ThreatMon
Under Cyber Wings

Digital War in the Middle East:
Cyber Threats in Israel-Iran Conflict

ThreatMon
Under Cyber Wings

Table of Contents

Introduction

Relations between Iran and Israel were peaceful until the 1979 Islamic Revolution in Iran. During these peaceful relations, Iran actually became the second state to recognize the State of Israel, despite its opposition to plans for the partition of Palestine.

The new leadership that came with the Islamic revolution led by Ayetulluah Ruhullah Humeyni in 1979 sought to build an identity that it said was based on defense of oppressed territories and rejection of the “imperialism” of the United States and its ally Israel. Under Ayatollah Khomeini, the country burned all bridges with Israel and stopped recognizing the passports of Israeli citizens.

Iran seized the Israeli Embassy in Tehran and handed control of it to the Palestine Liberation Organization, which is fighting against the Israeli government for the establishment of a Palestinian state.

After 1979, Iran wanted to assert itself “as a Pan-Islamist power supporting the Palestinian cause that the Arab Muslim countries had abandoned”. Against the backdrop of these developments, tensions between Iran and Israel escalated and continue today, sometimes with threats and sometimes with actual actions.

So how did this tension escalate in cyberspace?

Especially in the past 10-15 years, the world has witnessed the rise in cyber warfare between Israel and Iran, which have highly developed cyber capabilities. Groups that support both states and are supported by both states have started to attack each other, the infrastructures of countries, armies, state institutions, to collect various information, to gain access and for many other reasons.

The most well-known of these attacks was the “Stuxnet Worm” virus attack, which targeted Iran's nuclear facilities and was blamed on Western states, including Israel.

Originating in 2011, this worm disrupted the centrifuge field of the Natanz nuclear facility. This attack is considered a milestone in the history of cyberattacks and a type of computer network attack (CNA) that requires the highest level of cyber capabilities.

Later, when we approach the present day, in 2019, with the disinformation activities carried out by Iran called “Endless Mayfly” against Israeli citizens, fake news websites were established in order to influence the perception of Israeli public opinion on important security issues such as the conflict in Syria, and a holistic effect was aimed by conducting a large-scale disinformation work on both social media and online media.
Mutual cyber conflicts are still ongoing today. With the assassination in Iran of Ismail Haniyeh, the leader of the Islamic Resistance Movement, officially known as HAMAS, the tension between the two countries has increased due to the Iranian regime's support for Palestine and has moved to the cyber world. So how did the assassination of Ismail Haniyeh take place? Haniyeh arrived in Tehran to attend the inauguration ceremony of Masoud Pezeshkian, who won the elections in Iran. After the ceremony, he went to the military lodging of the Revolutionary Guards in the north of Tehran. In the early hours of July 31, 2024, he was assassinated in an attack on the lodge by the Israeli Army.

In light of the subsequent escalation of tensions and attacks in cyberspace, there are also strategic advantages to dealing with cyberspace. By enabling messages to be transmitted in the context of strategic conflict between two states, it allows conflict to develop without drastic measures and will shape the rules of cyber warfare in the coming decade.
The cyber war between Israel and Iran, especially as it has evolved over the last two years, is an example of a strategic and technological learning competition in which both sides have something to gain but may pay a price.
In this report, we will shed light on the repercussions of the tension between the two countries in the cyber world by examining various attacks, various malware activities and various phishing campaigns by examining threat actors or groups.

Overview of Groups and Parties in Cyber Conflict

In the Iran-Israel conflict, various groups and aggressors take political actions in support of their side. These actions include processes and attacks carried out for the side they politically support.

Pro-Iranian Groups and Supporters: Cyber groups that support Iran are known as pro-Iranian groups and are located on the Iranian side of the conflict. These groups strengthen Iran's cyber defense strategies in the conflict and engage in deterrent and disruptive actions against the Israeli government. These actions include planned activities targeting various sectors and institutions.

Some pro-Iran groups and supporters include well-known names such as "Cyber Fattah Team", "Anonymous Iran", "Ghost Of Gaza", "Khilafah H4ckers", "7 October Union", and "VoltActivist".

Pro-Israel Groups and Their Supporters: Cyber groups conduct cyber operations to strengthen Israel's cyber defense capacity and protect the interests of the State of Israel.

Hacktivist groups 'GlorySec, KromSec and WeRedEvils' are among the well-known pro-Israel groups and supporters at the forefront of this struggle.

Pro-Iran Groups and Supporters

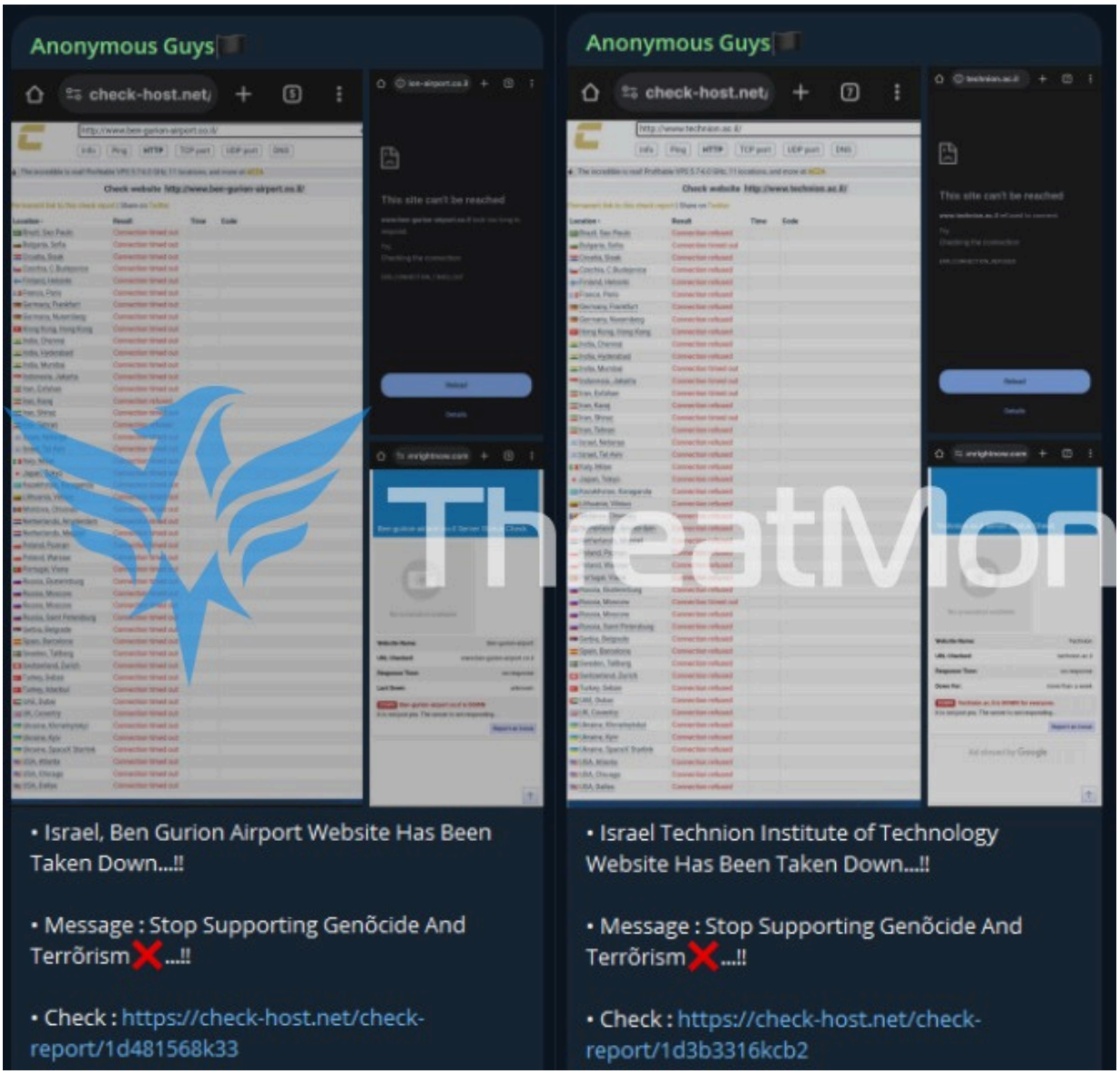
Cyber Fattah Team	Anonymous Iran
7 October Union	РУССКИЙ ЗАДАЧА СИЛА | РТФ
Z-BL4CX-H4T	VoltActivist
Team Ahadun-Ahad | {DEDSEC MUSLIMS}	Khilafah H4ckers
Anonymous Arabs	Noname057(16)
High Society	UserSec
Holy League	DEFACER INDONESIA
SYLHET GANG-SG	MaghrebSec
GhostSec	Black Maskers Army
Anonymous Guys	AnonymousActivist
Silent Cyber Force	Sumatra Selatan Cyber Team
Ghost Of Gaza	Anonymous Muslims
CyberDragon	Hacker Council Global
DXPLOIT	Al Ahad
Moroccan Black Cyber Army	CRYPTO CORP
Pro-Palestine Hackers Movement	Keymous
LAPSUS$	DoubleFace
KillSec	RipperSec
RCH-SEC	Team 1945
Team insane Pakistan	Moroccan Dragons
LulzSec Black	Evil of Anti ddos
Anonymous Collective	Alixsec

Beyond the 46 Hacktivist groups added to the table, many other groups have announced joining forces and becoming a global organization and union. The identified cybercrime groups are organizing cyberattacks targeting Israel. As an extension of the war on the digital front, these groups are taking the conflict into the virtual world, targeting Israel's infrastructure and sensitive systems.

