Reflections of the Israel-Palestine Conflict on the Cyber World

Published: 2023-10-09 · Archived: 2026-04-02 11:57:06 UTC

Welcome to our live blog, “Reflections of the Israel-Palestine Conflict on the Cyber World.” This blog actively documents significant cyber incidents occurring during the Israeli-Palestinian conflict.

You can navigate to a specific section of updates by clicking on the dates below.

[November 2, 2023] Concluding the live blog

[November 1, 2023] Anonymous Sudan Continues to Target Media Agencies

[October 31, 2023] Beyond Hacktivism: The Sabotage Strategies of APT Groups

[October 30, 2023] APT Groups Have Surfaced

[October 27, 2023] Old Tactics, New War

[October 26, 2023] War on the Google Maps

[October 25, 2023] Don’t Give a Man Fish, Teach Him How to Fish

[October 24, 2023] Google’s Intervention in Telegram

[October 23, 2023] Doubtful Claims and Hacktivist Cooperation

[October 20, 2023] An Iron Dome for cyber lands

[October 19, 2023] Quality over quantity

[October 18, 2023] The calm before the storm

[October 17, 2023] Hacktivists continue to share their attack methods

[October 16, 2023] Hacktivists are trying to maximize their potential

[October 13, 2023] Bombs Explode, and So Do the Borders of Cyber War

[October 12, 2023] DDoS, Defacement, Data Leaks, and now Ransomware are in the arsenal of hacktivists.

[October 11, 2023] Attacks are accelerating, cyber conflict has spread to a global scale

[October 10, 2023] Many hacktivist groups have come back to life, operations have begun

In the midst of the ongoing Israel-Palestine conflict, a notable upsurge of hacktivist collectives has emerged, announcing an unceasing barrage of digital assaults directed at a wide range of targets from both sides of the conflict.

This situation unfolds as a response to the ongoing Israel-Palestine conflict, which involves Palestinian militant groups led by Hamas initiating a large-scale offensive originating from the Gaza Strip and targeting Israel.

Although the cyber world sometimes seems like a stand-alone entity, it must be a reflection of the physical world, so just like the hacktivism resurgence that came with the Ukraine-Russia war, this sad conflict situation for humanity will also show an increasing business of war in the cyber world.

The Hacker Groups Involved in the Israel-Palestine Conflict

In the ongoing conflict, where the global landscape is mainly split into two factions, NATO and Western-aligned nations often lean towards supporting Israel. Conversely, many countries in Asia tend to align themselves with the Palestinian cause. However, it is worth noting that some nations, like India, may adopt positions that diverge from their geographic affiliations. Both political alliances and geopolitical priorities influence this dynamic.

When we analyze these events through this lens, it becomes increasingly challenging to categorize countries definitively into one camp or the other. This complexity is even more pronounced in the realm of cyberspace. While hacktivist groups typically align with the **political objectives** of their home country, there are instances where they may adopt alternative stances.

Pro-Israel Groups	**Pro-Palestine Groups**	**Neutral Groups**
Indian Cyber Force	KillNet	ThreatSec
UCC Team	Anonymous Sudan	Cyber Army Of Russia
Garuna Ops	UserSec	KromSec
SilentOne	Anonymous Russia	
IT ARMY of Ukraine	Ghosts of Palestine	
Kerala Cyber Xtractors	Team Azrael Angel of Death	
Termux Israel	Dark Strom Team	
ICD-Israel Cyber Defense	Pakistani Leet Hackers	
Gaza parking lot crew	Sylhet Gang-SG	
Isr@CyberH3ll	Team_insane_Pakistan	
Anonymous Israel	Hacktivism Indonesia	
GlorySec	Garnesia Team	
Team NWH Security	Blackshieldcrew MY	
Dark Cyber Warrior	Gb Anon 17	

Pro-Israel Groups	Pro-Palestine Groups	Neutral Groups
Indian Cyber Sanatani	Anonymous Morocco	
Indian Darknet Association	Ghost Clain Malaysia	
RedEvils	Mysterious Team Bangladesh	
	Ganosec team	
	Moroccan Black Cyber Army	
	Muslim Cyber Army	
	GhostClan	
	Eagle Cyber Crew	
	YourAnon T13x	
	Team Herox	
	SynixCyberCrimeMY	
	Panoc team	
	4 Exploitation	
	Team R70	
	Stucx Team	
	The White Crew	
	Cscrew	
	TYG Team	
	Hizbullah Cyb3r Team	
	Electronic Tigers Unit	
	StarsX Team	
	Dragon Force Malaysia	
	GhostSec	
	Cyb3r Drag0nz	
	1915 Team	
	Moroccan Defenders Group	

Pro-Israel Groups	Pro-Palestine Groups	Neutral Groups
	VulzSec	
	End Sodoma	
	Skynet	
	ASKAR DDOS	
	Storm-1133	
	Arab Anonymous Team	
	I.C.C	
	ACEH	
	Bangladesh Civilian Force	
	WeedSec	
	KEP TEAM	
	AnonGhost	
	Moroccan Defenders Group	
	Moroccan Ghosts	
	Garuda Security	
	Jateng Cyber Team	
	Jakarta Error System	
	T.Y.G Team	
	Esteem Restoration Eagle	
	US Nexus Cyber Team	
	Islamic Cyber Team	
	AnonGhostMedia	
	TengkorakCyberCrew	
	Haghjoyan	
	FakeSec	
	CYBER Sederhana Team	

Pro-Israel Groups	Pro-Palestine Groups	Neutral Groups
	Irox Team	
	ChaosSec	
	The Cyber Watchers	
	Anonymous Algeria	
	Dark Team	
	177 Members	

Here's a mapping of the threat groups involved in the Israel-Palestine conflict. You can navigate around the mind map by dragging and dropping.

