FORMS OF THE ISRAEL-HAMAS CONFLICT IN CYBERSPACE

Situational Report

03.11.2023

CERT-OWN

Version 1.1

TLP:GREEN
PAP:GREEN

TABLE OF **CONTENTS**

EXECUTIVE SUMMARY

As part of its activities, OWN-CERT has summarized the key elements identified in the transposition of the Israeli-Palestinian conflict into cyberspace. While not intended to be exhaustive, this study presents the main threats identified in terms of hacktivism, disinformation, and advanced persistent threats. OWN also offers operational recommendations for companies.

KEY FINDINGS

- In September 2023, the Hamas-linked APT group AridViper targeted Palestinian entities.
- Real life alliances apply in cyberspace. Hacktivists taking parti in the conflict on both sides are mostly launching DDoS attacks and sharing tips and tools to facilitate attacks.
- The Hamas attack on the 7th of October resulted in a "flood" of contents with accounts openly relaying disinformation, and among these accounts some specialized in conspiracy theories increase the volume of fake news currently flooding social media.

ANALYST'S ASSESSMENTS

- We assess with high confidence that the cyber activity affecting Israel and Palestine is, so far, mostly superficial, even if we will need time to assess the overall activity related to the conflict.
- We assess with medium confidence that while the actual involvement of MOIS- and IRGC-affiliated APTs is unknown, current political events, which may be perceived as provocative by Iran, could lead to the deployment of reconnaissance campaigns on Israeli military systems and cyber-attacks. Especially after the speech of the Lebanese Hezbollah leader Sayyed Hassan Nasrallah on Friday 3rd.

CONTEXT

On October 7th, 2023, the Izz ad-Din al-Qassam Brigades, the Gazan militia linked to Hamas, launched an Air, Land and Sea operation called "Deluge of al-Aqsa» (طوفان_الأقصى) while launching missiles on Israel, killing civilians and military personnel, and taking more than two hundred hostages. In reaction, Israel launched the operation "Iron Swords", took back all of Hamas positions in Israeli territory and has been bombing Gaza ever since, killing civilians and military personnel.

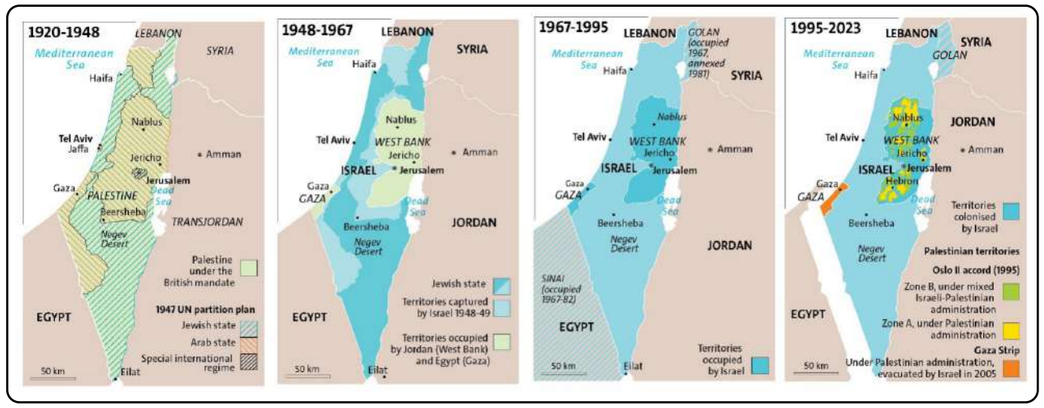


Figure 1 : Maps published by Le Monde diplomatique in October 2023.

THE CONFLICT

This conflict rooted in a historical context (increase of Israeli settlements in the West Bank despite the frontiers of 1967 and the government discourse causing strong resentment among the Palestinian population) is a trigger for the deployment of cyber capabilities, both in terms of hacktivism and advanced threats[1].

The conflict transposed in cyberspace with the mobilization of a wide range of actors in support of one side or the other.

- Hacktivists affiliated to the Anonymous movement are supporting both sides.
- Muslim hackers from Pakistan, Malaysia, Bangladesh[2] and Indonesia are targeting Israeli infrastructure and institutions websites in support of Palestine.
- Hacktivists a priori linked to Hamas are targeting Israeli infrastructure and institutions websites in support of Palestine.
- Indian hacktivists are targeting Palestinian infrastructure and institutions websites in support of Israel.

1. https://www.reuters.com/world/middle-east/israel-advances-peak-number-west-bank-settlement-plans-2023-watchdog-2023-07-13/ ; https://www.reuters.com/world/middle-east/palestinians-fear-growing-violence-israeli-settlements-expand-2023-06-15/ ; https://www.reuters.com/world/middle-east/israels-supreme-court-dismisses-petition-remove-west-bank-settlement-2023-08-03/ ; https://mondediplo.com/maps/palestine-four-maps

2. hxxps://t[.]me/s/bcfOfficialTelegramChannel

The overall identified targets belong to the following sectors:

- Energy
- Government
- Defense
- Transportation
- Media[3]

Most of the DDoS and defacement attacks set their targets on the basis of websites TLDs (in this case .IL) and thus hit any vulnerable websites as long as it is bears the .IL TLD.

Our research found that the cyber activity related to this region started in fact earlier than October 7th.

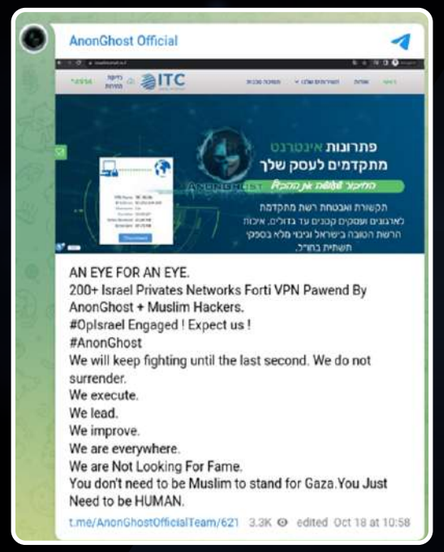


Figure 2 : hxxps://t.me/AnonGhostOfficialTeam/621

HAMAS

Created in 1987, Hamas is a Palestinian nationalist movement with an armed wing. Hamas considers itself as a resistance party against Israel - its very name "Hamas" is the acronym for "Islamic Resistance Movement" in Arabic – but both the party and its militia, the Izz ad-Din al-Qassam Brigades, were added on the terrorist groups list by the United States and the European Union (EU). The APT intrusion set associated with or attributed to Hamas is AridViper.

AN EARLY EFFERVESCENCE

Two types of activities were identified during September 2023 that can provide cyber context and shed light on last month's cyber activity related to the conflict: a hacktivist nuisance operation, and a malware infection launched by an Intrusion Set linked to Hamas and Iran.