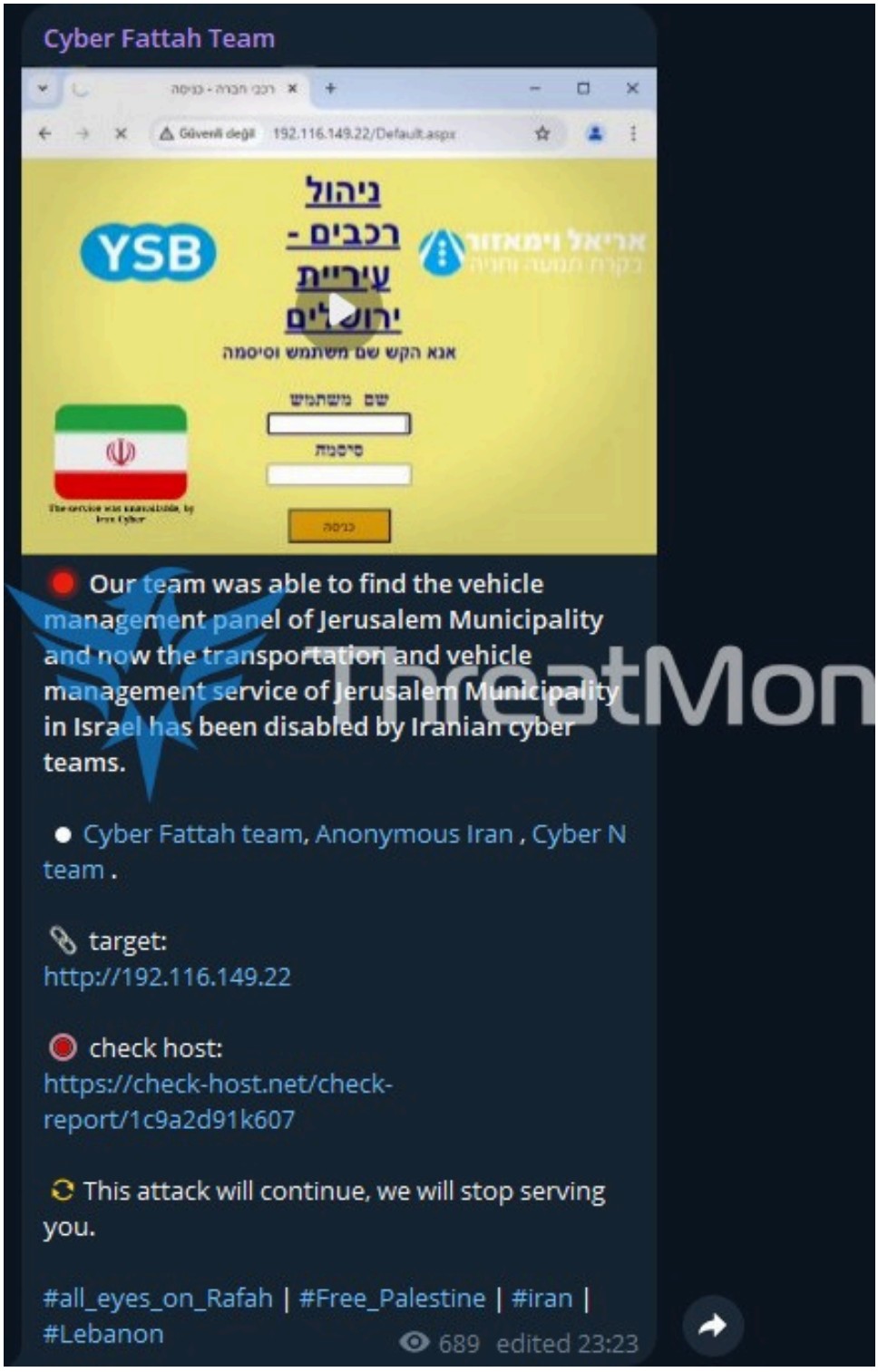
Examples of Attacks by Pro-Iranian Groups and Supporters

In the activity on Telegram detected by our team, the threat actor named “Moroccan Cyber Forces” claims to have leaked more than 200 login credentials of officials on Israeli WordPress websites.

In activity on Telegram detected by our team, a threat actor named “Anonymous Guys” targeted Ben Gurion International Airport, an international airport in Israel, and the Technion Institute of Technology in Israel. As a result of the DDoS attack, the websites became unavailable for a while.

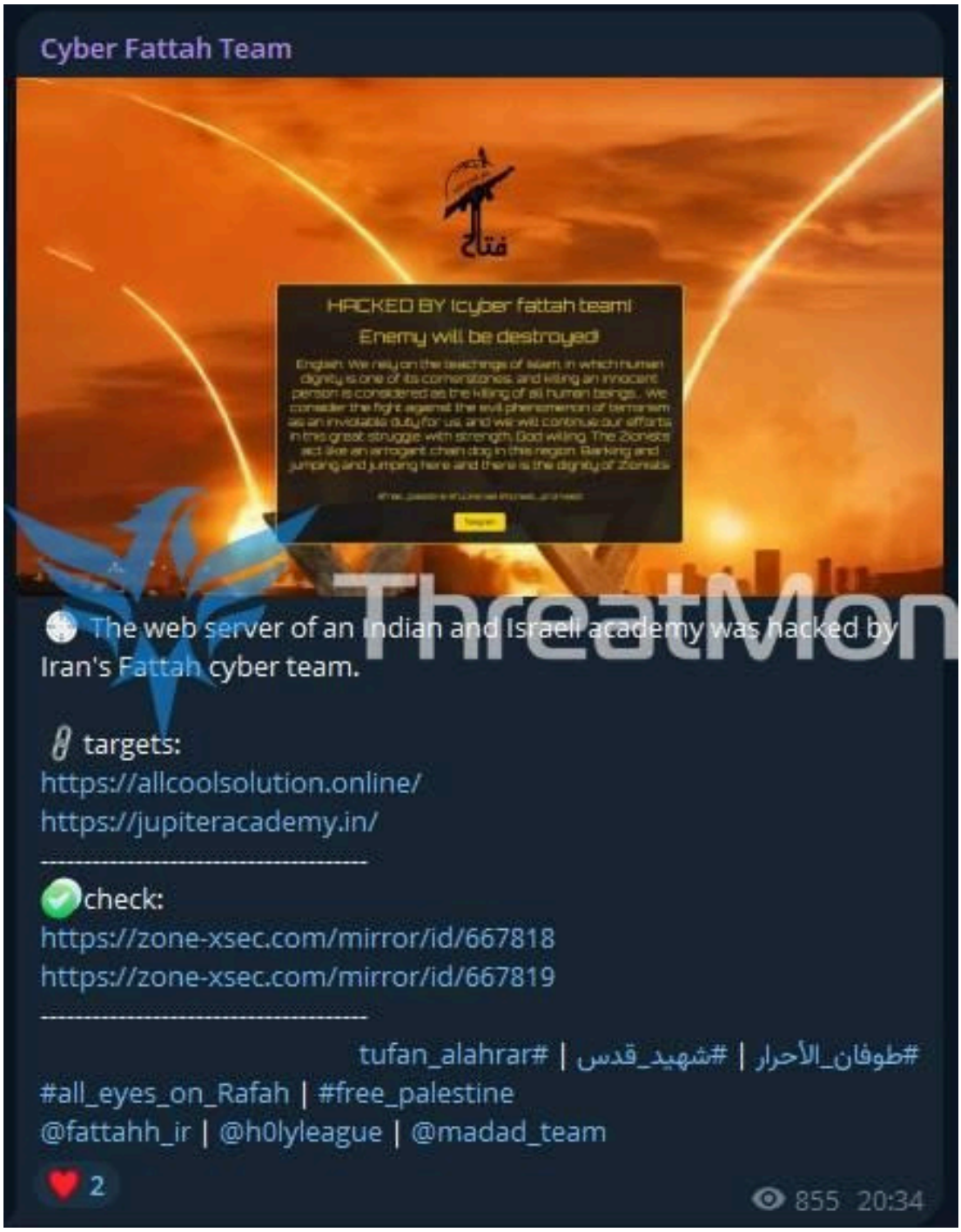


According to a detected telegram activity, the “Cyber Fattah Team”, which identifies itself as an Iranian cyber team, announced that it had disabled the transportation and vehicle management service of the Jerusalem Municipality in Israel. When the related attack was analyzed, it was seen that they made a denial of service attack on the IP they detected and left a check-host link as instant evidence.



In the activity detected by our team over Telegram, “Hacker Council Global” was found to be calling for all DDos hackers following the recent developments in the Israeli-Palestinian conflict, including the assassination of the Palestinian leader in Iran. The Hacker Council also mentioned the threat groups NoName(057)16 and Holy League at the end of the article.

