baffin bay

by

2023 Israel-Hamas conflict: **A cyber perspective**

December 2023

Table of content

Overview

Boots on the ground and bots in the cloud

Nowadays, conventional warfare is rarely fought exclusively with boots on the ground; armed assaults can effectively be accompanied by cyber attacks to achieve a more devastating and diversified impact on the adversary. Cyber attacks are not kinetic and rarely lethal, but they can be employed by a wide array of actors stretching far beyond the parties at war.

On October 7 this year, the Palestinian militant group Hamas conducted an unprecedented, large-scale attack on Israeli soil resulting in a rapid conflict escalation. The vast increase in hostilities, culminating into a ground invasion of the Gaza strip, can also be witnessed in the cyber realm. The Middle East has long been a region with active cyber crime syndicates looking to profit from ransomware attacks and data breaches, as well as state-sponsored threat actors conducting systematic espionage operations. However the recent ramp-up in the Israel-Hamas conflict has brought along a surge in malicious cyber activity, particularly from hacktivist groups. Let's dwell into the implications of this development and begin by mapping out the different threat actors engaging on the digital battleground; who are they and what are they trying to achieve?

Threat Actors

Israel

According to Microsoft Digital Defense Report, Israel is by far the most targeted nation in the Middle East receiving almost 40% of all recorded attacks. On the other hand, Israel also possesses one of the world's most advanced cyber defense apparatuses. Its vast array of private companies providing state-of-the-art cyber security solutions and commercial spyware further act as an extension of the country's national defense infrastructure. Yet very little is known about Israel's ongoing cyber warfare operations towards Hamas and its allies. Details of specific Israeli cyber units are closely guarded, even though it is well-known that they have in the past conducted attacks towards high-profile targets such as the Iranian nuclear program. It is believed that Israel has multiple state-sponsored groups at its disposal and that the primary goal of threat activity is to collect strategic intelligence and disrupt operations or industries that support Hamas. Cloudflare notes that Palestinian websites saw a surge in DDoS-attacks after October 7, but these attacks have not been traced nor attributed to Israel-affiliated groups.

Hamas

Unlike Israel, Hamas does not have a cutting-edge cyber security apparatus. Therefore it relies heavily on hacker groups loyal to its cause and allies in the region, most notably Iran and Hezbollah. There are also indications that Hamas collaborates with Middle Eastern hacker groups to not just perpetrate attacks on Israel, but help maintain the

functionality of websites and social media channels connected to the militant organization.

Iran

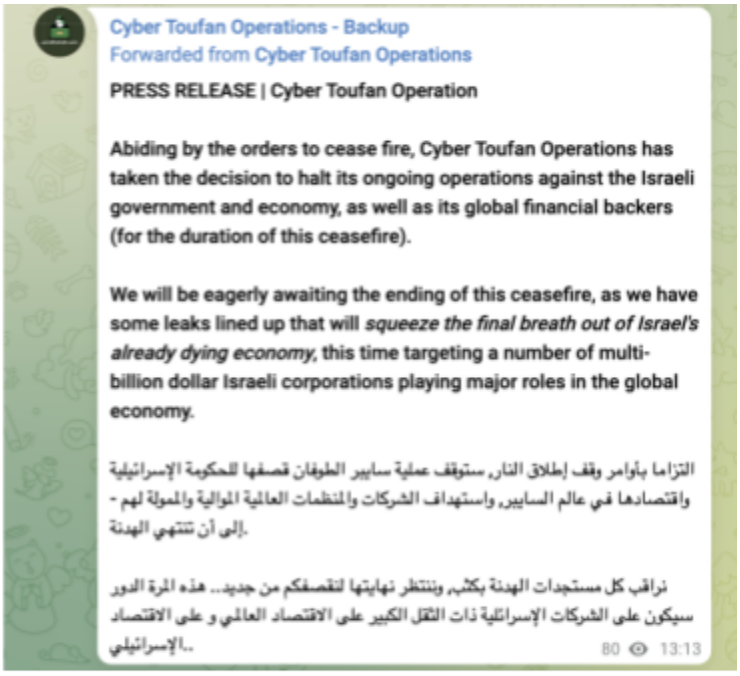
Iran is the primary, long-time benefactor of Hamas and antagonist of Israel. The Islamic republic has the strategic- and operational toolkit to launch both disruptive and covert cyber attacks. The Iranian cyber threat-ecosystem consists of two legs; its domestic intelligence services and state-sponsored hacking groups.