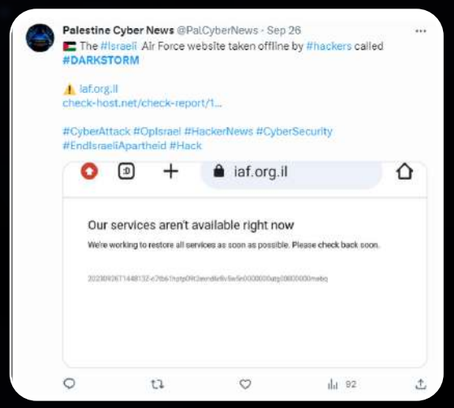
AN OPISRAEL WAS LAUNCHED PRIOR TO THE HAMAS ATTACK

Most hacktivist groups have been already engaged in an OpIsrael that was launched as early as September 2023.

Several accounts, including pro-Israeli accounts (see above), were created in September 2023. It seems as if an underlying activity started before the launch of the Hamas operation. For instance, the September OpIsrael was announced by the account @PatrickByrne and followed by @YourAnonTl3x.

3. *hxxps://twitter[.]com/all_israel_news/status/1713867195019559041*

As another example, on September 26th, 2023, the online media Palestine Cyber News attributed a DDoS attack on the Israeli Air Force website to a hacktivist group named DarkStorm.



Israel has experienced several OpIsrael campaigns through the years, and there is a constant low activity linked with the 75-year-old conflict. The OpIsrael campaign launched in September was probably part of a retaliation operation in reaction to an Israeli measure.

The campaign very likely continued after October 7th and Palestinian hackers even renamed the campaign #OpIsrahell[4].

Figure 3 : YourAnonT13x operation against Israeli governement websites on September 30th, 2023 and start of an #OpIsrael campaign on September 30th. Source : OWN-CERT.

4. *https://twitter.com/FalconFeedsio/status/1711033041827828087 ; https://twitter.com/DailyDarkWeb/status/1712521009654542470*

AN ARIDVIPER CAMPAIGN DISTRIBUTING MICROPSIA IN SEPTEMBER 2023

AridViper is an Intrusion Set attributed to Hamas, also known as: APT C-23, MoleRATs, Gaza Cyber Gang or Desert Falcon. The cybersecurity editor RecordedFuture found links between the Palestinian intrusion set AridViper and the Iranian Revolution Guards Corps (IRGC)[5]. OWN-CERT detected three files linked to AridViper uploaded on VirusTotal indicating that the group attempted to distribute malware in September 2023, prior to the al-Aqsa Flood operation[6].

FILENAME	SHA256
Palestinian heritage - what it is and what its forms are docx.ex	fa98139b94cc56890af27e6dd02deb4da64b930e-801492a966e0f13103808e2f
WindowsMediaProvisioningPlugin.exe WindowsMediaProvisioningPlugin.exe	af87a91c71b3cca1184b4b1250cacec041430264d0f8ac56b-de3a6b1173e84a2
ConsentUXUserServiceManager.exe	c1c5c4153fea7871e735cabaffaf64722235a374b890017ff-be2074ac0b11fe1

INFECTION CHAIN N°1

"Palestinian heritage - what it is and what its forms are docx.exe" uses the masquerading technique of double file extension (T1036.007). The program uses the domain porthopeminorhockey[.]net (created on June 14th, 2023) as a C2 server.

However, the domain has been inactive since the end of September 2023.

INFECTION CHAIN N°2

The executable « WindowsMediaProvisioningPlugin.exe » is masquerading as a Windows legitimate file (T1036.005) and relies on the domain izocraft[.]com for its C2 communications.

INFECTION CHAIN N°3

The executable « ConsentUXUserServiceManager.exe » (SHA256: c1c5c4153fea7871e735cabaffaf64722235a374b890017ffbe2074ac0b11fe1) is masquerading as a Windows legitimate file (T1036.005) and relies on the domain delooyp[.]com for its C2 communications.

PIVOTS

At the time of writing, the domain izocraft[.]com resolves to the IP address 91.199.147[.]84, as do two other doains:

- wellnesthealth[.]xyz
- iptvorange[.]store

One of these two domains, wellnesthealth[.]xyz shares the same SSL certificate with izocraft[.]com, already mentioned above as an AridViper C2 server.

For now, there is no activity allowing to assert that the domain wellnesthealth[.]xyz is used for malicious ends however CERT OWN is monitoring this domain.

It is difficult to say if the activity was meant to prepare the October attack or if it was a separate operation.

5. https://www.recordedfuture.com/hamas-application-infrastructure-reveals-possible-overlap-tag-63-iranian-threat-activity

6. The SaaS editor Sekoia.io published an extensive paper about the same campaign.

HACKTIVISMS : MULTINATIONAL TASKFORCES

This section does not aim at listing exhaustively all hacktivists taking part in the cyber war field; lists are being updated by fellow researchers and there is no need for us to redundantly publish another list[7].

However, our work is meant to carefully analyze the online activity in the light of the geopolitical context. It also aims at making a contribution to Figure 4 the existing analyses on the subject[8].

First of all, most of hacktivist's groups such as Ghost of Palestine[9], Arab Anonymous Team[10] and AnonGhost[11] declared they were supporting Palestine and not Hamas. These statements infer that the pro-Palestine groups consider their operations are in line with past operation instead of considering they support Hamas. In fact, groups mentioning the operation "al-Aqsa Flood" are in the minority[12].

Figure 4 : Message in support of Gaza. Source: Telegram, OWN-CERT.

MOST PRO-ISRAEL HACKTIVISTS ARE ... INDIAN

Pro-Israeli hacktivists groups are mostly composed of Indian hackers siding with Israel. This is not surprising since Indian far-right Bharatiya Janata Party (BJP) government tolerates hate crimes against Indian Muslims and is carrying out Islamophobic measures[13].

Indian pro-Israeli hackers targeted Palestinian government websites such as ministries' websites (Energy, Agriculture, Transport) and infrastructures such as schools, universities, hospitals, and power generators with DDoS attacks[14]. Groups like the INDIAN CYBER FORCE, Garuna Ops (@garunaops sur X) and SilentOne (@S1L3NT_0N3 sur X) are among the most active.

7. https://socradar.io/reflections-of-the-israel-palestine-conflict-on-the-cyber-world/

8. https://blog.checkpoint.com/security/evolving-cyber-dynamics-amidst-the-israel-hamas-conflict/

9. hxxps://t[.]me/s/GHOSTPalestine

10. hxxps://t[.]me/ArabAnonForce/567

11. hxxps://t[.]me/AnonGhostOfficialTeam

12. hxxps://t[.]me/s/abdalghnyWA1

13. https://www.hrw.org/news/2022/10/07/india-surge-summary-punishments-muslims ; https://www.amnesty.nl/actueel/india-hate-crimes-against-muslims-and-rising-islamophobia-must-be-condemned ; https://time.com/6320003/india-weaponizing-history-against-muslims/

14. hxxps://t[.]me/Indian_Cyber_Force_Official/96 ; hxxps://twitter[.]com/S1L3NT_0N3/status/1716690594205167803; hxxps://twitter[.]com/garunaops/status/1712175717650411879