Hacktivist Dynamics

The abundance of pro-Palestinian hacktivists can be attributed to one primary factor: Hacktivism enjoys greater popularity in the Eastern hemisphere. When examining the landscape, it becomes apparent that even pro-Israel groups have their origins in Asia.

Notably, significant hacktivist collectives like KillNet and Anonymous Sudan have not only drawn numerous followers but have also significantly inflated this number, leading to considerable disruptions. KillNet, a pro-Russian hacking collective, justified its actions against Israel by referencing Israel's support for Ukraine in 2022, which Russia perceived as a betrayal and this also applies to many pro-Russian groups.

Anonymous Sudan, highly suspected of having Russian support, targeted Israeli alert systems, claiming responsibility for disrupting Israel's **Tzeva Adom** early warning radar system and launching a DDoS attack on the **Jerusalem Post** news service.

Anonymous Sudan's Post on Telegram

Groups with Islamic tendencies gather on the Palestinian side. Furthermore, one of Stucx Team's claims is that they hacked an Israeli SCADA system's website.

Stucx Team's Post on Telegram

Stucx's claim about Israeli Scada

On the Israeli side, Indian hacktivist groups stand out, and it should be stressed that they call on non-Muslim hackers in the UCC's and Garuna Ops' post to take action for an anti-Palestinian stance.

UCC's Post on Telegram

Not every group with Russian origin has taken a completely anti-Israeli stance yet. The Cyber Army of Russia consults its users on what stance it should take, as seen in the figure below.

Cyber Army of Russia's Post on Telegram

Some groups are just looking for chaos, with Five Families member ThreatSec stating that they are not on any side, but adding that they will still target Israel.

ThreatSec's Post On Telegram

The IT Army of Ukraine posted a message stating it is on Israel's side, but it does not look like they will take action.

IT Army of Ukraine's post on Telegram

November 2, 2023

Targets such as Japan, Azerbaijan, and India continue to be targeted by hacktivists. There are also leak claims about an attack targeting a company in Japan. Yokajawa, an international company based in Japan specializing in information technology and digital services, is reportedly a victim of a cyberattack. Threat actors asserted that they had obtained sensitive employee information. Hacktivist groups also carried out DDoS attacks on many Japanese websites yesterday.

Alleged hacking of "Yokajawa"

The 4 Exploitation Channel group, consistently striving to guide website administrators during defacement attacks, expressed their fatigue and the desire for a temporary respite. Interestingly, today is the day we are concluding this live blog documentary and shifting to alternative content formats.

Closure announcement of the 4 Exploit

We will **no longer provide daily updates** to this live blog, which we've been consistently updating with the latest developments since October 9th, unless significant changes or developments arise.

November 1, 2023

We have entered a new month, and the cyber war storm has relatively calmed down. Today's highlights were as follows:

Anonymous Sudan is targeting AP News with DDoS attacks, and the site was down for 13+ hours. Anonymous Sudan, which also targets Fox News, has been targeting Sudanese press organizations for a while.

Anonymous Sudan's Telegram post after 13 hours

Although Team Insane Pakistan targeted the intergovernmental agency OECD Nuclear Energy Agency website with a DDoS attack, it seems like an attack that does not have much effect or logical purpose.

Team Insane Pakistan's Telegram post

The 177 Member group, a South Asian hacktivist collective, shares database leaks from its American and Indian targets.

The 177 Member's Telegram posts

October 31, 2023

As we mentioned yesterday, the activities of APT groups continue to come to light as time goes by, unlike hacktivists. Amid the ongoing Israeli-Hamas conflict, a pro-Hamas hacktivist group has introduced a new Linux-based malware named BiBi-Linux Wiper, specifically targeting Israeli entities. This malware, an x64 ELF executable, can potentially compromise an entire operating system if executed with root permissions. Notably, it's designed to corrupt files rapidly, overwrite them, and rename with a "BiBi" extension, a term associated with the Israeli Prime Minister, Benjamin Netanyahu.

Recent insights from Sekoia suggest that the suspected Hamas-affiliated threat actor, Arid Viper, operates in two distinct sub-groups, each focusing on cyber espionage activities in the conflict, against either Israel or Palestine. Their tactics include targeting specific individuals and broader groups from sectors like defense and government, using methods such as social engineering, phishing, and deploying a variety of custom malware for surveillance purposes. That being said, it seems that we will witness the actions of APT groups, the elite units of cyber warfare, in the coming days, months, and years.

Again, as we said before, hacktivist actions continue to decrease in number, but they still occur in high numbers. Global targets continue to be attacked by hacktivists, "defacements," and DDoS attack announcements regarding the US, India, and Israel continue to be shared on Telegram channels. However, the claims, especially in South Asian hacktivist groups, seem random and unfounded these days. Although many groups cannot even identify the institutions they target, they continue their random attacks, e.g., America Website Bank(?)

Garuda Security's claims

The Cyber Error System group continues its defacement attacks, with India being one of its primary targets, and does not forget to leave a note for the Web Administrator on the "hacked" web pages.

Cyber Error System's Telegram post

Today's most important incident came from a hacktivist group that can speak English. SiegedSec breached BEZEQ, the leading telecom firm in Israel. Moreover, the group alleges that the Embassies of Finland, Hungary, and the U.S. in Israel were affected by the intrusion.