A recent Microsoft report highlights that threat actors affiliated with the Iranian government have significantly improved the level of sophistication to the point where their capabilities are almost comparable to those of Russia and China. Even so, it is important to note that Iran has thus far stayed away from direct interference in the Israel-Hamas conflict, and there is no concrete evidence that Iranian threat actors had prepared cyber attacks in advance of October 7. More so, it appears that Iranian hacking groups are using the frameworks of existing operations and access points to carry out malicious attacks in support of Hamas.

In all likelihood, Iran will continue to advance its geopolitical goals through strategic long-term operations targeting key industries in Israel such as the defense, energy and telecommunications sectors. The infrastructure and ambitions to carry out attacks have existed long before the recent conflict escalation and the general increase in attack traffic that we have witnessed is not surprising given the close ties between Tehran and Hamas's leadership.

Multiple incidents have recently taken place where the threat actor and attack vectors are attributable to Iran. Here are a few examples:

Cyber Toufan, a newly emerged group with connections to Iran, has been targeting multiple businesses in Israel. Interestingly, the group released a statement after the ceasefire agreement stating that it is abiding by the brokered deal and thus halting its operations during the process. This further demonstrates how cyber threat actors are perceiving themselves as increasingly legitimate parties of armed conflicts.



Telegram post by Cyber Toufan Operations - Backup

In addition, the Iran-linked threat actor MuddyWater deployed advanced monitoring agents targeting file-sharing systems on Israeli entities. Another infamous ATP-group, Imperial Kitten, struck transportation, logistics and technology companies in Israel through strategic web compromise-tactics, using social engineering and phishing to gain access.

Hacktivists

Arguably, hacktivists have been dominating the digital battlefield. An especially vocal and dedicated pro-Palestinian hacktivist community has emerged since October 7. Hacktivists have, unlike state-sponsored

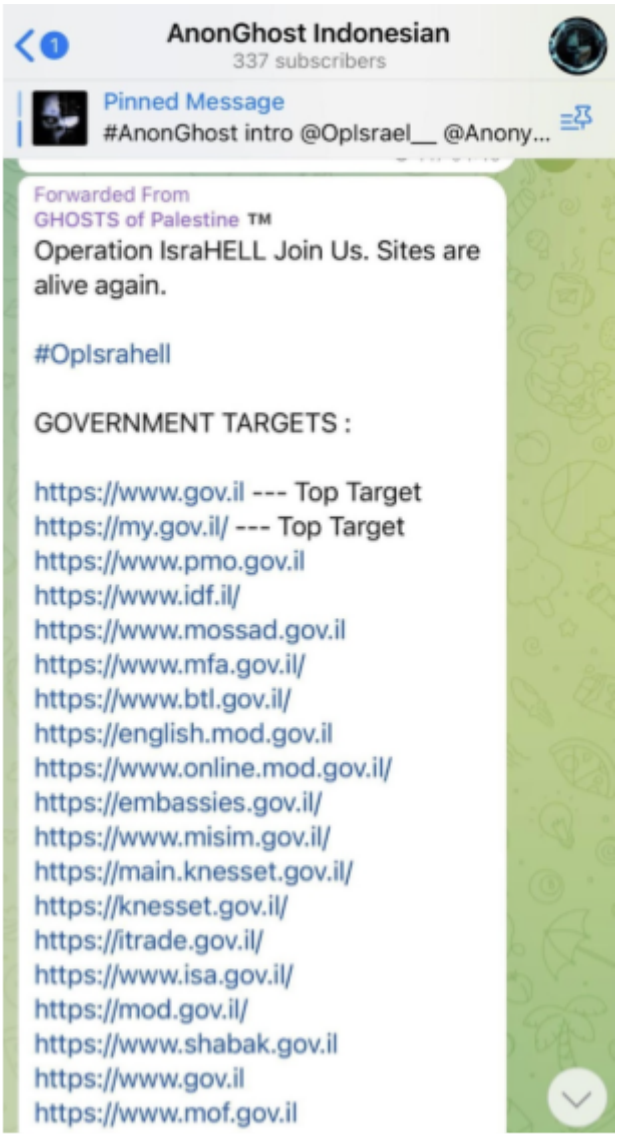
espionage operators, a motivation to conduct visible attacks and often claim direct responsibility for them. Distributed Denial of Service (DDoS) attacks are most frequently employed thus far, however targeted disinformation- and multifaceted malware campaigns have been common practice as well. Information is a valuable commodity and moving forward we may see more hacktivist groups adopting a so-called dual-approach, where they succeed in denying access to news outlets while simultaneously spreading disinformation through their own channels.