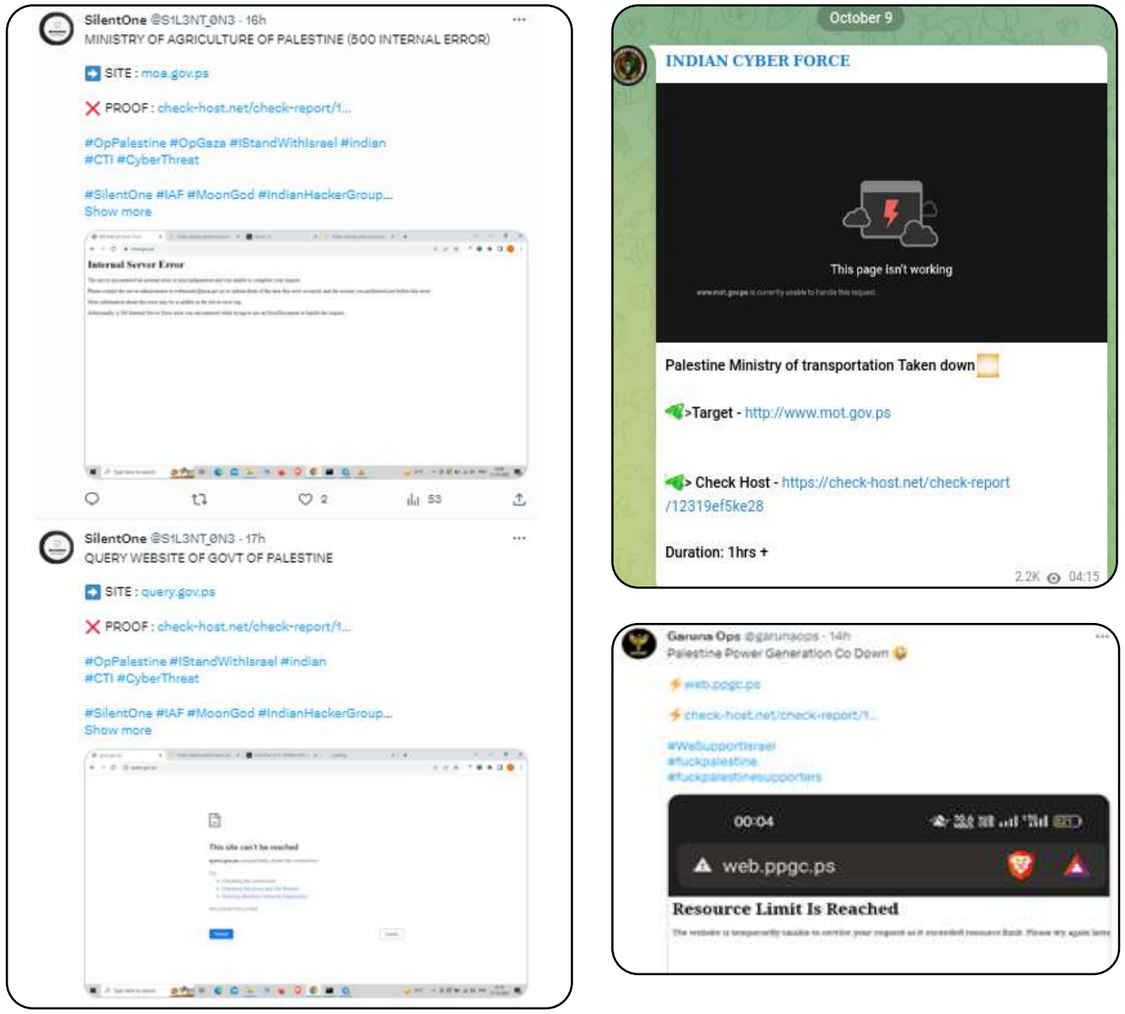


Figure 5 : Examples of attacks targeting Palestinian ministries and infrastructure. Source : Telegram, Twitter, CERT OWN.

CERT OWN noticed that several accounts were recently created. For example, Garuna Ops (@garunaops) was created on September 1st, 2023, and only has 441 subscribers at the time of writing, and the personal account (@garunaxd) only has 17 subscribers[15]. SilentOne (@S1L3NT_0N3), another Indian hacker, created its X account in September 2023 and has only 5 followers on October 26th, which indicates the account did not gain any visibility despite being very active. The Cyber Indian Army channel, in comparison, has 3.24K subscribers. Indian hackers not only targeted Palestine but also their usual targets Bangladeshi, Indonesian, and Pakistani websites, to "punish" them for siding with Palestine[16].

The Telegram channel Termux Israel (@termuxisrael2) seems to be managed by an Israeli operator and seems to share information related to cyber. This account is followed by 24.1K subscribers, which is rather significant. What is notable about this account is that it not only disseminates information about cyber-attacks targeting Palestine or Iran[17], but its operator claimed to be in contact with the ransomedvc ransomware controversial operators[18].

15. *hxxps://t[.]me/garunaxd*

16. *hxxps://t[.]me/Indian_Cyber_Force_Official/114 ; hxxps://twitter[.]com/S1L3NT_0N3/status/1717490193442488367 ; hxxps://twitter[.]com/S1L3NT_0N3/status/1716366540709515547; hxxps://twitter[.]com/garunaops/status/1711762673527099461*

17. *hxxps://t[.]me/termuxisrael2/1647*

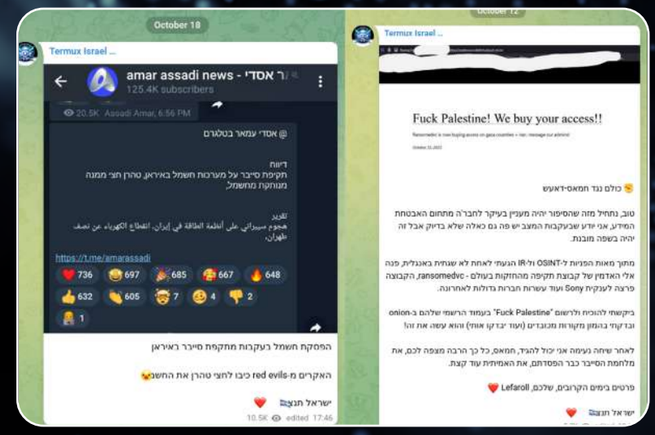


Figure 6 : @termuxisrael2 posts. On the left, the account shares a piece of news about Iran power plant being hit ; on the right a post in which the author claims to be in contact with ransomware operators. Source: Telegram, OWN-CERT.

Another Israeli Telegram account observed with more than 20K subscribers, @CyberSecurityIL, is specialised in cyber news. The channel tackles a wide range of cyber news, not only the ones related to the conflict. The operator uses the channel to convey some cybersecurity pieces of advice. For example, he/she warns the subscribers about phishing attacks that are leveraging themes

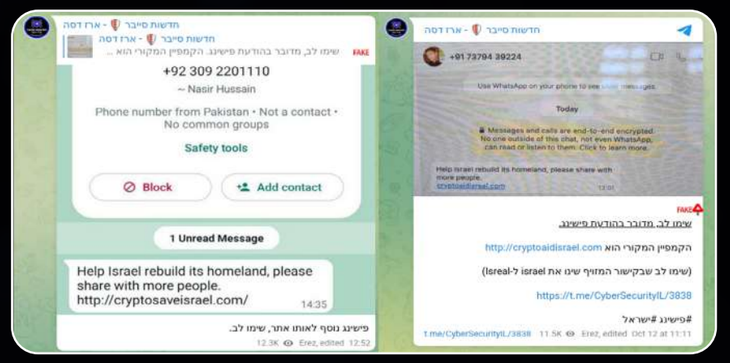


Figure 7 : Phishing attacks leveraging the war reported by @CyberSecurityIL. Source : Telegram, OWN-CERT.