SiegedSec's claims, posted on Telegram

October 30, 2023

While the cyber conflict ran in parallel with the ongoing Israel-Palestine war, hacktivist groups dominated the spotlight for an extended period due to the strength of their voices. However, this doesn't diminish the significance of their actions, as such activities can accumulate and lead to significant problems. Additionally, hacktivist movements can serve as distractions for other activities. Thus, the most profound cyber threats come from APT (Advanced Persistent Threat) groups, and the cyber realm is becoming increasingly crucial in the evolving warfare landscape. Naturally, this situation will inevitably have reflections on the Israel-Hamas conflict. Moses Staff, a pro-Iranian group APT, has now resumed full-scale operations, continuing their previous campaign

by executing data breaches and disruptive attacks. They have set up a comprehensive information operation and are present on platforms like X, Telegram, and their website.

Moses Staff's tweet about the incoming attacks

Team Insane Pakistan, a hacktivist group we frequently feature, targeted important government bodies from many countries today. It carried out a DDoS attack on the websites of many critical organizations, from the State Oil Company to the Ministry of Defense across many Pro-Israeli countries.

Team Insane Pakistan's Telegram post

The official spokesperson representing Anonymous Sudan has announced that Western media outlets sharing 'false information' will face Distributed Denial of Service (DDoS) attacks. Following this, CNN, NYPost, Washington Post, and Daily Mail UK were subjected to DDoS attacks, with the attacks lasting an average of approximately two hours. In the initial stages of the conflict, Anonymous Sudan had also targeted the Jerusalem Post for a similar motive, highlighting the ongoing trend of media companies being frequent targets for such attacks.

Anonymous Sudan's first post about the recent attacks on media

October 27, 2023

The heart of hacktivism beats in Asia in recent years, but the first group that came to mind for a long time was Anonymous. Although various subgroups of Anonymous have been on both sides of this conflict, An "official" announcement came from Anonymous today. Although they expressed their good wishes to people on both sides of the war without taking an ideological or political side, they still accused the Israeli government of warmongering and displayed a pro-Palestinian attitude. However, many Twitter users approached this announcement cynically, thinking that this event would not yield any results or that the so-called official Anonymous group would not take any action.

Screenshot of the Twitter profile @anonewsco's post

Similar to the targeting of Singapore and Japan, a new hacktivism target has become Thailand. Team Insane Pakistan group carried out a DDoS attack on a hospital's website of Thailand. Unfortunately, civilian infrastructures continue to be targeted in such attacks.

Team Insane Pakistan's Telegram post, a hospital is on the target

Again, one of the most preferred attacks continues to be data leaks, an example of which was posted today by Irox Team, an American E-tracker website database leaked for "supporting" Israel.

Irox Team's Telegram post, database leaked publicly

Lastly, although various sources provide new publications, if you follow this live blog regularly, you may not have come across anything that will surprise you, but we would like to share the IoCs of malware used by hacktivists included in SentinelOne's article that we found useful. The RedLine stealer, Private Loader and their current IoCs detected by SentinelOne in the Israel-Hamas:

- **Redline Stealer (SHA1)**

0b0123d06d46aa035e8f09f537401ccc1ac442e0

- **PrivateLoader (SHA1)**

a25e93b1cf9cf58182241a1a49d16d6c26a354b6

8ade64ade8ee865e1011effebe338aba8a7d931b

October 26, 2023

Google has temporarily suspended live traffic conditions on its mapping services, Google Maps and Waze, within Israel. According to CNN's news, This decision comes in response to the escalating conflict in the region and the ground invasion of Gaza. Notably, Google took a similar step during the Russia-Ukraine conflict, temporarily turning off real-time vehicle data in Ukraine.

After Google's decision, an interesting cyber attack or, in other words, vandalism took place. As stated in CNN's news, cyber activists have exploited a feature of Google Maps, allowing them to post anti-Israel messages on the platform, mainly targeting the Rafah border crossing with statements like "F**k Israel" and "May god curse Israel's Jerusalem."

Certainly, this situation doesn't point to any security breach or attack on Google's part. However, it does underscore the potential for manipulation in user-generated content. As we observe the growing role of smart devices and artificial intelligence in modern conflicts, a concerning vulnerability arises – the likelihood of orchestrating deceptive data flows to these devices, a threat we believe will gain greater significance.

While we understand the significant harm that disinformation and misinformation can inflict in the real world, it is evident that false narratives can propagate at an accelerated pace within the digital world. Moreover, digital communication platforms and methods like social media can generate confusion -within the concept of hyperreality- even seemingly minor actions, regardless of malicious intent, have the potential to exert substantial influence.

Google Maps image of Israel

On the cyber side of the war, South Asia continues to be a battlefield, at least as much as the Middle East. India continues to be under intense attack with its pro-Israel stance. An Indian military/aircraft company was one of the targets of this day.

A newly monitored threat actor-group(?) Dark Team in South Asian hacktivist arena

Other Indian websites are also continuing to be targeted with defacement attacks as well as DDoS attacks.

Defacement attack of Indonesian hacktivists

Indian hackers are responding to this situation by adopting an intriguing tactic that hinges on leveraging the relatively strong connection between Pakistan and Turkiye. Team Insane Pakistan is informing its followers that

Indian hackers are attempting to mimic Turkish hackers to deceive Pakistani hackers.

Alert for scamming campaign

However, it seems that even if Indian hackers do nothing, other South Asian hackers continue to have problems among themselves. The ACEH hacktivist group has announced that it's not in the alliance with Garuda Security, seemingly due to a personal dispute.

ACEH Group's announcement

Although the Arab world seems to be mostly consolidated on the issue, some countries take a different stance. Anonymous Algeria threatens the United Arab Emirates against this situation and claims that if this stance of UAE continues, they will be subjected to an attack of an unprecedented magnitude.