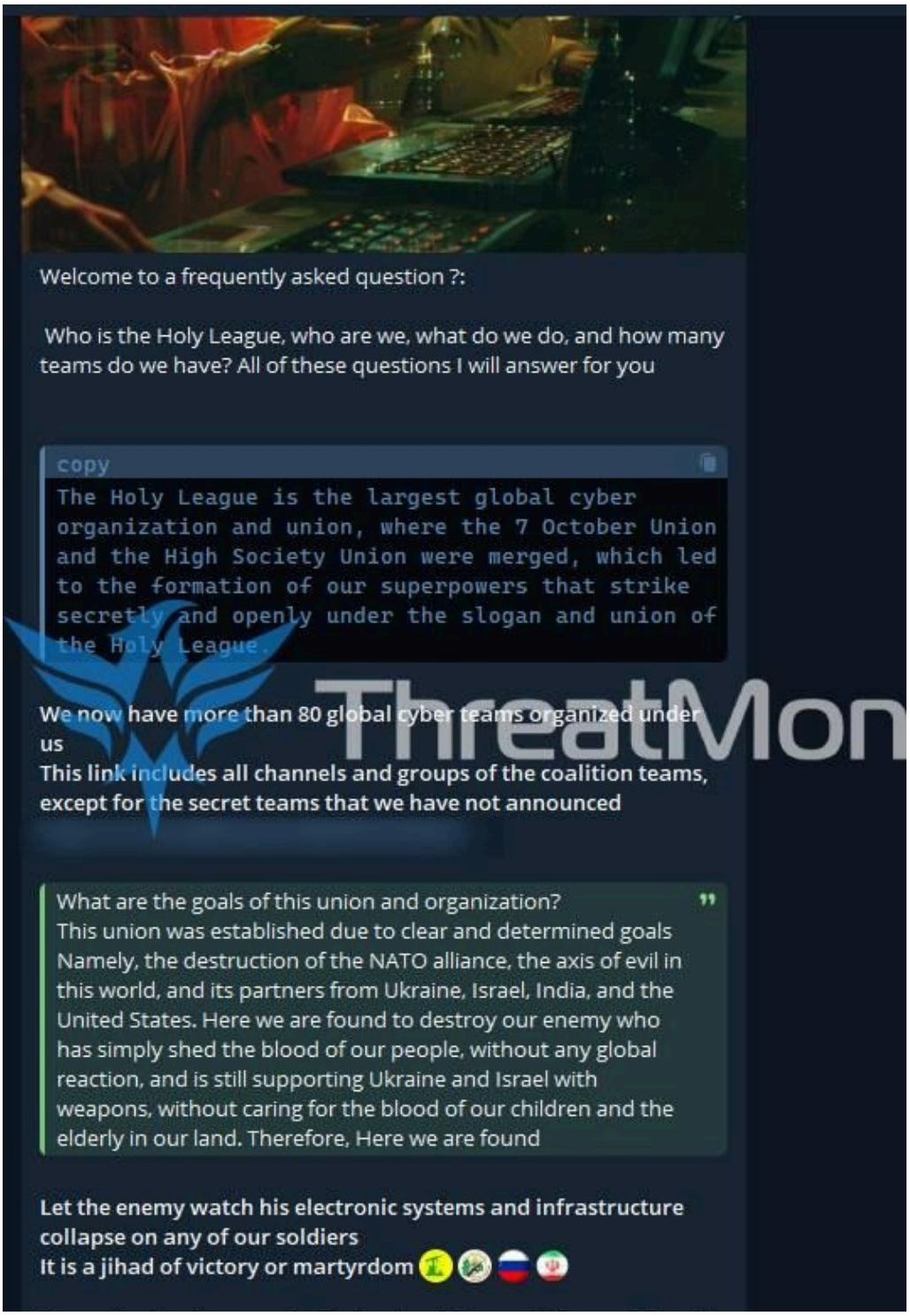
'Cyber Fattah Team' has announced that they have hacked the web server of an Indian and Israeli academy, this time targeting the education sector. They carried out a defacement attack and as a result published a zone log as evidence.



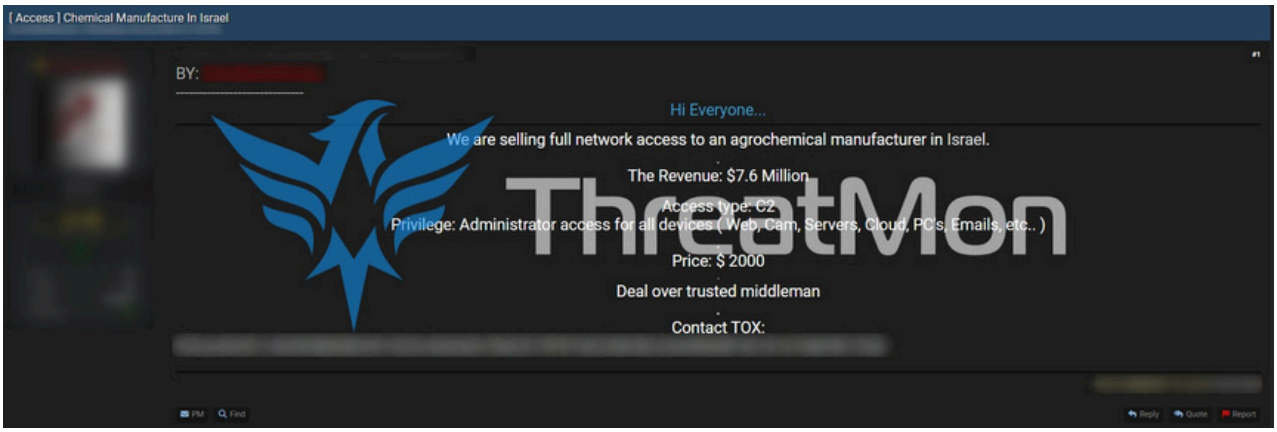
The “N Iran team” announced on its telegram channels that it had leaked Israeli economic, commercial, financial and tax data and put it up for sale. The threat group said it breached Israeli servers and gained access to financial records, asset lists, business information and more, with a total data size of 104 GB. Data allegedly leaked:

- Financial data of Israeli institutions.
- Assets, production, stock markets of Israeli businesses.
- World currency exchanges in Israel.
- Corporate correspondence
- Israel business directories.
- 66 GB email backup for tax authorities.
- Files and details of tax authorities.

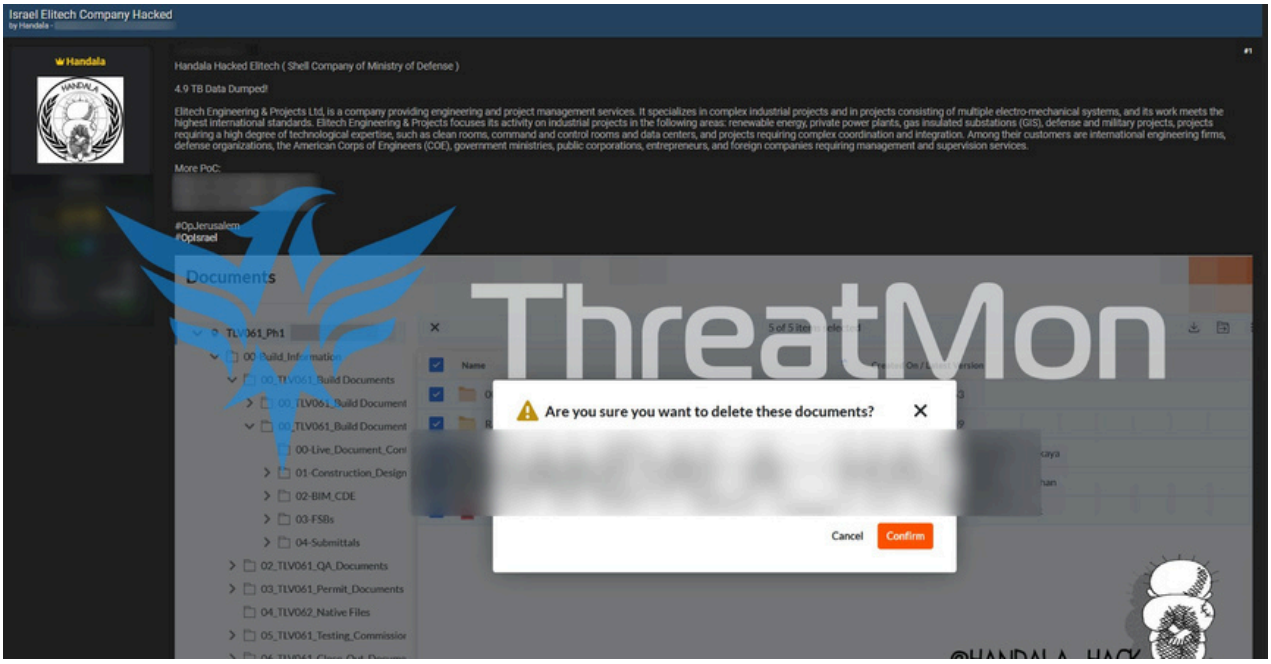
In a detected telegram activity, a threat group called “Holy League” announced that they are the major global cyber organization and union united by the Holy League, the 7th of October League and the High Society League, striking secretly and openly under the slogan and unity of the Holy League. The threat group claimed that they have more than 80 global cyber teams organized under them (excluding secret teams they have not announced).