18. *hxxps://t[.]me/termuxisrael2/1639*

19. *hxxps://t[.]me/CyberSecurityIL/3838 ; hxxps://t[.]me/CyberSecurityIL/3843*

PRO-PALESTINE HACKTIVISTS: TRYING HARD TO WEIGH IN THE CYBER BALANCE

SHARED TOOLS AND TECHNIQUES

Publications on Telegram channels related to the current conflict not only share recent compromises but also tools and techniques to hack Israeli websites.

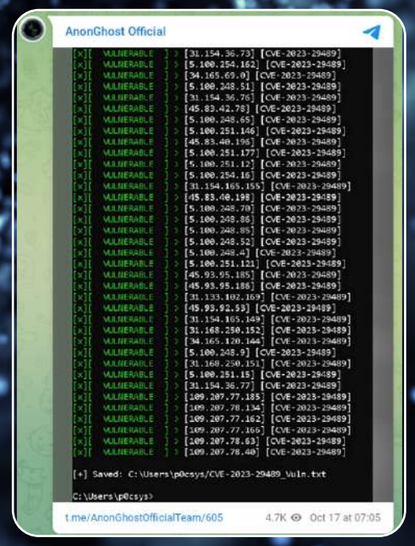


Figure 8 : AnonGhost screenshot displaying vulnerable servers. Source : OWN-CERT.

AnonGhost, one of the oldest groups monitored, publicly posted **two files:** a .TXT file and a Python file explaining the **exploitation** of the XSS (cross-site scripting) vulnerability referenced under **CVE-2023-29489** suggesting hacktivists could exploit it to target Israeli entities[20]. The group even posted a screenshot showing vulnerable servers[21].

The CVE-2023-29489 vulnerability affects cPanel versions prior to 11.109.9999.116. This vulnerability was transmitted to the editor by Assetnote on January 23rd, 2023, and was published on April 7th by MITRE and on April 27th by NIST.

The vulnerable software is a widely used configuration panel that manages websites hosting.

In order to exploit the flaw, the user must be using cPanel in its default configuration. In this case, the attacker can access and take control of web servers ports using cPanel and execute arbitrary code to steal data, download malware or alter websites hosted by cPanel. In its April 26th report, Assetnote disclosed the vulnerability could be exploited on cPanel management ports (2080,2082,2033,2086) regardless of whether or not they are externally exposed. In other words, any website on ports 80 and 443 is vulnerable if managed by cPanel.

Considering several PoCs (proof of concept) are available, and hacktivists share tips on their Telegram channels, the

Figure 9 : Screenshot of Arab Anonymous Team Telegram post sharing DDoS code in python allowinf easy attacks against websites. Source : OWN-CERT, Telegram.

20. hxxps://t[.]me/AnonGhostOfficialTeam/608 ; hxxps://t[.]me/AnonGhostOfficialTeam/606

21. hxxps://t[.]me/AnonGhostOfficialTeam/605

CVE-2023-29489 is all the easier to exploit even by inexperienced hackers, called script kiddies. It is very likely that AnonGhost posted about this vulnerability to urge hackers to participate in the effort against Israeli and pro-Israeli entities.

Another example of tips shared across Telegram channels is a python code to allegedly carry out DDoS attacks. Again, groups are inciting other hackers to take action. On October 10th, Arab Anonymous Team (@ArabAnonForce) shared codes in python, one to DDoS websites and the other to obtain the websites' servers IP addresses[22]. Both codes were first posted in September 2023 by another account: @abdalghnyWA1[23].

Readers should bear in mind that the means available to the pro-Palestinian cyber retaliation are mostly in the image on the Palestinians real-life resources: they do what they can with what they have.

OWN-CERT found several small Telegram channels trying to conduct attacks against Israeli websites. For example, the account @dd_os1 "هجوم على مواقع إسرائيلية" ("attack on Israeli websites"), calls for daily attacks on Israeli websites at 8 p.m. The group, which was followed by 219 subscribers at the time of writing, shared a VPN application that automatically launches DDoS attacks[24].

Figure 10 : @dd_os1 shares the VPN application to launch DDoS attacks. Source : Telegram, OWN-CERT.

However, OWN-CERT teams noticed that the chosen target inn.co[.]il is protected behind Cloudflare. The "attack" expectedly failed as shown in the screenshot below. The author suggested that too few members took part in the attack, but it is highly likely they hit the Cloudflare IP address instead of the website's. Regardless of the number of participants or the volume of the attack, this operation could not be successful. This illustrates the low skill level of (pro-)Palestinians cyber hacktivists.

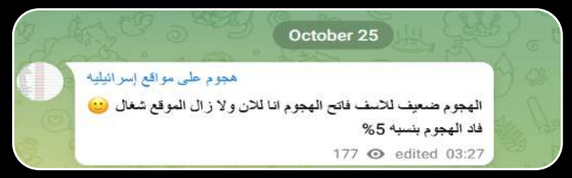


Figure 11 : @dd_os1 asks participants to stop the attack as the website is still up. Source: Telegram, OWN-CERT.

HITS AGAINST ISRAELI ENTITIES: REAL HACKS AND FAKE NEWS

As the DDoS operation described above shows, most of the websites targeted are common, vulnerable websites. Hacktivists carried out attacks against many websites, mostly common websites, but also websites belonging to Israeli's Energy, Government, Defense, Transportation and Media sectors. Attacks against the latter were especially wielded by hacktivists, whether they were successful, unsuccessful... or even fake.

On October 9th, the hacktivist group Team Azrael of Death (@Team_Azrael) announced on its Telegram channel that they compromised the Israeli ministry of Defense website's interface for discharged soldiers, hachvana.mod.gov[.]il[25]. In fact, it seems the group used stolen credentials to access a private account on the platform. There is no proof the group used this access to compromise the platform in any way. We can only assume Team Azrael of Death achieved to collect credentials either through phishing campaigns or by accessing (buying?) previous data leaks. The group indicated this operation was carried out as part of the OpIsrael international operation.

Another notable attack that got a larger media coverage was the compromise of the Red Alert application (by Kobi Snir) by the Palestinian hacktivists group AnonGhost. The vulnerable application - which has since been removed from Google App store – was used by Israeli forces to warn their population of missile launches. AnonGhost operators managed to compromise the application and use it to send a fake nuclear

22. hxxps://t[.]me/ArabAnonForce/548?single ; hxxps://t[.]me/ArabAnonForce/549?single

23. hxxps://t[.]me/abdalghnyWA1/3133

24. hxxps://t[.]me/dd_os1/1266

25. hxxps://twitter[.]com/Team_Azrael/status/1711489461320851906

strike warning, suggesting Israel was under nuclear attack. After this compromise, the group claimed it also compromised two other rocket alert applications also called "Red Alert" (RedAlert by Ela Nava and Red Alert by Cumta), but these claims could not be confirmed.

