I Spy With My Little Eye: Uncovering an Iranian Counterintelligence Operation

Mandiant ⋮⋮ 8/28/2024

Written by: Ofir Rozmann, Asli Koksal, Sarah Bock

Today Mandiant is releasing details of a suspected Iran-nexus counterintelligence operation aimed at collecting data on Iranians and domestic threats who may be collaborating with intelligence and security agencies abroad, particularly in Israel.

The data collected by this campaign may support the Iranian intelligence apparatus in pinpointing individuals who are interested in collaborating with Iran's perceived adversarial countries. The collected data may be leveraged to uncover human intelligence (HUMINT) operations conducted against Iran and to persecute any Iranians suspected to be involved in these operations. These may include Iranian dissidents, activists, human rights advocates, and Farsi speakers living in and outside Iran.

Mandiant assesses with high confidence this campaign was operated on behalf of Iran's regime, based on its tactics, techniques, and procedures (TTPs), themes, and targeting. In addition, we observed a weak overlap between this campaign and APT42, an Iran-nexus threat actor suspected to operate on behalf of Iran's IRGC Intelligence Organization (IRGC-IO). This campaign's activities are in line with Iran's IRGC and APT42's history of conducting surveillance operations against domestic threats and individuals of interest to the Iranian government. Despite the possible APT42 connection, Mandiant observed no relations between this activity and any U.S. elections-related targeting as previously reported by Google's Threat Analysis Group.

The activity used multiple social media accounts to disseminate a network of over 35 fake recruiting websites containing extensive Farsi decoy content, including job offers and Israel-related lures, such as images of Israeli national symbols, hi-tech offices, and major city landmarks. Upon entry, the targeted users are required to enter their personal details as well as their professional and academic experience, which are subsequently sent to the attackers.

The suspected counterintelligence operations started as early as 2017 and lasted at least until March 2024. In the past, similar campaigns were deployed in Arabic, targeting individuals affiliated with Syria and Hezbollah intelligence and security agencies. This may indicate Iran's counterintelligence activities extend beyond its own security and intelligence apparatus, possibly in support of its allies in Syria and Lebanon.

Mandiant worked to help ensure this activity was blocked and disrupted, the threat actor's accounts were terminated, and Google Chrome users and the users of other browsers were protected.

Attack Lifecycle

This activity leverages a network of fake recruitment websites posing as Israel-based human resources firms that use similar imagery in attempts to socially engineer Farsi-speaking individuals into providing personal details. The websites were disseminated online including through fake social media accounts, and used similar templates. The attack lifecycle is depicted in Figure 1.