What are some of the current narratives that are circulating in the hacktivist community? The pro-Palestinian cause is not straightforward; some threat actors attribute their malicious activity to a direct support of Hamas, whereas others are mainly engaging in action against what they perceive is an unfair and unjustified treatment of the Palestinian people. These two narratives are sometimes, but not always, intertwined. For example, Hezbollah-affiliated hackers are keen on emphasizing their support for Hamas whereas other groups such as KillNet and Anonymous Sudan channel anti-Western sentiments through attacking Israel and its allies in North America and Europe.

The cybersecurity firm SocRadar estimates that there are 50+ hacking groups who are pro-Palestine and about 20 supporters of Israel. Meanwhile, FalconFeeds suggests that there are almost 100 pro-Palestinian groups. It is not straightforward to verify the size, resilience and capabilities of hacktivist constellations, or even their mere existence beyond a social media channel. Rather, we ought to question the authenticity of statements that hacker groups

themselves release as they may seek to bolster their threat appeal through false narratives.

A Radware report notes that threat actors from Indonesia, Bangladesh and India can be found among the top hacktivist groups attacking Israel. These groups are equipped with ideological and religious motives and sympathize with the people in Gaza. Some of the hacktivist groups have coordinated their actions through social media hashtags, most notably #OperationIsraHELL.

