Cambridge Cybercrime Centre
Briefing Paper – 16 October 2023

Defacement Attacks on Israeli Websites

Anh V. Vu, Alice Hutchings, Ross Anderson

Since the Hamas attack on Israel on 7th October 2023 and Israel's declaration of war, hacktivists have hit Israeli digital assets via various cyberattacks such as distributed denial-of-service and website defacement attacks. One DDoS victim appears to have been the Jerusalem Post. Defacement was used in previous conflicts, most recently following the Russian invasion of Ukraine, to taunt opponents and disseminate propaganda. We report empirical evidence of defacement attacks on Israeli websites observed through our near-real-time monitoring system.

Quantitative datasets

We analyse 8 659 defacement attacks within 2 weeks before and 1 week after the event, as part of over 350k records in our collection of the five most popular defacement archives used by defacers as a hall-of-fame to self-report hacking achievements: Zone-H, OwnzYou, Zone-XSec, Haxor-ID, and Defacer-Pro. Data reliability and completeness are carefully verified with semi-automatic validation, de-duplication and correction [1]. Victims are identified based on ccTLDs, IP geolocation, and their hosting AS geolocation (excluding CDNs). To measure the change in hacking community sentiment, we extract 565 posts related to the ongoing war on Hack Forums from the CrimeBB dataset [2].

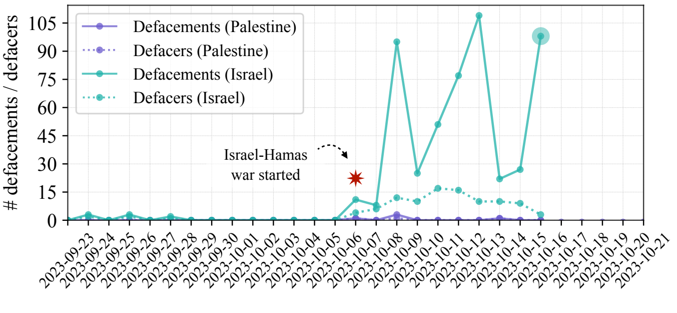

Figure 1: Defacements and defacers hitting two countries.

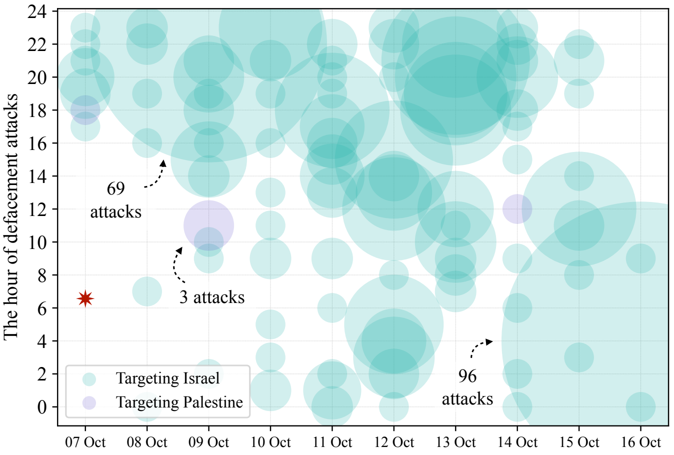

Figure 2: Defacements hitting Israel and Palestine by hour.

Israeli websites are being defaced

There is clear evidence of attacks against Israeli websites. While Palestine suffered only 5 defacement attacks by 3 defacers, we see 531 attacks on Israel by 102 defacers, making Israel the fourth top target country in our three-week study period, behind the US, India, and Indonesia: see Figure 1. Israel had suffered almost no defacement during the previous few weeks; attacks targeting Israel only started a few hours after the Hamas attack then escalated quickly; see Figure 2. A small spike occurred on 7th October; the next big one was two days later, following Israel's declaration of war, with 95 attacks (69 at around 10 PM); the peak of 109 attacks is on 13th October. The number of defacers did not increase proportionally but gradually, suggesting that new attackers have been drawn to target Israel over time, but they have done less on average despite some days of significant activity.

Defacement patterns exhibit some similarity with what happened when Russia invaded Ukraine in 2022; see Figure 3. The surges in attacks occurred quickly, while the attacker peaks lagged by a few days, presumably as more defacers heard and joined. Participation then dropped steadily, with only three attackers still active on 16th October – following the pattern in the Russia-Ukraine conflict. Offensive activity against Israel was less than that against Russia but more than that against Ukraine, whether measured by attacks or attackers. While attacks targeted both sides in the Russia-Ukraine conflict, the Israel-Hamas war has been one-sided, with no significant attacks against Palestine thus far. One significant caveat is that Palestine has many fewer websites, many of which are hosted overseas. Defacement attacks on Israel also appear to be more persistent than those on Russia or Ukraine, and it remains to be seen if and when these attacks will tail off.

