Iran Cyber Threat Overview

blog.sekoia.io/iran-cyber-threat-overview/

5 June 2023

Maxime A. and TDR (Threat Detection & Research) June 5 2023

15 minutes reading

This blogpost aims at understanding and contextualising cyber malicious activities associated with Iran-nexus intrusions sets over the **2022-2023 period**. It does not establish an exhaustive list of campaigns or reported intrusion sets, but rather offer a strategic analysis pertaining to the Iranian cyber threat. Information cut-off date is 5 May 2023.

CONTEXT

The Islamic Republic of Iran does not publicly communicate on their cyber offensive doctrine. However, the observed use of their capabilities shows pragmatic cyber operations pursuing three strategic objectives that align with **Iran's geopolitical objectives**.

First objective relates to **Iran's domestic stability**. Cyber operations are used to maintain and support the regime by surveilling political dissidents, journalists and activists seen as potential vectors of foreign influence. Second objective pertains to **national territory protection**, based on a perceived military and cyber threat level originating from enemies (USA, Israel, Saudi Arabia), leveraging strategic cyber espionage operations to collect intelligence about adversarial intentions. Third objective applies to **foreign policy**, Iran operates cyber operations as a tool to promote and secure its regional influence.

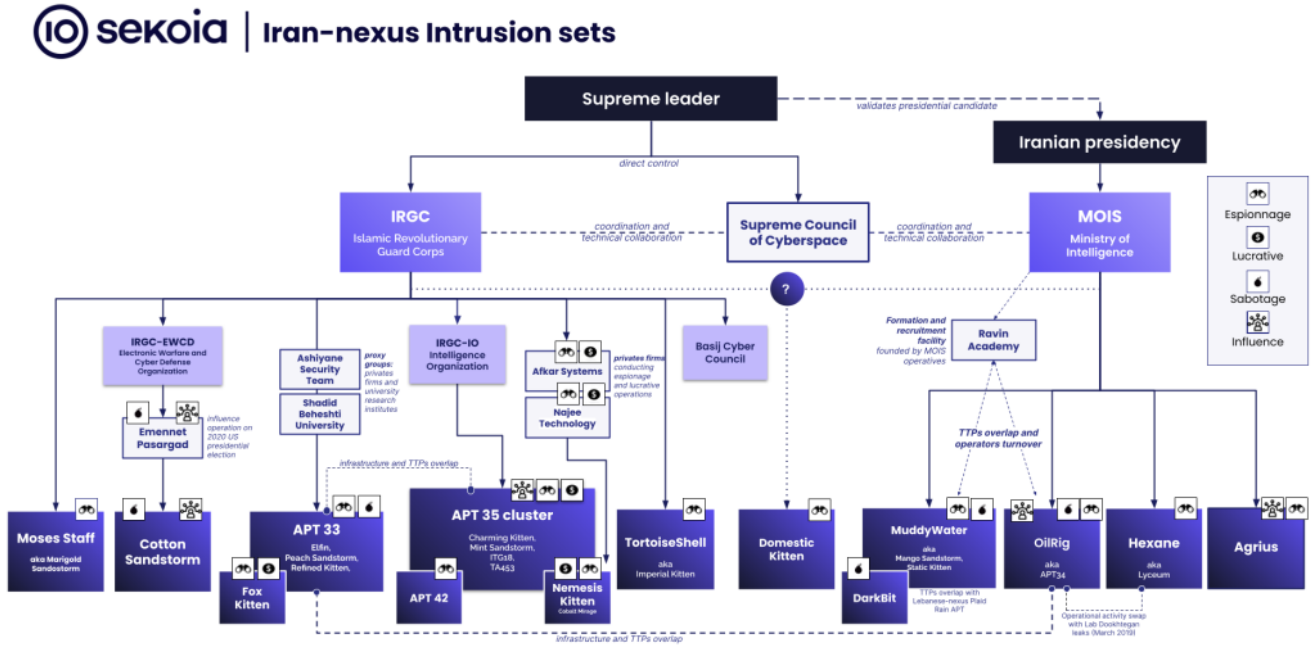
Iran was, and still **is**, **a target** of multiple reported cyber operations. This aspect is important for a better understanding of the Iranian cyber strategy , as Iran often conducts **retaliation operations**. The **origin** of Iranian use of offensive cyber operations is related to two main events, the **2009 Green Movement** where civilians protested the reelection of President Ahmadinedjad; and **Stuxnet** detection in 2010, a malware allegedly developed by the USA

and Israeli services to damage nuclear centrifuge machines. Iranian leaders likely perceived the necessity for the surveillance of the Internet, specifically social media, to maintain the stability of the regime, and realised the potential of offensive cyber operations, both as a target and as an instigator.

