2 Month Review of Cyber Activities in the Israel Hamas Conflict

By DarkOwl Content Team

Published: 2023-12-14 · Archived: 2026-04-05 12:52:28 UTC

December 14, 2023

Introduction

It has been 2 months since Hamas's October 7th surprise attack on Israel. In that time there have been many developments both on the ground and in the cyber realm. A number of groups emerged in the aftermath of the attack pledging their support to either Hamas, Palestine or Israel and cyberattacks increased in the region targeting both sides to varying degrees of sophistication. DarkOwl analysts have been tracking these events and activities, and in this blog we review some of the notable cyberattacks that have occurred and the groups that have taken responsibility.

In the first few days of the conflict, attention was largely focused on images and media reportedly coming out of Israel and Gaza highlighting the atrocities which were occurring. Telegram, which is monitored by DarkOwl, appeared to be being used as a de-facto news source, providing details of what was happening in certain areas and also posting images of the aftermath. Channels appeared or grew in size supporting one side or the other and while sharing information, there were also reports of false or fabricated information and media being shared stoking the flames on both sides.

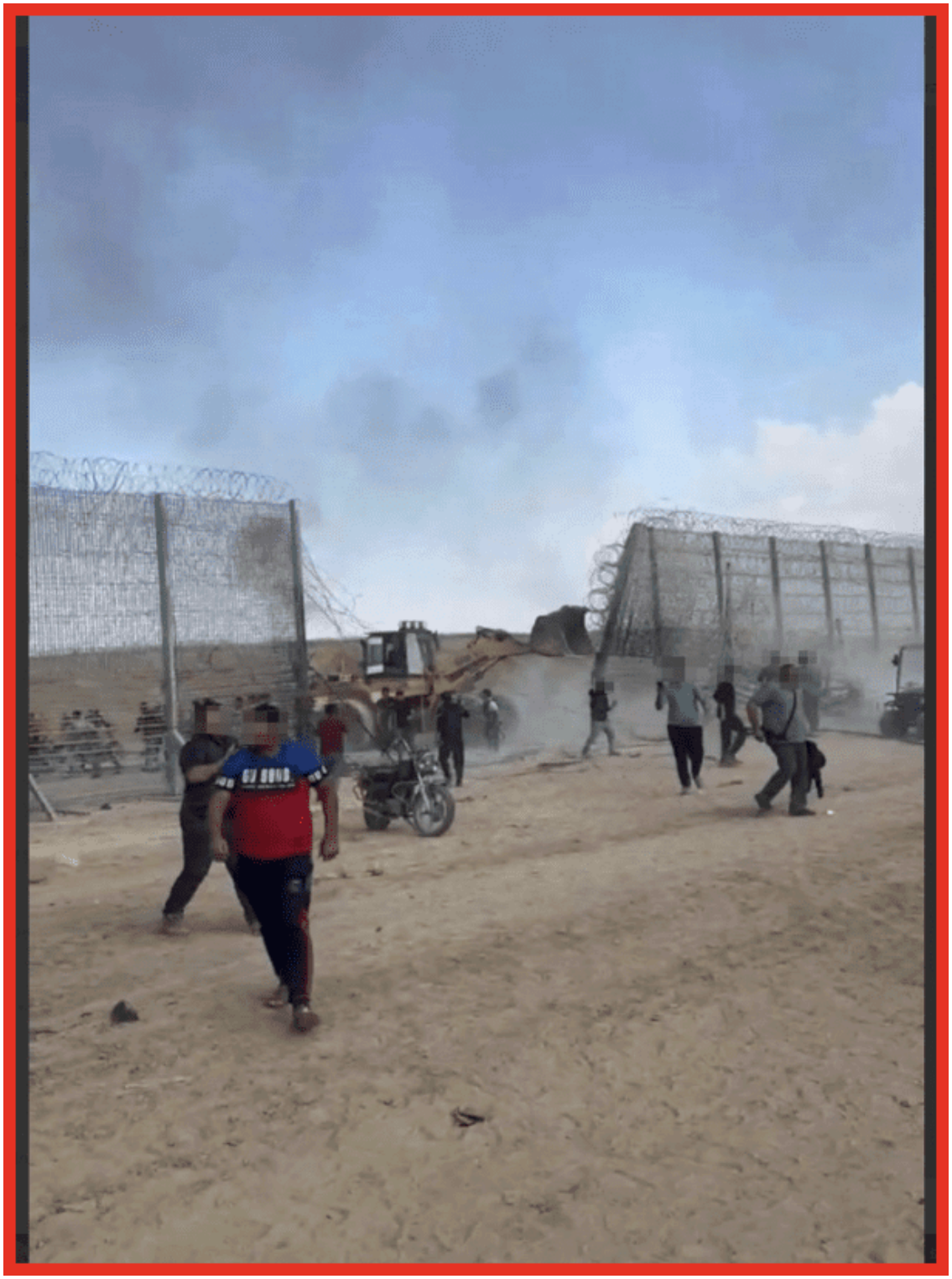

Figure 1: Telegram channel posts image of Hamas breaching into Israel

The cyber world also reacted to the conflict with existing hacktivist groups quickly pledging allegiance to their chosen side or already fighting for the cause. Groups quickly began to post online about the targets they had successfully compromised with attacks ranging from DDoS (distributed denial-of-service), defacements to data leaks. As the conflict has progressed, the level of activity has ebbed and flowed, with some groups turning their attention back to previous targets.