Anonymous Algeria's threat to UAE

October 25, 2023

The GlorySec hacktivist group has adopted an intriguing strategy in their recent Telegram post. This pro-Israeli hacktivist group has claimed that Palestinian websites employ rudimentary, low-budget firewalls, rendering them susceptible to manipulation. They have directed this message toward Israeli officials, aiming to spotlight this vulnerability. It's worth noting that GlorySec claims not to disseminate the data they've acquired due to its false usage with the intention that it should be leveraged by Israel as needed.

In addition to addressing cybersecurity issues, GlorySec has taken a critical stance toward other hacktivist groups. They have accused pro-Palestine groups of supporting terrorism and being involved in Russian proxy warfare.

While hacktivism typically involves specific cyber actions, GlorySec's approach seems to lean more towards a strategic rather than a purely tactical orientation. By highlighting vulnerabilities and sharing some sort of TTP, they may inadvertently aid not only fellow hacktivist groups but also the authorities of one side in the ongoing conflict. However, it's essential to recognize that such public disclosures may also help adversaries identify their weak points.

GlorySec's mentioned Telegram post

As we've discussed on numerous occasions, various sectors often face cyber attacks based on the political alignment of their host nations. Whether it pertains to government entities or not, industries like Transportation and Aviation are prime targets due to their critical role in a country's logistical infrastructure, especially since they are points where a country's capabilities can be damaged.

Mysterious Team Bangladesh targeting Italian airport

Countries with alignments -other than Israel-Palestine- and especially countries that have concrete contributions to one side are affected by this situation a lot. Two airports in the UK and Italy were also the targets of DDoS attacks due to their pro-Israel attitudes.

Sylhet Gang targeting English airport

Not only airports but also aircraft companies are targeted. Hacktivists targeted the website of a Canadian aircraft company.

Canadian website defaced by the Garuda Security

Of course, they are trying to limit Israel's logistics capacity as well. Even though this time, the port is of the sea rather than of the air, the aim is the same. Team Insane Pakistan claims to have dumped the entire database of the Haifa Port website.

Team Insane Pakistan's database dump of Haifa Port

Although it is not very similar to the incidents we have discussed so far, we see an interesting pattern and another example of the Indian educational sector – and the healthcare sector – being targeted heavily. It is not known how conscious hacktivists are on this issue, but the fact that South Asian hacktivists generally attack India and prefer to disrupt civilian life instead of targets that can make a concrete contribution to the war seems to be an insight worth taking note of.

Cyber Error System's Telegram post, targeting Indian Governmental School

October 24, 2023

Hacktivist groups on both sides have predominantly used Telegram for coordination and sharing since the conflicts began. However, a recent development may bring a change to this situation. According to the Jerusalem Post, the "official" Telegram channels of Hamas and the al-Qassam Brigades were blocked for users who had installed the app via the Google Play Store on Sunday night. In response, Telegram explained, "Some of the channels you follow may no longer be accessible on your version of Telegram due to Google Play's guidelines." They also noted that these channels can still be accessed on other platforms or by downloading the Telegram for Android app directly from Telegram's website.

Additionally, Pavel Durov, Telegram's CEO, has defended the decision to maintain Hamas-related channels on the platform. He argues that this can potentially save lives by providing information and serving as a resource for researchers and journalists. Durov contends that removing these channels may not necessarily prevent harm, as Telegram users only see content they subscribe to. The debate revolves around the balance between preserving freedom of information and the risk of propagating misinformation and propaganda during conflicts.

Telegram post from pro-Israeli hacktivist group; The two "official" Hamas-Daesh channels on Telegram have been blocked for access

Yesterday, we discussed how pro-Palestinian groups extended their targeting to countries like Japan and Singapore. As the initial attacks were underway, numerous hacktivist groups and individuals initiated efforts to focus on international entities supporting Israel and generated hashtags on social media.

A hacktivist's call to OpIsrael hackers on Twitter

Similar calls and hashtags were circulated within hacktivist Telegram communities, resulting in the targeting of nations that supported Israel.

GanoSec's Telegram post

Iranian hackers remain actively involved in these attacks, as evidenced by their sharing of an Excel sheet containing the personal information of 7,000 Israelis. Moreover, within the same Telegram group, there have been recent reports of attacks on healthcare institutions in India.

Iranian hacktivist Telegram group, a proof video shared

Industrial plants, water treatment facilities, and SCADA systems are consistently targeted. The CyberAv3ngers group claimed they had successfully hacked Netanya's Waste Water Treatment Plant, sharing screenshots from the facility's systems. Similarly, the Stucx Team, known for numerous SCADA hacks, shared images from an unidentified SCADA system.

Alleged screenshots from various SCADAs

October 23, 2023

As the ongoing Israel-Palestine conflict persists across various fronts, we continue to witness daily fluctuations in activities, but even the "cyber warriors" seem to take a breather on weekends. So, we encounter fewer incidents compared to weekdays.

In this ongoing conflict, it's inevitable that everyone involved becomes a potential target for hacktivists. Japan and Singapore recently joined the global players in this arena.

GHOSTS of Palestine hacker group launched Distributed Denial-of-Service (DDoS) attacks on Japanese government domains as part of their '#OpJapan campaign in response to Japan's vote in support of Israel at the UN. Additionally, other pro-Palestinian hacker groups targeted Singapore. These groups include AnonGhost Indonesian from Indonesia and 4 EXPLOITATION from Malaysia and Ghost Team. Their combined efforts resulted in a cyber attack on a theater institution in Singapore, leading to website defacement and a data leak.

Screenshot of the defaced website by Pro-Palestine hacktivists

One of the important claims in recent days came from the **Anonymous Algeria** group. Although the hacktivist group said that they infiltrated Israeli police devices and accessed some sensitive files, they do not yet have any evidence of the accuracy of the claims.

