Threat Actor Activity Related to the Iran Conflict

By by Nozomi Networks Labs | July 8, 2025

In light of the most recent Iranian conflict, Nozomi Networks Labs has observed a 133% increase in cyberattacks coming from well-known Iranian threat actor groups during May and June. From what Nozomi Networks Labs researchers have observed so far, US companies appear to be the primary target as warned in a June 30th Fact Sheet published by CISA and last week's National Terrorism Advisory System Bulletin from the U.S. Department of Homeland Security.

Our researchers observed **MuddyWater, APT33, OilRig, CyberAv3ngers, FoxKitten** and **Homeland Justice** targeting Transportation and Manufacturing organizations. Industrial and critical infrastructure organizations in the U.S. and abroad are urged to be vigilant and review their security posture. Nozomi Networks customers can review their Nozomi Threat Intelligence for any signs of activity from these groups. If you subscribe to the Nozomi Networks Threat Intelligence feed (including a separate Mandiant TI Expansion Pack) you're covered, as signatures have been in place for some time.

Current Cyber Threat Trends

As part of our daily operations, Nozomi Networks Labs researchers constantly track various threat actors, including nation-state groups. We receive anonymized telemetry from participating customers which allows us to publicly share current trends related to the attacks associated with these actors.

During May and June, we observed 28 attacks related to Iranian threat actors. Compared to the previous 2-month period, where we saw only 12, this represents a 133% increase in their activity.

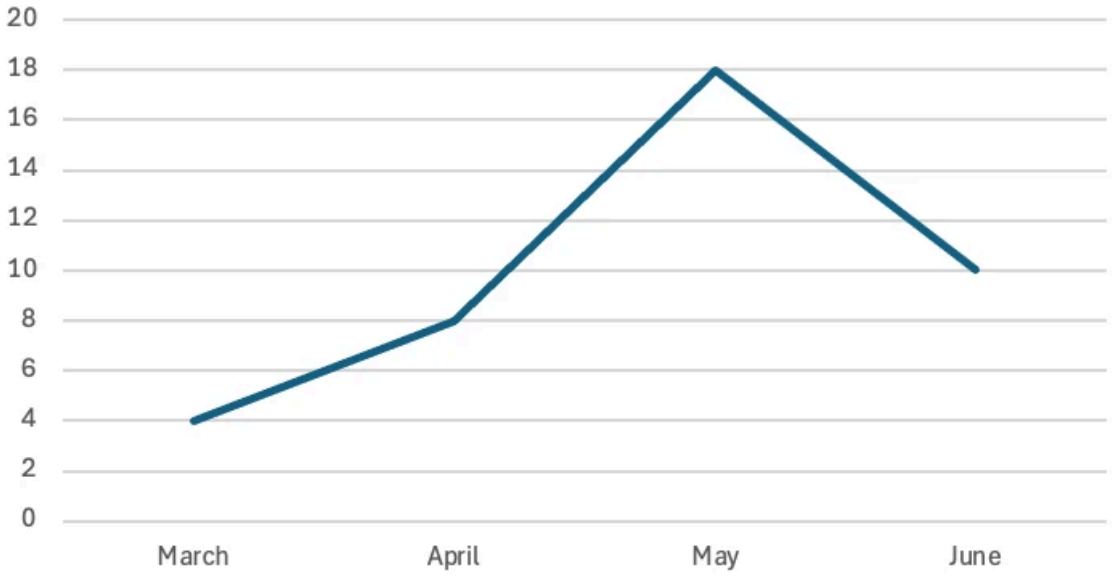

Figure 1. Nozomi Networks data shows a recent spike in attacks linked to Iranian actors in comparison to March and April 2025.