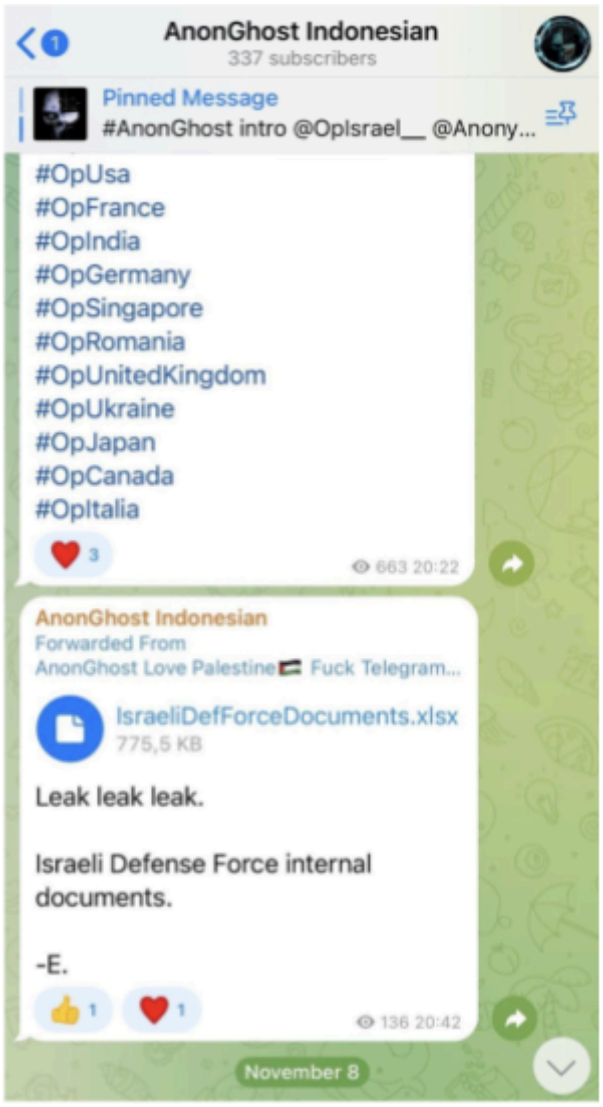


Telegram post by AnonGhost Indonesian

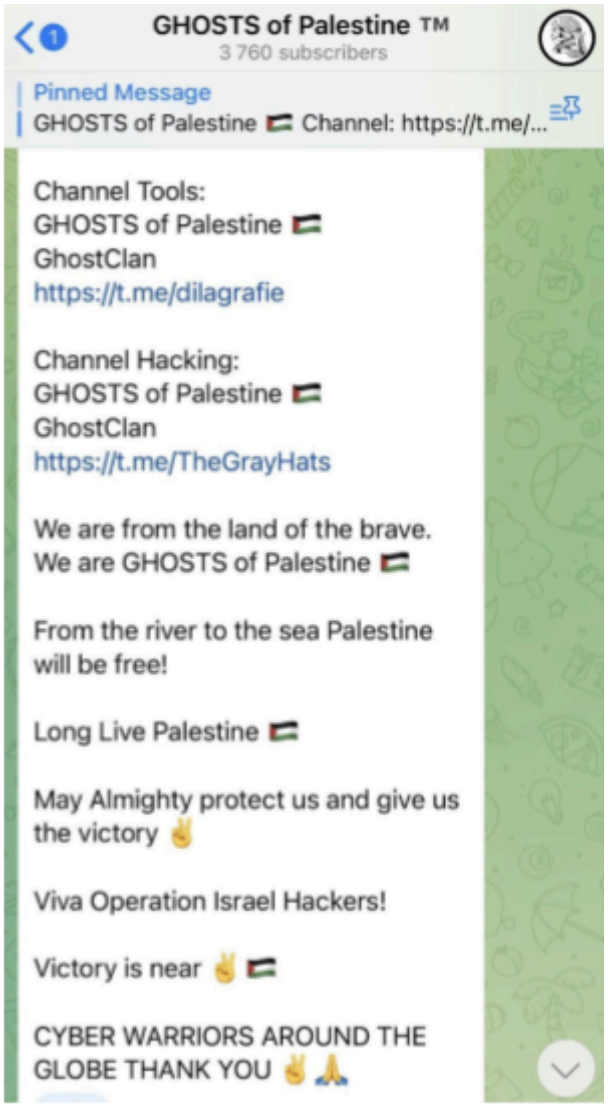
Indian Cyber Force has announced its support towards Israel, likely harbouring anti-Muslim sentiments. The group has claimed attacks towards Palestine's National Bank and its telecommunication services. In return, multiple hacker groups have called for retaliatory attacks against Indian businesses and government services.

Telegram post by Indian Cyber Force

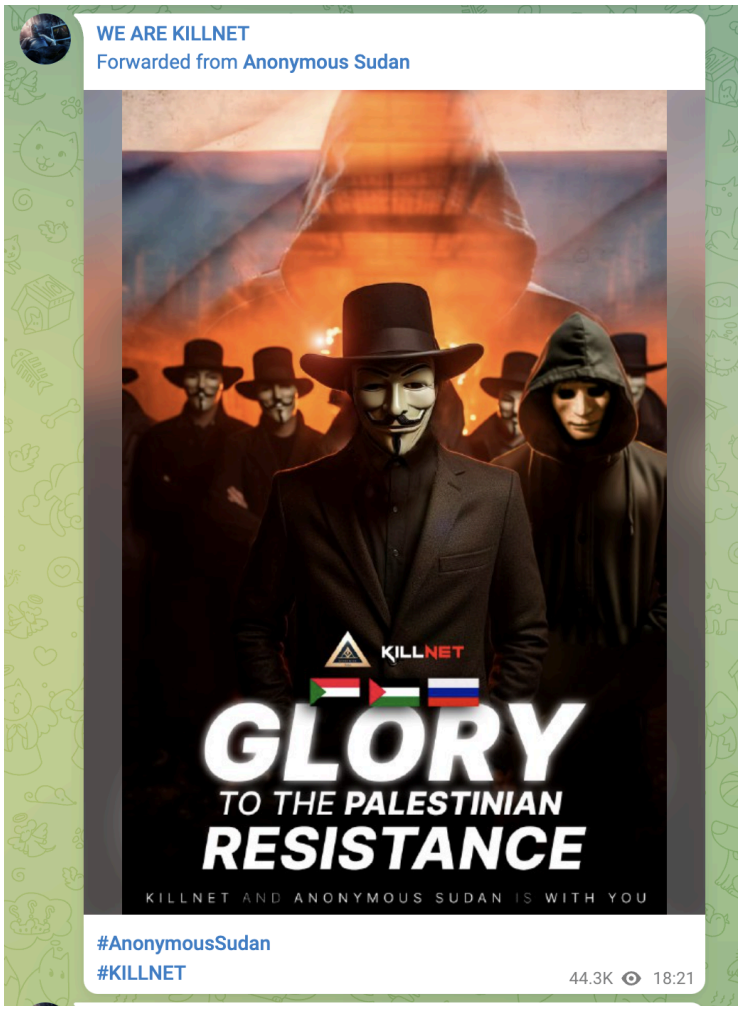
One of the most active groups attacking Israel is AnonGhost. The group leaks sensitive data that it has collected through multiple breaches and conducts regular DDoS-attacks. AnonGhost collaborates with Islamic hacker groups, for example Anonymous Indonesia and Ghosts of Palestine. These groups, beyond conducting attacks of their own, seek to inspire others to target websites of various Israeli government entities and companies by listing their addresses and IP-information on Telegram.