Figure 2: Selection of Cyber groups profile images

After the initial invasion and activity, several cyber incidents accompanied the air and ground conflicts in the Middle East. Key activities we identified as part of the conflict are detailed below although this is not an exhaustive list and does not describe all reported activities.

October Events

- **Dragon Force Malaysia** targeted and defaced several Israeli websites
- A leak purportedly from the **Palestinian Foreign Ministry** was published on cracking[.]org which contained details of Chinese and Palestinian projects as well as correspondence documents and PII for approximately 500 people. DarkOwl was able to obtain this leak for review.
- **Ghosts of Palestine** openly announced they will target NATO countries who support Israel although Turkey was excluded from targeting.

- JFK airport was targeted by hacktivist group **R_70** which is a Pro-Hamas group. The groups reported via their Telegram channel that they had taken down the JFK website due to their links to “Zionism.”
- **BlackSec** joined the digital operations arena, claiming it would target Israel and not remain neutral in the conflict.

- The RedAlert app which was used to alert Israelis to rocket attacks was subject to a spoof attack which was reported to collect personal information. It was unclear who was behind this attack but demonstrated cyber actors taking advantage of the military conflict for their own gain.

- **Stucx Team** claimed an attack on an Israeli SCADA system via their Telegram channel, Supervisory Control, and data acquisition (SCADA) controls industrial processes. Targeting these types of systems can bring down water plants and electrical facilities and are usually one of the most concerning attacks for cyber security experts. A high level of sophistication is usually required to successfully attack these processes. However, they became a common Israeli target as the conflict continued.

Figures 3 and 4: STUCX Team Telegram post from DarkOwl Vision and on the channel

- The group **GlorySec** posted on Telegram that they considered a firewall on Palestinian websites, indicated Palestine had prepared well in advance for a conflict in the cyber realm as well as the physical realm. They also said they'd release the data right to Israel to support their operations and encouraged them to investigate this. It is unclear what information they had or if this was shared.

Figure 5: Telegram post by GlorySec via DarkOwl Vision

- **Anonymous Algeria** publicly warned the UAE and alerted its airline, Emirates, to a possible system compromise for what they view as “not supporting Palestine”:

Figure 6: Anonymous Algeria Telegram Post

- Reports indicated that Pro-Hamas hacktivists groups were targeting Israeli Entities with Wiper Malware, the destructive malware appeared to have signatures within it linking it to the Middle East. This development highlighted the use of sophisticated tools as part of the ongoing conflict and suggests a “cyber war” may also be taking place.

As the month of October concluded, hacktivist activity relating to the Gaza conflict appeared to decrease. While the start of the conflict saw a large amount of emerging activity, with actors and groups choosing sides and issuing threats online, digital activity surrounding the Israel-Hamas conflict tapered down. However, increases were expected as the conflict continued.

November Events

- **AnonGhost Indonesia** & **Anonymous Indonesia** warned the Japanese government that for supporting Israel that they would carry out cyberattacks, the groups had already been active in targeting countries they deemed to be anti-Palestine or Pro-Israel.

- **GhostSec** claimed to have successfully targeted several Israeli PLCs via their Telegram channel.
- **Anonymous** claimed to have information relating to Mossad spies which they threatened to disclose on Telegram it is unclear where this information came from or if it relates to valid data.

Figure 7: Anonymous post on Telegram

Although the hacktivist groups on Telegram appeared to quiet in this period security research reported on several activities which indicated that Iranian hackers were using new tools to target Israel and that a Hamas linked APT was also targeting Israel with a new backdoor tool. Indicating that nation states and Nation State sponsored groups continued to be active in the cyber sphere. These groups tend to avoid the publicity that hacktivist groups seek.

December Events So Far…

Cyber incidents began to increase after the temporary ceasefire between Hamas and Israel completed.

- Pro-Palestinian hackers reportedly stole Israeli Defense Force (IDF) patient records as part of a cyberattack on Israeli hospital

- **Cyber Toufan** hacking group claimed to have breached Israeli company SodaStream, and exfiltrated 100,000 records:

Figure 8: Post for SodaStream data on dark web forum via DarkOwl Vision

Conclusion

Hacktivist groups and cyberattacks have been a component of the Israel Hamas conflict since it began, with many groups getting involved and attacks across of a scale of sophistication being conducted on both sides. Although the activities have ebbed and flowed in the first two months of the conflict, it is clear that they are likely to continue for the length of the military conflict – if not longer. DarkOwl will continue to monitor the activities of these groups as the conflict continues.