Since 2022 and throughout 2023, the Islamic Republic faces heightened geopolitical challenges, potentially influencing its strategy for cyber operations. The election of Ebrahim Raisi as Iranian president in August 2021 brought back to power radical conservatives that impacted the negotiations to recover the Joint Comprehensive Plan of Action (JCPOA) **nuclear deal**, increasing political confrontation between Teheran and western countries, also fueled by the supply of Iranian weapons to Russia in the context of the Russo-Ukrainian conflict. Iran suffers from **domestic instability**, both economically – 2022 inflation rate was near to 50% – and politically with the longstanding and widespread Mahsa Amini civilian protests from September 2022 to February 2023. Lastly, in April 2023, **Tehran and Riyad** announced they will **resume their diplomatic relations** that were cut off from 2016, an initiative facilitated by China.

IRANIAN CYBER OFFENSIVE ORGANISATION

Iran presents a cyber offensive capability mostly operated by the two main intelligence and security services, the **Islamic Revolutionary Guard Corps (IRCG)** and the **Ministry of Intelligence (MOIS)**.



Islamic Revolutionary Guard Corps

The IRCG is a branch of the Iranian Armed Forces, founded after the 1979 Iranian Revolution as an **ideologically-driven** militia **responsible for the protection of the Islamic Republic political system**. IRGC key positions are appointed by the Supreme leader of the Islamic Republic presently Ali Khamenei, guaranteeing a direct reporting to him, thus bypassing the President's office. IRGC can be seen as a **military elite corps** with **specific missions**, including ground, aerospace, naval and cyberspace forces. IRGC includes the Basij militia, a paramilitary volunteer militia, and the Qods special force. Both substructures were reported leveraging cyber offensive operations.

Few open-source information can be found on **IRGC internal cyber organisation**. Sekoia.io TDR analysts established a **partial organisational diagram from leaked data**, available at the end of the post.

Active intrusion sets associated to IRGC – **APT35**, **APT42**, **Nemesis Kitten** and **Cotton Sandstorm** (ex-NEPTUNIUM) – mainly focus on targets linked to foreign government, military, energy, maritime transportation and research entities (think tanks, NGOs, academics) working on Iran and Middle-East subject matters. They conduct cyber operations using social media spear phishing techniques as initial vector and aiming at strategic objectives including espionage, sabotage, information operations and, to a lesser extent, lucrative.

Sekoia.io, along with some cybersecurity vendors, **consider APT35 as a cluster** assessed to be operated by **IRGC-Intelligence Organisation** (IRGC-IO) composed of multiple aliases or subgroups such as Charming Kitten, ITG18, TA453, Cobalt Mirage, **including APT42**, a newly exposed intrusion set focused on individuals working for NGOs and think tanks. Sekoia.io assess **Nemesis Kitten** is also part of APT35 cluster.

Ministry of Intelligence

The Ministry of Intelligence of the Islamic Republic of Iran (**MOIS in english**, or **VEVAK** for its farsi acronym), is the main foreign intelligence service. MOIS is the successor of SAVAK, the intelligence service from the previous Shah's regime. It is responsible for both **foreign operations** and **domestic surveillance**. Its missions **often overlap with IRGC** to which the relations are competitive.

MOIS is **responsible** for **signals intelligence** and collecting information from electronic communications. Contrary to IRGC, the Ministry of Intelligence reports to the President, not the Supreme Leader. If both structures aim at protecting the regime, MOIS is assessed to be **more technical** and **less ideology-driven than IRGC leaders**.

Active intrusion sets associated to MOIS – **MuddyWater**, **Oilrig** (aka APT34), **Hexane, Agrius** and the newly exposed **DarkBit (aka DEV-1084)** – mainly focus on sectors such as government, energy, telecommunications, maritime transportation. They carry offensive operations with espionage, sabotage and influence purposes.