Telegram post by AnonGhost Indonesian



Telegram post by Ghosts of Palestine



Telegram post by Killnet

In April 2023, Russian-linked hacker group Anonymous Sudan manifested its dissent with Israel's military activity in Palestine through launching an attack on a number of Israeli websites. After the latest conflict escalation, it claimed to have conducted multiple DDoS attacks towards Israel industries. Anonymous Sudan was also keen on showcasing its collaboration with Killnet through Telegram posts on October 8, a day after Hamas's attacks. Killnet was quick to repost and reaffirm their common cause.

Insights from our Global Sensory Network (GSN)

Baffin Bay Networks[1] gathers, aggregates and enriches data through our extensive Global Sensory Network (GSN) consisting of multiple data collectors dispersed across the globe. The sensors capture exploits, attack attempts, malicious uploads and OSINT[2], allowing for the discovery of unique threat intelligence. After Hamas' deadly raid on October 7 and the escalation of hostilities that followed, our GSN was quick to identify a change in regional attack traffic:

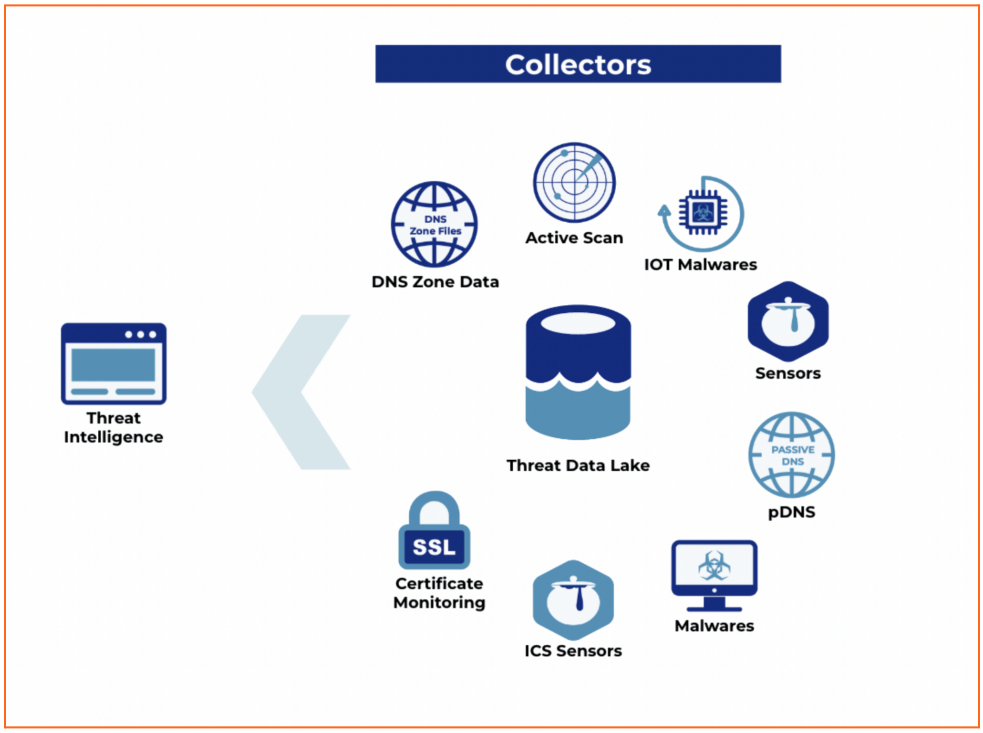


Image 7: Illustration of the GSN's data collectors

[1] A Mastercard company

[2] The exploits, attack attempts, malicious uploads and OSINT captured by Baffin Bay Networks' GSN account for unsolicited traffic, i.e. traffic that is not targeting any specific individual, entity or organization, but rather passes through the collectors that are being monitored.

Between the period of October 7 to October 25, Iran[3] ranked among the top 5 countries that launched the most malicious traffic, accounting for roughly 5% of all recorded attacks (see graph 1).

N.	Country	Region	Hits	%
1	India	AS	27.35 Mil	10.96
2	Russia	EU	23.65 Mil	9.48
3	United States	NA	20.90 Mil	8.37
4	China	AS	19.89 Mil	7.97
5	Iran	AS	12.24 Mil	4.90
6	Egypt	AF	10.23 Mil	4.10
7	Vietnam	AS	9.27 Mil	3.71
8	Bulgaria	EU	8.71 Mil	3.49
9	Singapore	AS	6.69 Mil	2.68
10	Estonia	EU	6.42 Mil	2.57

Graph 1: Attack traffic 2023.10.07 - 2023.10.25

[3] As Palestine is not represented in the dataset of source countries, it is deemed relevant to instead examine Iran as the primary threat country attacking Israel.

In the same time period a year earlier, Iran stood for only 1% of GSN's recorded attacks and placed itself 21st on the list of top source traffic countries (see graph 2).

