Evolving Cyber Dynamics Amidst the Israel-Hamas Conflict - Check Point Blog

By etal

Published: 2023-10-30 · Archived: 2026-04-14 02:00:33 UTC

Highlights:

- **Pro-Palestinian cyber activists have broadened their scope beyond Israel, targeting countries perceived as Israeli allies in the war against Hamas.**
- **The cyber operations mainly serve as informational and retaliatory tactics, with limited reported damage.**
- **Target selection is influenced by previously established focus areas of these groups and evolving geopolitical events.**

As the war between Israel and Hamas, named “Iron Swords,” commenced on the morning of October 7, it also marked the beginning of intensified cyber engagements from various threat actors.

In our prior analysis, which explored cyber incidents in connection with the Israeli-Hamas war, we primarily examined attacks targeting Israeli interests. Yet, as the conflict has unfolded, nations expressing support for Israel have also been drawn into the cyber fray.

In our prior blog post, which addressed the cyber incidents intertwined with the ongoing Israeli-Hamas war, we focused on cyberattacks directed at Israeli entities. However, Israel has not remained the hacktivists’ exclusive target. Since the beginning of the conflict, in particular as foreign leaders expressed their solidarity with Israel, additional nations were added to the roster of potential targets.

Unlike in the Russian-Ukrainian conflict, where a shift in focus towards third-party nations took months, for Russian-affiliated groups like Killnet to reorient their focus towards non-Ukrainian targets, in this instance, cyber groups have swiftly transitioned to these new targets immediately following statements of solidarity with Israel.

These groups have often reoriented their efforts towards their established targets, albeit reframed under the context of the current conflict.

The United States, France, India, and more recently, Italy have seen a notable uptick in cyber activities against them. French digital infrastructure, for instance, experienced over 300 incidents, predominantly DDoS attacks and website defacements with minimal impact.


Attacks Timeline and Examples

Attacks Timeline and Examples

Simultaneously with the war's commencement, several cyber groups announced their intentions to engage digitally. Mysterious Team Bangladesh, a group that has regularly participated in various cyber operations against France for its colonialist past, as well as against India and Sri Lanka, declared its readiness to initiate cyberattacks against Israeli targets and promoted collective action with the hashtag **#OpIsraelV2.**


OpIsraelV2

This team collaborated with "Team_insane_Pakistan," exchanging target information and successes. Their attacks targeted various Israeli entities including the space agency, port authorities, media outlets, the Israel Defense Forces (IDF), and financial institutions, yet the inflicted damage was minimal.
By October 8, a mere day after hostilities began, cyber collectives signaled that countries aligned with Israel would be subject to their campaigns.

By October 9, numerous claims of cyberattacks on U.S. entities emerged, correlated to the United States' support for Israel. Pro-Palestinian channels have since been rife with discussions of over 60 such incidents.

The EU’s suspension of financial aid to the Palestinians on October 10 led to a flurry of cyber operations targeting European organizations.

https://www.euronews.com/my-europe/2023/10/09/brussels-backs-israels-right-to-self-defence-as-it-halts-aid-to-palestinians

In response, several groups asserted that they had directed their efforts toward European entities.

Other targeted entities included the Central European University, EU GDPR site, EU Parliament programs and more. The rationale behind these attacks was articulated by another actor, SYLHET GANG-SG. France was overall the most targeted country with more than 300 reports of attack listings.

Although there is a certain degree of correlation between target allocation and recent news events, the selection of targets was also influenced by factors such as availability and the group's prior activities. For example, groups like "Cyber error system," which typically concentrate their efforts in Asia, particularly India, continued to maintain their focus on the region. They justified their ongoing attacks by citing the ongoing conflict as a rationale. The number of attacks on India exceeded 230.

As various world leaders arrived in Israel for discussions and to show solidarity, their countries received special attention from the attackers.

During his visit to Israel on October 17, German Chancellor Scholz declared, “Israel: Germany is at your side.” In response to this statement, reports of Distributed Denial of Service (DDoS) attacks targeting German entities increased. These attacks claims included airline organizations such as German Airways and others.

However, many of these attack declarations did not wait for official visits. In fact, many of the attacks on Western targets occurred before the visits of notable figures such as US President Biden on October 18, UK Prime Minister Sunak on the 19th, and French Prime Minister Macron on the 24th. For example, Prime Minister Sunak’s personal website experienced a DDoS attack by the hacktivist actor SYLHET GANG-SG. Similar attacks were also launched against the Cyprus police, several Canadian entities, the British military, and other targets.


Cyprus president post

Even UNICEF has been listed as one of their targets.

Arab nations that did not declare their clear support for the Palestinians faced criticism and, in some cases, came under cyberattacks.

Targeted Islamic entities included the Organization of Islamic Cooperation (OIC), who were lambasted for their lack of assistance.

Starting on October 23, over the past few days, there has been a notable emphasis on targeting Italian entities. This has manifested in disruptions at several Italian airports and governmental ministries, including the Italian Ministry of Foreign Affairs office, municipalities, the Office for Digital Italy, Italian banks, AeroItalia, news agencies, the Italian Acosta airport, the Italian Bari Karol Wojtyła Airport website, Italy Calabrian Airports Systems website, and the Naples International Airport website.

Conclusion

The digital landscape serves as a mirror to geopolitical tensions, with hacktivist groups rapidly adapting their strategies to reflect the unfolding developments on the global stage. The ongoing war between Israel and Hamas showcases this dynamic, with the scope of cyber operations extending well beyond the immediate theater of war. These collectives, highly attuned to political shifts, leverage cyber tactics to influence public perception and national policies.

The cyberattacks, primarily through DDoS campaigns and website defacement, have targeted a diverse array of entities — from national infrastructure to individual political figures' digital assets. Each operation carries a message, an attempt to disrupt the normalcy of digital operations and to signal the hacktivists' presence in the global conversation.

While the direct damage inflicted by these cyberattacks remains relatively contained, the broader implications are significant. The persistence and evolving nature of these threats underscore the need for robust cybersecurity measures. Nations and organizations must recognize the complex interplay between physical conflicts and their digital counterparts. As such, a proactive approach in cyber defense is not just prudent; it is imperative to safeguard against the cascading effects of these targeted operations.

This landscape of cyber warfare serves as a stark reminder that in our interconnected world, allegiances and actions have consequences that reverberate through the digital ether. It is a call to action for continual vigilance, improved cybersecurity collaboration, and strategic responses that can adapt as quickly as the threat actors themselves. As we observe the meticulous execution of these cyber operations, it becomes clear that in the theater of modern conflict, the digital front is as critical as the physical one.

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