

Israel-Hamas War Cyber Operations

From terrorism to war, overview and analysis of cyber operations carried out alongside asymmetric warfare.

By Jeremy Makowski
Cyber Crime and Terrorism Intelligence Expert

October 2023

Table of Contents

1. Introduction 3
2. Cyber Forces Involved in the War 4
    2.1. Israel's Cyber Capabilities 4
    2.2. Pro-Israel Hacking Groups 5
    2.3. Hamas' Cyber Capabilities 6
    2.4. Hama's Cyber Operations Overview 6
    2.5. Hamas, Gaza, and Palestine Financial Support 10
    2.6. Pro-Gaza Hacking Groups 16
3. Type of Cyber Attacks Carried Out During the War 19
    3.1. DDoS Attacks 19
    3.2. Website Defacement 23
    3.3. Network Access and Data Breach Claim 24
    3.5. Malware Delivery 32
4. Psychological Warfare and Disinformation 34
5. Use of Artificial Intelligence and Face Recognition 34
6. Conclusion 36
7. About The Author 37
8. References 38

1. Introduction

For several years, symmetrical and asymmetrical wars have occurred in the physical world and cyberspace, which became the fifth battlefield after land, sea, air, and space. Today, cyber is part of the arsenal used by states and armed and terrorist groups. Cyber attacks launched during these wars or conflicts have varying intensity and emanate from cyber forces on both sides and numerous cyber supporters worldwide. In March 2022, we could observe the effects of cyberwarfare in parallel to the war on the ground between Russia and Ukraine. The phenomenon is the same concerning the current war between Israel and Hamas.

Since October 7, 2023, the beginning of the attacks perpetrated by Hamas against Israel, multiple groups of hackers and hacktivists affiliated with or supporting the terrorist group Hamas and others supporting Israel are engaged in numerous cyber operations alongside offensive activities on the ground. Like other countries in conflict with their neighbors (Ukraine-Russia, India-Pakistan, etc.), Israel suffers daily from multiple cyberattacks from terrorist groups, hackers, hacktivists, and APT groups. In that case, the Ongoing cyber attacks are likely of an intensity the country has never experienced before. In this cyber war, the number of hacking/hacktivist groups supporting Hamas and Gaza is much higher than those supporting Israel. (Pro-Hamas groups about a hundred against about twenty-five pro-Israeli) Finally, even though this war between Israel and Hamas leads to cyberattacks against multiple infrastructures, it also gives rise to a war of image and disinformation aimed at sowing disorder and psychological destabilization.

Regarding the cyber operations perpetrated alongside the war between Israel and Hamas but also that between Russia and Ukraine, we can see that the different hacker groups and hacktivist groups are much more present on Telegram than they are on social networks, which constitutes a change in the diffusion of their activities and their results. Suppose Telegram has already become an essential platform for cybercriminals for several years. In that case, it has become, for some time now, a valuable platform for different groups of hackers and hacktivists.

The purpose of this document is not to provide a timeline of the different cyber attacks launched on both sides but rather to give an overview and analysis of the cyber capabilities and other operations conducted by both sides alongside warfare.

2. Cyber Forces Involved in the War

2.1. Israel's Cyber Capabilities



Over the past twenty years, Israel has experienced intense and notable technological development in the cyber domain. Many software and services companies specializing in cyber defense, cyber attack, and cyber intelligence have emerged thanks to an incredible ecosystem between the military, high-tech companies, and universities.

The Israeli government has also implemented the National Cybersecurity Strategy in 2017, which is the country's first official global cyber strategy. This strategy includes, on the one hand, direct actions by the State to deal with cyber risks and attacks and, on the other hand, indirect actions aimed at supporting and collaborating with the private sector. The country has several cyber forces at both the defensive and offensive levels, with well-known civil and military units, without forgetting Israeli intelligence agencies and police.

Israel is also developing what they call the Cyber Dome. Inspired by the Israeli Iron Dome air defense system, the Cyber Dome is developed to include generative artificial intelligence platforms to help filter real threats from the sea of threat intelligence and allegations of cyberattacks that the country analyzes daily. Plans were initially announced in the summer of 2022, but the development of the Cyber Dome is now progressing in light of the conflict in Gaza; the Israeli technological ecosystem being very developed and cooperative, the country can count on the support of numerous cyber companies putting their skills at the service of the state to counter cyber attacks and secure critical infrastructures. In addition, other Israeli companies, such as NSO Group, Rayzone, or Anyvision, specializing in cyber intelligence and facial recognition, helped the government to identify and locate Israeli hostages from the Hamas attack on October 7. Several analysts specializing in easy recognition, big data, and image processing work together to identify as many people as possible. If Israel has excellent cyber-offensive capabilities and can count on various hacking groups supporting the country, It seems to be more of a cyber defense strategy. As mentioned earlier, Israel faces massive cyberattacks that must be countered and managed as best as possible to preserve the integrity of its critical systems.

2.2. Pro-Israel Hacking Groups

Apart from Israeli cyber forces, the country appears to be supported by several hacker and hacktivist groups carrying out cyber attacks mainly against Palestinian, Lebanese, and Iranian Targets. The following non-exhaustive list indexes the groups supporting Israel.

- Anonymiss
- Anonymous India
- Anonymous Israel
- AresLeaks
- Arvin
- Cyber Club (Support)
- Dark Cyber Worrior
- Garuna Ops
- Gaza parking lot crew
- GlorySec
- GonjeshkeDarande
- ICD- Israel Cyber Defense
- Indian Cyber Force
- Indian Darknet Association
- IT ARMY of Ukraine
- Kerala Cyber Thunders
- Kerala Cyber Xtractors
- Silencers_of_evil
- SilentOne
- Team NWH Security
- TeamHDP
- Termux Israel
- UCC Team

2.3. Hamas' Cyber Capabilities

For over a decade, Hamas has engaged in offensive cyber operations against Israel, sometimes the United States, and specific Palestinian targets. Their cyber operations are mainly focused on espionage and information. Hamas uses its intelligence branch to provide its leaders with information to make strategic decisions in the political and military fields. The intelligence branch of Hamas comprises members of the al-Majd security forces belonging to the larger Izz al-Din al-Qassam Brigades, which is the military wing of Hamas.

Cyber espionage campaigns operated by Hamas increased over the past decade with some evolution in the modus operandi, which became more sophisticated over time. In 2013, the tactic used by the organization focused on a broad approach by sending general emails with malicious attachments to many targets in the hope that some of them fall into the trap. Later, Hamas changed its attack mode by using links to infect its targets. On the other hand, social engineering is also a technique used by Hamas to target Israeli soldiers through Facebook to infect their smartphones with malware. While most of Hamas's cyber operations focus on intelligence gathering, another part aims to hack data, expose it, and use it for psychological manipulation. The organization claims several hacks, including Cellcom, Egged, and IAI. Additionally, DDoS attacks for nuisance, Defacement, and propaganda are also part of the cyber operations carried out by Hamas.

2.4. Hama's Cyber Operations Overview

- In 2012, Hamas claimed responsibility for a cyberattack on the Israeli army's website, including that of the IDF Spokesman's Homefront Command.

- In 2013, Palestinian hackers claiming to be from the Hamas' armed wing Izz ad-Din al-Qassam launched a distributed denial-of-service (DDOS) cyberattack against the website of American Express.

- In 2014, Hamas claimed responsibility for hacking into the classified IDF network and released several videos taken earlier in the year of Israel's Operation Protective Edge in the Gaza Strip.

- In 2018, Hamas launched a cyber operation using fake Facebook profiles of attractive women to contact Israeli soldiers and take control of their computers and smartphones. They also exploited WhatsApp by impersonating Israeli soldiers and sending messages to army personnel to gain access to confidential information. According to the threat intelligence company ClearSky, Hamas members attempted to infect the smartphones of Israeli citizens with malware by using an application that imitated the "Red Alert" application, which provides real-time alerts of missile launches at Israel. According to Clearsky, Hamas planted a download link for the malicious app in fake Facebook and Twitter profiles. Once downloaded, the malicious program enables full access to the mobile device for monitoring purposes.

- In 2019, the Israeli army bombed one of Hamas' buildings, serving as its cyber base (Figure 1). While this attack partly affected the organization's cyber capabilities, Hamas has not stopped its cyber operations.



Figure 1 - One of the Hamas' cyber command buildings destroyed by the IDF in 2019

- In 2020, Hackers affiliated with Hamas exploited Facebook, Dropbox, and Google Drive to spread spyware that aimed to target Arab leaders and states, using lures mentioning Israeli Prime Minister Benjamin Netanyahu and the Saudi Arabian Crown Prince, Mohammed bin Salman (MBS).

- In 2021, the Hamas-affiliated Molerats claimed to be a part of the Gaza Hackers Team. They took part in cyberattacks using malware and targeting Middle Eastern entities, including governments, think tanks on foreign policy, and a state-affiliated airline.