Unsurprisingly, the attacks targeted organizations in the US. The most active Iranian threat actor was MuddyWater, which we cover in more detail below. In the last two months, it attacked at least five different U.S. companies, mainly associated with Transportation and Manufacturing. It was followed by APT33, responsible for attacks against at least three different U.S. companies. Finally, we were able to see OilRig, CyberAv3ngers, Fox Kitten and Homeland Justice associated with attacks against at least two different US companies each, again mainly belonging to the Transportation and Manufacturing sectors.

An interesting fact, this time CyberAv3ngers decided to re-use an IP address associated with their previous attack utilizing infamous OT-focused OrpaCrab aka IOCONTROL malware that was discovered in December last year. Regardless of whether the OT, IoT or IT domains are going to be targeted, Nozomi Networks Labs will continue to closely monitor all these actors, making sure our customers are protected.

Global Threat Actor Activities

Below are images from the Nozomi Platform highlighting Iranian threat actor activity by country as reported in our Threat Intelligence services.

MuddyWater

MuddyWater (also known as SeedWorm) is a threat actor group originating from Iran. They have been active since 2017, targeting primarily countries in the Middle East, specifically Saudi Arabia, Iraq, and Turkey. Their main focus is on government entities, telecommunications, and the energy sectors.

Figure 1 - Nozomi Threat Intelligence is tracking MuddyWater targeting organizations in these countries.

APT33

APT33 (also known as Elfin) is a threat actor group believed to originate from Iran. They have been involved in cyber espionage activities targeting organizations in the aerospace, energy, and petrochemical sectors. APT33 was first observed in 2013 and has been active up to the present day, with a focus on stealing sensitive information to further Iranian national interests.

Figure 2. Nozomi Threat Intelligence is tracking APT33 targeting organizations in these countries.

OilRig

OilRig (also known as APT34, Helix Kitten) is a threat actor originating from Iran. They have been active since at least 2014, targeting primarily Middle Eastern countries such as Saudi Arabia, United Arab Emirates, and Qatar. Their focus is on espionage and collecting sensitive information from government, financial, energy, and telecommunications sectors. The group is known for using spear-phishing emails and custom malware tools to breach their targets' networks.

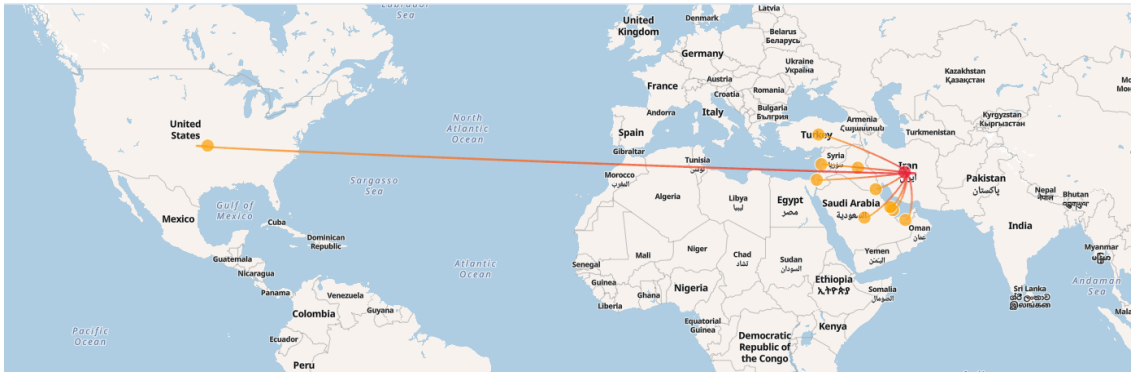

Figure 3. Nozomi Threat Intelligence is tracking OilRig targeting organizations in these countries.

CyberAv3ngers

CyberAv3ngers is an Iranian threat actor group known for its cyber-espionage and politically motivated operations, targeting critical infrastructure, government entities, and private organizations. The group is characterized by its sophisticated use of advanced persistent threat (APT) tactics, leveraging custom-built malware, spear-phishing campaigns, and zero-day vulnerabilities to achieve its objectives. CyberAv3ngers typically operates with a focus on Middle Eastern and Western nations, aligning its activities with Iranian geopolitical goals.