This same Threat Actor published on its Telegram channel a list of IP addresses suggesting that they belonged to Israeli's Iron Dome infrastructure (the Israeli anti-missile defense system) . This list was reposted by other groups such as the Bangladesh Civil Force.

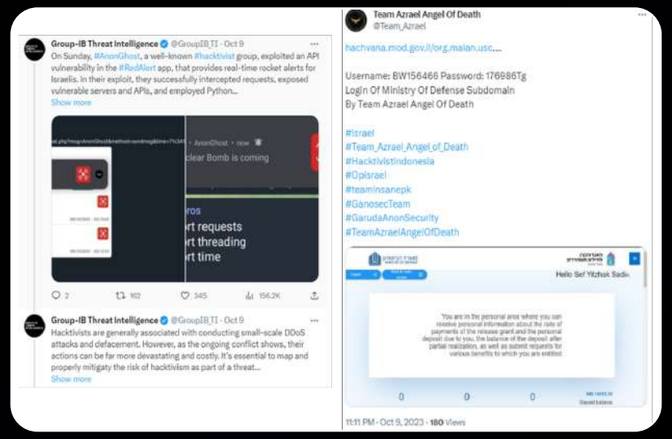


Figure 12 : Screenshot of a post about the RedAlert compromise by Group-IB and the account compromise by Team Azrael Angel of Death. Source: Group-IB, OWN-CERT.

AnonGhost also published two URLS linking to a **data leak** attributed to the Intrusion Set Storm-1133 and concerning the Israeli MoD:

- hxxps://pixeldrain[.]com/u/qBEdrdd1
- hxxps://files.catbox[.]moe/ctcevx.rar

Storm-1133 was identified as a Hamas-linked Intrusion Set by Microsoft at the beginning of 2023. This Intrusion Set is believed to be (logically enough) specializing in the targeting of the Israeli defense sector[27].

OWN-CERT observed on several forums such as BreachForums, DoxBin and XSS that other actors have been sharing leaks on both sides. According to the posts, the leaked data was stolen from hacked local companies, although a few accounts claim to have collected data of Israel government agents.

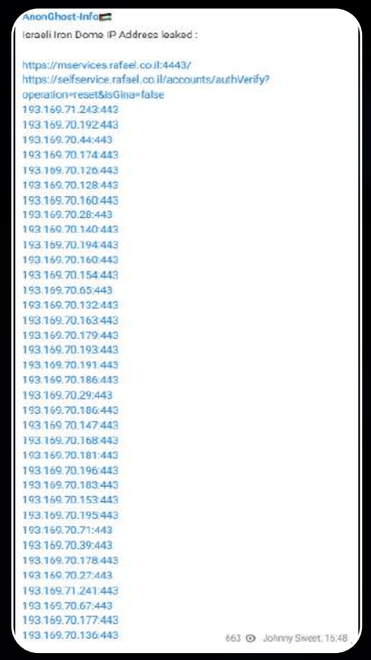
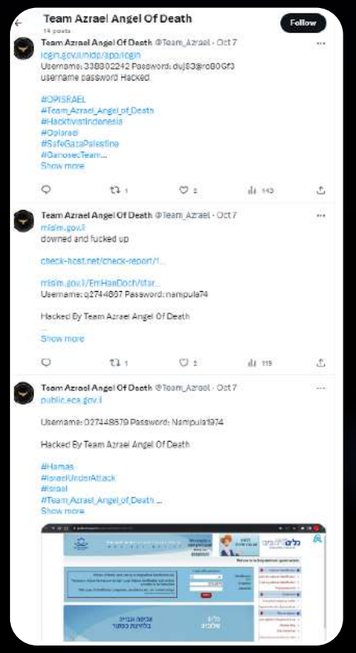


Figure 13 : Screenshot of the IP addresses list published by AnonGhost. Source : OWN-CERT.

26. *hxxps://t[.]me/s/anonghostinfo*

27. *hxxps://thehackernews[.]com/2023/10/gaza-linked-cyber-threat-actor-targets.html*

Government websites were also affected by the hacktivists' campaigns. For example, the Israeli aerospace agency was DDoSed by YourAnonT12x (@YourAnonTI3x) and Team Azrael of Death (@Team_Azrael) downed several government websites and used stolen credentials to compromise users accounts.



Pro-Palestine hacktivists also targeted India after Indian cyber hacktivists sided with Israel and started hitting Palestinian institutions websites with DDoS attacks[28].

Figure 14 : Left - @Team_Azrael focuses on government websites. Right - : YourAnonT12x (@YourAnonTI3x) hits the Israeli Aerospace Agency. Source : Twitter, Telegram, OWN-CERT.

OWN-CERT considers these posts as a communication campaign for a few reasons. First, the hacktivists' posts appear as advertisements for their own capabilities. Second, it is as if hacktivists wanted to display an attack range longer than their actual reach.

Furthermore, some hacktivists disseminate fake news to make believe that they are in capacity to hit Israel badly. The example of the group Cyber Av3ngers is quite interesting. The group edited and posted screenshots of an old hack to trick the audience into believing they successfully hit Israel DORAD power plant on October 8th and Israel National Water company (Mekorot) on October 10th among other targets.

One should wonder which objective is pursued by hacktivists. In addition to it being easier and faster than carrying out real attacks, reposting previous hacks or fake hacks has also two potential audiences with two different purposes:

- On the one hand, the (pro-) Palestinian audience who will see these hits as part of a resistance effort.
- On the other hand, the (pro-) Israel audience who will understand from these posts that Palestine will not submit easily or that Israel is still somewhat vulnerable.

Figure 15 : Cyber Av3ngers release fake proof or hacks. Source : Telegram, OWN-CERT.

28. *hxxps://t[.]me/s/ganosecteam/5424 ; hxxps://t[.]me/sultengblackhat/63*

The X GhostPrincessTM (@barbbyofficial) account illustrates the communicating role of posts as it shares any new hack publication[29].

These posts create the impression that important targets are hit when most targets are common people and vulnerable common websites[30].

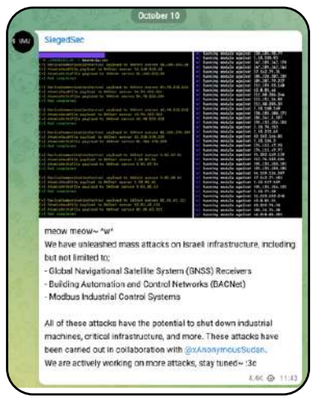
Above all, the exact same analysis can be applied to the pro-Israeli communication on social medias.

CONCLUSION AND FURTHER OBSERVATIONS

To conclude, the cyber activity affecting Israel and Palestine seems, so far, mostly superficial, even if we will need time to assess the overall activity related to the conflict.

There are claims of successful hits on ministries, if true, DDoS attacks against websites remain – let's face it – the least feared attacks among cyber-attacks. Were we not in a war context, most cybersecurity analysts would have met these incidents with nonchalance. Most of the activity can be assimilated to political gesticulation with the intent of influencing the public opinion, and can be compared mutatis mutandis, to NoName057(16), a pro-Russia hacktivist group that is used to DDoSing institutions' and entities' websites of countries supporting Ukraine.