- In 2022, according to research performed by the cybersecurity firm Cybereason, a Hamas-linked attack group, APT-C-23 (AKA Arid Viper, Desert Falcons), was involved in a sophisticated intelligence-gathering campaign targeting senior Israeli officials. Beyond social engineering using fake Facebook

accounts, the group introduced new malware, including a fake messaging app known as VolatileVenom, a downloader known as Barbie Downloader, and theBarbWire Backdoor (Figure 2).

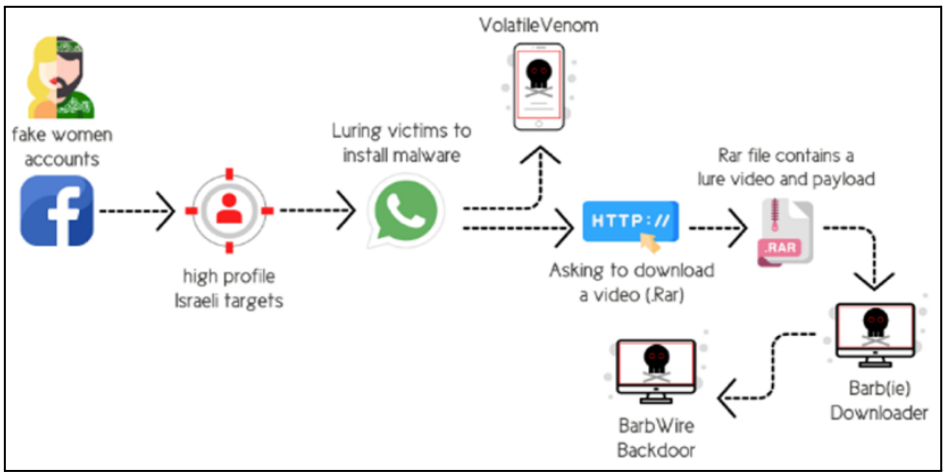


Figure 2 - Hamas Volatile Venom malware infection method (Source: Cybereason)

- In 2022, Hamas officially revealed in a video that it had operated a cyber unit for eight years with multiple cyberattacks against Israel (Figures 3 and 4). Hamas claimed the team was established in October 2014 by Juma al-Tahla, the former head of Hamas' cyber command, whom the IDF had killed during the 2021 Gaza conflict.



Figure 3 - A Hamas cyber fighter from their official Video



Figure 4 - Hamas' alleged cyber operations list

- In October 2023, following the terrorist attack by Hamas against Israel, Hamas and its affiliates launched many cyber attacks against Israeli infrastructures and private companies.

- In addition, the armed wing of Hamas Izz ad-Din al-Qassam Brigades recently released an application distributed on Telegram channels used by Hamas members and supporters (Figure 5), according to an analysis by researchers from the Recorded Future company. The application is reportedly configured to communicate with the Hamas Izz ad-Din al-Qassam Brigades website. An analysis of the infrastructure associated with the website led to the identification of a group of domains that mimic the domain registration system of TAG-63, aka APT-C-23. According to several Israeli Cyber Intelligence companies, this group is an Arabic-speaking and politically motivated group that acts on behalf of Hamas. Recorded Future adds that they also observed these domains were interconnected via Google Analytics code. One of the domains associated with the cluster hosted a website that spoofed the World Organization Against Torture (OMCT). The company explains that based on domain registration patterns, they observed a likely connection to Iran related to this domain.



Figure 5 - Alqassam application broadcasted in one of the Izz ad-Din al-Qassam Brigades Telegram channel

2.5. Hamas, Gaza, and Palestine Financial Support

Decades ago, terrorist financing relied on traditional methods until terrorist groups began to use cryptocurrencies to send and receive funds anonymously and securely. Hamas and its affiliates have practiced using cryptocurrencies for a few years already. On January 31, 2019, Abu Ubaydah, the spokesman for the Az ad-Din al-Qassam Brigades, the military wing of Hamas, announced that Hamas had begun accepting donations in Bitcoin and published the link to wallets associated with the organization on their website. Hamas also provides an email address to contact someone for a gift. (Figure 6). They allow their supporters to donate anonymously and securely via a unique Bitcoin address automatically generated for each donor. Once received, funds are often transferred from wallet to wallet to hide the source and path of payment. The funds are then withdrawn using mediators with money (money mules). For those who prefer to make a more traditional donation,

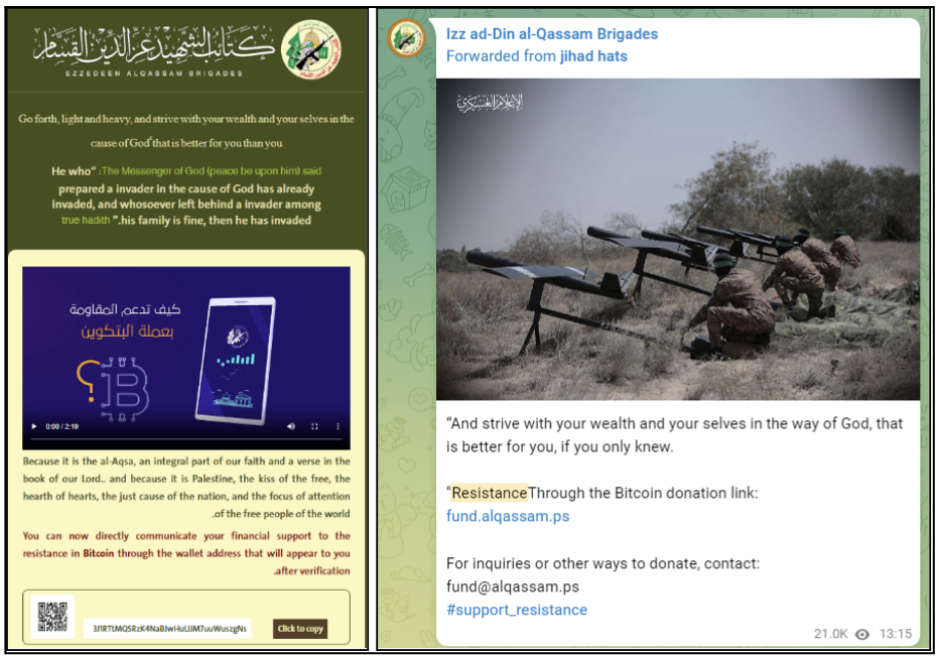


Figure 6 - Messages on the Hamas website and Telegram for people who want to financially support them by sending Bitcoin or contacting them by email.

In April 2023, the military wing of the Hamas terrorist group, the Izz ad-Din al-Qassam Brigades, announced that it would stop raising funds using the cryptocurrency Bitcoin, citing increased hostile activity against donors. The group could, however, continue to use cryptocurrencies in addition to more traditional means of financing. Indeed, in October 2023, a bank account at the British bank Barclays used to raise funds for the Palestinian militant group Hamas was frozen. According to the Israeli police statement, the bank account details were published by Hamas to deposit the donation funds. Israel also froze cryptocurrency accounts used for donations to the terrorist group. Apart from these official fundraising campaigns launched by Hamas, various supporters of the Palestinian and Gazan causes have also opened Telegram groups to ask for donations in cryptocurrencies. (Figures 7, 8. 9, and 10).



Figure 7 - A Telegram channel for donations in cryptocurrencies supporting Palestine

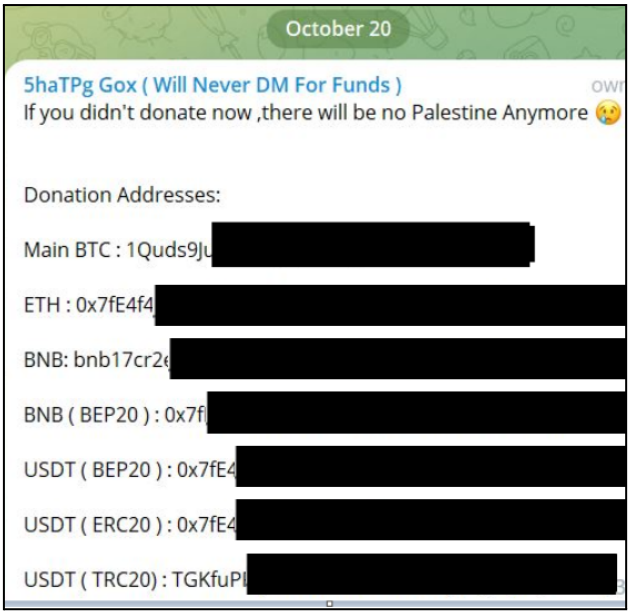


Figure 8 - A list of different cryptocurrencies addressed for donations in support to Palestine