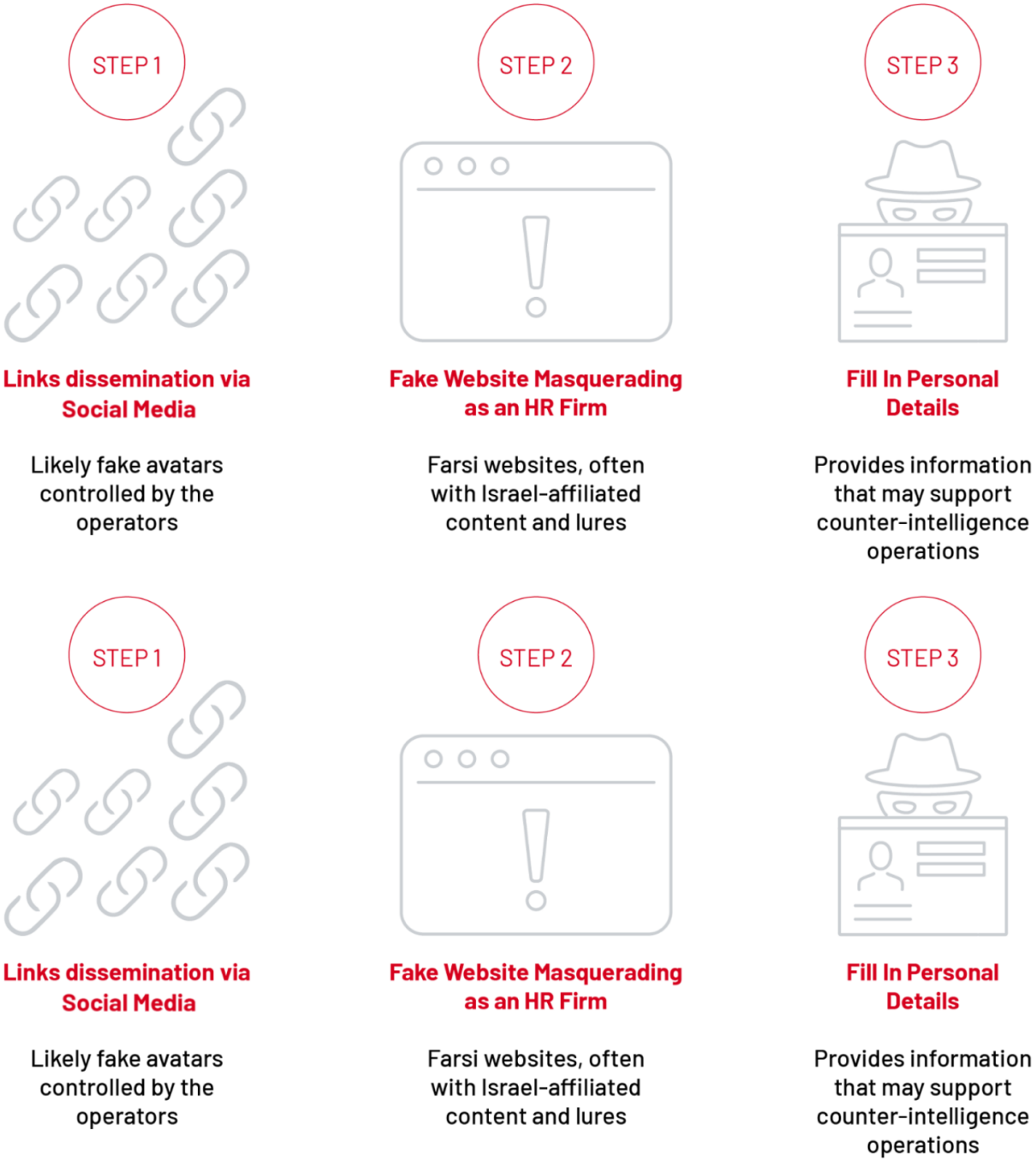

Figure 1: Attack lifecycle

The activity consists of several stages.

Step 1: Disseminate Links to Fake Recruitment Websites

Mandiant identified multiple fake social media accounts promoting the websites on various social platforms, such as X (formerly Twitter) and Virasty, commonly used in Iran.

The following X post contains a link to the malicious website, topwor4u[.]com, as well as the following description translated from Farsi:

“In the past year, we were able to attract hundreds of information and cyber professionals and achieve unique successes at the global level.

If you have information and cyber work experience, join us”.

Figure 2: Posts by @MiladAzadihr, a Twitter profile promoting the fake recruitment website topwor4u[.]com

Figure 3: Post by @A_Soleimani_Far, a Virasty (Iranian social network) profile promoting the fake recruitment website joinoptimahr[.]com

Step 2: Fake Job Offer Websites Presenting Israel-Related Decoy Content

Upon entering the website, the user is presented with the alleged purpose of the fake human resources firms: “[to] recruit employees and officers of Iran’s intelligence and security organizations.”

- The fake recruitment websites share templates and content, posing as HR firms, like “Optima HR” or “Kandovan HR.”
- The websites contain an elaborate description written in Farsi, presenting the alleged human resources firm as “active in the fields of international information and security/cyber consulting and research worldwide”.
- The websites contain a Farsi description of the “Terms of Cooperation” with the fake HR firm:

“Having relevant documented experience and resume in the field of information and cyber in related institutions and organizations (Mandatory).

Protecting your privacy is our priority.
Excellent salary for the chosen ones.

Our center invites you to contact us to submit a job offer and receive special and unique projects!!

Join us to help each other impact the world.
Our duty is to protect your privacy.”

- Mandiant observed both desktop and mobile versions of the websites beparas[.]com displaying similar contents and lures affiliated with Israel, including Israel’s flag and major city landmarks.