According to the post shared by the threat actor identified in the dark web forum as a result of the scans, access to a chemical manufacturer in Israel was put up for sale.

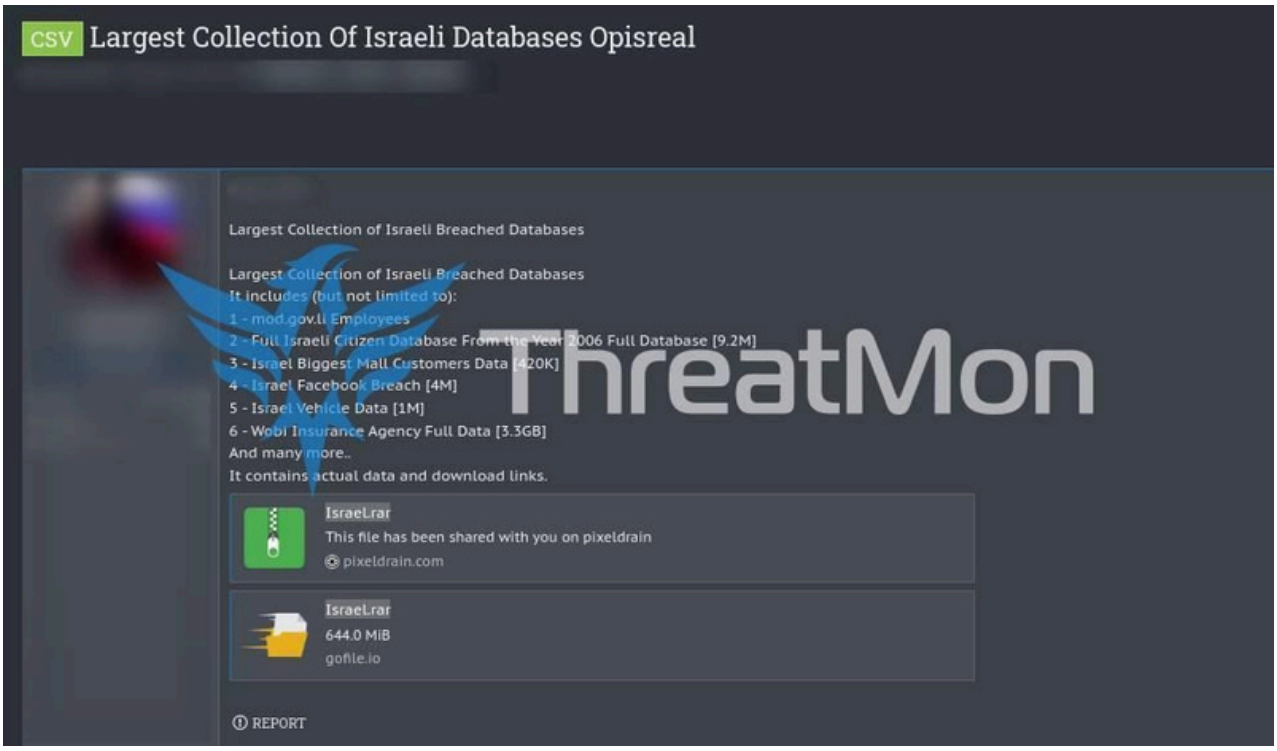


According to the post shared by the threat actor codenamed “Handala”, which was detected in the dark web forum and telegram as a result of the scans, the Israeli Elitech Engineering & Projects company was targeted. Elitech Engineering & Projects develops projects such as renewable energy, private power plants, gas insulated substations (GIS), defense and military projects, clean rooms, command and control rooms and data centers, and projects that require integration. As a result of the attack, Elitech Engineering & Projects claims that 4.9TB of data belonging to the company was drained.

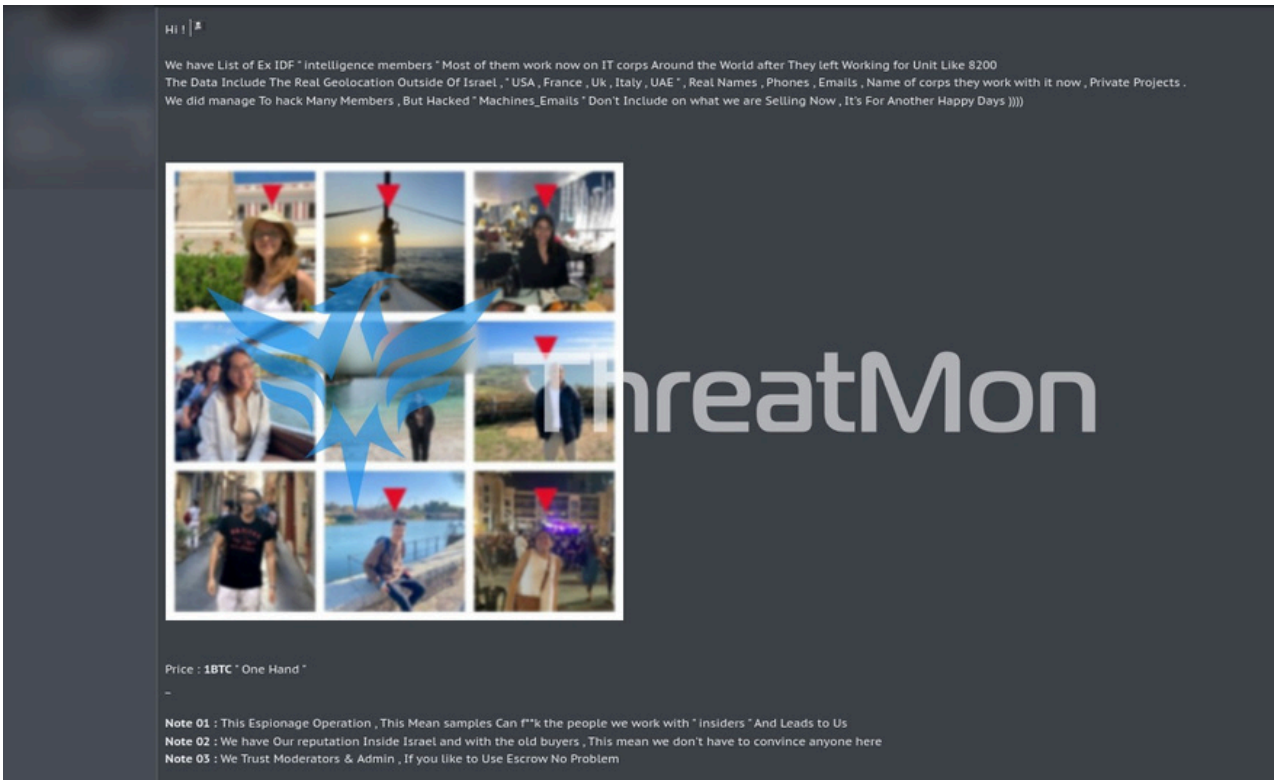


According to a post shared by a threat actor identified in a dark web forum and telegram as a result of scans, he claims to have leaked documents belonging to the Israeli Defense Ministry. The content of the leaks includes documents, e-mails, financial information and signed documents.