Anonymous Algeria's claim

South Asian hacktivist groups continue to work together, as we saw in targeting Singaporean organizations. The Civil Aviation Authority of Israel was one of the common targets.

AnonGhost Indonesian post is also forwarded by other hacktivist groups.

The Turkish hacker group Ayyıldız Tim, known for its large Twitter following, has claimed that they've acquired **classified military data**, exercise records, and personnel details from the Israeli Ministry of Defense. Nevertheless, the screenshot they posted seems to only display citizen identification information. Furthermore, some Twitter users have pointed out that the shared data matches what was previously posted on "breachforums,"

casting doubt on the validity of the claim. This serves as a reminder that it's wise to approach any assertions made by hacktivist groups with a measure of skepticism.

Ayyıldız Tim's twitter post

One last incident of significant importance and contention revolves around the alleged intrusion by the Yemeni hacker group R70 into the systems of the Israel Electric Corporation, effectively gaining control. While Yemeni hackers may find themselves on opposing sides in the Yemen-Saudi Arabia conflict regarding pro-Palestinian hacktivist groups, the concept of a shared adversary appears to be a unifying factor.

R70 claims to breach Israeli energy company

October 20, 2023

We witness day by day that the cyber field is one of the most significant fronts of the war. Israel, which makes great efforts in defense, is also seeking complete coverage in this field. Israel is swiftly developing a cyber defense system called the **Cyber Dome**, inspired by the Iron Dome. It uses AI to filter cyber threats and involves experts from government departments, including the IDF and intelligence agencies. The Israel National Cyber Directorate is leading the effort, with contributions from private entities. While initially announced in 2022, it's apparently gaining momentum by now, due to recent events. Specific system details are yet to be disclosed.

However, before the cyber dome is closed to Israel's cyber lands, pro-Palestinian hacker groups will apparently continue sending their cyber missiles in **DDoS format**. Government bodies, one of the most obvious targets, have been subject to DDoS attacks since the first day of the war. The Israeli Ministry of Defense is at the top of these targets.

GanoSec's Telegram post with check-host verification

After announcing yesterday that it would take the pro-Palestinian side, ChaosSec said it would target gov[.]il, an Israeli government website.

ChaosSec's Telegram post: The main state website of Israel is going to hell

Unfortunately, one area where cyber missiles fall seems to be hospitals and clinics. Israeli hospitals and Israeli Ministry of Health websites were again targeted by GanoSec.

Shared by user named Xv888 on GanoSec's channel

WeedSec, on the other hand, carried out a defacement attack on a clinic, and its effect seems to continue.

WeedSec's Telegram post with defaced website

Alleged screenshots from SCADA systems continue to come from groups every day. However, sometimes, it can be not easy to verify these images.

The Cyber Watchers' forwarded Telegram post, breached SCADA screenshots

The Cyber Watchers group that we recently observed shared many screenshots from various Israeli SCADA systems.

The Cyber Watchers' Telegram post, breached SCADA screenshots

In the update we shared yesterday, we included a call for unity and common purpose for hacktivists on the Anonymous (D) channel. Maybe we may have started to see the fruits of this today. This evening, a call was made on the 4 Exploitation channel to unite and attack against Israel. It was also emphasized that the type of attack made does not matter, but the same target is key.

4 Exploitation's call to hackers

As we have memorized by now, targeting allied countries other than Israel has become a classic situation. Turk Hack Team (THT) targeted a US-based organization in the context of conflict and shared a major database leak. Yet, one of the interesting points is that the targeted organization is an organization called The Art Story, a foundation, which unfortunately reveals that all kinds of institutions are potential targets.

THT's Database leak post in a Turkish-speaking forum

The ongoing conflict between India and South Asian states extends into cyberspace, where they find themselves on opposing sides of this war. In response to BlackDragonSec's declaration of support for Israel, the Infinite Insight group released a retaliatory message.

Infinite Insight's answer to BlackDragonSec

In a recent update to WhatsApp, a structure similar to Telegram channels was offered to users, and hacktivist groups also started to use it. Although WhatsApp allows participants to hide their personal information while joining the channel, but if misconfigured, critical personal data such as phone numbers can expose you to these groups where hackers take part.

Team Insane Pakistan's WhatsApp channel announcement

October 19, 2023

Even if the silence continues relatively in the Israel-Palestine conflict, a few incidents today are critical. Soldiers Of Solomon, a hacktivist group, claimed to have taken control of assets such as over 50 servers and security cameras in the Israeli Nevatim military area.

They then made a huge and hard-to-believe claim that they had exfiltrated 25TB of data and encrypted it with ransomware. They also shared screenshots, satellite images, and security camera images from many computers and servers as proof of concept. Moreover, they added that they also collected information about Nevatim air base pilots' personnel data and their families.

Soldiers Of Solomon's Telegram post, flood continues with proof of concept images

Blacksec, in collaboration with the owner of Ghostsec, is directing its efforts towards more than 100 Modbus systems. Should they achieve their objective, this attack could potentially disrupt industrial systems and other vital

infrastructures.

BlackSec's Telegram post, they added that the attacks will continue

Another issue we have become accustomed to is targeting pro-Israel countries. Dark Strom also joined this trend, threatening all of Europe, and they said that its first attack would target France.

Dark Strom's Telegram post targeting France

South Asian hacktivist groups, on the other hand, seem to spare time for Israel when they are not targeting India. In a Telegram post, they are trying to carry out an extreme amateur attack at 9 PM in Malaysian time and 4 PM in Israeli time. Attack methods consist of fraud facts, swearing, and insults.