Figure 4: Mobile version of the fake website beparas[.]com, used between January and March 2024

Figure 5: Desktop and mobile versions of the website beparas[.]com used in February 2024; the left web page also includes a form and a Telegram contact link

- The websites contain Telegram contact links, using handles that contain “IL” (Israel) references, further enhancing the perceived Israel-affiliation of the campaign. For example:

hxxps://t[.]me/Phantom**IL**13

hxxps://t[.]me/getDm**IL**

- Several fake recruitment websites also contained a link to join a Telegram chat:

hxxps://t[.]me/joinchat/AAAAAFgDeSXaWr2r_AQImw

- Further inspection of the domain beparas[.]com indicated the WordPress user data for the website is publicly available and lists the username “miladix” as well as Gravatar URLs likely affiliated with this user (see the following screenshot). The value "b7e2f4a5bc67256189e6732fbce86520" in the Gravatar URLs is the Sha256 value of the user’s email, according to Gravatar documentation.

- The nickname "Miladix" might be related to “Milad Azadi,” the name of the X account used by the campaign and previously mentioned. In addition, "Milad" is a Persian name, further strengthening the campaign’s affiliation to Iran.

- Mandiant observed a domain miladix[.]com, affiliated with an Iranian software developer, although no links were found tying the campaign to miladix[.]com or its operator.

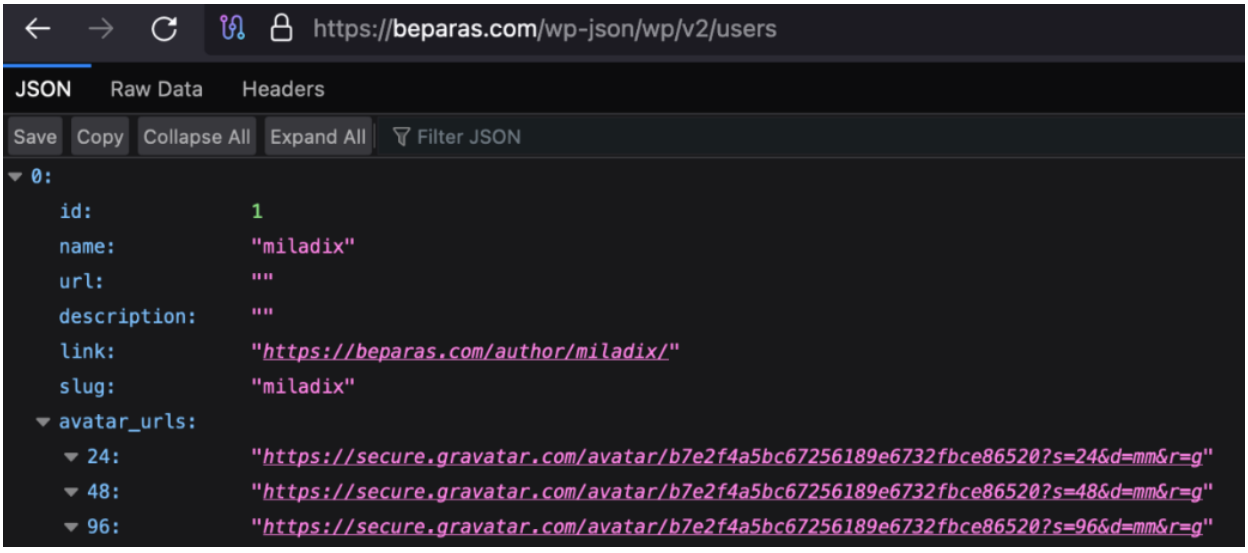

Figure 6: Screenshot of the WordPress user's URL of beparas[.]com

Step 3: Targeted User Fills Out Form, Personal and Professional details Sent to Attackers

The fake recruitment websites contain a form that includes the fields: name, birth date, email, home address, education, and professional experience.