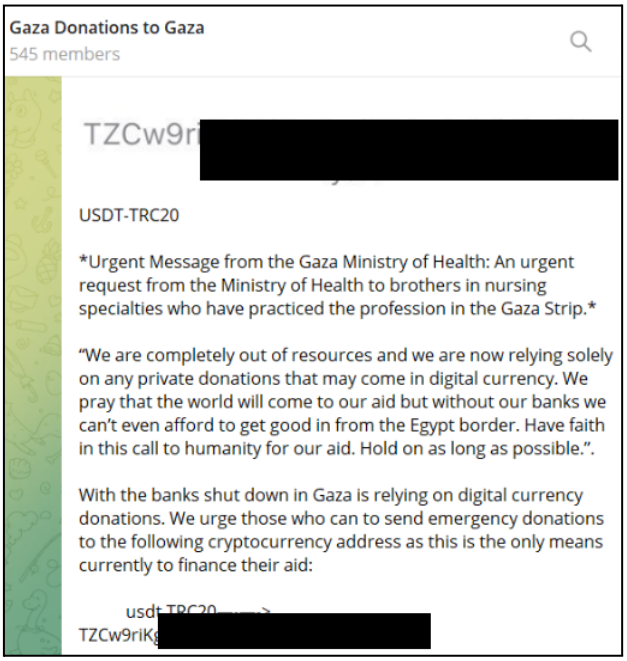


Figure 9 - A Gaza donation Telegram channel

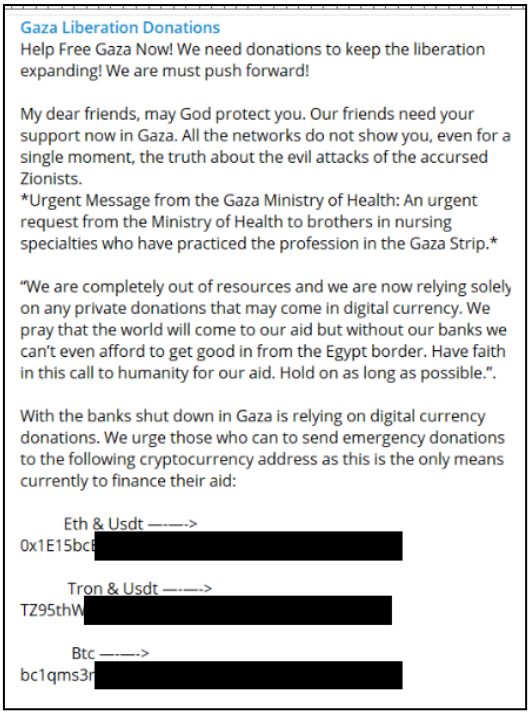


Figure 10 - A Gaza donation Telegram channel

Furthermore, some people supporting Gaza have launched a financial initiative called Gaza Coin which they promote through the digital communications platform Telegram and the social network X (Figures 11 and 12).



Figure 11 - Gaza coin Telegram channel

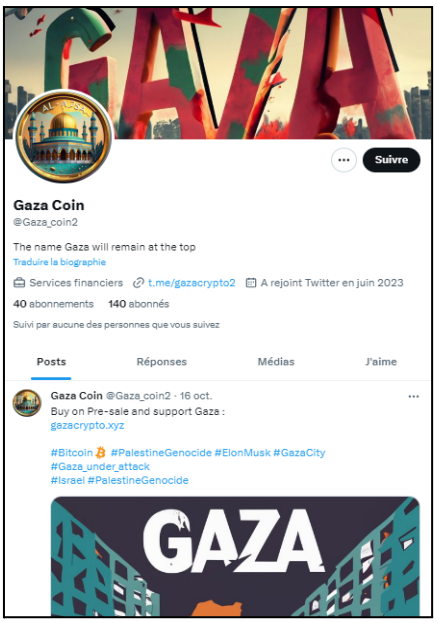


Figure 12 - Gaza coin account on the X platform social media

The message on the Gaza coin message is the following (Figure 13):

" The Gaza coin is one of the symbols of the meme that will build an integrated society across all platforms that opposes the policies of Israeli occupation. All traders in the world will have to stand up on this issue. The number of currency symbols will be based on the population of the Gaza Strip. 50 percent of the currency will be distributed to humanitarian organizations in the sector, sponsored by Islamic Relief Worldwide. The rest of the coins will remain distributed to circulate on the platforms, immortalizing the name of Gaza everywhere".

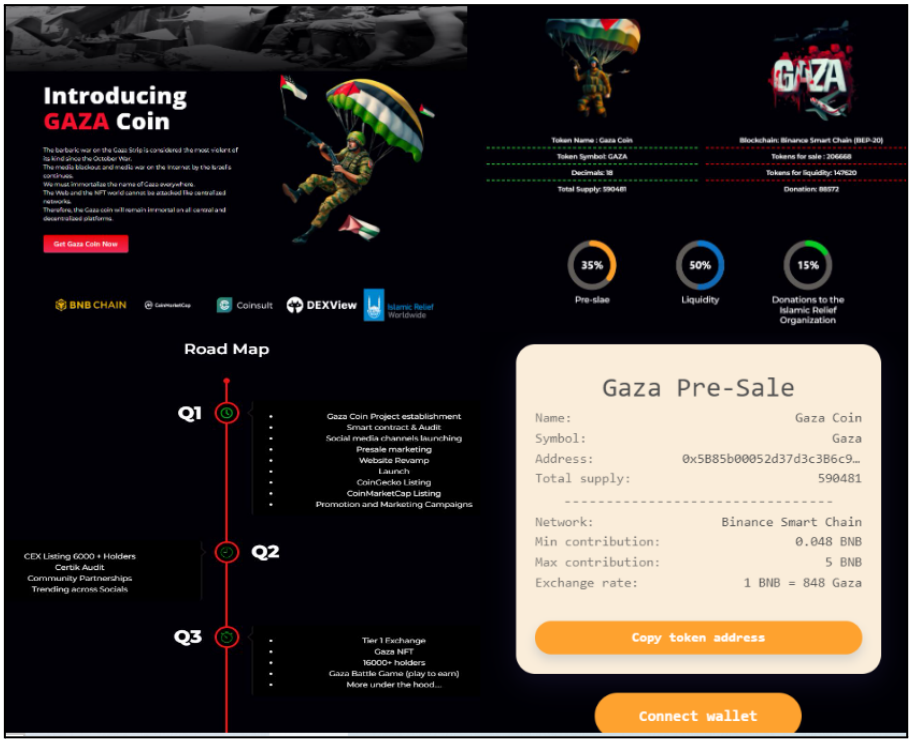


Figure 13 - Gaza coin website

Some cybercriminals try to divert these calls for cryptocurrency donations to their advantage. They are using the Israel-Hamas conflict to trick unsuspecting victims into sending them funds. According to Bleeping Computer, several websites claiming to be legitimate and calling for donations to support Gaza are scams (Figures 14 and 15).



Figure 14 - A fake pro-Palestinian website seeking crypto donations (Source: Bleeping Computer)

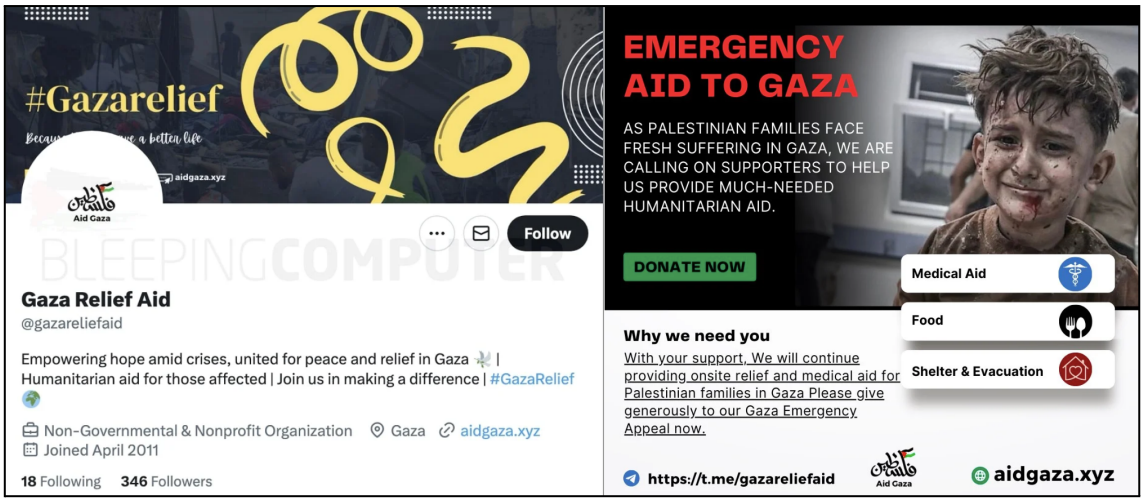


Figure 15 - Suspected scam of fake Twitter page and fake fundraising site for Gaza (Source: Bleeping Computer)

2.6. Pro-Gaza Hacking Groups

Pro-Gaza hacker and hacktivist groups mainly come from Arab countries but also from South Asia and Russia. They are engaged in large-scale cyberattacks against Israeli infrastructures and businesses. What makes the pro-Gaza side powerful is not the sophistication of their attacks but rather the number of supporters and, for some, their cooperation. Since the beginning of Hamas operations, these groups have continued to seek vulnerabilities and attack Israeli systems. Apart from these hacktivist groups, the company Recorded Future points out that the Islamic Revolutionary Guard Corps (IRGC), notably the Quds Force, would be the only Iranian entity known to provide cyber support to Hamas and other groups. threatening Palestinians. It is important to remember that Iran is undoubtedly, with Israel, one of the greatest cyberpowers in the Middle East. The Iranian regime also supports Hamas and Hezbollah, whose cyber fighters it trains. The following non-exhaustive list includes pro-Gaza support groups.