Mentioned Telegram post, translated via Google

Another scheduled attack came from the IRoX Team. IRoX Team has declared cyber war against Israel and the countries supporting Israel. The group shared their target countries (scheduled ones):

Oct 20: Brazil, Canada, Poland, Spain

Oct 25: India, United Kingdom, Australia

Oct 30: France, Norway, Austria, Germany

IroX Team's cyber attack warning

The ChaosSec group, which remained silent on the issue for a long time, was one of the groups that announced that it would take the Palestinian side.

ChaosSec's Telegram post

A post was shared on the Telegram channel called Anonymous (D) as a criticism that hacktivists sometimes conflict with each other even when they have common goals. Anonymous (D), who also uploaded a video, invites peace among hacktivists.

Anonymous (D)'s Telegram post

Another piece of news that was not an action but gave insight into future actions was the reactions to US President Joe Biden's visit to Israel, which was shared in hacktivist groups.

AnonGhost's Telegram post about the visit

On the GhostLocker Telegram channel, we covered in an article yesterday, they shared that they thought GhostLocker worried Israel. It is not known how much concern it will cause in Israel, but the new RaaS model they have introduced has the potential to start a new trend in the world of cybercrime.

GhostLocker developed by Pro-Palestinian GhostSec, mentioned Telegram post

October 18, 2023

In the aftermath of the heart-wrenching tragedy that claimed the lives of numerous civilians, the cyber world has seen many responses. However, it's a relatively subdued day in terms of tangible actions. Naturally, it's evident that this tranquility may well be the precursor to more turbulent times ahead.

This situation was called "Bloody Tuesday" by pro-Palestinian groups, and Israel was condemned. However, no action plan was shared.

KillNet's Telegram Post condemning Israel

Pro-Palestinian groups are consistently working on expanding their numbers. The AnonGhost group is trying to bolster its ranks as part of the #OpIsrael protests, and other hacktivist organizations are disseminating this message.

The AnonGhost's message shared on other Telegram channels as well

The ICC's manifesto, which we shared yesterday, appears to be yielding results as Pakistani hacktivist factions are allegedly uniting.

ICC's Telegram post with a video announcement

The Cyber Avengers group asserts that Israel's vital infrastructure has again fallen victim to hacking, with several distressing incidents reported in Yavne and Nahariya. The group has shared screenshots with cybersecurity companies, although there has been no confirmation yet.

Screenshots shared by Cyber Av3ngers regarding their claim

We have witnessed hacktivists and threat actors sharing **various tools and scripts** to serve their cause and increase the number of people taking action, a case we have been witnessing for days. A similar script is shared on a Turkish-speaking hacking forum to support Palestine, but they do not hesitate to ask for a fee this time.

The post on a Turkish-speaking hacker forum

October 17, 2023

Today, hacktivists continue to share their attack methods with their followers, as we observed yesterday. For instance, the AnonGhost group is distributing a script that helps users identify and exploit a vulnerability called CVE-2023-29489. The effectiveness of this script may be questionable, but it reflects the ongoing trend of information sharing within the hacktivist community.

AnonGhost's Telegram post, sharing Python script for the mentioned CVE

Similarly, the ./CsCrew group regularly selects new targets and recommends Denial of Service (DoS) tools to their followers in their Telegram channels. They claim that these tools can bypass Cloudflare's security measures, highlighting hacktivist activities' bold and audacious nature.

./CsCrew shares their targets and tools daily

The Islamic Cyber Corps group issued a rallying call by releasing a jihadist manifesto, urging all Muslim hacktivists to come together, articulate their objectives, and encourage them to pursue more substantial actions, emphasizing that common attacks like DDoS and defacement fall short of their aspirations.

I.C.C's statement and call to action

While hacktivism typically revolves around causing disruptions, the convergence of such a large hacktivist community is poised to generate disruptions that extend beyond the immediate horizon. What further underscores the significance of this situation is the realization that not only the Israeli government and military will be in the crosshairs, but also allied nations and occasionally even civilian infrastructure.

India, which has been exposed to more intense hacktivism than Israel, still maintains its throne. Numerous database leaks, such as the News Database India leak, are shared in South Asian hacktivist groups.

South Asian hacktivist groups continue to target India primarily

Apart from India, NATO countries, which are also intense targets, frequently face disruptions. Banque Banorient France and German Airways websites are critical sectors and targets exposed to DDoS attacks.

A bank in France was the target of DDoS attack

A popular target amongst the hacktivists, German Airways

When looking at the agendas of hacktivist groups, it sometimes seems that the issue is entirely outside of Israel, but Israel continues to be targeted as well. Cyb3r Drag0nz Team allegedly took down the Israeli Air Force website and shared it on their Twitter accounts.

Cyb3r Drag0nz Team's tweet about the alleged attack

Israeli hackers employed a noteworthy attack technique. The RedEvils group somehow gained access to the Gaza Now Telegram channel, boasting **over 1 million** followers, and successfully wiped out all its content. However, it appears they were unable to shut down the channel.

RedEvils' different approach to hacktivism

October 16, 2023

As we move into the second week of the Israel-Palestine conflict, the media is increasingly flooded with sorrowful images, and this grim reality is further amplified in the cyber world as more distressing visuals emerge. Cyber operations are rising in the landscape of hacktivism, which seem to increase like an uncontrollable avalanche.

KillNet, a prominent figure in the hacktivist landscape in recent years, has remained relatively quiet regarding significant actions, limiting its activities to sporadic incidents and threats. However, they have recently taken a new step by establishing an exclusive Telegram channel dedicated to engagements related to Palestine. Operating under the name **KILLNET PALESTINE**, the group has publicly reaffirmed its collaboration with Anonymous Sudan and declared its intention to focus its efforts on targeting Israel.

KILLNET PALESTINE's first Telegram post

While pro-Israeli hacktivist collectives, predominantly originating from India, occasionally launch minor attacks, they pale compared to the sheer scale of pro-Palestinian groups. The number of pro-Palestinian groups, which we identify in dozens daily, persists in conducting a diverse array of cyberattacks.