N.	Country	Region	Hits	%
1	United States	NA	6.61 Mil	16.28
2	Netherlands	EU	2.83 Mil	6.96
3	Vietnam	AS	2.76 Mil	6.80
4	Russia	EU	2.50 Mil	6.15
5	Germany	EU	2.26 Mil	5.57
6	China	AS	1.90 Mil	4.67
7	Hong Kong	AS	1.65 Mil	4.05
8	India	AS	1.58 Mil	3.90
9	Philippines	AS	1.24 Mil	3.06
10	Indonesia	AS	1.19 Mil	2.92
21	Iran	AS	487.82 K	1.20

Graph 2: Attack traffic 2022.10.07 - 2022.10.25

During the month of September in 2023, i.e. prior to Hamas's surprise assault, Iran was not represented in the top 20-list of most attacking countries but again placed 21st (see graph 3).

N.	Country	Region	Hits	%
1	United States	NA	22.64 Mil	13.40
2	China	AS	19.84 Mil	11.75
3	Estonia	EU	18.32 Mil	10.84
4	Russia	EU	13.81 Mil	8.17
5	Philippines	AS	8.20 Mil	4.85
6	Bulgaria	EU	7.96 Mil	4.71
7	India	AS	6.82 Mil	4.03
8	Singapore	AS	5.84 Mil	3.46
9	Thailand	AS	5.59 Mil	3.31
10	Vietnam	AS	4.68 Mil	2.77
21	Iran	AS	1.77 Mil	1.05

Graph 3: Attack traffic 2023.09.01 - 2023.09.30

These findings signal that the increase in threat activity from Iran coincides with Hamas's attacks on October 7.

The GSN derives source traffic-related trends through the geographical origins of IP addresses. Here we must emphasize that the geosource of IPs does not, by default, mean that state-sponsored actors, individuals, or organizations based in the country are responsible for the threat activity. Indeed, the attack traffic could be coming through a proxy server, compromised system or IoT devices with IP addresses assigned to Iran. As such, it is relevant to

corroborate the findings with other data sources. In this case, an examination of most attacking Automatic System Numbers (ASN) yields a strikingly similar pattern: between October 7 - 25 in 2023, Iran's largest AS[4] stood for 2.5% of all malicious traffic captured by our sensory network, placing it 7th on the list of most attacking ASNs globally (see Graph 4).

N.	ASN	AS Org	Hits	%
1	AS14061	DIGITALOCEAN-ASN	17.24 Mil	6.89
2	AS132203	Tencent Building, Kejizhongyi	9.24 Mil	3.69
3	AS50360	Tamatiya EOOD	7.90 Mil	3.16
4	AS8452	TE-AS	7.67 Mil	3.07
5	AS208091	Xhost Internet Solutions Lp	7.65 Mil	3.06
6	AS45090	Shenzhen Tencent Computer Syst	6.25 Mil	2.50
7	AS58224	Iran Telecommunication Company	6.19 Mil	2.47

Graph 4: Top attacking ASN 2023.10.07 - 2023.10.25

Meanwhile, in the same time period a year earlier and during the month of September 2023, the AS placed 53rd vis-a-vis 29th.

These ASN-based results reinforce the proposition that the surge in malicious traffic from Iran, captured by the GSN, is reasonably attributable to Iranian threat actors. Yet we still have to be cautious about the possibility that other groups are behind a portion of the activity. These groups may have