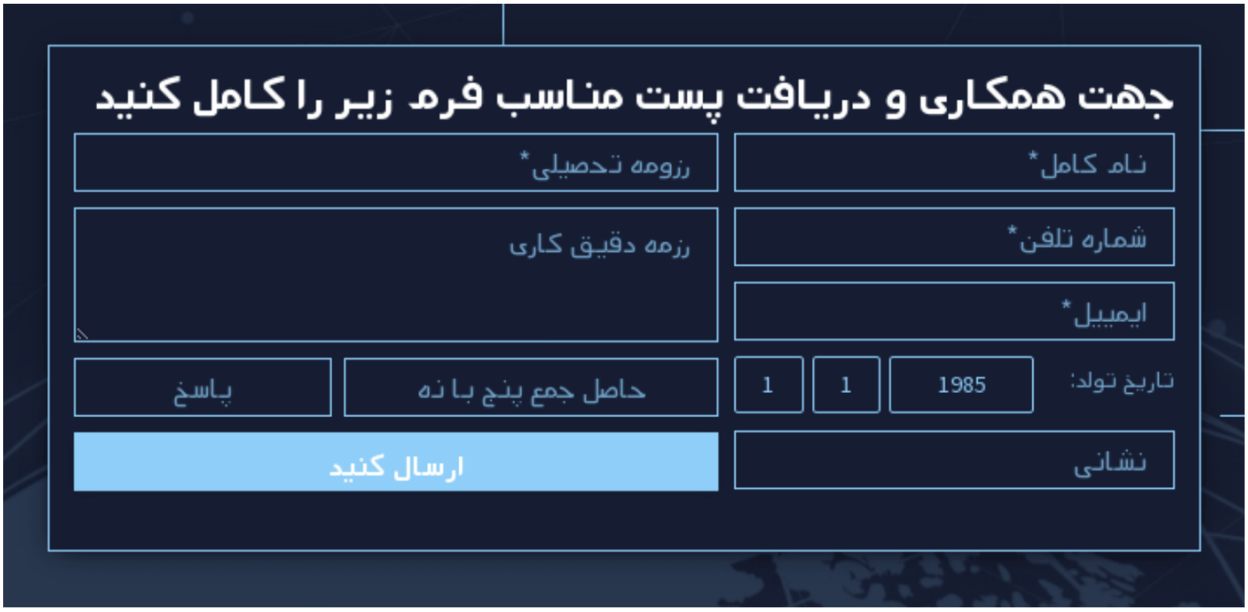

Figure 7: Fake personal details form

“Axis of Resistance”: Historic Operations Targeting Syria and Hezbollah

Close inspection of the fake “Optima HR” websites revealed a previous network of fake recruitment websites that targeted Farsi speakers as well as Arabic speakers affiliated with Syria and Lebanon (Hezbollah) masquerading as a different HR firm named “VIP Human Solutions.”

The “VIP Human Solutions” sites used very similar imagery and themes, purporting to recruit for security- and intelligence-related jobs using Israel-affiliated decoy content, as can be seen in the Figure 8.

Figure 8: Logos of VIP Human Solutions (2020–2023, left) and Optima HR (2022–2024, right)