- 4 Exploitation
- 1915 Team
- ./CsCrew
- ./Tea Party
- Aceh About Hacked World
- AnoaGhost
- AnonHamz
- AnonT13x Group
- Anonymous 070
- Anonymous Indonesia
- Anonymous Morocco
- Anonymous Russia
- Anonymous Sudan
- Arab Anonymous Team
- ASKAR DDOS
- Awham
- Bandung Cyber Team
- Bangladesh Civilian Force
- Black Security Team
- Blackshieldcrew MY
- Boom Security
- Cubjrnet7
- Cscrew
- Cyb3r Dragonz Team
- Cyber Error Team
- Cyb3r Gang

- Cyber Sederhana Team
- CyberActivism
- Dark Storm Team
- DumpDataBase
- Dragonforce Malaysia
- Eagle Cyber Crew
- Electronic Tigers Unit
- End Sodama
- Esteem Restoration Eagle
- F7 Xpl0it3r
- Fr3dens of Security
- Ganosec team
- Garnesia Team
- Gb Anon 17
- Ghost Clan Malaysia
- GhostClan
- Ghost Hunter Illusion
- GhostSec
- Hacktivism Indonesia
- Hizbullah Cyb3r Team
- Haghjoyan
- IndoGhostSec
- Islamic Cyber team | Indonesia
- islamic hacker army
- Jateng Cyber Team
- JATIM RedStorm Xploit
- KEP TEAM
- khalifah cybercrew
- Khan cyber Army
- KillNet
- Kingman world official
- Kuningan Exploiter
- LGH
- Malaysia cyber defacer
- MeshSec
- Milad Hacking
- M.H.T
- Moroccan Black Cyber Army
- Moroccan Defenders Group
- MrWanz
- Muslim Cyber Army
- Mysterious Team Bangladesh

- xNot_RespondinGx
- Pakistan Cyber Hunter
- Pakistani Leet Hackers
- Panoc team
- Royal Battler BD
- Russian tools
- Siber Team
- Siegedsec
- Skynet
- StarsX Team
- Storm-1133
- Stucx Team
- Sukowono Blackhat Team
- Sylhet Gang-SG
- Synix CyberCrimeMY
- Systemadminbd Official (BCF)
- Team Anon Force
- Team Azrael Angel of Death
- Team Herox
- The key40
- Team R70
- Team R
- Team_insane_Pakistan
- Teng Korak Cyber Crew
- The Ghost Squad
- The White Crew
- Toyonzade
- Turk Hack Team
- TYG Team
- UserSec
- VulzSec
- WeedSec
- x7root
- Yemen Legions Team
- YourAnon T13x

It also appears that some cybercriminal groups are taking sides in the war between Israel and Hamas. On October 28, the famous BlackCat ransomware group published a message on its darknet site specifying that they support the Palestinians. The group mentioned that, for the moment, they have not threatened Israel with any cyber attack (Figure 16).

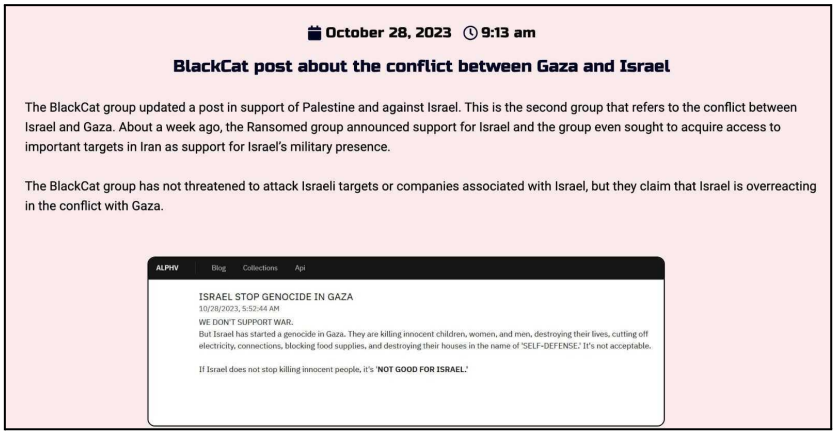


Figure 16 - BlackCat ransomware group announces support for Palestinians

3. Type of Cyber Attacks Carried Out During the War

3.1. DDoS Attacks

DDoS attacks in geopolitical conflicts are not new. Indeed, in 2007, Russia launched a series of massive DDoS attacks against Estonia's cyberinfrastructure to destabilize the government. However, the intensity with which DDoS attacks have increased in recent years is staggering. According to the security company Netscout, 2022 will have been a record for DDoS attacks. This increase is partly due to the Russian-Ukrainian conflict.

Regarding cyber operations carried out in the context of the war between Israel and Hamas, DDoS attacks are the most popular and intense. According to the company Imperva, the number of DDoS attacks mainly targeting the Israeli government and financial sites is ten times higher than the average since the attacks of October 7. At present, the DDoS attack, the most massive, took place on October 7 and targeted an Israeli government site. This attack would come from 13,000 IP addresses. Since the start of the war, numerous hacker groups and hacktivists have coordinated to launch DDoS attacks against Israeli sites. Pro-Russian hacker group KillNet has vowed to target Israeli government systems with DDoS attacks, accusing Israel of supporting Ukraine and NATO. Separately, Anonymous Sudan, another hacktivist group affiliated with KillnNet, declared its support for Palestine and claimed responsibility for an attack on the Israeli news site Jerusalem Post (Figures 17 and 18).



Figure 17 - A joint claim on Telegram by KillNet and Anonymous Sudan against Israel.



Figure 18 - Anonymous Sudan's Post on Telegram regarding the DDoS attack on the Jerusalem Post's website

One of the most prominent DDoS attacks since the beginning of the war is the Israeli Ministry of Defense, which is the top target (Figure 19).



Figure 19 - Ghost Clan target list on Telegram

On its side, the Moroccan Black Cyber Army claimed their coordination with the Indonesian actor Garnesia and other hacktivist groups to target an Israeli website (Figure 20).

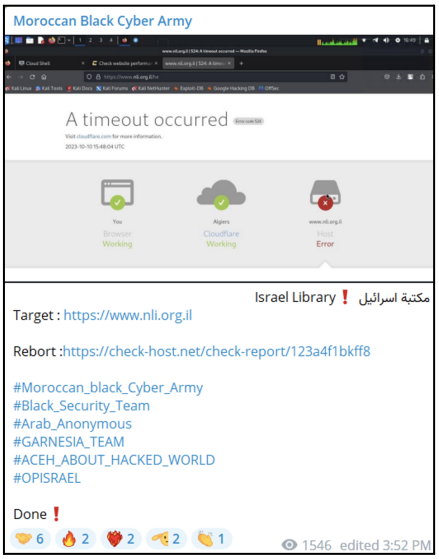


Figure 20 - Israeli website takedown claim by the Marocan Black Cyber Army

On the pro-Israeli side, the Indian Cyber claims to have taken down several Palestinian websites, including the Palestinian Ministry of Transportation and some commercial Palestinian sites (Figures 21 and 22). While some pro-Israel groups have so far launched a few DDoS attacks against Palestinian targets, their number is much lower than the attacks launched by pro-Gaza supporters, who are much more numerous.

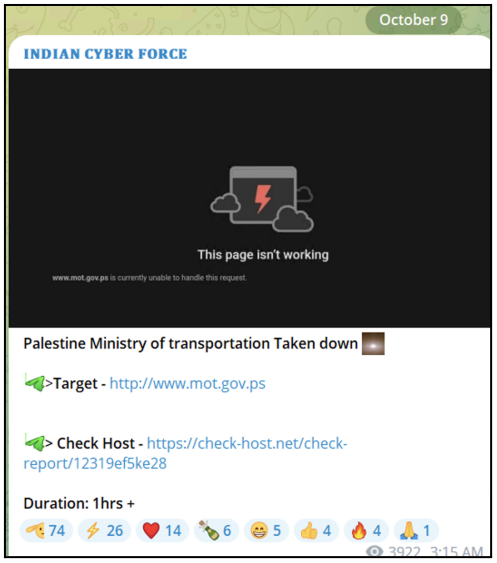


Figure 21 - Palestinian Ministry of Transportation website takedown claim by the Indian Cyber Force