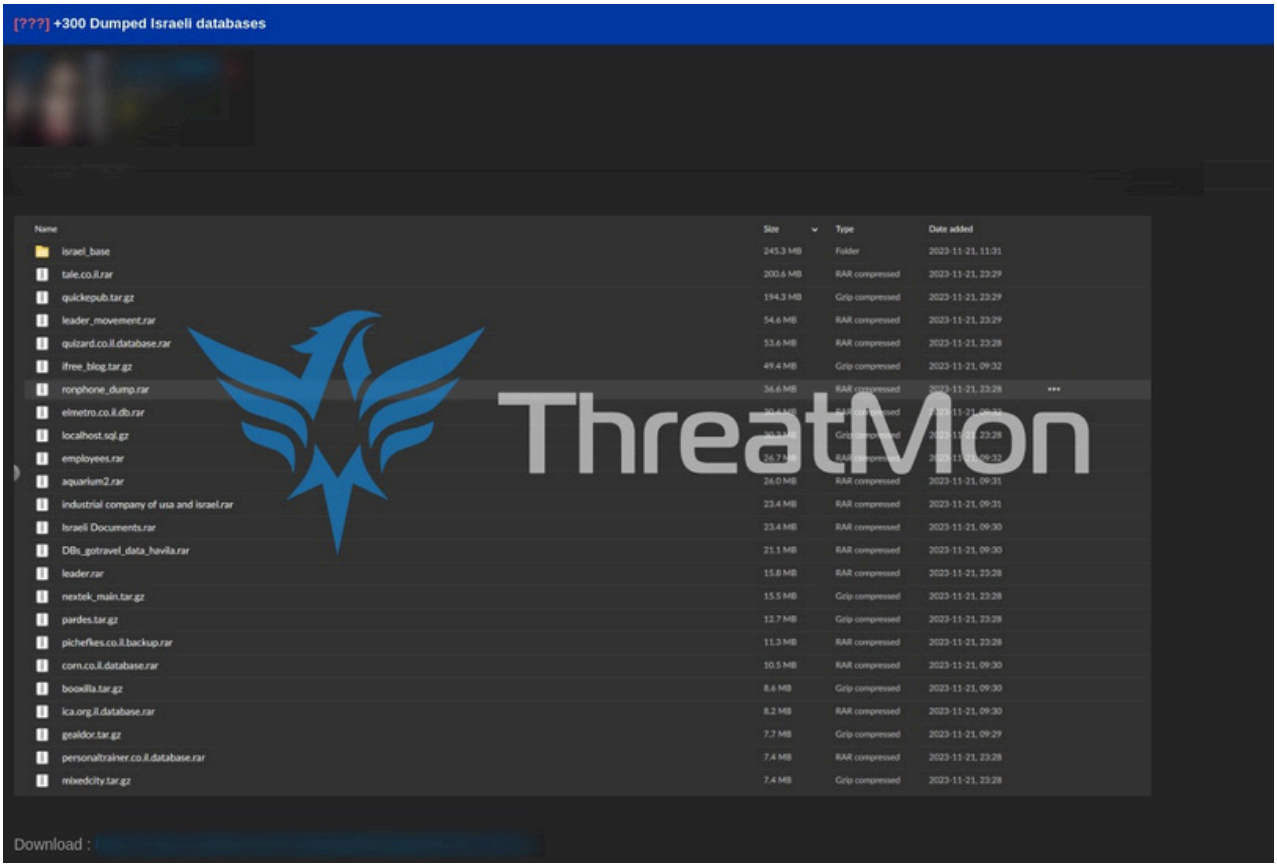
Various dark web forums have shared a leak of what is claimed to be the largest collection of Israeli databases as part of the OpIsrael project. The leak includes government, citizen, shopping mall, social media, vehicle, insurance and much more. This shows that with the escalation of the conflict, both sides are taking actions with opposing goals.



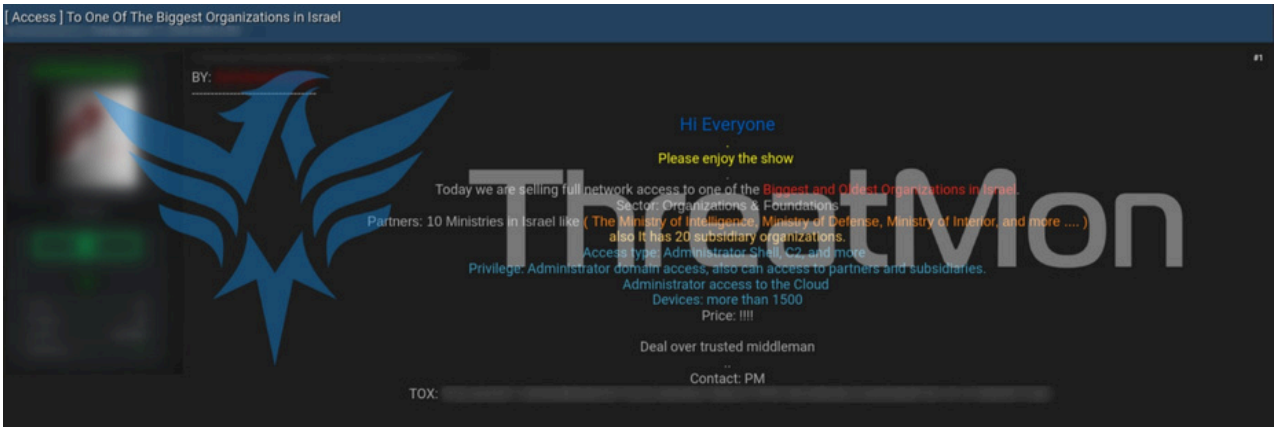
An important finding during the conflict is Israel Defense Forces data put up for sale on a dark web forum. A threat actor on the dark web forum announced that he had a list of former IDF “intelligence members”. The data allegedly includes the actual geographical location outside Israel, real names, phones, emails, the name of the corps they currently work for, special projects. The threat actor also claimed that he managed to hack many members and that he will put this data up for sale at another time.



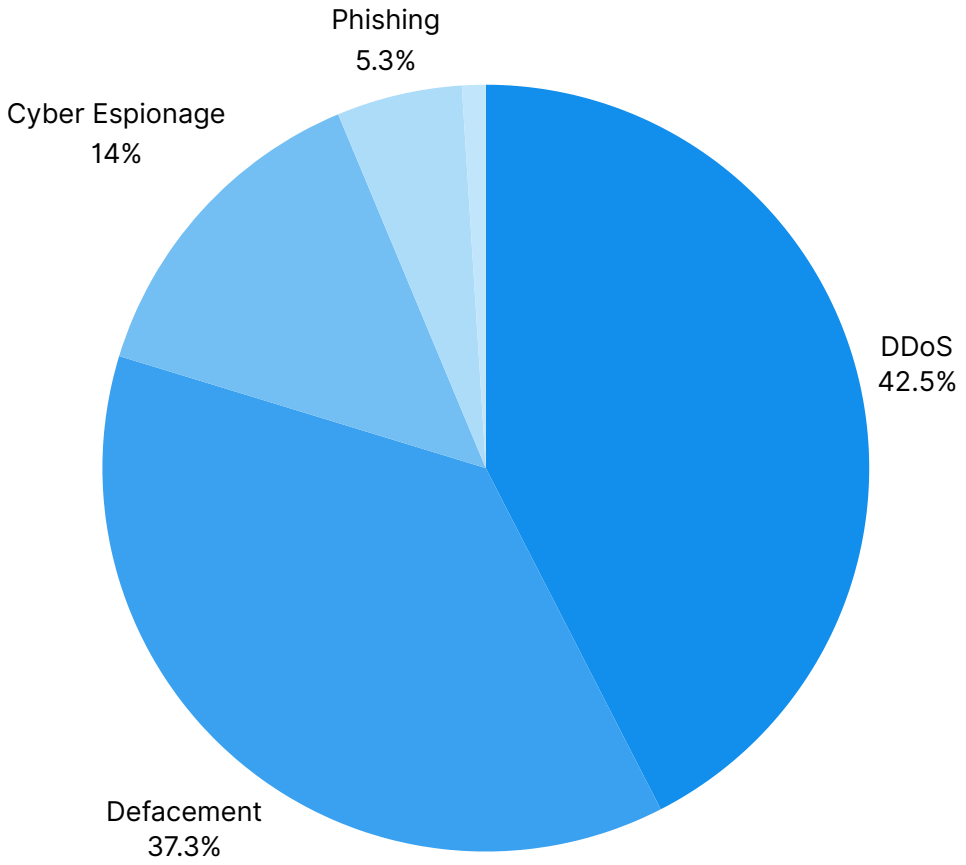
A member on a dark web forum announced that +300 Israel had leaked its databases. Although the content of the database appears to date back to 2023, the actors trying to take sides in the hot conflict have shown their involvement in this conflict by serving their databases.



A popular dark web forum member has announced that one of Israel's largest and oldest organizations has put its full network access up for sale. This organization is partnered with 10 ministries in Israel (Ministry of Intelligence, Ministry of Defense, Ministry of Interior and more). The type of access is claimed to be admin shell, C2 and more. Admin domain access can also access partners and affiliates.



Attack Tactics and Techniques Used by Pro-Iranian Groups and Their Supporters



DDoS Attacks (%42.5): Pro-Iranian groups frequently use Distributed Denial of Service (DDoS) attacks against Israeli online services. These attacks involve sending massive traffic to make targeted websites temporarily inaccessible.

Website Defacement (%37.3): Groups supporting Iran may make unauthorized changes to the appearance or content of a targeted website. These changes are usually made to the site's homepage and include a page with the attackers' message or intent.

Cyber Espionage and Information Collection (%14): Pro-Iranian groups may engage in cyber espionage to collect sensitive data from specific individuals or organizations.

Phishing Attacks (%5.3): In some cases, pro-Iranian organizations may resort to phishing attacks to obtain sensitive information from targeted groups or individuals. In April 2024, APT42 appears to have intensified targeting users located in Israel.

Social Engineering and Ransomware (%1): Pro-Iranian groups use social engineering tactics to achieve their goals. They may also use ransomware to harm their targets or steal information.

An analysis of the attack tactics and techniques used shows that these tactics and techniques reflect the diversity of cyber operations by groups supporting Iran.