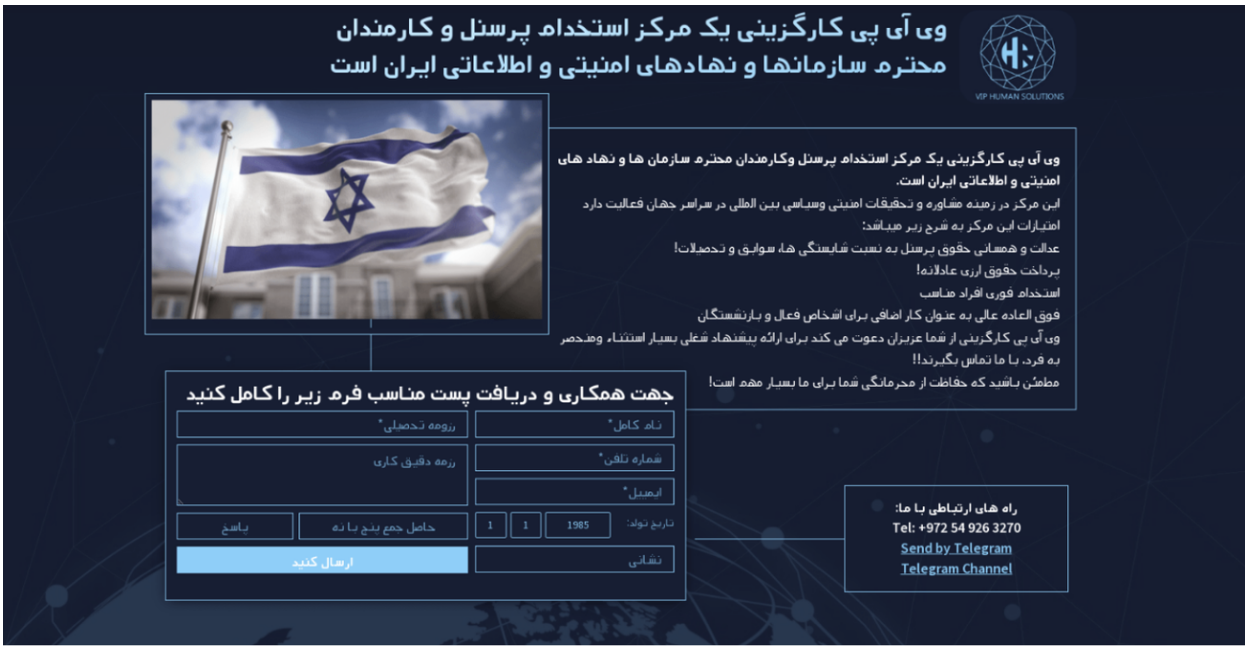

Figure 9: dreamy-jobs[.]com, a fake “VIP Human Solutions” website used in 2022

The “VIP Human Solutions” website’s contents, template, and personal details form are almost identical to the “Optima HR” website. The headline translates to:

“VIP job selection is a recruitment center for respected personnel and employees of Iran's security and intelligence organizations and institutions.”

Mandiant observed significant overlaps between the historic “VIP Human Solutions” campaign and the ongoing “Optima HR” campaign, and considers both to be deployed by the same threat actor. The activity was mentioned publicly in the past and was suspected to be related to the Israeli Mossad.

Figure 10: A Tweet from January 2021 mentioning “VIP Human Solutions”

- Mandiant observed the aforementioned Telegram group chat active, which has been active since at least 2021 and used by the two clusters:

hxxps://t[.]me/joinchat/AAAAAFgDeSXaWr2r_AQImw

- The same link was embedded in multiple “VIP Human Solutions” websites, occasionally along with Israel (+972) phone numbers and additional Telegram accounts:

hxxps://t[.]me/DreamyJobs_com
hxxps://t[.]me/wazayif_IL
“wazayif” is the English transcription of the word “jobs” in Arabic (وظايف)

The “VIP Human Solutions” recruitment websites were likely in use from at least 2018 to at least 2023. In addition to Farsi websites, the cluster used Arabic websites with similar templates.

Translation of the Arabic website’s title:

“VIP Recruitment, a center for recruiting respected military personnel into the army, security services and intelligence from Syria and Hezbollah, Lebanon.”

Figure 11: wazayif-halima[.]com, an Arabic-language “VIP Human Solutions” website, used in 2021–2022 to target Syria and Hezbollah's intelligence personnel

Mandiant also observed another version of the same website in 2023, which includes the “Loren Ipsum” dummy text in Arabic, possibly indicating that the updated version of the website was not operational yet. The template includes the Syrian flag and map, an Israeli phone number (+972), and a Telegram contact link: hxxps://t[.]me/DreamyJobs_com.