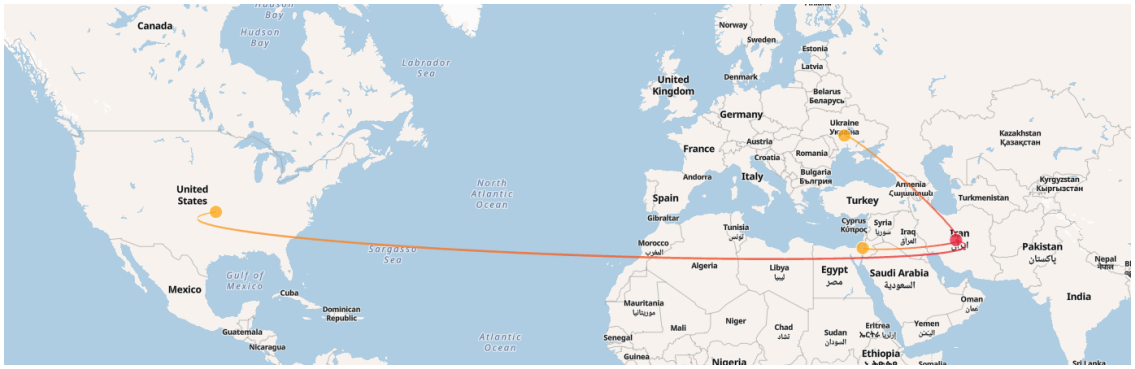

Figure 4. Nozomi Threat Intelligence is tracking Cyberv3ngers targeting organizations in the these countries.

Fox Kitten

Fox Kitten (also known as Pioneer Kitten) is a highly sophisticated Iranian advanced persistent threat (APT) group, active since at least 2017. It is widely believed to be state-sponsored and operates as part of Iran's broader cyber-espionage and sabotage apparatus. Fox Kitten is primarily focused on cyber-espionage, long-term access, and pre-positioning for potential disruptive or destructive cyber operations. It targets organizations that are strategically valuable to Iranian geopolitical interests, especially in the Middle East and beyond.

Figure 5. Nozomi Threat Intelligence is tracking Fox Kitten targeting organizations in these countries.

Homeland Justice

Homeland Justice is a cyber threat actor group attributed to Iranian state-sponsored operations. It gained notoriety for a series of disruptive cyberattacks targeting Albanian government infrastructure in 2022.

Figure 6. Nozomi Threat Intelligence is tracking Homeland Justice targeting organizations in these countries.

Nozomi Is Here to Help

In the modern world, global and regional conflicts are always accompanied by the increased activity of cyberthreat actors, sometimes playing a significant role in their outcomes. Tracking them daily in addition to exercising fundamental all-year-round due diligence is essential to stay on top of the game and making sure your organization has the best cybersecurity posture possible. At Nozomi Networks, we take these threats seriously. We transform actionable intelligence into continuously updated detection logic, delivered daily to our customers through our dedicated Threat Intelligence subscription—including the TI Expansion Pack Powered by Mandiant—and our standalone Threat Intelligence Feed, which integrates seamlessly with any cybersecurity solution, even without our sensors.

As we continue our mission to safeguard critical infrastructure, we invite organizations worldwide to join us in the fight against cyberattacks by sharing insights that can help strengthen collective defenses for all.

List of IoCs

- 159.100.6[.]69
- 169.150.227[.]230
- 95.181.161[.]50
- 164.132.237[.]65
- 5.199.133[.]149
- 104.200.128[.]71
- 104.200.128[.]206
- 31.192.105[.]28
- 185.118.66[.]114
- 194.187.249[.]102
- 185.162.235[.]29
- 144.202.84[.]43
- 64.176.173[.]77
- 64.176.172[.]101
- 64.176.172[.]235