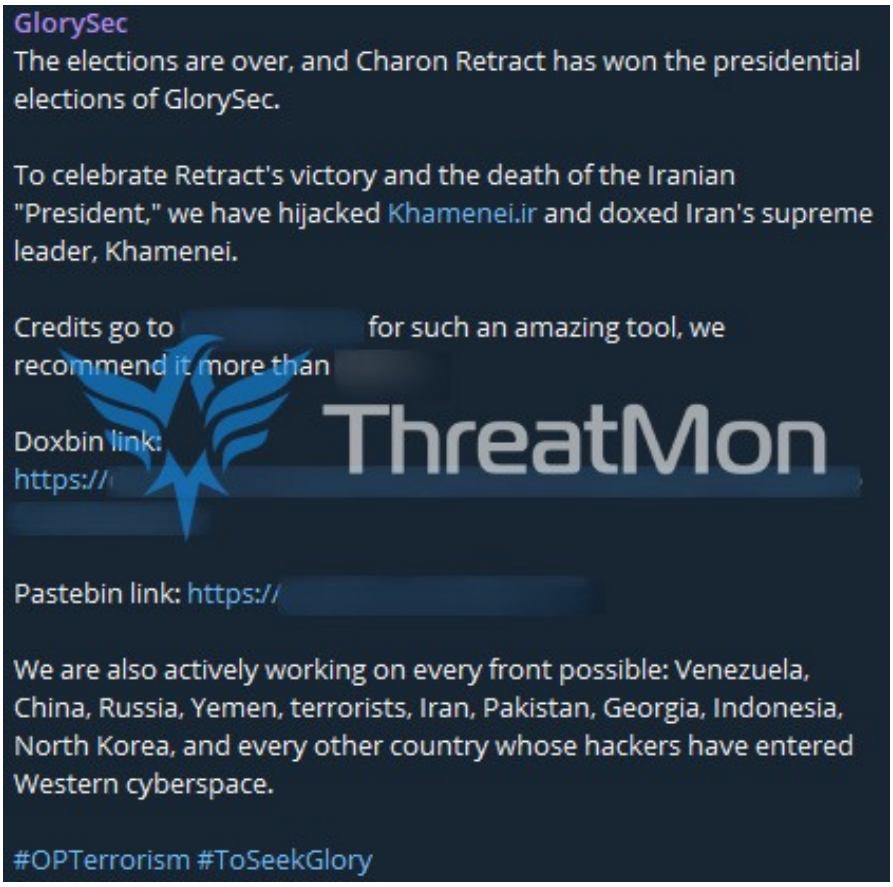
Pro-Isreal Groups and Supporters

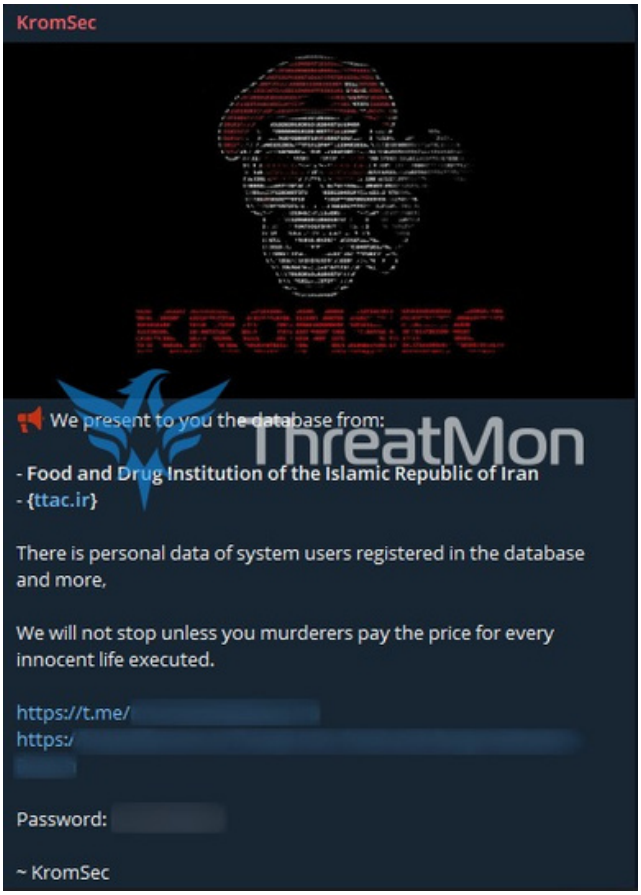
GlorySec	WeRedEvils
KromSec	S1L3NT_0N3

Four different groups supporting Israel are mobilizing against Iran's influence. Each with different motivations and strategies, these groups are launching cyber attacks targeting Iran. As an extension of the war on the digital front, these groups are taking the conflict to the virtual world, targeting Iran's infrastructure and sensitive systems.

Examples of Attacks by Pro-Israel Groups

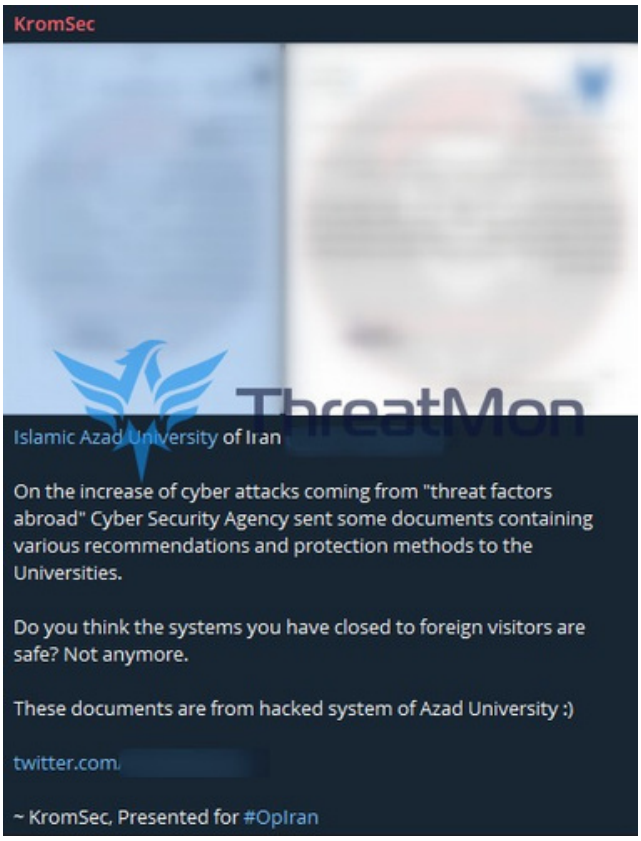
According to a detected telegram activity, GlorySec claims to have breached Khamenei, the official website of Ali Khamenei, Iran's supreme religious and political leader, and leaked Ali Khamenei's information as a result of the breach.





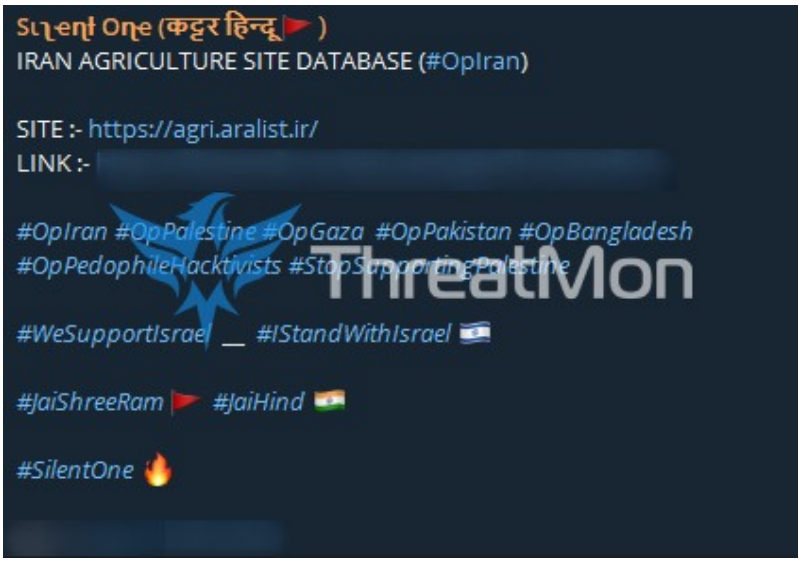
According to a detected telegram activity, KromSec claims to have leaked the database of the Islamic Republic of Iran's Food and Drug Administration. The database allegedly contains personal data of registered system users and more.

According to a detected telegram activity, KromSec claims to have leaked data belonging to the Islamic Azad University of Iran. The documents allegedly belong to Azad University.