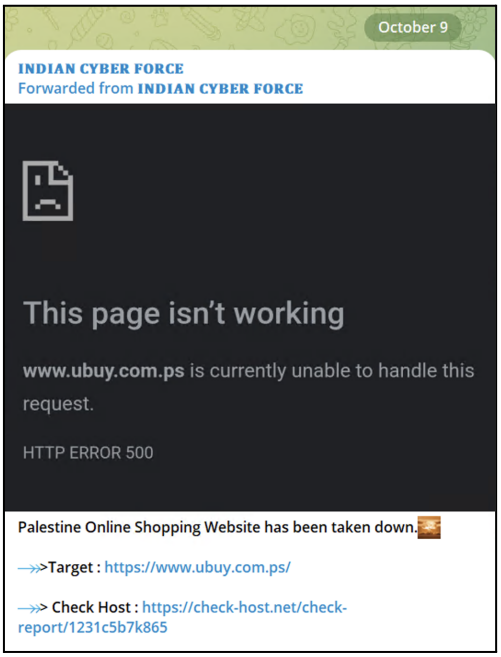


Figure 22 - Palestinian online shopping website takedown claim by the Indian Cyber Force

According to security company Radware, the most common DDoS attack vectors seen include:

- HTTPS Floods
- IPv4 UDP Floods
- IPv4 UDP-FRAG Floods
- IPv4 ICMP Floods
- ARMS floods
- Chargen Floods
- UDP Flood Port 80
- TCP FIN-ACK Flood
- DNS Amplification flood
- HTTP SYN Floods

3.2. Website Defacement

Website defacement is also one of the favorite attacks of hacktivist groups during wartime. Such an attack allows them to prove two things. First, they succeed in their attack since the website is defaced by a message. Second, they can spread their political and ideological message to the world. As with DDoS attacks, but to a lesser extent, the war between Israel and Hamas has generated attacks to deface various websites, particularly Israeli ones (Figure 23). Generally speaking, the most popular techniques in website defacement are as follows:

- Unauthorized access.
- SQL injection.
- Cross-site scripting (XSS)
- DNS hijacking.

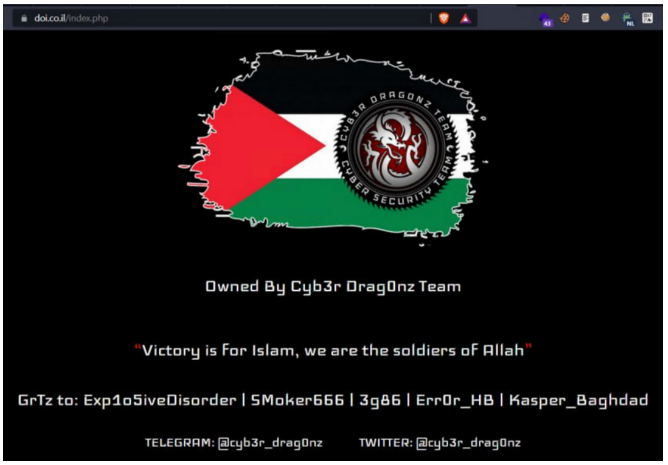


Figure 23 - An Israeli defacement claim from the Cyb3r Drag0nz Team

3.3. Network Access and Data Breach Claim

- **Databases**

  Vulnerable network access points are likely the best attack vectors for threat actors. Once they gain initial access, they can penetrate deeper into the network to search for sensitive data and other valuable assets. Threat actors usually seek personally identifiable Information (PII) and other valuable information that could be leaked or sold to other threat actors on Telegram or underground cybercriminal forums. Hackers use different techniques, including social engineering, phishing, vulnerability exploitation, and malware. Unlike DDoS or website defacement attacks, which have a limited effect over time, database hacking has a longer-term effect because the data stolen and disclosed is carefully kept and can be used long afterward. If passwords can be changed relatively quickly, the same cannot be said for stolen documents having a high value due to what they may contain. In the context of the war between Israel and Hamas, many pro-Gaza groups claim to have hacked numerous Israeli databases. The following examples illustrate some of his hacks (Figures 24, 25, 26, and 27).

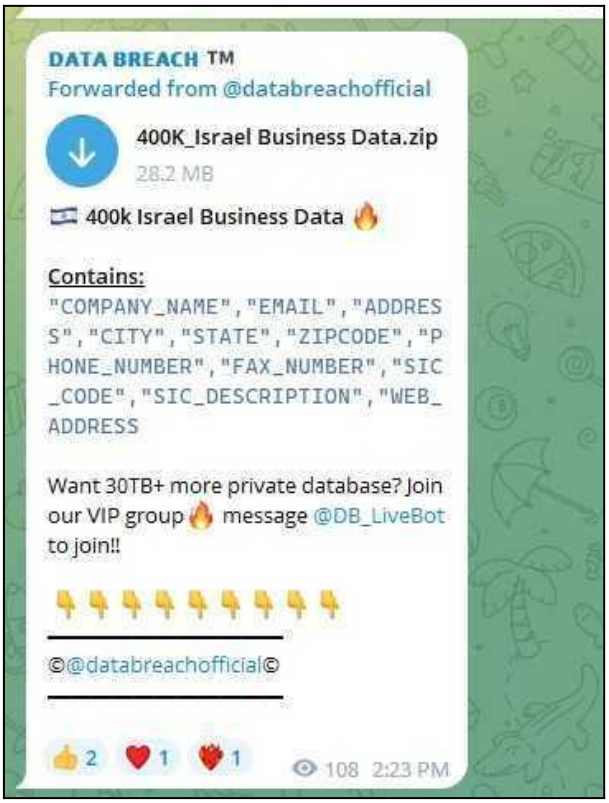


Figure 24 - 400K Israeli Business Data Leak on Telegram

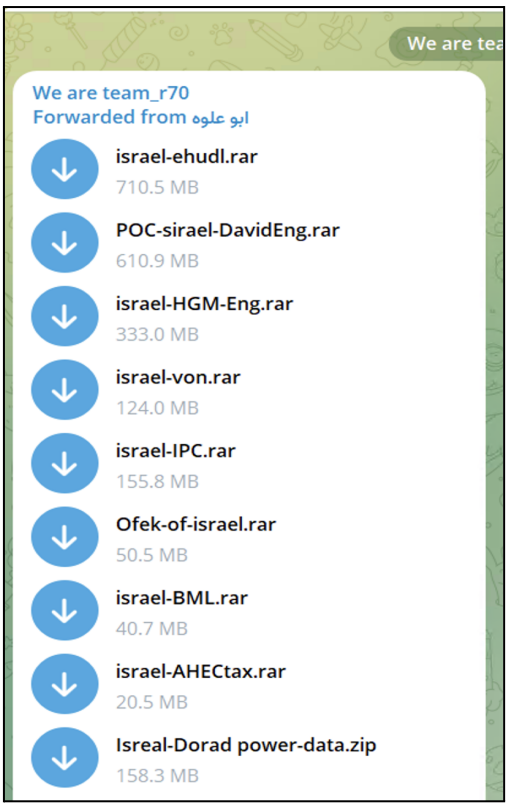


Figure 25 - Several Israeli databases leaked by the Yemenit hacktivist group team r_70



Figure 26 - Leak of ID documents from Israeli citizens from different municipalities

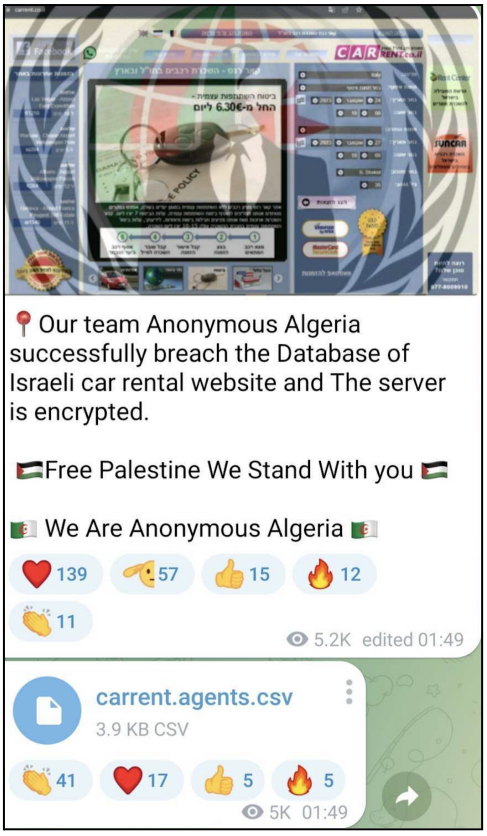


Figure 27 - Claim of the breach and database leak of Israeli car rental company by the hacktivist group Anonymous Algeria

On the pro-Israeli hacker's side, among multiple cyber attacks, they published Palestinian government databases on a cybercriminal forum and the database of a Palestinian communications company on Telegram (figures 28 and 29).