A hacktivist group known as the Haghjoyan Team, boasting over 40,000 followers on Telegram, boldly asserts that they have infected more than 5,000 Israeli citizens with malware and claims to have gained access to a staggering two terabytes of data.

Haghjoyan's Telegram post, screenshots posted as proof

Hacktivist groups are not just content with various attacks. They are trying to maximize the damage they will cause by sharing the websites they have detected vulnerabilities with their followers and other hacktivist groups.

> A list of 4300 Israeli websites with SQL injection vulnerability is shared on many Telegram channels.

Of course, the targets are not only military and government organizations. The Israeli mobile application called Pango Car was claimed to be hacked, and while its data is shared publicly, credit card information is sold separately. This shows that the actions taken are not always guided by ideologies.

Another group, Cyber Av3ngers, allegedly breached Orpak, a retail fuel market solutions provider in Israel. The released data suggests that the hackers managed to infiltrate Orpak's internal systems.

> Mobile Application Pango Car allegedly hacked.

The database leak of Cyber Tech Israel, held in Tel Aviv, is also shared on Telegram, but the fact that it is 2.8 MB in size and PDF format raises doubts about the leak.

Database dump of CyberTech Global shared on Telegram

An illustration of the frequent cyberattacks we expected for NATO and its allies emerged as a Singaporean hacktivist group conducted an attack. This Hacktivist Group asserted responsibility for the takedown of the Naples International Airport website in Italy and declared its intent to intensify its targeting of Italy.

Sylhet Gang's Telegram post about the incident

One of the countries highly targeted since the first day of the war was India due to its political agenda, and this situation continues. Educational institutions, in particular, are frequently targeted, and sensitive data is leaked.

Data leak of Zakir Husain Delhi College posted on Telegram

As we previously pointed out, hacktivists aim to amplify the extent of their impact, and here's another instance: the creation and unveiling of a mobile application designed to coordinate diverse attacks. According to reports about the app named MyOPECS, shared by Stucx Team, while it currently functions as a DDoS toolkit, it is expected to incorporate additional features in the near future, including DNS Enumeration, Port Scanning, Directory Busting, and Password Attacks.

MyOPECS PenTest mobile application

Although hacktivist groups can be serious threats, they lack complete organization. The hacktivist group Moroccan Ghosts apologized for hacking a target by mistaking it for an Israeli.

> *Rawad Company's RADIUS system was mistakenly hacked, thinking they were Israelis. As an apology from us, we have closed the security loophole in the system and will help them protect their data…*

October 13, 2023

Today's hot topic is the escalation of cyber warfare to a global scale, a development that has been gaining momentum in recent days. Numerous pro-Palestinian organizations have initiated cyberattacks against governments and nations sympathetic to Israel worldwide.

It seems that South Asian hacktivists have decided to join forces with Dragonforce Malaysia and act together. Of course, their target will be Israel and its supporter countries, but we can also predict that India will get a larger share of the attacks.

The announcement shared on the channels of many South Asian hacktivist groups

Mysterious Team Bangladesh announced they would target all NATO countries, India and South Korea, but they added that they excluded Turkey. The reason seems to be Turkey's neutral approach to conflict, and the fact that it is loved by the people of South Asia, which has a high Muslim population.

Mysterious Team Bangladesh's Telegram post targeting NATO

As they previously announced, Ghost of Palestine is one of the active groups aiming to continue cyber warfare globally. It seems like they will target more pro-Israel countries.

Ghosts of Palestine's Telegram post threatening Israeli allies

Mysterious Team Bangladesh had threatened South Korea, but another South Asian hacktivist group today claimed responsibility for the DDoS attack targeting the South Korean Ministry of Foreign Affairs.

Sylhet Gang brought cyber warfare to South Korea

India continues to be targeted even more than Israel, and one of the many attacks was on Madhu Vachaspati Institute India today.

Ghost of Palestine's Telegram post about the attack

Stucx Team, on the other hand, not only targets Red Alert, the famous Israeli missile protection system but also reveals how to do it to its followers. This system, which is of critical importance for Israel, has been one of the number one targets of hacktivists since the day the war began.

Stucx Team's guide to disrupt the mail server of the Red Alert

Even though KillNet announced its support for Palestine, there has been no major activity so far. But today, de-facto KillNet leader KillMilk announced that he would take action with his legion of **10,000 hackers**. KillNet's more active role may also indicate that larger cyber conflicts will occur in the coming days.

KillMilk's Telegram post

October 12, 2023

In the ongoing Israel-Palestine conflict in the cyber world, DDoS and defacement attacks and data leaks are frequently disseminated within hacktivist channels. However, quantifying the extent of harm inflicted on the entities they aim for remains a challenge. While targets like government websites, humanitarian organizations, and infrastructure systems do experience certain disruptions, these actions typically result in no significant consequences beyond temporary website blockages and annoyance.

Although it does not seem to cause immediate damage, one of the events that will cause the most extensive damage in the long term may be the **leaks containing many PII**.

Moroccan Ghosts hacktivist group shared a dataset containing many PII and credentials.

As we discussed not long ago, Indian hacktivist factions represent the predominant share among the few groups providing cyber support to Israel in the ongoing conflict. This scenario places India in the crosshairs of numerous hacktivist collectives, particularly those of South Asian and Pro-Palestinians. Thus, the underlying cause of this extra heightened attention is the political discord between India and South Asian nations with substantial Muslim populations, which adds a distinctive dimension to the situation.

Ganosec Team threatens India in their Telegram channel

South Asian hacktivist collective, defacement attack on National Savings Institute of India.