[4] AS58224, Iran Telecommunication Company PJS

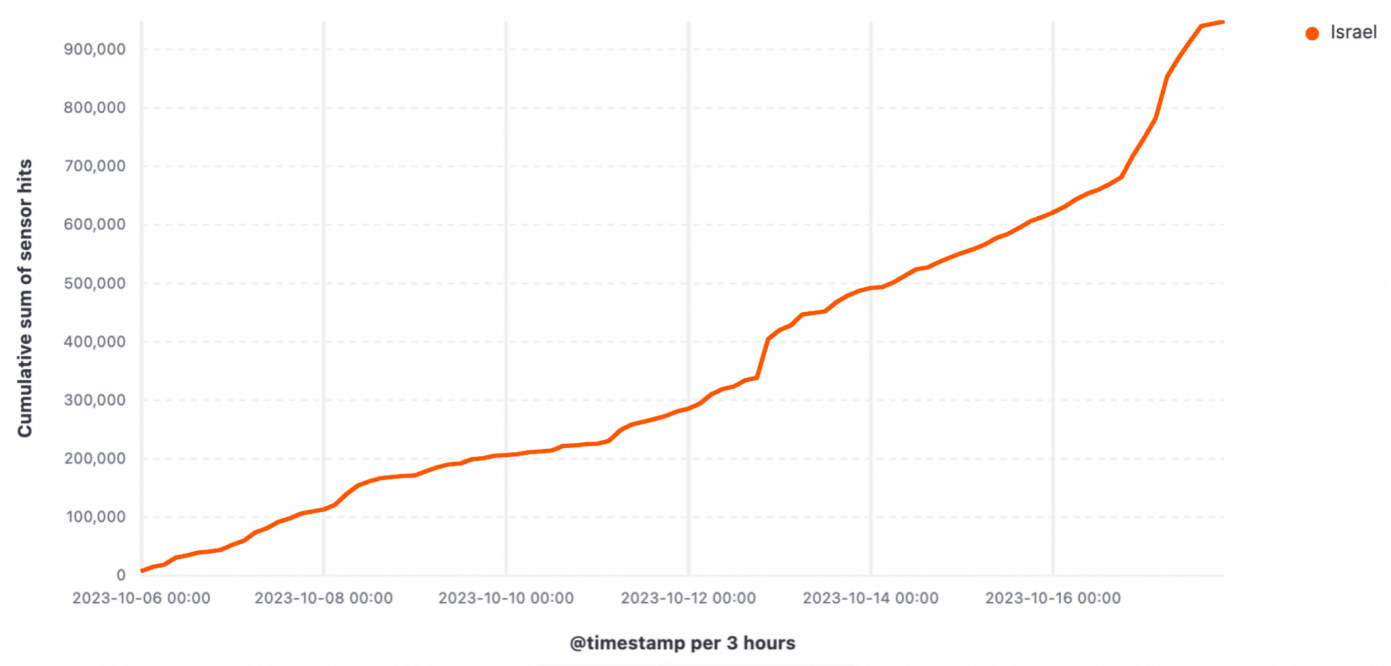
deliberately or unintentionally operated through Iranian IP-addresses.

Attack traffic originating from Israeli IPs is substantially more limited. The country cannot be found among the top 50 most attacking countries for any of the three time periods examined above[5]. Also, none of Israel's largest Automatic Systems[6] (AS) are represented in the top 100 attacking ASN dataset for these time frames. Here, we ought to again entertain a scenario where Israel launches its attacks through proxies or other sophisticated methods that conceal the geographical origin of the traffic. Such behavior resonates with the notion brought forward in the previous section, where Israel as a threat actor is considered to be hard-to-trace and evasive.

From a target point of view however, Israel experienced a clear spike in cyber attacks immediately following the war (see graph 5). Interestingly, the amount of recorded attacks first hiked right after October 7, but the real increase in attack traffic designated to Israel came about ten days after Hamas's deadly attacks. Such a trend may either indicate that many new threat actors became involved around this time, or that there was an escalation of attack intensity among the existing ones.

[5] Graph 1, Graph 2, Graph 3

[6] AS12400, AS1680, AS8551, AS378, AS12849



Graph 5: Attack traffic towards Israel between 2023.10.06 - 2023.10.18

A comparison to the Russian-Ukrainian war

In February 2022, Russian forces invaded Ukraine and the war has managed to cause unprecedented levels of polarization in cyberspace. Experts were quick to draw parallels between the Russo-Ukrainian war and the situation unfolding in the Middle East. Indeed, there are certain similarities in features and formations of the digital battleground and its participants, but also a set of characteristics that set these two conflicts apart from a cyber threat-perspective.

One striking similarity is the extensive hacktivist involvement and the way in which these communities are eager to launch attacks not just towards the perceived adversary, but its allies. It is well known at this point that pro-Russian hacker groups frequently target supporters of Ukraine. Nonetheless, countries pledging their loyalty to the Kremlin are vulnerable as well. Last year, the Belarusian railway's computer system was breached by a politically motivated hacker group. The act was meant to halt the movement of Russian troops and ammunition to the Ukrainian border.

Another resemblance can be found in the very early stages of both conflicts: when Russia attacked Ukraine, state-sponsored hackers immediately targeted media- and broadcasting sites in the country. Similarly, news outlets and media websites in Israel received over 50% of all recorded DDoS attacks in the first week after Hamas's surprise assault. This has of course a tangible impact on the civilian population who rely heavily on media for updates in uncertain times.