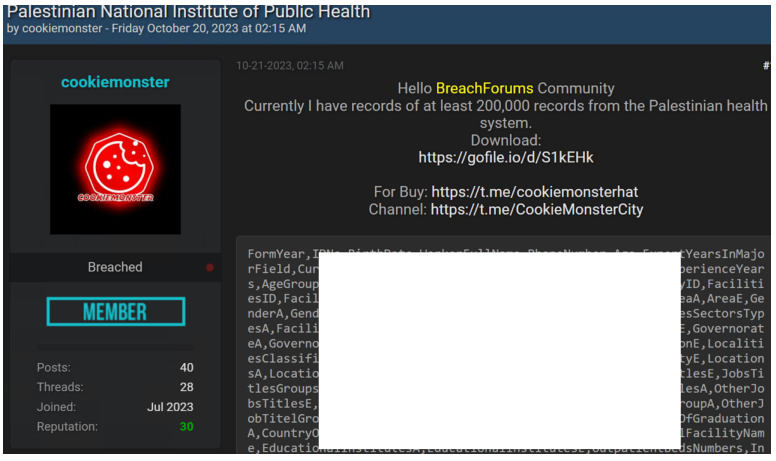


Figure 28 - Palestinian National Health Institute database for sale on a cybercrime forum

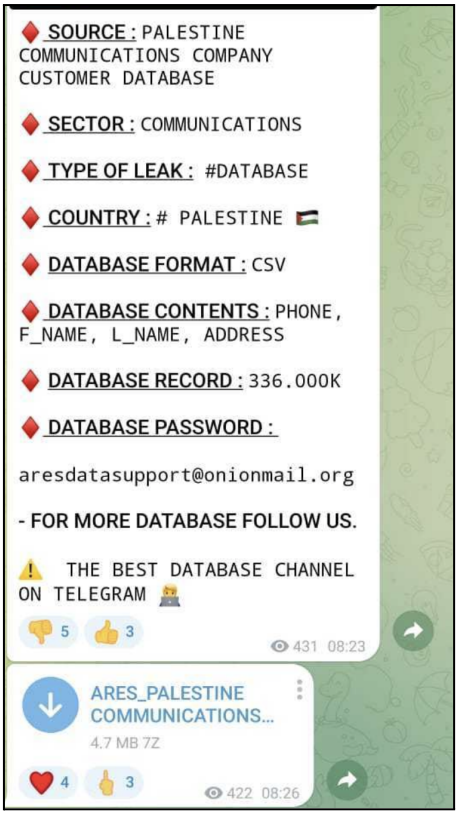


Figure 29 -A claim of a leaked database of a Palestinian communications company on Telegram

- **Surveillance Camera (CCTV)**
  Many Israeli CCTV appear to have been hacked. These video surveillance systems were probably not or poorly secure, which poses a significant risk. Hacking video surveillance to monitor strategic and sensitive locations can give a strategic advantage to the adversary (Figures 30, 31, and 32). These multiple network, system, and data violations may result from a lack of security policies and strict measures on the different networks, devices, and systems access to critical assets.

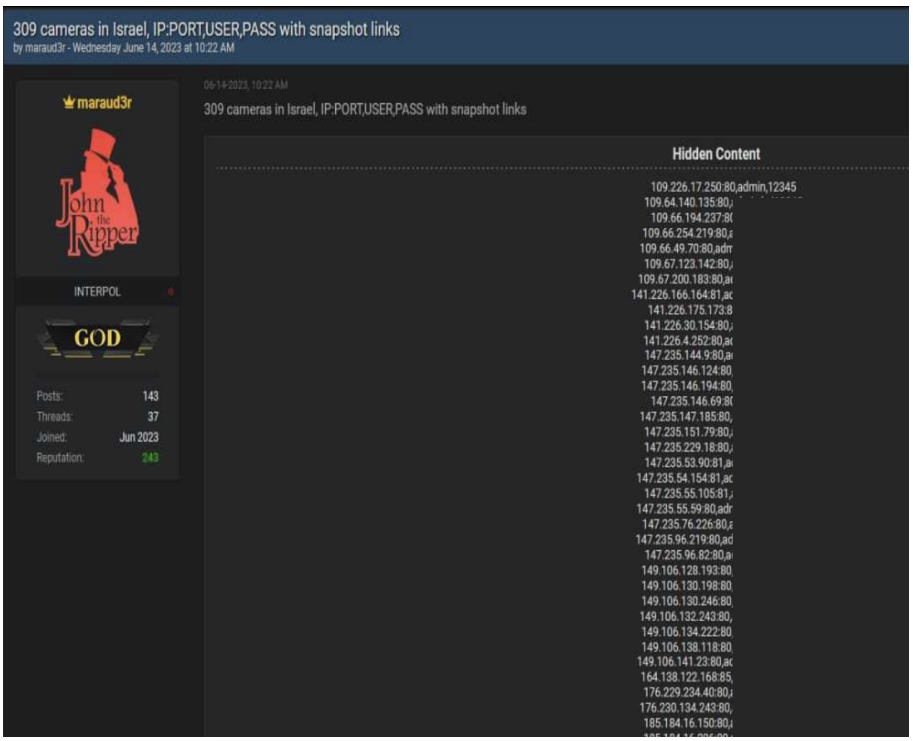


Figure 30- List of Israeli IP CCTV with users and passwords leaked on a cybercriminal forum

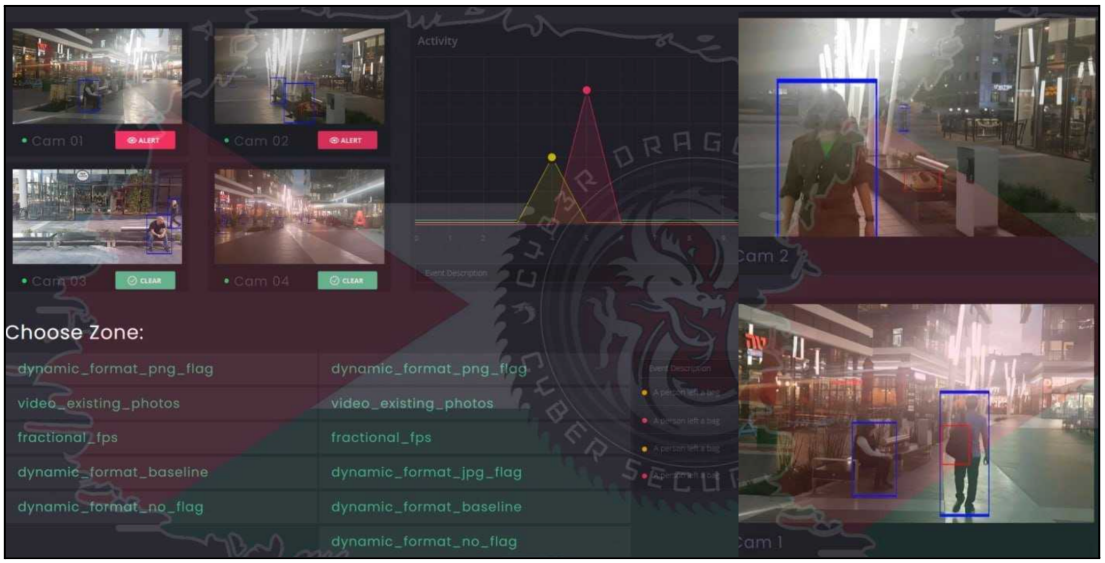


Figure 31 - Several Israeli CCTV images leaked by Cyb3r Drag0nz

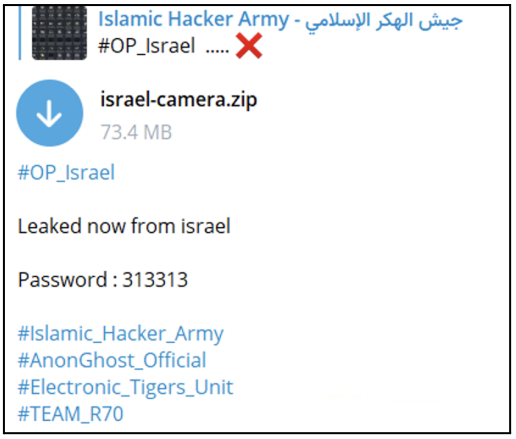


Figure 32 - Israeli camera images leaked on Telegram by the Islamic Hacker Army

- **Industrial Control Systems (ICS).**
  Industrial control systems include multiple elements, such as various sensors and devices, to manage many functions of industrial facilities remotely. They can be very vulnerable to cyberattacks if they are poorly or not protected. Generally speaking, regardless of system type, major ICS security issues include

  - Unpatched or outdated systems.
  - Insecure authentication process
  - Lack of security solutions in small and remote devices.
  - Unsecure mobile and web applications

  It has been observed that several pro-Gaza hacking groups claim to have targeted various Israeli industrial control systems by publishing screenshots. However, not all these attacks have been confirmed or verified. (Figures 33 and 34).