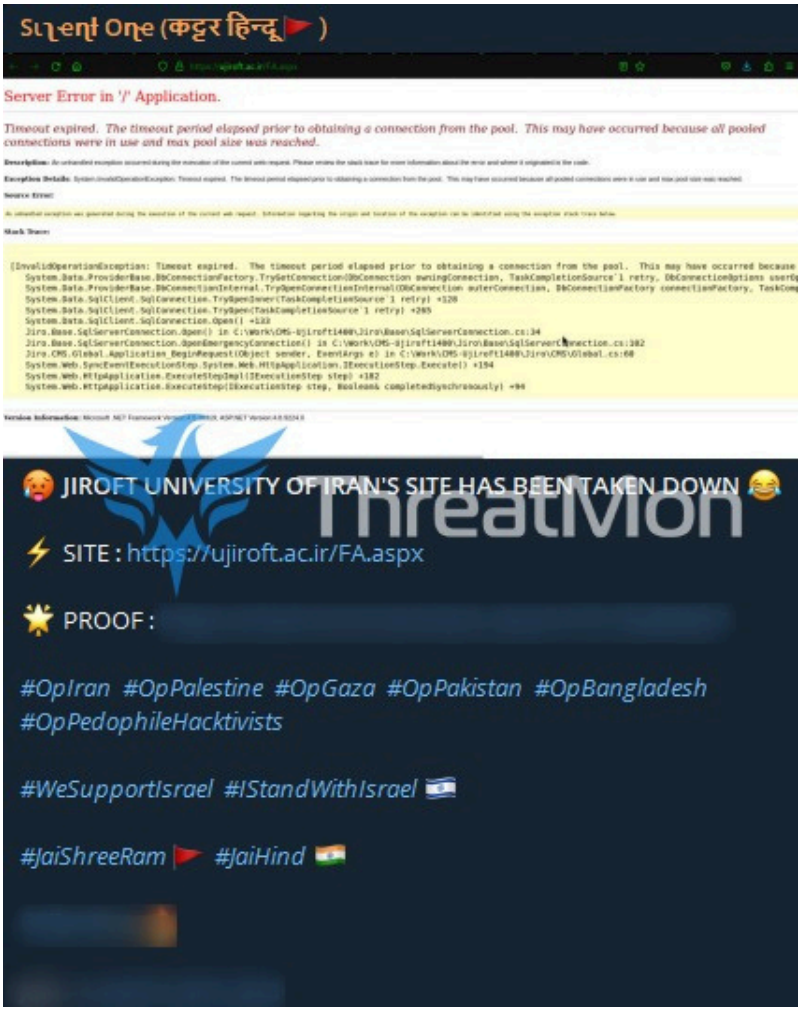


According to a detected telegram activity, KromSec claims to have leaked data belonging to the Iranian ministry of industry, mines and trade. The data allegedly contains information on 2.5 million people, including first name, last name, store address, store description, store description, phone number and city ID.

According to a detected telegram activity, S1L3NT_0N3 claims to have leaked the database of Iran's agricultural website.



According to a detected telegram activity, S1L3NT_0N3 claims to have launched a DDoS attack on the site of Iran's Jiroft University. The website of Jiroft University has allegedly become temporarily unavailable.

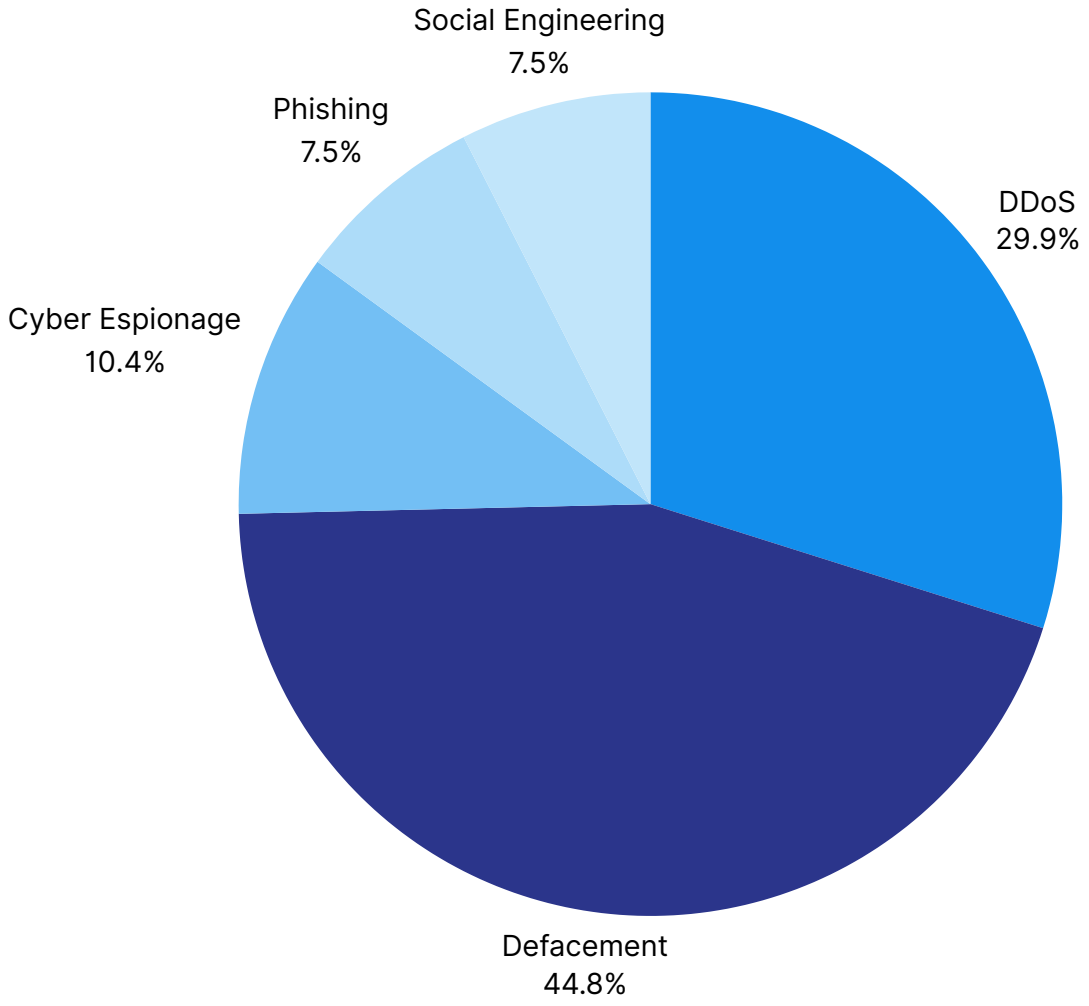


According to a detected telegram activity, S1L3NT_0N3 claims to have launched a DDoS attack against the official website of Ran Airlines of Iran. The official website of Ran Airlines allegedly became temporarily unavailable.

According to a detected telegram activity, Red Evils claims to have leaked data belonging to Sepah, an Iran-based bank. The data allegedly includes name, account number, card number, expiration date, pin code information.

In activity detected by our team over Telegram, “WeRedEvils” claimed to have attacked and blocked access to ict[.]gov[.]ir[.]html from Telegram Groups following recent developments in the Israeli-Palestinian conflict, including the killing of the Palestinian leader in Iran.

Attack Tactics and Techniques Used by Pro-Israel Groups and Their Supporters



Website Defacement (44.8%): Groups supporting Israel may make unauthorized changes to the appearance or content of a targeted website. These changes are usually made to the site's homepage and include a page with the attackers' message or purpose.

DDoS Attacks (%29.9): Pro-Israel groups have been using Distributed Denial of Service (DDoS) attacks against Iranian online services. These attacks involve sending massive traffic to make targeted websites temporarily inaccessible.

Cyber Espionage and Information Collection (%10.4): Pro-Israel groups may engage in cyber espionage to collect sensitive data from specific individuals or organizations.

Social Engineering and Ransomware (%7.5): Pro-Israel groups use social engineering tactics to achieve their goals. They may also use ransomware to harm their targets or steal information.

Phishing Attacks (%7.5): In some cases, pro-Israel organizations may resort to phishing attacks to obtain sensitive information from targeted groups or individuals.

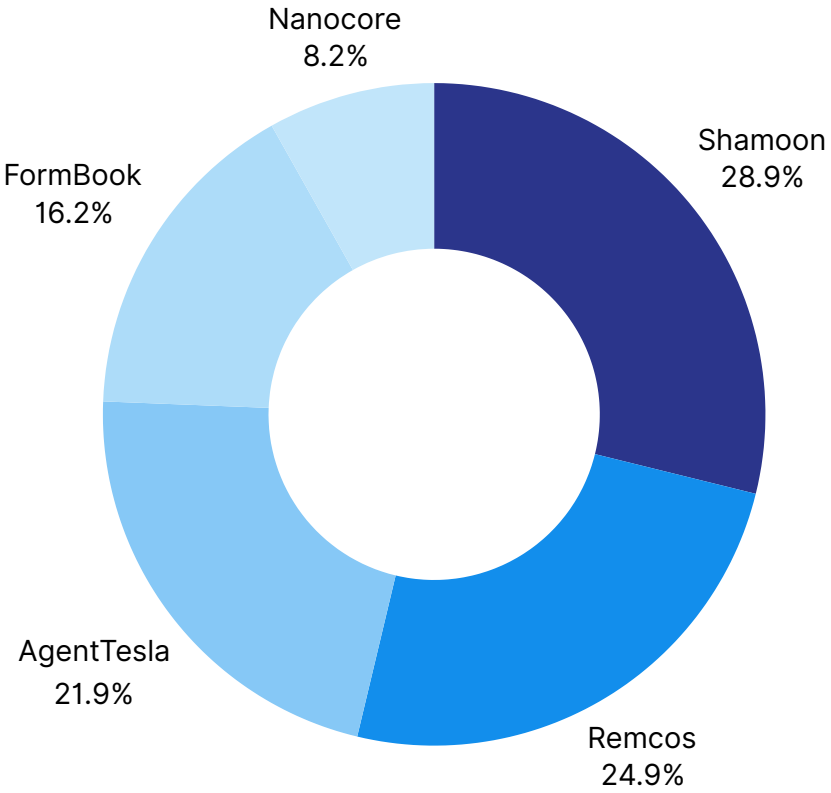
The Role Of Malware In Iran-israel Tensions And Its Detailed Analysis

As the ThreatMon team, the tensions between Iran and Israel, which have been on the agenda from the past to the present and especially in recent times and which are closely related to the Middle East geography, have hosted various malware distributed using these methods rather than techniques such as phishing, social engineering, etc., which are widely seen in the cyber warfare environment.