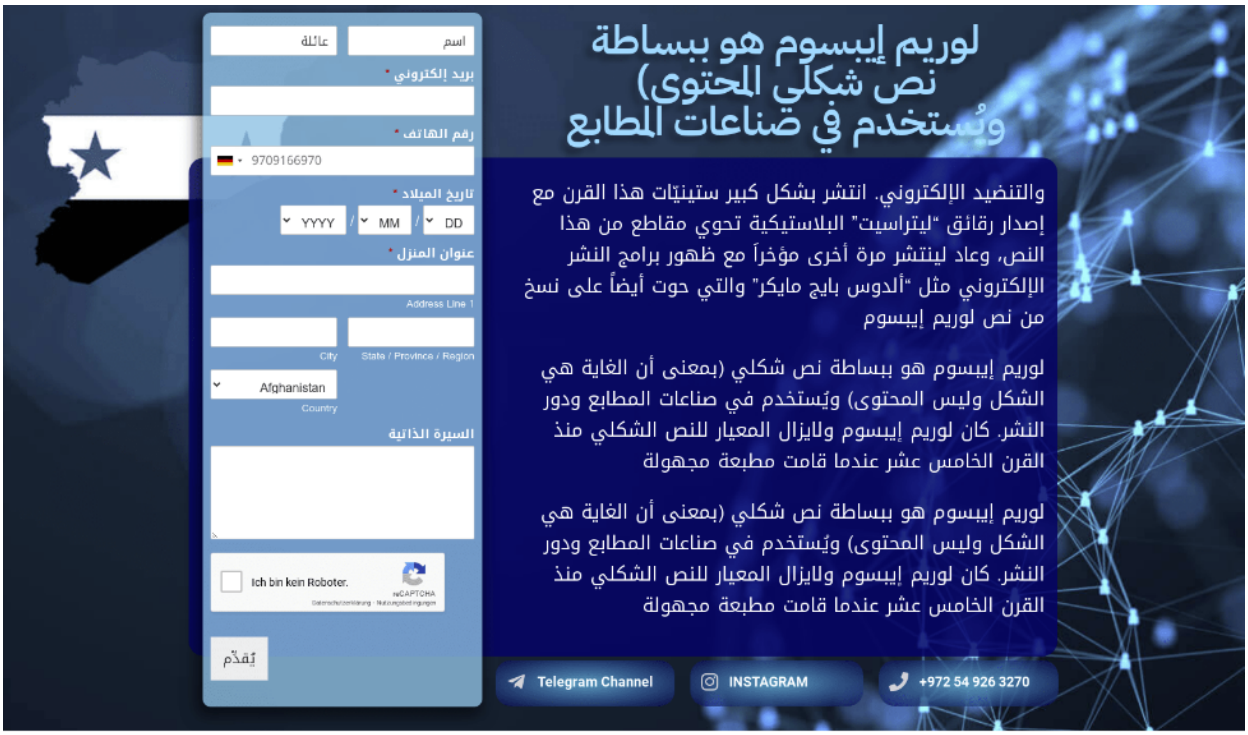

Figure 12: An updated version of wazayif-halima[.]com observed in July 2023

While the “VIP Human Solutions” domains were registered beginning in 2020, Mandiant observed further historic evidence suggesting that the campaign has been active since at least 2018.

Specifically, a YouTube channel named “VIP Human Solutions” was created by “Alireza Ebrahimpoor” in November 2018. The channel contains a single video by “VIP Jobs Global,” with a Farsi description very similar to the fake recruitment websites’, presented as a “recruitment center for retirees and employees of Iran’s security and intelligence organizations and institutions”. The threat actor-controlled YouTube channel is no longer available.

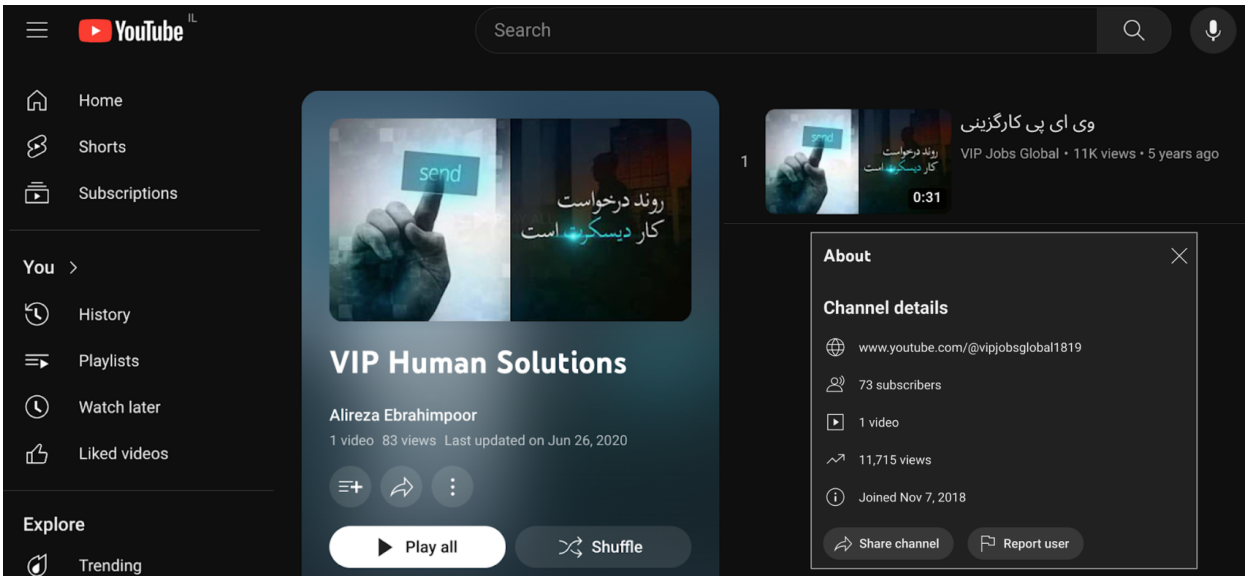

Figure 13: “VIP Human Solutions” YouTube channel: hxxps://www[.]youtube[.]com/@vipjobsglobal1819

The video has very similar content and theme as the fake recruitment websites, including the use of the unique logo of “VIP Human Solutions.”