MuddyWater, Oilrig and Hexane are **likely directly operated by MOIS operatives** as some techniques, tactiques and procedures (TTPs) overlap, or operational tempo coordination were observed by Sekoia.io analysts. It is not clear whether **DarkBit** (aka DEV-1084) is a subgroup of MuddyWater, or a newly observed intrusion set conducting post-intrusion and destructive operations.

Contractors, private firms and universities associated to Iran cyber operations

Iran cyber organisations were reported contracting private companies and institutes linked to universities to conduct domestic and foreign cyber offensive operations. This contracting system is used for both highly technical attacks and for domestic social media influence

operations.

Nemesis Kitten, an intrusion set associated with the APT35 cluster, is operated by two private companies working together, **Afkar System** and **Najee Technologies**, assessed by the US Treasury to be contracted by IRGC-IO. Both companies were observed conducting strategic espionage activities as well as **lucrative ransomware campaigns**. It is not clear whether the lucrative activities are part of an IRGC-IO mandate, or are leveraged by the companies for their own profit.

Another example of private contractors is **Emennet Pasargad**, a private company associated with Cotton Sandstrom (ex-NEPTUNIUM) intrusion set and assessed to conduct espionage and **ideology-driven influence operations** on behalf of the IRGC-Electronic Warfare and Cyber Defense Organisation.

The Ministry of Intelligence also uses contractors, notably **Ravin Academy**, a company co-founded in 2019 by MOIS' members Seyed Mojtaba Mostafavi and Farzin Karimi, both MuddyWater and Oilrig ex-managers, to **train and recruit offensive operators for the MOIS**.

Sekoia.io is aware of former contractors such as Mabna Institute, Rana Institute, ITSecTeam, Ashiyane Security Team or Shadid Beheshti University, all involved in the past with Iran cyber operations. Intrusion sets associated with those contractors were **not observed as active** in the 2022-2023 period.

OBJECTIVES OF IRAN CYBER OPERATIONS

Strategic espionage and domestic cyber surveillance

Iran conducts cyber operations aiming at **intelligence collection for strategic purposes**, essentially targeting neighbouring states, in particular Iran's geopolitical rivals such as **Israel**, **Saudi Arabia** and **arabic Gulf countries**, a continued focus observed in all operations since 2011. For instance, the intrusion set Oilrig was observed targeting the Jordan foreign Ministry in March 2022 using the group's Saitama backdoor, a malware detected in multiple Middle East entities in the same period. Due to the strategic nature of espionage operations, few details on the scope of the compromission or impacted interest resources are available in open source publications.

Domestic surveillance is also a **strong focus** for Iran-nexus intrusion sets. Among the ones Sekoia.io follows, at least four were observed carrying out domestic surveillance (APT35, APT42, Domestic Kitten and MuddyWater). In October 2022, ESET documented a newly discovered malware (FurrBall) used by **Domestic Kitten**, an intrusion set active since at least 2016 and conducting a longstanding mobile surveillance operation against Iranian citizens. It is worth noting that domestic surveillance shows a particular focus on mobile

espionage. Another illustrative example is the detection of TelegramGrabber malware used by APT35, detailed by PWC in August 2022, as all victims' mobile numbers contained the Iranian country code and Farsi was the main language seen in victim databases.

Destructive cyber operations

Iran is known to conduct destructive operations as the first documented Iran cyber attack, Shamoon 2012, leveraged a destructive wiper that had a strong impact on the Saudi company Saudi Aramco. The attack was later interpreted as a retaliation on a US ally for the Stuxnet operation.

In 2022-2023, Iran-nexus intrusion sets continue to conduct **destructive campaigns with an operational evolution** : the use of hacktivist fronts claiming responsibility and justifying the operation. In July 2022, a front named HomeLand Justice claimed credit for the **disruptive and destructive activity** that impacted the **Albanian government**. The operation was assessed to be conducted by intrusion sets, mainly **OilRig** and **Hexane**, operating on behalf of the Ministry of Intelligence.