Defacement motives. Defacers are highly centralised: the top 10 most active accounted for 78.54% of attacks, while the top one contributed 20.34%. To understand their motivations, we analyse messages left on defaced pages, considering a political sentiment to be supporting one side if a support or objection is expressed. Defacer signatures without a clear war-related statement are considered self-aggrandisement; they are marked as financially motivated if we see adverts for hacking services e.g., '*contact me for shells*'. Among 536 defacement attacks targeting Israel and Palestine, 199 are self-aggrandisement (37.13%). While only one supports Israel, 331 defaced Israeli sites support Palestine (61.75%) with hashtags such as #opisrael, #freepalestine, #savepalestine, and #savegaza. That proportion is much higher than we saw in the Russia-Ukraine war, where only around 7% of attacks explicitly expressed support for either side [1]. There are three expressing warlike sentiment but without clear support for either side, and two are financially motivated.

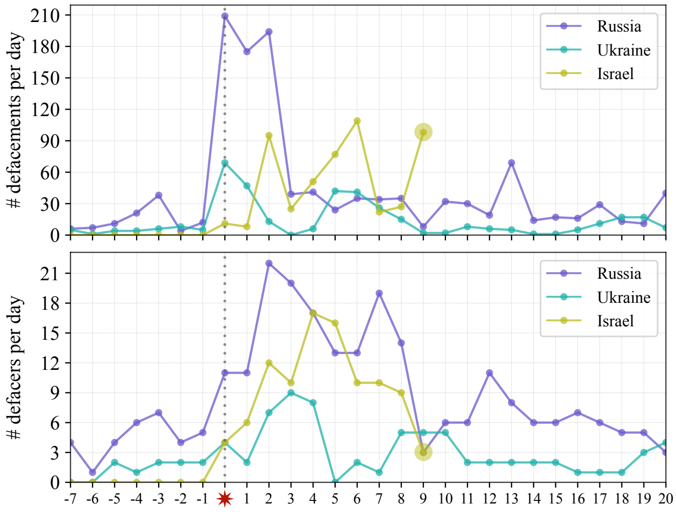

Figure 3: Number of defacement attacks (top) and defacers (bottom) targeting Israel around 7 Oct 2023, in comparison with those seen with Russia and Ukraine on 24 Feb 2022.

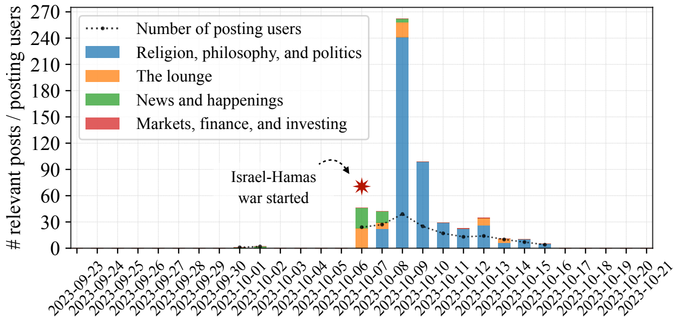

Figure 4: Hack Forums posts about Israel and Palestine.

Choice of targets. There is very little evidence of high-profile targets. 443 (82.65%) are businesses under `.co.il` and 16 (2.99%) are organisations under `.org.il`. The few special compromised targets include an Israeli housing association, partly exploited on 13th October 2023, a subdomain of the Israel Defense Forces under `.idf.il`, and nine subdomains of the largest public college in Israel. We see five `.ps`; the rest are under generic ccTLDs: `.com` (42), `.net` (4), `.org` (2), `.club` (3) `.biz` (1), and nine IP addresses that are not identifiable. As in the Ukraine war, most defacement targets are strategically unimportant.

Hacking community discussions

As the conflict escalated, there was an immediate surge in relevant posts on Hack Forums, as depicted in Figure 4. A similar pattern with defacement attacks and defacer activity is that posting volume relating to the war peaked a few days after Hamas attacked Israel, at around 270 relevant posts. The number of posting users increased then decreased steadily, suggesting that while users were highly active on 9th October, their engagement waned over time. Despite a surge in activity, forum users did not discuss ways to attack either country, presumably as Hack Forums has discouraged users from committing cybercrime. The primary discussion board on 7th October was general chats and *'news and happenings'*, but traffic shifted to *'religion, philosophy, and politics'* in the following days, while other boards exhibited trivial activity. Interest then declined, dwindling to around 10 posts per day after a week.

Concluding remarks

The attacks on Israel and its declaration of war sparked an outbreak of website defacement attacks, with a similar pattern to what have been seen in the aftermath of the Russian invasion of Ukraine [1]. The main difference is that it is one-sided. Supporters of Palestine have attacked Israeli websites, but the number of attacks on Palestinian websites has been trivial. We will analyse additional attack vectors and keep monitoring the situation with follow-up reports.

[1] Anh V. Vu, Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton, and Ross Anderson. "Getting Bored of Cyberwar: Exploring the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict". *In Proceedings of the ACM Web Conference (WWW)*, 2024.

[2] Sergio Pastrana, Daniel R. Thomas, Alice Hutchings, Richard Clayton. "CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale". *In Proceedings of the ACM Web Conference (WWW)*, 2018.

At the Cambridge Cybercrime Centre, we make our research data available to other academics, see: `https://cambridgecybercrime.uk/`.