Notably, real life alliances are also found in cyberspace. For instance, Indian hackers sided with Israel following their government's position. Similarly, Muslim populations tend to side with Palestine even against their governments (Egypt, Jordan, Mauritania, Bahrain, Morocco, Sudan and the United Arab Emirates all recognized Israel), thus, pro-Palestine hackers are from predominantly Muslim countries. Some hackers overtly display their ties with foreign countries. The hacktivist group @CyberAveng3rs overtly displays its Iranian ties. Also, in real life, Hamas and its militia are supported by Iran, and in cyberspace - according to the cybersecurity editor RecordedFuture – it appears the Hamas-tied APT group AridViper is linked to the Iranian Revolution Guards Corps (IRGC)[31]. Several groups seem to be linked with Russian actors. The group SiegedSec (mentioned above) could be related to Killnet through AnonymousSudan as it communicates on joint operations against Israel. Also, the alleged Vietnamese group @YourAnonl3x reposted KillNet content on its Telegram channel. In fact, AnonymousSudan and KillNet themselves sided with Palestine – and again not the Hamas – in a public post. Siding with Palestine could be a means for Russian hacktivists to easily further upset Western countries.



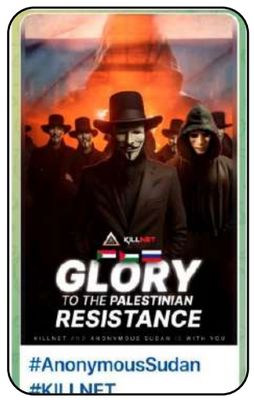


Figure 16 : Above - Post from SiedgedSecc suggesting the group works with AnonymousSudan, and a post from KillNet siding with Palestine.
Below - An account sharing KillNet content. Source : Telegram, OWN-CERT.

31. https://www.recordedfuture.com/hamas-application-infrastructure-reveals-possible-overlap-tag-63-iranian-threat-activity

From the point of view of Palestine supporters however, the pro-Palestine cyber activity is meaningful to the extent that it is perceived as a substitute for a foreign help that never comes, whether it be from Arab countries or from the international community.

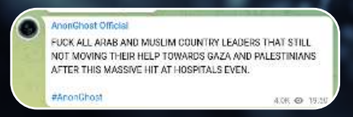


Figure 17 : AnonGhost desperate post. Source: Telegram, OWN-CERT.

Plus, all cyber activity supporting Palestine appears desperate as several accounts share tips in hope of a significant hit. And sometimes, authors let their despair out as the post below published by AnonGhost demonstrates.

OWN-CERT has been monitoring all the activity since October 9th, and thus far it appears that the intensity and nature of the cyberactivity is stable and monotonous.

However, a few notable elements can be mentioned.

On October 23rd a new domain for the al-Qassam Brigades was registered:

- alqassamps[.]com

On October 24th another new domain was registered:

- tufanalaqsa[.]net

The original domain alqassam[.]ps redirects towards tufanalaqsa[.]com.

Both new domains were registered at Cloudflare, also both were unavailable on October 24th and responded as if they had been taken down.

At the end of October and the first days of November, new kinds of activities were detected: ransomware attacks, claims of an Israeli TV channel disrupted during live stream and a wiper malware with two versions (one for Linux OS and one for Windows OS) is being distributed[32]. In the next weeks the cyber activity could enter a new phase as Israel is conducting a ground operation in Gaza.

INTRUSION SETS	AFFILIATION	ESTIMATED TECHNICAL LEVEL
Storm-1133	Hamas	HIGH
SiegedSecc	- / Pro-Palestine	HIGH
CyberAveng3rs	Iran / Pro-Palestine	N/A
AnonGhost (@AnonGhost)	Palestine / Pro-Palestine	MEDIUM
Team Azrael of Death (@Team_Azrael)	Pro-Palestine	BASIC
Garnesia Team	Indonesia / Pro-Palestine	BASIC
YourAnonT13x (@YourAnonTl3x)	Vietnam / Pro-Palestine	BASIC
Ghostsofpalestine	Palestine /Pro-Palestine	/

32. https://www.bleepingcomputer.com/news/security/new-bibi-linux-wiper-malware-targets-israeli-orgs-in-destructive-attacks/

DISINFORMATION AND MISINFORMATION

As many different news media outlets and analysts have already enlightened, the Hamas attack on the 7th of October generated a flood of content on social media platforms amongst which fake news and conspiracy theories have been identified[33]. But before diving in, the very first issue we faced when focusing on the information aspect is precisely this "mass" of content generated after the 7th of October.

According to X, 50 million of publications were generated within 48 hours[34], which makes it difficult for the observer not to be overwhelmed by content and information to analyse.

As many online resources already analysed and checked disinformation (we share those online resources in appendices), this part of this blogpost aims at sharing several results of our research and investigation.

Going through our collected data, we identified several accounts relaying false information about the conflict. For instance, a TikTok account shared videos saying Russia or Iraq were about to send troops to defend Palestine. Below is a screenshot of a video in French which translation is: "Putin has decided to launch a military rescue operation for/to Palestine".

Figure 18 : Screenshot of a TikTok video published on the 13th of October stating that "Putin has decided to launch a military rescue operation Palestine", Source: TikTok

Another TikTok account was found sharing a video on the 22nd of October saying that the attack on the 7th of October was faked, implying that Israel would have let the attack happen or worse created the attack to rightfully invade the Gaza strip.

Interestingly, this same account is also sharing a video to denounce the "disinformation campaign" allegedly conducted by Israel, while at the same time it relays false information from the disinformation and conspiracy website globalresearch.ca questioning the terrorist attack on the World Trade Center[35].

Another interesting point to rise is that the author of the "Zionist Cycle" leveraged a common talking point of the Israeli government to build the fake news credibility, which is comparing crimes against Israel/Jewish people with the Holocaust and 9/11. By doing so, the author gives the impression that his diagram is valid from an intellectual point of view as it is apparently built on a data anyone can check.

This phenomenon is bringing more complexity and confusion to the flood of information generated by the Hamas attack on the 7th of October.

Figure 19 : Screenshot of a TikTok video published on the 22nd of October implying that the Hamas attack on Israel might be "Fake", Source: TikTok

34. https://www.francetvinfo.fr/replay-radio/complorama/guerre-entre-israel-et-le-hamas-un-nouveau-moment-complotiste_6127971.html

35. This website created in 2005 is documented on the website Conspiracy Watch https://www.conspiracywatch.info/notice/mondialisation-ca

Figure 21 : Screenshot of an example of a video published on the 11th of October denouncing alleged false information, Source: TikTok

Figure 20 : Screenshot of an example of a video published on the 11th of October denouncing a disinformation campaign allegedly conducted by Israel, Source: TikTok

In the case of the first example mentioning footage of children in cages, this information has already been spotted and documented as a false information both used by pro-Israeli and pro-Palestinian accounts[36].