The DarkBit personna is another example. In February 2023, MuddyWater conducted an operation targeting Technion Israel Institute of Technology based in Haifa, with a **false ransomware operation masquerading a destructive operation**, using a front named "DarkBit group". According to Microsoft, two intrusion sets conducted the operation. MuddyWater carried the initial intrusion and handed off access to the DarkBit intrusion set (aka DEV-1084) which conducted extensive reconnaissance, established persistence, and moved laterally to finally launch a destructive command.

It is worth noting that this is the first time a **distinct intrusion set is used for post-intrusion and destructive activity**. Sekoia.io TDR analysts assess the use of **fronts blurring for destructive operations** will likely pursue and increase, given the general increase of front use by Iran-nexus intrusion sets, notably to conduct information operations.

Iranian information operations

Information operations (info ops) led by Iranian actors **increased significantly** in 2022 and 2023, contributing to Iran's geopolitical objectives to promote and secure its regional influence.

Among the multiple intrusion sets leveraging info ops, Cotton Sandstorm (ex-NEPTUNIUM) is the most active. According to the US Treasury, Cotton Sandstorm is operated by **Emennet Pasargad,** an Iran-based **private company** operating on behalf of the IRGC-Electronic Warfare and Cyber Defense Organisation (IRGC-EWCD). The group was first indicted in 2020 for an information operation targeting Donald Trump's close staff in order to compromise his Twitter account and influence the 2020 US presidential election against his reelection.

In January 2023, Cotton Sandstorm conducted an info ops targeting French satirical newspaper **Charlie Hebdo**, perceived as insulting Islam, leading to an exfiltration of customers data. In February 2023, the same group impersonated Al-Toufan, a persona that claimed a defacement campaign targeting **Bahrain's news website**, likely to fuel Shia Islam majority protests against a Sunni government aligned with Saudi Arabia. Other reported info ops impacted Israel, inciting the Palestinian resistance or promoting counter-narrative against the normalisation of Arab-Israeli diplomacy. Each info ops conducted by Cotton Sandstorm was amplified by **fake social media accounts** relaying their narrative.

Sekoia.io assess Iran-nexus intrusion sets **Agrius, Oilrig** and **in particular Cotton Sandstorm**, will **continue** and **increase information operations** leveraging fronts, targeting Iran geopolitical adversary neighboring countries such as **Gulf Cooperation Council members** and **Israel**.

Iran-originating lucrative operations

Few intrusion sets were reported conducting lucrative operations, however both of them, Fox Kitten and Nemesis Kitten, are suspected to be operated by private firms contracted by IRGC.

As previously mentioned, Nemesis Kitten is operated by two private companies contracted by IRGC and Sekoia.io considers the group as part of the APT35 cluster. In May 2022, Nemesis Kitten was accused by the US CISA to conduct a **long term ransomware** and **crypto-mining campaign** exploiting the **Log4J 1-day vulnerability** impacting multiple US public entities. For Sekoia.io it remains unclear whether this lucrative activity was part of the alleged IRGC mandate or a tolerated initiative conducted by Afkar System and Najee Technology as a side activity.

GEOGRAPHICAL AND ECONOMIC VICTIMOLOGY

Most impacted sectors

Energy – The energy sector is an historic target for Iran. Over time, IRGC-associated APT33 leveraged the destructive malware Shamoon for multiple operations (2012, 2018, 2020), impacting Saudi Aramco, the most important economic asset for Saudi Arabia, one of Iran regional rivals. Energy is still a major target for Iran-nexus intrusion sets, yet few recent (2022-2023) open-source cases are available due to the strategic nature of impacted entities. In April 2023, Microsoft published about IRGC-associated APT35, described as an intrusion set capable of direct targeting of US critical infrastructure including energy companies and a major US utility and gas entity.

Telecommunications – Since the end of 2021, the telecommunications sector is increasingly impacted by Iran-nexus intrusion sets. Recently, in January 2023, Microsoft identified a MuddyWater spear phishing campaign aiming at employees of **Middle-East**

telecom operators, which concurs with Talos' findings of MuddyWater interests for an Armenian Internet service provider. Such focus was also shared by Hexane, which conducted an espionage campaign targeting telecom operators based in Saudi Arabia, Tunisia, Morocco and Israel early 2022. **Sekoia.io assess** this focus is possibly related to the MOIS SIGINT mandate, as this sector is mostly impacted by MOIS-associated intrusion sets.

