OpIsrael: A Decade in Review

By Radware

Archived: 2026-04-19 02:00:21 UTC

OpIsrael is an Anonymous operation that was launched in November 2012 in response to an Israeli military operation, Pillar of Defense.

Download a Copy Now

Anonymous and several cornerstone operations like OpIsrael have faced a significant decline in support and backing for years. This was the result of the fragmentation of Anonymous, competition from other threat groups, and the general escalation of the threat landscape. But over the last year, the war in Ukraine and geo-political tensions around the world have resulted in a renewed growth in hacktivism that has revolutionized the way armed conflicts will be fought in the future.

Background

OpIsrael is an Anonymous operation that was launched in November 2012 in response to an Israeli military operation, Pillar of Defense. Pillar of Defense was an eight-day operation launched by the Israel Defense Force on November 14th, 2012, in response to 100 rockets that were fired at Israel within 24 hours from the Hamas-governed Gaza Strip.

At the time, OpIsrael was not an official operation, but rather a battle tag the group of hacktivists associated with Anonymous chose to use for their response to the Israeli operation. During the Anonymous operation in 2012, hundreds of Israeli websites were targeted with data breaches, defacement, and denial-of-service attacks. This left many security professionals wondering if this was what the future of war would look like and if a hacktivist group such as Anonymous could be considered a legitimate army.

The following year, Anonymous moved to create an annual coordinated campaign against Israel under the battle tag, OpIsrael. The inaugural campaign was launched on April 7, 2013, parallel to Holocaust Remembrance Day, with the goal to "erase Israel from the internet." The operation targeted networks and applications in Israel for what Anonymous perceived as human rights violations against the people of
Palestine in hopes the campaign would bring attention to the ongoing Israeli-Palestinian conflict.

Timeline

Over the last decade, OpIsrael has evolved both in its impact and relevance. In November 2012, OpIsrael was just a one-off response to an Israel military operation in the Gaza Strip. Still, OpIsrael gained widespread attention in April 2013 after Anonymous announced a dedicated yearly campaign. As the years passed, the operation continued to target Israeli institutions to raise awareness about the Israeli-Palestinian conflict. However, the collective's impact slowly declined in recent years due to the fragmentation within Anonymous, improved cybersecurity measures, shifting public opinion, and the rise of other hacktivist groups. As a result, OpIsrael's influence and effectiveness have diminished substantially, causing the campaign to lose much of its initial momentum and support.

2014 - During OpIsrael 2014, Anonymous and its affiliates continued their operations against Israel, hoping their attacks would raise awareness and support the people of Palestine. Attacks at that time mainly consisted of crowdsourced-based denial of service attacks, website defacements, and data breaches. In some cases, the hacktivist leaked personal information, including email addresses, passwords, and phone numbers. It is important to note that in 2014, several hacktivists were seen repackaging and publishing old data dumps and new leaks. This is a tactic that would be used heavily in the future as OpIsrael relevance declined. It was also important to note that a second operation, OpIsrael Reloaded, was launched in July 2014 by a pro-Muslim, Indian-based hacktivist.

2015 - During OpIsrael 2015, we began seeing Anonymous share knowledge with other members in IRC chats and on paste sites1. This is likely due to the group realizing the increased challenges they faced with maintaining a yearly operation with the same level of impact. Despite the hacktivist claims of widespread outages, the 2015 campaign was relatively limited due to Israeli authorities and organizations taking the appropriate measures to prepare for an attack.

2016 - During OpIsrael 2016, Anonymous began repeating many of its slogans and reposting content from the previous operations. At the time, the collective was distracted by the US presidential election. Before this year, Anonymous was mainly a voice for the powerless but had begun supporting political candidates as election-related cyberattacks started to take center stage. As a result, OpIsrael suffered and began to lose complete support for the operation.

2017 - During OpIsrael 2017, Anonymous once again attempted to leverage all the resources it could to combat the escalating defensive measures deployed by the government and organizations in Israel. In addition to repacking old data leaks, the group began searching for unprotected websites of small and medium-sized businesses in hopes of a more significate impact than the years prior. What was left of Anonymous—and its affiliates associated with OpIsrael—started focusing on maximizing effort by building groups and social channels to better organize those involved. Inside those channels, Anonymous began sharing more toolkits, loaded with denial-of-service scripts, but there was no large adoption of IoT botnets by the collective.

2018 - During OpIsrael 2018, members of Anonymous continued to attempt to transfer knowledge to new hacktivists by sharing tools and recommendations for launching attacks. As a result, more defacements and simple denial-of-service attacks occurred compared to previous years. The collective started sharing detailed information about how to run reconnaissance operations, launch web application attacks and use Shodan2 or Google Dorks3 to increase their overall impact. One of the main concerns for many organizations during 2017 was the shift away from targeting well-protected assets to targeting small to medium-sized businesses and Israeli citizens who were indirectly involved with the conflict in Palestine.

2019-2020 - In 2019 and 2020, OpIsrael suffered a significant loss in support as Anonymous fell apart due to political infighting and a shifting of public opinion related to the Israeli-Palestinian conflict. The threat landscape evolved dramatically during these years as geo-political tensions flared up, making way for state-affiliated cyberattacks related to regional disputes. 2019 was also the year that the Israeli government targeted and killed a group of Hamas-linked hacktivists in Gaza with an air strike after the group launched a cyberattack against Israel, forcing many threat actors to think about the potential consequences of their attacks. The following year, a newly formed group called Hackers of Savior launched a one-off defacement campaign in May that targeted thousands of Israeli websites showing a video and a countdown related to Quds Day.

2021 - Following the downfall of Anonymous and the lack of support for OpIsrael, a group of pro-Muslim hacktivists from Southeast Asia launched a new campaign called OpsBedil to fill the void. In 2021, cyberattacks in general were mainly reactionary in the Middle East, with minor cases of hacktivism in the region typically following physical or political confrontation. Specifically, OpsBedil was a political response by DragonForce Malaysia to the Israeli ambassador to Singapore stating that Israel was ready to work towards establishing ties with Southeast Asia's Muslims-majority nations. As a result, the group and several affiliates launched a series of DDoS and defacement attacks against several organizations in Israel during June and July.

2022 - Following the success of OpsBedil the year before, DragonForce Malaysia launched OpsBedil Reloaded in response to tension in the Middle East during Ramadan. Over the year, the group grew to over 13,000 members who mainly communicated on their private forum. During this campaign, DragonForce Malaysia and other threat actors targeted several organizations in Israel with defacements, denial-of-service attacks, and data leaks. Hacktivist campaigns like OpsBedil, while nowhere close to as notorious as OpIsrael once was, present a renewed level of risk for the region. Unlike Anonymous, which had very little bandwidth remaining to target Israel, DragonForce Malaysia and its affiliates had the time, the resources, and the motivation to present a new moderate level of risk for Israel and overshadowed anything that resembled OpIsrael in the month of April.