Similarities aside, there are also key differences to take into account. First and foremost, the distribution of hacktivism is far more one-sided in the Israel-Hamas war, where the former has received the bulk of all disruptive attacks. In contrast, both Russia and Ukraine have hacker groups and state-sponsored actors launching malicious activity in their favor. As a result, we have a larger knowledgebase of the motivations and capabilities of threat actors on both sides, whereas information regarding attacks conducted directly or indirectly through Israel is lacking. This finding resonates with data we see through our global sensory network: Russia, Iran and Ukraine all feature in the top 20 list of most

attacking source traffic countries while Israel did not even qualify in the top 50.

N.	Country	Region	Hits	%
1	Russia	EU	254.41 Mil	12.77
2	United States	NA	246.81 Mil	12.38
3	China	AS	137.61 Mil	6.90
4	India	AS	134.95 Mil	6.77
5	Estonia	EU	87.33 Mil	4.38
6	Vietnam	AS	86.98 Mil	4.36
7	Bulgaria	EU	74.18 Mil	3.72
8	Singapore	AS	63.56 Mil	3.19
9	Germany	EU	55.33 Mil	2.78
10	Philippines	AS	50.26 Mil	2.52
11	Netherlands	EU	47.04 Mil	2.36
12	Iran	AS	46.04 Mil	2.31
17	Ukraine	EU	33.74 Mil	1.69

Graph 6: Attack traffic 2023.01.01 - 2023.11.30

Future outlook

So, what can we expect moving forward? Even if the boots would vanish off the ground for the time being, the bots in the cloud and the access points that have been created are likely to persist. Perhaps the hacktivist spirits will dampen as threat groups find new causes to engage with. Covert espionage and data-theft operations will remain relevant, particularly from Israel's side as they are coming to terms

with the biggest intelligence blunder of the century. Improving their ability to forecast similar surprise assaults in the future will be a national priority for decades to come.

Both actors are likely to employ so called influence operations (i.e spread propaganda and disinformation) alongside other malicious cyber activity. It is also possible that threat actors affiliated with Hamas will look to collect funds for future operations through acts of ransomware. These attacks do not necessarily have to target Israel, and rather stem from the fact that warfare is costly, and cybercrime presents lucrative opportunities for making illegal, financial gains.

Hacktivist groups will continue to fight proxy-wars in cyberspace in the name of political or ideological agendas and explore avenues to bolster their threat-profiles. It is fair to reiterate that we ought to be cautious about these groups' victory-narratives shared on social media platforms as they may not reflect the actual impact of the claimed attack. There is a stark difference between having the ability to execute an attack and the ability to cause serious harm. Many cybersecurity researchers agree that the threat activity we have seen so far in connection to the war has been relatively modest in that the scope of attacks is widely exaggerated.

Regardless of attack type and vectors, the global cyber intelligence community must continue to monitor ongoing cyber threat campaigns in order to understand how threat actors leverage armed conflict to achieve ideological, political or financial objectives in the digital landscape. New vulnerabilities and tactics can be exposed as stakes grow

among the parties involved in the war. From a threat protection point of view, we can learn which industries become the main targets of cyber intrusions and attacks in the early vis-a-vis later phases of conflict. From the threat intelligence side, we gain a deeper understanding of the intersection between conventional warfare and cyber warfare. Perhaps the lines will blur over time, perhaps the contrasts remain defined.

We may conclude that the increase in geopolitical instability has brought on a significant upstream of cyber attacks, further fuelling the already ferocious hacktivist community in the Middle-East and beyond. Hacktivists are prone to use disruptive methods and often resort to sizable DDoS-attacks. With the right protection, the impact of such attacks can be seamlessly mitigated. However, most companies and institutions have been prone to adopt a volumetric protection model, rather than application-based solutions. Threat actors, and hacktivists in particular, have been quick to take advantage of this security gap. Baffin Bay Networks, a Mastercard company, offers a cloud based service designed to provide comprehensive protection against both volumetric and application-layer DDoS attacks. Baffin Bay Networks' Threat Protection Service combines simplicity of on-boarding with comprehensive features. It protects any of your web applications, anywhere - regardless of if you are running them in a public cloud, a private cloud or in your on-premise datacenter. You can learn more about our products and solutions here.

About the research

Baffin Bay Networks' Threat Intelligence team continuously monitors the cyber threat landscape and provides insights, predictions and business solutions based on its extensive global sensory network (GSN) and Threat Protection platform. We are committed to delivering world-class intelligence to help our customers and fellow practitioners in the cyber security community navigate the ever changing, dynamic domain of threat activity.

This report is solely distributed for informative purposes. The conclusions brought forward in this document are subject to potential errors as the conflict in question is ongoing, and the threat actors involved can be prone to fabricate, alter or refute their own or others' attack attributions.