Figure 14: Screenshot of the “VIP Human Solutions” video

The video also contains the following contact details:

- Email address: sendcv@vipjobsglobal[.]com. The domain vipjobsglobal[.]com was registered in March 2018.
- Facebook page: hxxps://facebook[.]com/358690841262928, which started operating in December 2017 and is no longer active.

The following table compares the historic activity with the new activity described in the previous section:

	“VIP Human Solutions”	**“Optima HR”**
Years Active	2017-2022	2022-2024
Languages	Farsi Arabic	Farsi
Targeted Regions	Iran, Syria and Hezbollah	Iran
Example Domains (full list in the IOCs section)	bilal1com[.]com (Farsi) jomehjob[.]com (Farsi) dreamy-job[.]com (Farsi) damavand-hr[.]me (Arabic)	optima-hr[.]com joinoptimahr[.]com opthrltd[.]me beparas[.]com

	wazayif-halima[.]org (Arabic)	darakeh[.]me topwor4u[.]com
Contact Details	hxxps://t[.]me/DreamyJobs_com hxxps://t[.]me/wazayif_IL hxxps://t[.]me/joinchat/AAAAAFgDeSXaWr2r_AQImw +972 (Israel) phone numbers	hxxps//t[.]me/PhantomIL13 hxxps://t[.]me/getDmIL hxxps://t[.]me/joinchat/AAAAAFgDeSXaWr2r_AQImw

Outlook and Implications

Mandiant estimates this activity supports Iranian counterintelligence efforts to identify individuals affiliated (or interested in working) with intelligence and security agencies.

Specifically, the activities described in this blog post are of concern to Iranian individuals who are suspected to be collaborating with countries Iran might perceive as adversaries. These may include Iranian dissidents, activists, human rights advocates, and Farsi speakers living in and outside Iran.

The campaign casts a wide net by operating across multiple social media platforms to disseminate its network of fake HR websites in an attempt to expose Farsi-speaking individuals who may be working with intelligence and security agencies and are thus perceived as a threat to Iran's regime. The collected data, such as addresses, contact details, as well as professional and academic experience, might be leveraged in future operations against the targeted individuals.

Additional Protection Information for Google Cloud Customers

For Google Chronicle Enterprise+ customers, Chronicle rules have been released to the Emerging Threats rule pack, and IOCs listed in this blog post are available for prioritization with Applied Threat Intelligence.

Indicators of Compromise (IOCs)

A Google Threat Intelligence Collection featuring IOCs related to the activity described in this post is now available for registered users.

Cluster 1: "Optima HR", "Kandovan HR" and "Paras IL", active 2022-2024			
beparas[.]com	parasil[.]me	darakeh[.]me	kandovani[.]org
topwor4u[.]com	opthrltd[.]me	joinoptimahr[.]com	optimax-hr[.]com
optimac-hr[.]com	optima-hr[.]com	titanium-hr[.]com	
Cluster 2: "VIP Human Solutions", active 2017-2023			
azadijobs[.]me	bilal1com[.]com	damavand-hr[.]me	damkahill[.]com
dream-jobs[.]org	dream-jobs[.]vip	dreamy-job[.]com	dreamy-jobs[.]com

dreamycareer[.]com	golanjobs[.]me	hat-cast[.]com	irnjobs[.]me
jomehjob[.]com	radabala[.]com	rostam-hr[.]vip	salamjobs[.]me
shirazicom[.]com	syrtime[.]me	topiranjobs[.]me	trnjobs[.]me
vipjobsglobal[.]com	wazayif-halima[.]com	wazayif-halima[.]org	wehatcast[.]com
youna101[.]me	younamesh[.]com		

Posted in

- Threat Intelligence