As we have seen above, a theory on an alleged "false flag attack" has been spreading. This theory aims at finding an explanation of why a military-advanced country could be attacked by a less military-advanced country. This theory has also been relayed on X with the hashtag #FalseFlag.

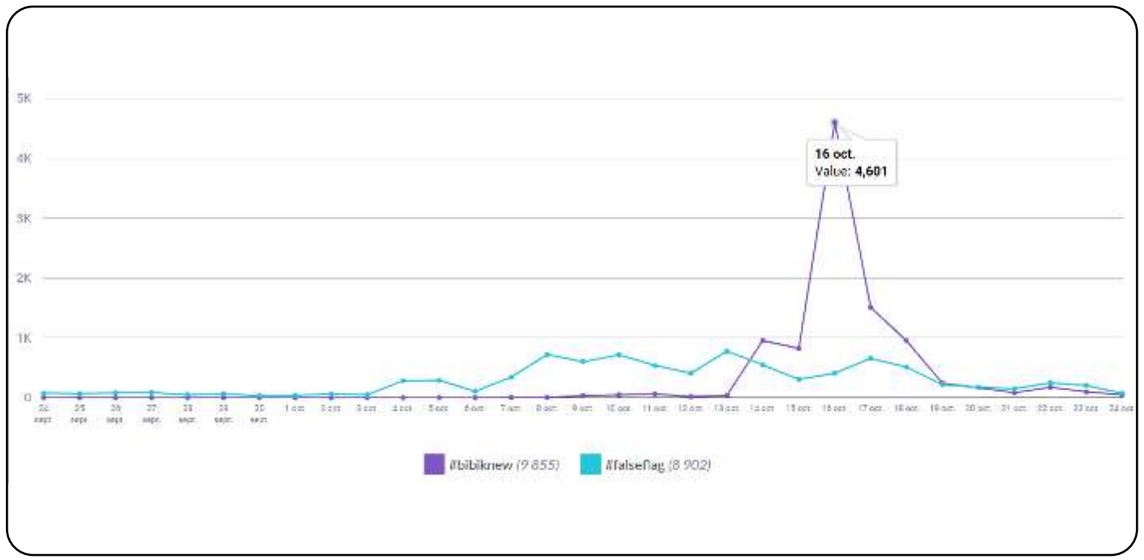
As we can see in the X publication above, other hashtags that refers to conspiracy theories such as "#NWO", standing for "new world order", and "#GreatReset" have been used.

Another hashtag spotted on X is #Bibiknew, which carries the idea that Israeli PM Benjamin Netanyahu knew about the Hamas attack beforehand but ordered the Israeli army to "stand-down". This conspiracy theory was created by far-right American influencer Charlie Kirk[37].

36.https://www.lemonde.fr/les-decodeurs/article/2023/10/16/guerre-israel-hamas-les-fausses-images-et-videos-qui-circulent-depuis-le-7-octobre_6193612_4355771.html#anchor=d_edito_undefined

37. https://www.forbes.com/sites/mattnovak/2023/10/16/conspiracy-theorists-go-viral-with-unsubstantiated-claim-about-israel-hamas-conflict/

Figure 22 : Screenshot of a Telegram publication relaying the "False flag" theory and the hashtag #Bibiknew, Source: Telegram.



Comparison of the activity related to the hashtags mentioned above, Source: Visibrain

When conducted research on the hashtag #Bibiknew, we could observe that a message published on the 14th of October by an account openly relaying conspiracy theories also relayed this hashtag and was published on the French conspiracy website - qactus[.]fr[38]. The analysis of the tweet relayed on the website associates the Israel-Palestine conflict to the conspiracy theories of the so-called "deep state" and "Q".

38.This French conspiracy website has been documented by Conspiracy Watch - https://www.conspiracywatch.info/notice/qactus

Translation:

"#IsraelPalestineWar #BibiKnew

Video in "French"

Is the Prophecy coming true before our very eyes?

@X account shares this disturbing video questioning the events we are living through #Israel #Hamas #Iran #Russia and the Prophecies in the Bible.

If we transpose to current events and the BIBLICAL BATTLE OF Q AGAINST THE KHAZAR DEEP STATE, many similarities.

[The Euphrates is actually drying up I've looked....]

Figure 23 : Screenshot of an extract of the tweet mentioning the conspiracy theories of the "deep state" and "Q", Source: X

This post is significant as it shows that accounts relaying conspiracy theories leverage the conflict to spread their theory to potential new targets, in this case supporters of Palestine.

As a conclusion, we didn't intend to have an exhaustive view since several analyses already covered this topic, but we wanted to share the results of our investigations and contribute to the comprehension of disinformation and misinformation generated by the Hamas attack on the 7th of October. From a global perspective, we observe a "flood" of content with accounts openly relaying disinformation, and among these accounts some specialized in conspiracy theories increase the volume of fake news currently flooding social media. However, only focusing on these accounts shouldn't put aside the consequence that many users are exposing themselves to misinformation and, by doing so, they may relay that false information.

IRANIAN STATE-SPONSORED GROUPS - THE CALM BEFORE THE STORM?

Iran seems to have benefited from the Hamas attack on Israel, which undermined the rapprochement between the Hebrew state and Saudi Arabia and rallied pro-Palestinian Arab opinion. Based on this observation, we believe that Iranian APTs could be involved in attacks or attack campaigns targeting Israel or allied countries, to increase its credibility and influence in the region.

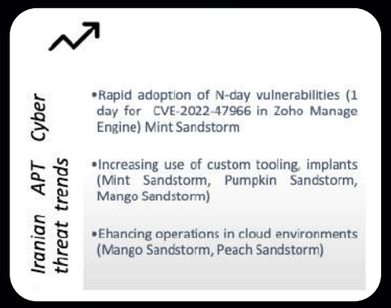
In this regard, the proximity observed between Hamas and the Islamic Revolutionary Guard Corps (IRGC), both from a geopolitical and cyber standpoint with the sharing of infrastructure, calls for great vigilance. Although there is no direct information about Iran's involvement in organizing or planning Operation Flood of al-Aqsa[39], we do know that Iran has been widely known to support Hamas for many years[40]. On the cyber component, as seen above, the infrastructure of an application distributed on the Telegram channel Brigades du Martyr Izz ad-Din al-Qassam (@qassambrigades) allowed researchers to link the AridViper intrusion set, tied to the Hamas militia, to the IRGC.

For the moment, while the actual involvement of MOIS- and IRGC-affiliated APTs is unknown, current political events, which may be perceived as provocative by Iran, could lead to the deployment of cyber-attacks. On October 11th, 2023, U.S. senators and politicians issued a letter calling on the U.S. government to **freeze** the **$6 billion** that the U.S. recently authorized to be **returned to Iran** as part of sanctions relief. This decision comes just a few weeks after the announcement of an agreement between the USA and Iran on this issue. Given the importance of **retaliatory** operations in Iran's cyber strategy, we believe it is possible that Iran could retaliate against the freezing of funds, either directly or through proxy groups they support. This event is, according to our analysis, a specific trigger for Iranian APT intervention.