In parallel with the targets of physical warfare, pro-Israeli groups targeted a Lebanese governmental website and temporarily blocked access. This is another indicator that the war in the cyber world has spread everywhere.

Indian hacktivist's DDoS attack on Ministryinfo[.]gov

We mentioned that ransomware groups are also starting to get involved, and today, in a channel we observed, we saw that T.Y.G Team announced that they began ransomware attacks.

T.Y.G Team's Telegram post,"Ransomware attacks have begun…"

Another interesting point observed today offers a strange insight into the internal structure of hacktivist groups. END SODOMA group threatens people who leave their Telegram channel.

END SODOMA's threat

October 11, 2023

Today, the groups are carrying out attacks at an accelerating rate, and it's noteworthy that these attacks are also directed at various targets on a global scale.

The Pro-Palestinian groups targeting at US and European organizations, including the alleged DDoS attack on the European Parliament Traineeships website by a group known as Mysterious Team Bangladesh.

Team Insane Pakistan's Telegram post, service was unavailable for a brief time

Civilian targets, particularly those related to fundraising efforts, are vulnerable to attacks from both sides, as seen when Team UCC targeted "Defending Human Rights in Palestine."

Team UCC's Telegram post, Alhaq's website was down for a brief time but continued to have access problems throughout the day

Ghosts of Palestine, one of the most active hacktivist groups, has also announced its intention to target not only Israel but also Europe and the United States.

Ghost Of Palestine's Telegram post

On the pro-Israeli front, they claim to be targeting Iran, which supports Hamas and have shared a substantial database related to The Lorestan Petrochemical Company, totaling nearly 1 GB.

Gaza Parking Lot Crew's Telegram post

Other significant incidents for today are as follows:

AnonGhost claimed to get the API key for Israel's Red Alarm system.

AnonGhost's Telegram Post about alleged incident

Team Insane Pakistan is targeting Bank Israel with DDoS attack.

Team Insane Pakistan's Telegram Post and screenshot of proof

SkyNet allegedly published 6.5 million people's data from Israel.

SkyNet's Telegram post, 7zip file attached

Another prominent topic of today was the fact that posts in the context of the Israel-Palestine conflict began to be made in hacker forums. Posts from threat actors from both sides fill trending topics. Israel Military Personnel data, Israeli insurance company's database, Palestine Ministry of Higher Education and Ministry of National Security credentials and Palestine Ministry of Foreign Affairs database are among the few.

On many hacker forums Israel-Palestine conflict-related posts and leaks are published

Below are domain names created in support of Israel in the ongoing Israel-Palestine conflict. While some of these domains are legitimate, the majority serve the purpose of phishing.

Domain names created to support Israel

October 10, 2023

As the intensity of the conflict, which has become an official war, increases, it continues to be reflected in the cyber world similarly. As of October 10, many hacktivist groups have come back to life, and countless operations and attacks continue to be shared non-stop on Telegram channels.

Last week, the International Committee of the Red Cross (ICRC) released a set of guidelines outlining rules of engagement for civilian hackers participating in conflict scenarios. However, looking at the attacks, it seems that this call did not have much of a response. Civilian infrastructures and organizations are also under attack.

Pro-Palestinian hacktivist group END SODOMA shared a piece of code to disable Israeli alarm systems. Again, according to the post they shared on Telegram, it seems they disrupted alerts, at least for a while.

END SODOMA's Telegram Post, Code piece for disrupting alert systems

END SODOMA's following post

Israeli government sites, media agencies, and military systems are the most targeted systems. The preferred attack vector is usually DDoS. Israel Space Agency was also among the targets targeted today.

YourAnon's Telegram Post about disruption of Israel Space Agency's website

Although the main target is governmental organizations, the civilian infrastructure also receives its share of attacks. Healthcare, education and water systems are governmental bodies but, they are also targets that affect civilian life.

Mysterious Team Bangladesh is disrupting the governmental organizations.

Team_insane_Pakistan is targeting Israeli healthcare

Many of the few pro-Israel hacktivist supporters are Indian hacktivists. In the cyber world, this situation also sparks conflicts between hacktivist groups and leads to the targeting of Indian groups.

Telegram post of CYBER ERROR FORCE targeting India.

In a major attack today, SiegedSec and Anonymous Sudan teamed up and targeted Israeli Infrastructures. It seems that their collaborations, like their operations, will continue.

SiegedSec's Telegram post

There was only one recorded attack during the day from pro-Israeli Indian hacktivists. Palestinian network devices were targeted in the attack, in which Team UCC and Anon_Sec_101 worked together.

Team UCC's Telegram Post, forwarded by Garuna Ops

One of the interesting events is that the conflict has also attracted the attention of ransom groups. Ransomed.vc is trying to purchase access available in Iran and Gaza-affiliated countries.

Ransomed.vc's Telegram post, seeking for access sales

Track Dark Web Activity with SOCRadar

With SOCRadar's Cyber Threat Intelligence and Digital Risk Protection modules, you can effortlessly keep a constant watch on threat actor activities in every surface of the web, including Telegram channels.

SOCRadar's **Digital Risk Protection** module makes it simple to monitor the actions of threat actors. The Dark Web Monitoring tab automatically provides pertinent information about products and technologies discovered within your digital assets. Conversely, Dark Web News shares significant updates from deep and dark web forums, social media platforms, and communication channels like Telegram, complete with screenshots and textual content.

Discover whether your data is at risk from threat actors and take steps to mitigate these risks in your digital assets. SOCRadar conducts routine internet scans to identify new Telegram groups where your company's leaked data may be found. Moreover, it promptly alerts you to any information related to your organization.

> *SOCRadar, Dark Web Monitoring*