When we look at the latest tension, we see that Israel's cyber espionage activities have a cyber espionage usage rate of 10.4%, while Iran's cyber espionage usage rate is 14%.

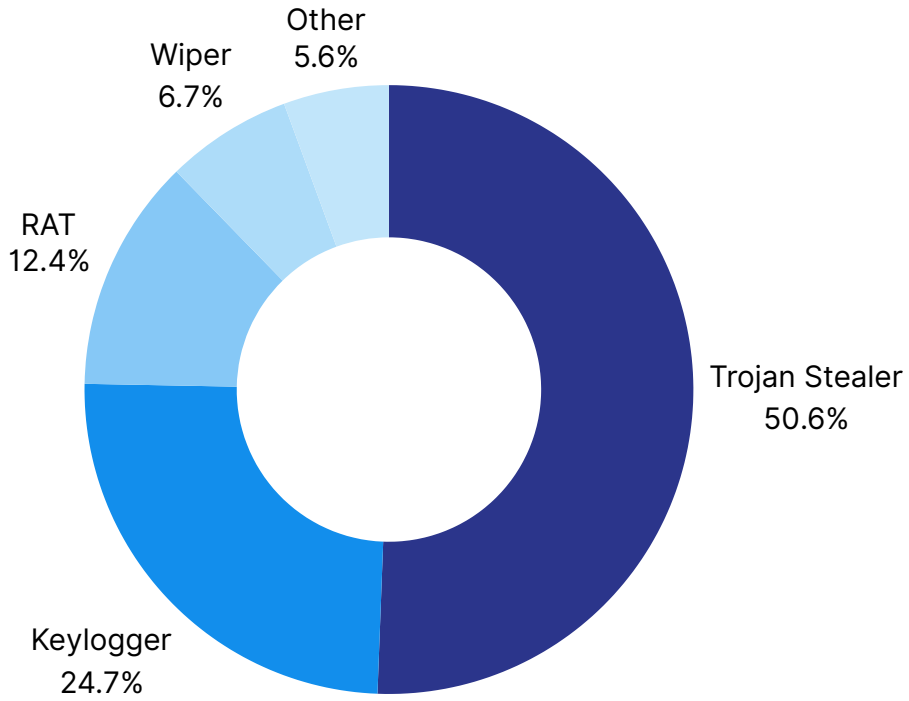
Iranian and Israeli threat actors have managed to carry out various attacks on each other through various malware in this process.

According to ThreatMon's findings, the graph below shows the names of the malware based on the dates before and during the escalation.



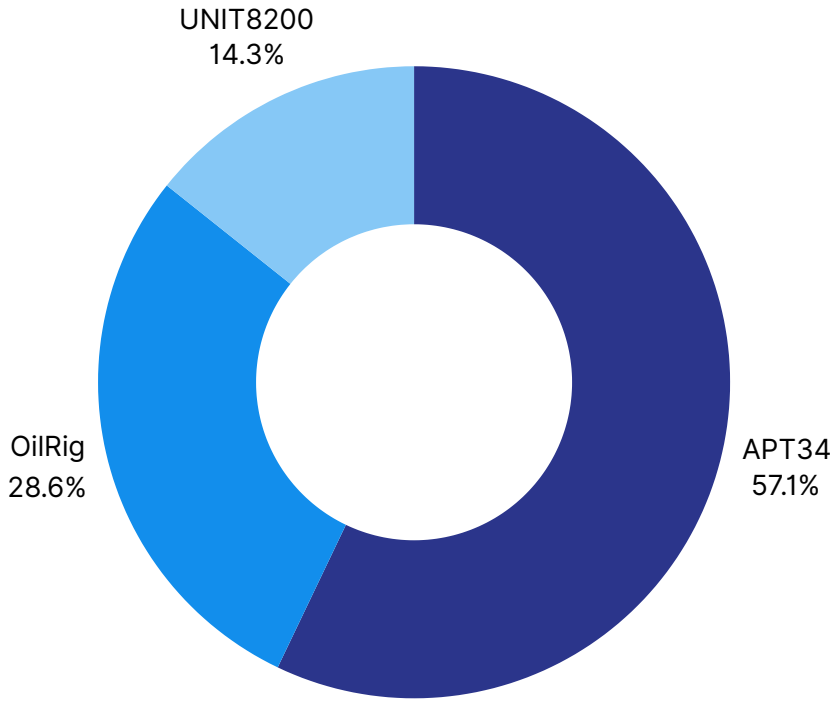
When we examine this graph, we see that the parties mutually attacked each other with various types of malware and data is given on the detection of these malware.

In the Middle East geography, it is very difficult to detect such malware because both countries are strict and restrictive. However, as ThreatMon, we have provided the following analysis on this malware.



According to the relevant graph, the types of malware detected are indicated. According to this graph, in the analysis made for each malware file detected; 56.1% Trojan Stealer, 24.7% Keylogger, 12.4% Remote Access Trojan, 6.7% Wiper and the rest of the malware are Ransomware, Riskware, etc.

In addition, as a result of the studies we conducted on some of the malware files we detected as ThreatMon, we also found that these files belong to three different APT groups.



Conclusion

This report argues that the long-standing Iran-Israel conflict is not limited to its military and political dimensions, but is also characterized by cyber warfare.

Both sides are conducting cyber attacks against each other through state-sponsored threat actors. These attacks pose threats to critical infrastructure, financial systems and state institutions.

Extending beyond the Middle East, the Israeli-Palestinian war followed by the Israeli-Iranian conflict has caused countries to take sides in line with their interests. This situation has increased mass groupings in the region and caused various global hacktivist groups to come together. Therefore, in a cyber conflict environment, the parties are expected to carry out more sophisticated attacks against their targets.

As with real-world wars, wars in cyberspace can have significant consequences and have a profound impact on societies. While physical wars are mostly fought in areas where military forces, economic resources and infrastructures are targeted, cyber wars target digital infrastructures, information systems and public opinion. In this context, the cyber war between Iran and Israel can be seen as a digital extension of physical warfare.

It is hoped that this report will shed light on this important issue and be a useful resource. The report is a guide for all companies operating in the region.

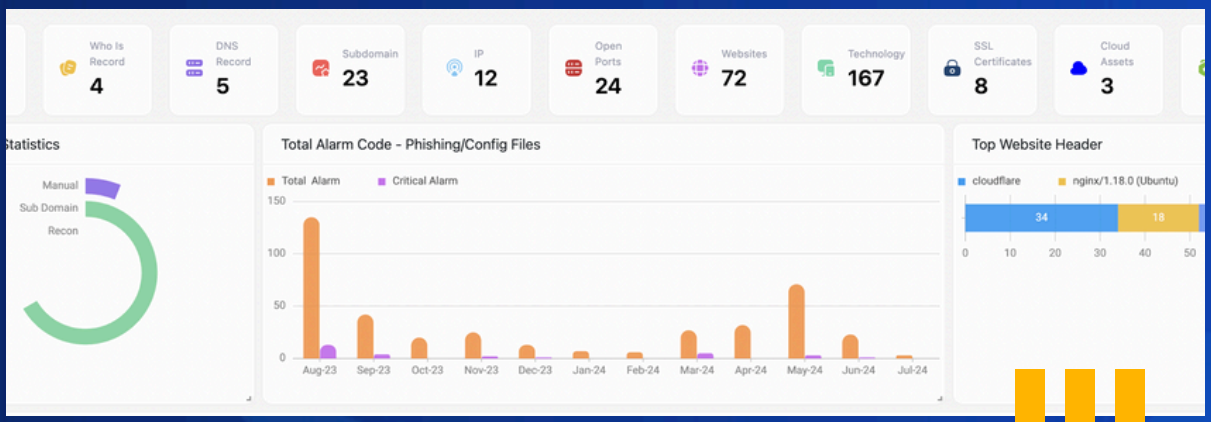
Whenever you have any questions or requests for additional information, do not hesitate to contact ThreatMon End-to-End Threat Intelligence team. We will be happy to support you.

We wish you to stay safe in the cyber world.

ThreatMon | Cyber Threat Intelligence Team

ThreatMon
Under Cyber Wings

More Information About ThreatMon



One Platform for all intelligence needs.

ThreatMon End-to-end intelligence is a cutting-edge, cloud-based SaaS platform that continuously monitors the dark and surface web, providing early warnings and actionable insights into emerging threats.

We are a SaaS platform designed to help businesses proactively detect and address threats before a cyber attack occurs. Unlike traditional cyber threat intelligence, we provide comprehensive and holistic cyber intelligence.

- *Attack Surface Intelligence*
- *Fraud Intelligence*
- *Dark and Surface Web Intelligence*
- *Threat Intelligence*

APPLY

FREE ACCESS

Contact Us:

Email Address
team@threatmonit.io

https://x.com/MonThreat

https://x.com@TMRansomMonitor

https://www.linkedin.com/company/threatmon