In addition, on the night of October 26th[41], the United States struck Iranian Revolutionary Guard installations in Syria. For the same reasons set out above, we believe that retaliation will be launched by Iranian APTs, mainly associated with the IRGC.

Two MOIS affiliated APT groups have resumed their activity in the context of the conflict. Not only, Deep Instinct demonstrated that **MuddyWater** has launched a new spear-phishing campaign targeting Israel with a legitimate public document from the Israeli government as decoy ; also **Agonizing Serpens** (aka Pink Sandstorm) has continued targeting Israeli Education and Technology sectors with new wipers (Multi-Layer wiper, PartialWasher, wiper BFG Agonizer wiper) throughout October 2023 .

Microsoft Threat Intelligence has detected an Iranian actor carrying out **reconnaissance** of an **Israeli water company** and scanning the web interfaces of **industrial control systems** based in Israel at the end of 2022. Cisco Talos discovered a new family of malware called «HTTPSnoop» used by an Iranian intrusion set called **Shrouded Snoop** and deployed against **telecommunications** providers in the Middle East, particularly Israel. In the current context, should Iranian cyber forces further enter the conflict, we expect **destructive attacks** against **key sectors** such as energy, water, and telecommunications using previous reconnaissance operations. We evaluate with medium confidence that cyber operations will be lead under Ministry of Intelligence Service (**MOIS**) supervision.



39. https://www.cnbc.com/2023/10/08/blinken-says-us-has-not-yet-seen-evidence-of-iran-involvement-in-hamas-attack-on-israel.htm

40. Ibid

41. https://www.defense.gov/News/Releases/Release/Article/3570798/secretary-of-defense-lloyd-j-austin-iiis-statement-on-us-military-strikes-in-ea/

42. https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/

43. https://blog.talosintelligence.com/introducing-shrouded-snooper/

Iran is also likely to use its cyber capabilities to carry out reconnaissance and gather intelligence on Israeli military systems or on countries involved in the conflict. One example, which has not yet been verified, is the claim by the APT group «**Moses Staff**» on **October 28th, 2023**, to have hacked into surveillance **cameras** positioned above the **headquarters** of **Mossad** and Unit 8200 (the Israeli electronic intelligence unit).

Figure 24 : @moses_staff_se_17 claims to have access to 8200 Aman Unit and Mossad CCTV

Similarly, Moses Staff published a «military.zip» file on its telegram account, containing two excel files of 714.04KB and 318.81 KB which, according to the threat actor, contain data from reserve military units.

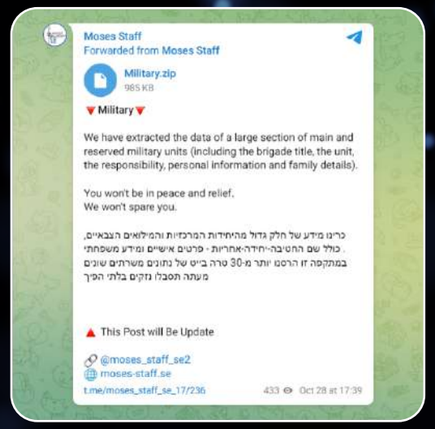


Figure 25 : @moses_staff_se_17 publishes leaked data from an Israeli military unit. Source : Telegram, OWN-CERT.

After checking the file, we were able to observe that the information published was that of the unit «חיר 7006 גד», also known as the Oded Division or 9th Brigade. It is in fact a reserve infantry brigade subordinate to the Bashan Division, a regional division of the Northern Command. A number of personal details have been published, including divisions, units, personal numbers, ID numbers, first names, last names, dates of birth and various certifications. However, as the information relates to soldiers attached to the Northern Command, whose headquarters are in Safed, on the border with Lebanon and Syria, we can assume that this is not really a strategic attack, as the data collected has no direct links with Israeli operations in Palestine.

APPENDICES

IOCS

FILES

SHA256	IPV4 RESOLUTION	CONTEXT
fa98139b94cc56890af27e6dd02deb4da-64b930e801492a966e0f13103808e2f	Palestinian heritage - what it is and what its forms are docx.exe	Micropsia Sample
af87a91c71b3cca1184b4b1250cacec-041430264d0f8ac56bde3a6b1173e84a2	WindowsMediaProvi-sioningPlugin.exe	Micropsia Sample
c1c5c4153fea7871e735cabaf-faf64722235a374b890017f-fbe2074ac0b11fe1	ConsentUXUserServiceManager.exe	Micropsia Sample

NETWORK

DOMAIN	IPV4 RESOLUTION	ASN	CONTEXT
porthopeminorhockey[.]net	5.181.23[.]41	44477	Micropsia C2 domain (inactive)
izocraft[.]com	91.199.147[.]84	62212	Micropsia C2 domain
delooyp[.]com	45.144.29[.]251	44477	Micropsia C2 domain
wellnesthealth[.]xyz	91.199.147[.]84	62212	Suspected Arid-Viper domain

TTPs

ARIDVIPER

TACTIC	ID	NAME
Initial Access	T1566.001	Phishing: Spearphishing Attachment
	T1566.002	Phishing: Spearphishing Link
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.005	Command and Scripting Interpreter: Visual Basic
	T1059.007	Command and Scripting Interpreter: JavaScript
	T1204.001	User Execution: Malicious Link
Persistence, Privilege Escalation	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Execution, Persistence, Privilege Escalation	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
	T1027	Obfuscated Files or Information
	T1553.002	Subvert Trust Controls: Code Signing
	T1218.007	System Binary Proxy Execution: Msiexec
Discovery	T1057	Process Discovery
Command and Control	T1105	Ingress Tool Transfer

OTHER REFERENCES

- ApNews, Misinformation about the Israel-Hamas war is flooding social media. Here are the facts, October 2023; https://apnews.com/article/israel-hamas-gaza-misinformation-fact-check-e58f9ab8696309305c3ea2bfb269258e
- Reuters, R. Kennedy, Israel-Hamas war: Fact-checking online misinformation, October 2023; https://www.reuters.com/world/middle-east/fact-checking-online-misinformation-israel-hamas-conflict-2023-10-09/
- Le Monde, A. Maad , R. Geoffroy , H. Valat and W. Audureau, Guerre Israël-Hamas : les fausses images et vidéos qui circulent depuis le 7 octobre, October 2023 ; https://www.lemonde.fr/les-decodeurs/article/2023/10/16/guerre-israel-hamas-les-fausses-images-et-videos-qui-circulent-depuis-le-7-octobre_6193612_4355771.html

ABOUT US

Interested in this report? Do you have any questions? Would you like to find out more?

Would you like to know the state of the threat to your industry and your organization?

contact@own.security

We carry out forensic analysis, threat detection, cybercrime fighting, geopolitical analysis and infrastructure monitoring of adversarial modus operandi.

OUR CERT TEAM IN FIGURES:

- 25+ analysts
- Over 10 languages spoken, including Russian, Chinese, Arabic, Korean, Ukrainian, Romanian, German, Spanish and English.
- 700+ cybercriminal forums and marketplaces monitored
- 2000+ open and closed cybercriminal discussion channels monitored
- 400+ reports produced per year

Téléphone
+33 (0) 805 -690-234

contact@**own.security**

www.own.security