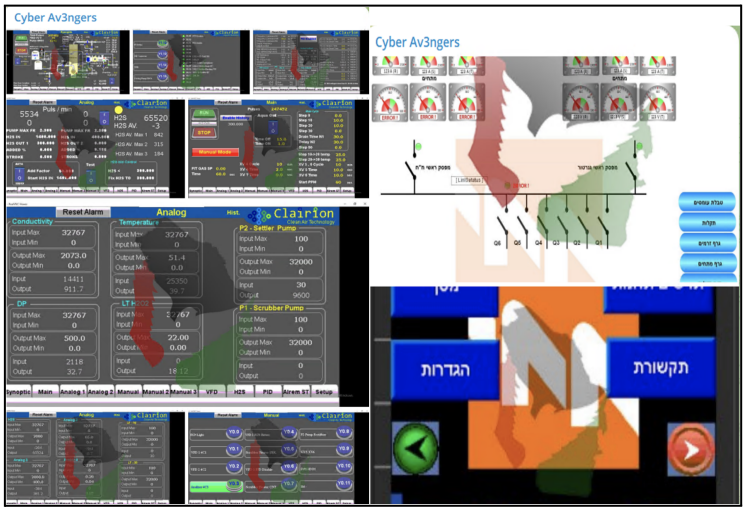


Figure 33 - Images from an Israeli SCADA system shared on Telegram by the group Cyb3r Av3ngers



Figure 34 - Unidentified Israeli SCADA system images shared on Telegram by the group Stucx

Pro-Israel hackers also claim to have targeted several industrial control systems. A group, formerly named Gaza Parking Lot Crew on Telegram, claimed responsibility for targeting an Iranian petrochemical company because Iran supports Hamas. The pro-Israeli group shared a database linked to the petrochemical company Lorestan containing approximately 1 GB of data (Figure 35).

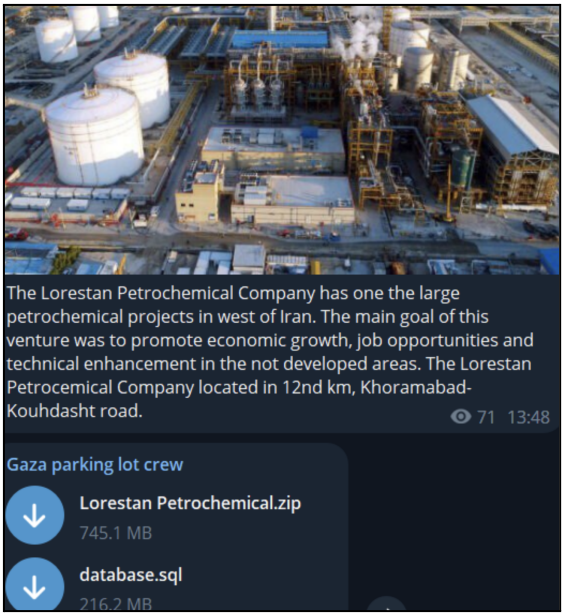


Figure 35 - A leak claim of an Iranian company data from a pro-Israel group formerly named Gaza Parking Lot Crew.

Another pro-Israel hacking group named RedEvils claimed to have managed to disable an electrical grid in Tehran for two hours. The group declared, *"In recent days, we managed to hack several sensitive systems in Iran, which we will not specify, among them the electricity grid in Tehran and the surrounding villages"* (Figure 36). Additionally, the group claimed responsibility for hacking several Iranian industrial companies related to the Revolutionary Guards in Iran (Figures 37 and 38).

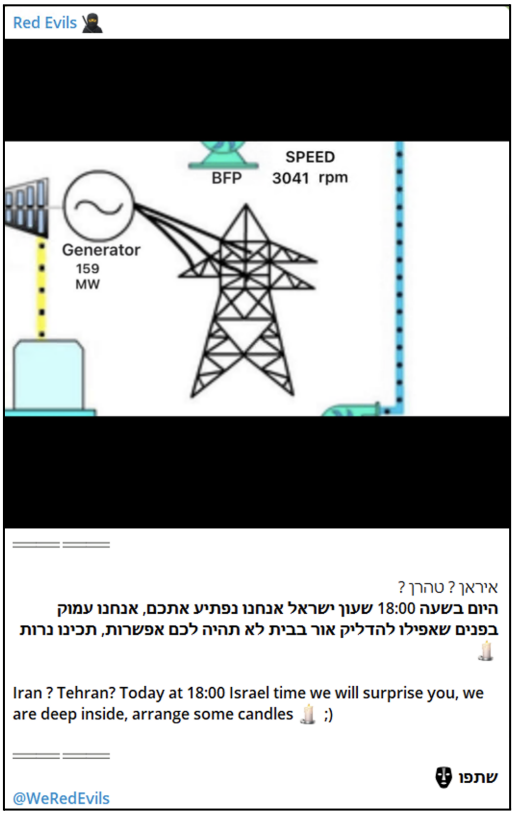


Figure 36 - A claim from the RedEvils group about taking down an Iranian power grid.

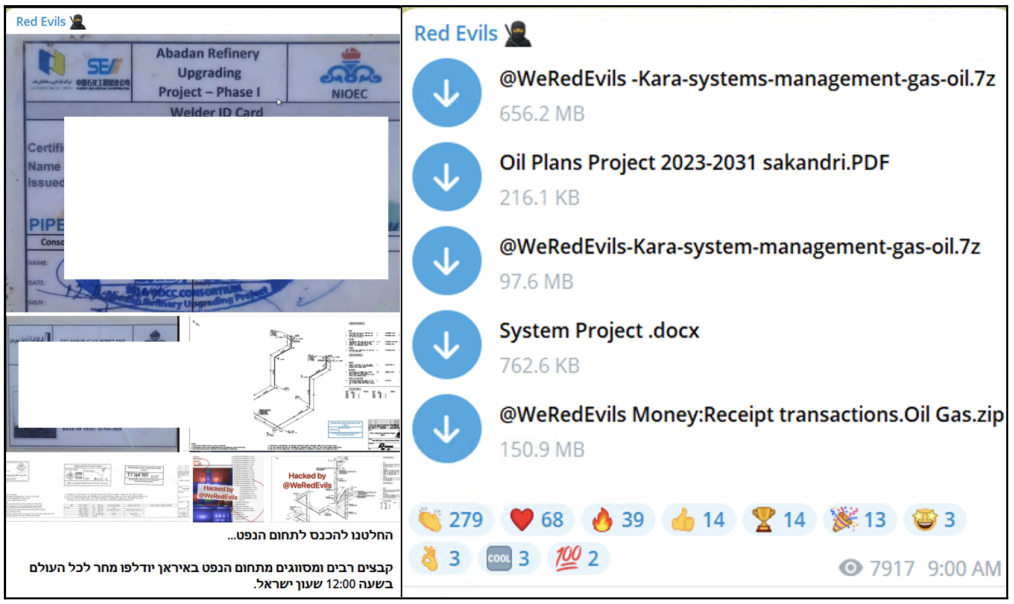


Figure 37 - Iranian documents the RedEvils group leaked from an Iranian oil company.

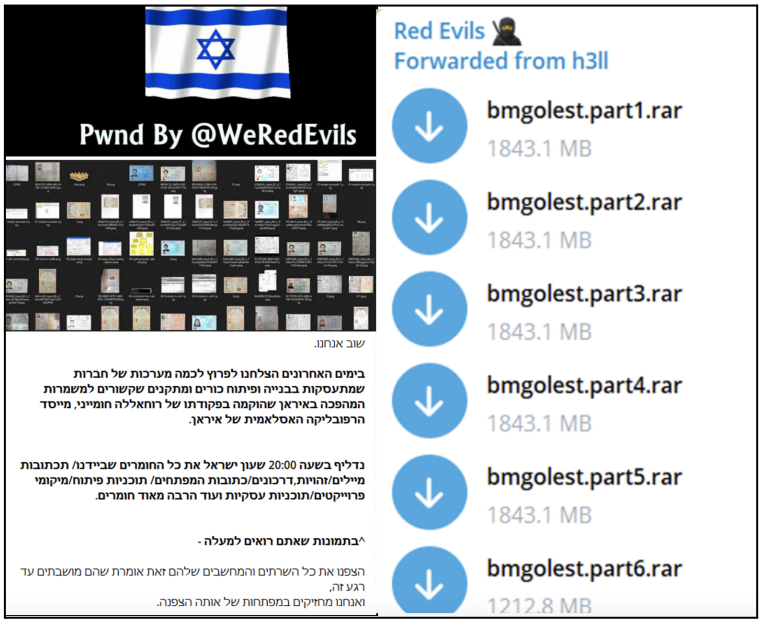


Figure 38 - Iranian documents leaked by the Red Evils group from the construction and development of reactors and facilities related to the Revolutionary Guards in Iran.

However, some groups also use the mass of information published mainly on Telegram to publish the results of old hacks and databases. This technique is well known and allows certain threat actors to increase their success. It is also not always easy to sort through this mass of information. If some of the multiple cyberattacks are significant, others are less significant but remain presented as such.

3.5. Malware Delivery

In this asymmetric warfare, cyberspace is not only used to launch direct cyberattacks against websites, databases, video surveillance systems, or control systems. Since Hamas terrorists launched their attack in southern Israel and launched thousands of rockets simultaneously, many Israelis have used the Red Alert application to get early warning of impending airstrikes in their area. RedAlert is a legitimate open-source app commonly used by Israeli citizens to receive notifications of rockets targeting the country. The application is very popular in the country, with over a million downloads on Google Play. According to protection company Cloudflare, unidentified malicious actors took advantage of increased interest in the app and fear of attacks to distribute a fake version that installed spyware (Figure 39).

