Hacktivist Groups Use Defacements in the Israel Hamas Conflict

By DarkOwl Content Team

Published: 2023-10-26 · Archived: 2026-04-02 12:37:08 UTC

October 26, 2023

Disclaimer: DarkOwl is not affiliated with any of the groups mentioned in this article and do not support the actions of cybercriminals regardless of their motivations. This information is provided for informational purposes only and has not been independently verified.

Introduction

Defacement attacks, involve the unauthorized modification or vandalism of a website or web application. These attacks typically result in the alteration of the website's content, appearance, or functionality by attackers with malicious intent. The primary goals of defacement attacks are usually to deface the targeted website, display a message or image, and often to spread a message or agenda, drawing attention to the attacker's cause or skills.

It's important to note that defacement attacks are just one form of cyberattacks, and they usually don't involve data theft or damage to the website's infrastructure. However, they can still have a significant impact on the website's reputation and the trust of its visitors as well as voicing political messages.

As the events in Israel and Gaza have unfolded, defacements have been a common technique used by cyber actors to target opponents. Here we examine some of the groups conducting these attacks and the victims.

DragonForce Malaysia

DragonForce Malaysia is a pro-Palestinian group located in Malaysia. The group are active on social media with accounts on Telegram, Twitter and Instagram. They also have their own website and forum where they detail their activities.

Historically the group have primarily conducted distributed denial-of-service (DDOS) and defacement attacks, and this pattern is being replicated in response to the October 07 attack on Israel. However, they have also been seen to use other exploits.

Since the beginning of the conflict, DragonForce have mounted defacement attacks against approximately 125 websites with .il domains. There does not seem to be a pattern to the websites that are targeted other than their affiliation to Israel, although multiple Op names have been used on their various defacement messages. As shown below they have also used their defacements to encourage other hackers to join their cause.

Their Telegram channel has also been used to highlight other attacks that they have conducted, including a claim to have accessed the “Israel Telephone system Management,” as well as other Israeli Telcos. Samples of the data have been posted on their telegram channel. They are also sharing leaked databases as seen in the image below.

Cyb3r_Drag0nz_Team

Similarly, to DragonForce Malaysia the Cyb3r_Drag0nz_Team is a pro-Palestinian group which has been active creating defacements since the beginning of October. However, they appear to have cast a wider net in terms of who they are targeting with a number of US victims in the education space as well as in other countries, including Israel.

As well as providing details of the group in their defacement message they also supply the usernames/Aliases of individuals who have assisted in the attack as shown below. They also provide details of their Telegram and Twitter accounts.

This highlights the fact that groups which conduct defacement attacks are usually looking for notoriety and often are active on social media in order to publicize their actions. This group have conducted defacement attacks against approximately 157 websites since October 08, 2023, as of the writing of this article.

The Telegram account of this group has been used to promote the defacements it has conducted; this appears to be the main activity that they conduct although they have also released leaked information purporting to contain

Israeli citizen data. This underscores that with this conflict normal citizens are being targeted as well as governments and military organizations.

X7root

This group has also conducted defacement attacks against Israeli websites, including kdh.org.il which is the Jewish Burial society, this appears to still be active. This defacement message also includes an image from the Holocaust likely to cause the most amount of offense possible. The image is not included here but the accompanying message is shown below.

Little is available about this group, but they do also have a Telegram channel which has previously been used to sell exploits and requires a $90 subscription fee. However, recent posts on the channel have been anti-Israel in nature and provide details of the websites which have been defaced. In posts made on Telegram the user states that he is Arab and shows support for individuals in Gaza. The user is using the #OpIsrael which has been used by many pro-Palestinian groups.

Conclusion

Defacement attacks are not a new technique, but they can become particularly effective in times of conflict, as they were in Russia and Ukraine, in order to share the attacker's message. The majority of defacement attacks that we have observed have been conducted by Pro-Palestinian groups, but Pro-Israel groups are also conducting cyberattacks. Defacements are a powerful tool for hacktivist groups seeking to use their skills to share a message.

Defacements are in some ways unique in that they seek to publicize the actors behind them, their views and their activity. Therefore, they are more prominent and easier to detect than some other attacks and usually less destructive as they do not tend to affect the underlying infrastructure. As hacktivists seek to take a stand, they differ from the more traditional cyber espionage which seeks to stay in the shadows, but it is very likely those attacks will escalate in the coming months.

Stay up to date with the latest research from the DarkOwl analyst team and subscribe to our email newsletter.
