capabilities in influence operations. To mitigate the risk of Handala hack-and-leak operations, Insikt Group recommends organizations:

- Prioritize vulnerability and patch management to counter exploitation of zero-days and supply-chain vulnerabilities; implement virtual patching and continuous monitoring for active exploits tied to organizations' tech stacks
- Harden identity and access management by enforcing phishing-resistant MFA, limiting partner network access, and monitoring credential use anomalies, thus mitigating credential abuse and spearphishing-driven initial access
- Enhance email and endpoint defenses through sandboxing and content disarmament for risky attachments, and leverage EDR tools to detect persistence techniques such as DLL sideloading, PowerShell abuse, and obfuscated binaries
- Segment and monitor critical R&D and manufacturing networks to prevent lateral movement and data exfiltration; apply strict outbound traffic controls, inspect encrypted C2 traffic (for example, via Azure or Google services), and deploy data loss prevention (DLP) to detect unauthorized transmissions of sensitive information
- Prepare for wiper, ransomware, and hacktivist activity by maintaining regular, offline backups, hardening exposed web infrastructure, and validating DDoS mitigation capacity
- Establish rapid-response workflows to verify or dismiss false hacktivist breach claims

Following the beginning of the Iran War, the majority of external physical attacks claimed by Handala and other Iran-nexus operational personas have involved sabotage, arson, and defacement targeting facilities or property. Attacks on facilities have frequently occurred during non-business hours and involve paid recruits; both of these factors very likely indicate that they were not intended to cause human casualties. Insikt Group expects Handala-claimed physical threat activities will likely continue to

[17] *t[.]me/httestimonies*

follow a similar model, given the personas' focus on financially recruiting operatives. While these attacks are very difficult to prevent outright, we recommend the following mitigations to limit their impact:

- Integrate this report and its assessments of Iran-nexus physical threat actors' TTPs into structured tabletop exercises for physical security teams
- Review and, where necessary, implement governmental guidelines for physical protection of business facilities, particularly with regard to electronic surveillance, secure lighting, and security personnel
- Conduct vulnerability assessments to enable effective contingency and resiliency planning in the event of an incident of sabotage, arson, or defacement, with particular focus on successful incidents disrupting communications, transportation, and energy infrastructure
- Limit voluntary publication of information about the functions, layout, and location of critical infrastructure assets at facilities, or security measures at a facility, beyond the levels necessary to comply with legal or regulatory requirements

Outlook

Iran's consolidation of external cyber, physical, espionage, and influence operations under the Handala brand likely amplifies the risk and impact of each of these threats. The cyber threat actor group's international profile has almost certainly increased since the start of the Iran War, largely due to high-profile claims by Handala Hack Team to have breached the personal email accounts of senior US and Israeli officials. For MOIS, tying physical threat and influence personas to the Handala brand likely further magnifies the effect of multidomain external operations. HPRF, VIPEmployment, MOISIRAN, and Brave Israel's operations have very likely benefited from amplification by Handala Hack Team through additional online reach and engagement. This, in turn, very likely increases their access to potential recruits for espionage and sabotage operations, amplifies their ability to spread fear, uncertainty, and doubt (FUD) about their capabilities, and increases their own online profiles. Meanwhile, Handala Hack Team likely benefits from perceptions that it operates across multiple domains, has dedicated physical threat actor teams, and is responsible for threats to the US and Israel beyond hack-and-leak operations.

Operators within MOIS are almost certainly leveraging relationships between different threat actor clusters within the Handala umbrella to support multidomain external operations involving cyber, physical, and influence operations components. Layering capabilities to support full-spectrum hybrid and irregular operations increases potential threat vectors. For instance, Handala Hack Team could breach the personal accounts of a senior official and provide Handala recruits and proxies with information obtained through the breach that could support physical attacks or surveillance. Combining various threat types into a single operation would likely increase its overall impact, particularly if it targets a specific individual or facility.

MOIS and other Iranian military and intelligence entities responsible for external operations will almost certainly continue to target US and Israeli assets with the types of operations described in this report — regardless of a ceasefire, formal cessation of hostilities, or agreement to end the Iran War. MOIS-linked

entities, including various Void Manticore personas, VIPEmployment, and Brave Israel, all engaged in influence or physical threat activities targeting the US and Israel prior to the start of the war, alongside numerous efforts by Iran state threat actors (including the IRGC) to solicit physical attacks or assassinations of senior US and Israeli personnel during the past decade. Iran will almost certainly judge these operations as taking place below the formal threshold of armed conflict; they are unlikely to view any agreement with the US or Israel as a barrier to this type of activity.

Appendix A: Indicators of Compromise (IoCs)

Handala Hack Team
handala-hack[.]ps
handala-hack[.]tw
handala-redwanted[.]ps
handala-alert[.]ps
handala[.]red

t[.]me/CYBER_HANDALA
t[.]me/HANDALA_INTEL
t[.]me/HANDALA_BREACH

Homeland Justice
justicehomeland[.]org
justicehomeland[.]info
justicehomeland[.]ru

t[.]me/justice_homeland
t[.]me/JusticeHomeland1

Street Vendor
t[.]me/shitesirruges

Handala Popular Resistance Front
t[.]me/HANDALA_PARTISAN

VIPEmployment
t[.]me/VIPEmployment_bot
t[.]me/Ir_intel_voice
t[.]me/Ir_intel_voice_ar
t[.]me/ir_intel_voice_ar_dis
t[.]me/@iranvipemployment_bot
t[.]me/@VIPEmploymentBot
t[.]me/@VIPEmployment01Bot
t[.]me/@VIPEmployment02Bot

tiktok[.]com/@vipemployment

MOISIRAN
t[.]me/moisiran
t[.]me/@vipconnect_iran

Brave Israel
t[.]me/brave_il

```
t[.]me/@Braveil
t[.]me/@Brave_2025
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com