Maritime-transportation – In 2022, the transportation sector and in particular maritime transportation were impacted by Iran cyber operations. Since at least July 2022, APT35 conducted an espionage operation targeting employees of an **Egypt-based shipping and marine services** companies. At the same time, UNC3890, an intrusion set Sekoia.io assess part of APT35 cluster, focused on Israel entities including maritime shipping companies. Earlier, in December 2021, Microsoft reported on Iran-nexus DEV-0343, an intrusion set notably targeting Persian Gulf ports of entry and global maritime transportation companies with business presence in the Middle East. **Sekoia.io assess** with high confidence the maritime-transportation sector is a primary target for IRGC-associated intrusion sets, as the Persian Gulf and the Hormuz strait are critical areas supposed to fall in the IRGC mandate.

Critical infrastructure – According to multiple US agencies assessment pertaining to cyber threats, Iran-nexus intrusion sets are able to impact US critical infrastructures. However, very few infrastructure targeting can be observed in open source, apart from an Iran-originated operation aiming to **disrupt and allegedly tamper with Israel's water supply** in June 2020.

Individuals linked to NGOs, think tanks and universities

Sekoia.io TDR analysts observe a trend in targeting individuals conducting research related to Middle-East and Iran affairs, whether they are academics, NGOs members or employees of western-funded think tanks. Among others, APT42, an intrusion set part of the APT35 cluster, focuses only on such targets, such as Human Rights Watch staff members and activists, or an American political commentator expert on sanctions and counter-terrorist financing policy. Of note, Sekoia.io observe **advanced social engineering** is **central for initial intrusion**, specifically when considering the social profiling, creation of fake profiles or progressive contacting.

Most impacted regions

As a continuation of previous observations pertaining to Iran cyber threats, **every Iran-nexus** intrusion set includes **Middle-East targeting,** and nearly all of them aim at targeting **Israel**. However, most open source publications pertaining to cyber operations targeting the Middle-East **do not specifically detail impacted countries**. This lack of granularity does not allow an exact representation of impacted states.

On a second position comes the **USA**, a country where reported operations originating from Iran increased over the 2022-2023 period. Some cybersecurity vendors' analysis, to which Sekoia.io concurs, assess IRGC-associated intrusion sets such as APT35 are now less bounded in their operations targeting the USA. **Other regions**, such as the European Union or the Balkans, are less but still impacted, as we observed with the disruptive and destructive activity that impacted the Albanian government. Of note, the **consequences of the operation on Albania show the impact Iran can have on moderately cyber protected countries**.

IRAN CYBER THREAT RECENT EVOLUTION

Iran-nexus intrusion sets seem to **increase their technical skills** and **operational reactivity to publicly disclosed vulnerabilities**. Some of them were also observed as reactive to public reporting, namely Oilrig when its tactics, techniques and procedures (TTPs) were partially leaked on a Telegram channel named Lab Dookhtegan in May 2020. An operational activity takeover from Oilrig to Hexane was perceptible, suggesting operators swap from two groups associated to MOIS. In 2023, APT35 showed a **rapid exploitation** of publicly disclosed vulnerabilities CVE-2022-47966 and CVE-2022-47986, exploiting them between one to five days after they became public. Before 2023, the group often required weeks to weaponize exploits for vulnerabilities like **Proxyshell** and **Log4Shell**, according to Microsoft.

Active collaboration between intrusion sets associated to the same structure was perceptible in 2022, as observed with the disruptive and destructive campaign on Albania involving participation of Hexane, Oilrig and at least 3 other less-known intrusion sets, all assessed to be operated by MOIS. Sekoia.io assess it is plausible that such cooperation is facilitated by initiatives like **Ravin Academy**, already mentioned in this report, which allow operators and TTPs exchange among MOIS-associated intrusion sets. Plaid Rain (ex-POLONIUM) is another exemple, the **Lebanon-based intrusion set** active since early 2022 is suspected of coordination with other actors affiliated with MOIS, based on TTPs and victimology overlap. If confirmed, a collaboration with a Lebanese group would be coherent with the links Iranian intelligence services share with Shia political groups such as Hezbollah, now including cyber intelligence.