This malicious version is distributed from the “redalerts[.]me” website, created on October 12, 2023, and includes two buttons to download the iOS and Android applications. The iOS download redirects a user to the legitimate project page on the Apple App Store, but the Android button directly downloads an APK file to install on the device. According to Cloudflare, the application would request additional permissions from users, including access to contacts, numbers, SMS content, list of installed software, call logs, phone IMEI, account accounts, etc., connected messaging and applications, and other information. Once the application launches, a service runs in the background and abuses these permissions to collect data, encrypt it with AES in CBC mode, and upload it to a hardcoded IP address.

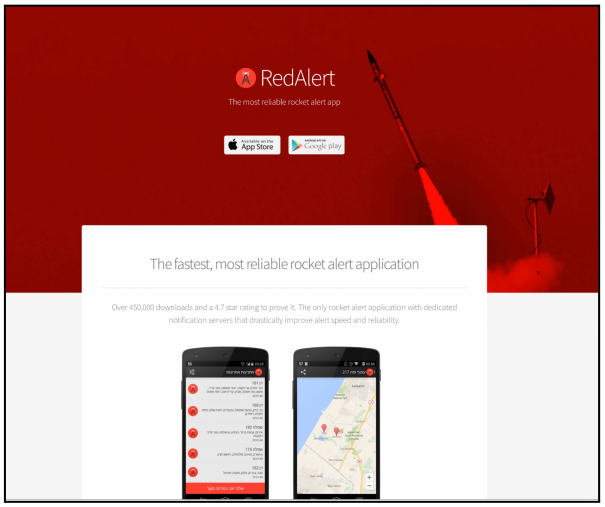


Figure 39 - The fake website used for distributing spyware redalerts[.]me (Source: Cloudflare)

This is not the first time the red alert application has been used to infect people using it. According to a cyber intelligence company Clearskky investigation in 2018, Hamas attempted to trick Israelis into downloading malware to their smartphones to take control of their devices and spy on them (Figure 40). At the time, the malware allowed the user to take control of the cell phone and the operator to track the device, receive geolocation, take photos, record sound, make phone calls, and send messages.

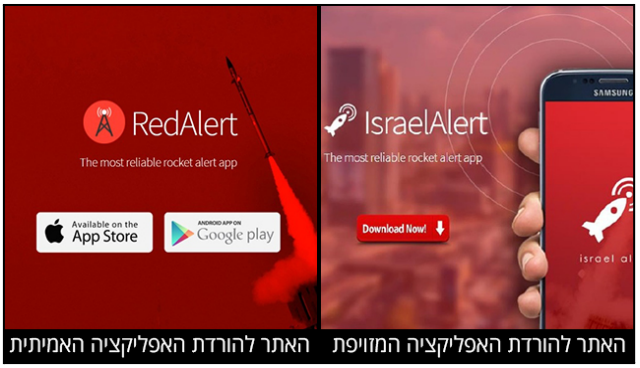


Figure 40 - On the left is the download of the official application, and on the right is the fake application launched in 2018 (Source: Clearsky).

4. Psychological Warfare and Disinformation

If this online war involves many cyberattacks, it is also a war of image, disinformation, and psychology. Since the beginning of the war, Hamas has never stopped broadcasting videos and images to demonstrate its firepower but, above all, to impact the Israeli people psychologically. Hamas has a well-established communications plan which has been implemented for years.

During the October 7 attack, Hamas terrorists wore body cameras to film their attacks. The broadcast of horrific videos and images of acts against civilians and soldiers aims to create a feeling of fear and psychologically destabilize Israel. Once broadcast, these images become viral and spread through different platforms like Telegram, Instagram, TikTok, and Snapchat. The impact of dissemination of barbaric images and videos and unspeakable violence can have a traumatic psychological impact on many people. This is also a disinformation war with specific false images or others taken out of context. Some images from Gaza have been created from scratch or taken out of context, which can have serious consequences.

5. Use of Artificial Intelligence and Face Recognition

As previously mentioned, this war is a war of images and disinformation in which generative artificial intelligence is also used. The Internet has been flooded with thousands of images of the conflict and even more rumors. However, some videos and photos broadcast on the web are fake. Two images recently published went viral (Figures 41 and 42). The first image purports to show an Israeli refugee camp illegally built on Palestinian territory. The second would represent a Palestinian baby injured during Israeli offensives. However, on the pro-Palestinian side, even if generative AI is used, it does not constitute a significant element in this war of image and disinformation. The dominant threat lies in publishing authentic images taken out of Context.



Figure 41 - Fake image released by pro-Hamas and generated with AI system



Figure 42 - Fake image released by pro-Hamas and generated with AI system.

For its part, Israel uses artificial intelligence and various facial recognition technologies to try to identify civilians kidnapped by Hamas and certain terrorists. Several groups of former experts in cyber intelligence but also in artificial intelligence, data analysis, and image recognition have been created to help the Israeli security forces and the victims' families. Through the use of AI algorithms and computer facial recognition tools, these Israeli volunteers were able to identify some of the people kidnapped by Hamas. By leveraging AI-based tools, these people help improve the efficiency of victim identification processes. Advanced algorithms in AI systems enable the analysis and recognition of missing persons by cross-referencing data from various sources, such as photographs, medical records, and descriptions.

6. Conclusion

If so far, the war between Israel and Hamas has caused many victims, it has also generated a war within cyberspace. This cyber war with an unfair number of supporters between the two parties gives rise to multiple cyberattacks, particularly against Israeli infrastructure. For several weeks, several pro-Gaza hacking groups have been targeting various Israeli government and private entities, which seem to suffer from a significant lack of security. Although not all these cyberattacks are too large, many can cause significant damage.

Israeli cyber forces are trying to manage and counter some of these cyberattacks to avoid what could seriously harm critical infrastructure and potentially prevent the country from functioning correctly. Furthermore, groups of pro-Israeli supporters have also targeted Palestinian or Iranian entities in response to these cyberattacks, but to a lesser extent. The majority of cyberattacks resulting from this war are carried out by groups of hackers and hacktivists supporting both sides rather than by Israel and Hamas themselves.

Finally, this war is also a war of images where Hamas seems comfortable with the use of body cameras and the broadcasting of terrific and shocking images to scare the Israeli population. Moreover, disinformation also plays a significant role in this war, with fake images disseminated by pro-Palestinian groups and generated by AI or taken out of context. But AI is also used by Israel to try to identify victims killed or kidnapped by Hamas. There is no doubt that this cyber war will continue as long as operations on the ground continue and will continue even after.

7. About The Author



I am a cyber intelligence expert who has worked in various environments over the past ten years, including academia, high-tech, military, and law enforcement. My field of expertise is cyber intelligence, including strategy, collection, research, and analysis, and the lead of Cyber HUMINT operations on criminal and terrorist activities within cyberspace. I have trained many civilian analysts and Military and Law Enforcement officers on the Deep and Dark Web environments, Cyber intelligence collection, and Cyber HUMINT operations.

8. References

1. Recorded Future Insikt Group, Hamas Application Infrastructure Reveals Possible Overlap With TAG-63 and Iranian Threat Activity, October 2023. https://www.recordedfuture.com/hamas-application-infrastructure-reveals-possible-overlap-tag-63-iranian-threat-activity

2. Imperva, DDoS Attacks Leveraged by Attackers in Israel Conflict, October 2023. https://www.imperva.com/blog/attackers-use-ddos-in-israel-conflict/

3. Bleeping Computer, Fake 'RedAlert' rocket alert app for Israel installs Android spyware. https://www.bleepingcomputer.com/news/security/fake-redalert-rocket-alert-app-for-israel-installs-android-spyware/

4. Ynet news, Hamas launches fake app to hack Israeli cell phones, 2018. https://www.ynetnews.com/articles/0,7340,L-5326309,00.html

5. Cyberscoop, AJ VICENS, Cyber operations linked to Israel-Hamas fighting gain momentum, October 2023. https://cyberscoop.com/cyber-israel-hamas-gaza/

6. Soc Radar, Reflections of the Israel-Palestine Conflict on the Cyber World, October 2023. https://socradar.io/reflections-of-the-israel-palestine-conflict-on-the-cyber-world/

7. Ezzedeen Al-Qassam Brigades website https://en.alqassam.ps

8. The cyber strategy and operations of Hamas: Green flags and green hats, Simon Handler, 2022 https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats/

9. Forbes, Israel Hospital Uses Facial Recognition To Identify Dead And Wounded From Hamas War, October 2023 https://www.forbes.com/sites/thomasbrewster/2023/10/11/hospital-uses-facial-recognition-to-identify-israel-hamas-war-dead/?sh=1f8e17370120

10. Euronews, Israel-Hamas War: This viral image of a baby trapped under rubble turned out to be fake, October 2023, https://www.euronews.com/my-europe/2023/10/24/israel-hamas-war-this-viral-image-of-a-baby-trapped-under-rubble-turned-out-to-be-fake

11. X Social network page of CyberKnow.
https://twitter.com/Cyberknow20

12. X social network page of FalconFeeds.io
https://twitter.com/FalconFeedsio