CONCLUSION

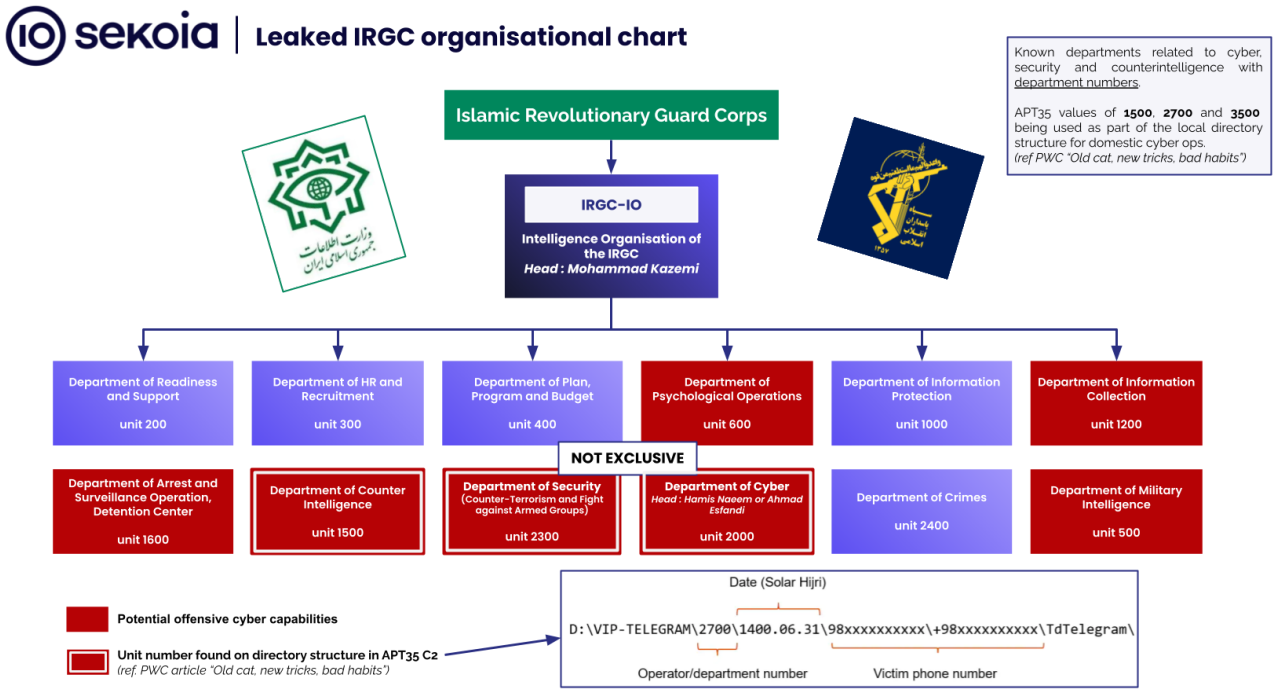
Sekoia.io assess **Iran cyber threat will likely continue to grow** in the next years as its technical and operational capabilities advance while the country is increasingly in a geopolitical confrontation with Israel, Western countries and allies due to a return of the ultraconservatives to power.

The geopolitical confrontation is **likely to carry on against** Gulf Cooperation Council members as well, including **Saudi Arabia** despite the normalisation of diplomatic relations between Riyad and Tehran. Indeed, before 2016, diplomatic relations did not prevent Iran and Saudi Arabia to indirectly confront in the Yemeni civil war nor contain Iran to conduct major cyber destructive operations toward Saudi Aramco.

Iran-nexus intrusion sets will **highly likely continue** to **use cyber personna fronts**, either to cover destructive activity and / or to amplify information operations aimed at contributing to securing Iran regional influence and to legitimise the Islamic Republic's narrative against its geopolitical adversaries.

The targeting of **Middle-East telecom operators** and **maritime transportation** sectors by respectively MOIS and IRGC is likely to continue, probably as part of a **pre-positioning strategy** in the event of an open conflict where Persian Gulf navigation and telecommunications would be critical for Iran.

Appendix – IRGC partial organisational diagram from leaked data



Thank you for reading this blogpost. **We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io**

Feel free to read other TDR analysis here :

Chat with our team!

Would you like to know more about our solutions?
Do you want to discover our XDR and CTI products?
Do you have a cybersecurity project in your organization?
Make an appointment and meet us!

Contact us

Comments are closed.