March 26, 2025

OpIsrael 2025: Hacktivist Coordination Intensifies Ahead of April 7

Key Insights:

- OpIsrael and OpJerusalem are recurring hacktivist operations targeting Israel around April 7 and the last Friday of Ramadan.
- Rising OpIsrael mentions signal imminent attacks; usage spiked after March 18, 2025.
- 2025 messaging expands targets to include Israel's global allies like the U.S. and U.K.
- Groups like Holy League represent growing, multi-national hacktivist coalitions.
- Advanced Web DDoS attacks have replaced traditional methods, rising 550% in 2024.
- Legacy DDoS tools and WAFs can't stop modern Layer 7 attacks; behavioral AI defenses are essential.

Initiated by the hacktivist group Anonymous in 2013, OpIsrael is an annual coordinated cyber campaign that targets Israeli websites and online services. The campaign typically occurs on April 7, aligning with significant dates such as Holocaust Remembrance Day and, in recent years, the anniversary of conflicts involving Israel.

OpJerusalem is another annual cyber campaign orchestrated by anti-Israel hacktivist groups to coincide with Iran's Al-Quds Day, observed on the last Friday of Ramadan. In 2025, the last Friday of Ramadan falls on March 28. Established in 1979, Al-Quds Day symbolizes opposition to Israeli control over Jerusalem. The campaign's objective is to conduct cyberattacks against Israeli entities, including website defacements, distributed denial of service (DDoS) attacks, ransomware distribution and data leaks. In 2024, Israel's National Cyber Directorate alerted organizations to the increased risk of attacks around Al-Quds Day, advising them to bolster their cybersecurity measures to mitigate potential disruptions.

The inaugural #OpIsrael was launched in response to Israeli military operations in the Gaza Strip, with the stated goal of "erasing Israel from the internet." Hacktivists employ various cyberattack methods during these campaigns, including DDoS attacks, website defacements and data breaches.

Over the years, OpIsrael has drawn participation from various hacktivist groups worldwide, including pro-Palestinian and pro-Muslim collectives. While the effectiveness of these attacks has varied, they have occasionally led to temporary disruptions of Israeli government, military and private sector websites. Since its inception, OpIsrael has developed into a multifaceted movement that operates across several fronts. At its core are cyber operations aimed at disrupting Israeli government, corporate, and institutional digital infrastructure, while also extending attacks to international allies and entities that support Israel's policies. Alongside these digital offensives,

the campaign promotes economic boycotts, urging individuals and organizations to avoid products and businesses seen as complicit in the occupation or directly supplying the Israeli military—an effort designed to apply financial pressure and disrupt economic support. Social media activism plays a vital role in the movement, with participants working to raise global awareness of Palestinian struggles by exposing alleged human rights abuses and amplifying Palestinian voices through storytelling, documentation and digital campaigns. Beyond the digital sphere, OpIsrael encourages on-the-ground advocacy, calling for participation in protests, solidarity movements and meaningful public discourse—all aimed at building sustained international support for Palestinian rights and justice.

Preparatory actions such as reconnaissance, vulnerability scanning, and light probing generally begin in late March, ramping up significantly during the first week of April. Meanwhile, propaganda, recruitment efforts and operational coordination through platforms like Telegram, X (formerly Twitter), Pastebin and various public and private forums usually intensify between the end of March and April 5.

In both 2023 and 2024, the bulk of coordinated DDoS attacks were executed around April 7. However, in October 2023, the onset of the Hamas conflict triggered a significant escalation in cyberattacks targeting Israeli institutions, marking a shift toward more aggressive and persistent cyberattack activity outside the traditional April window.

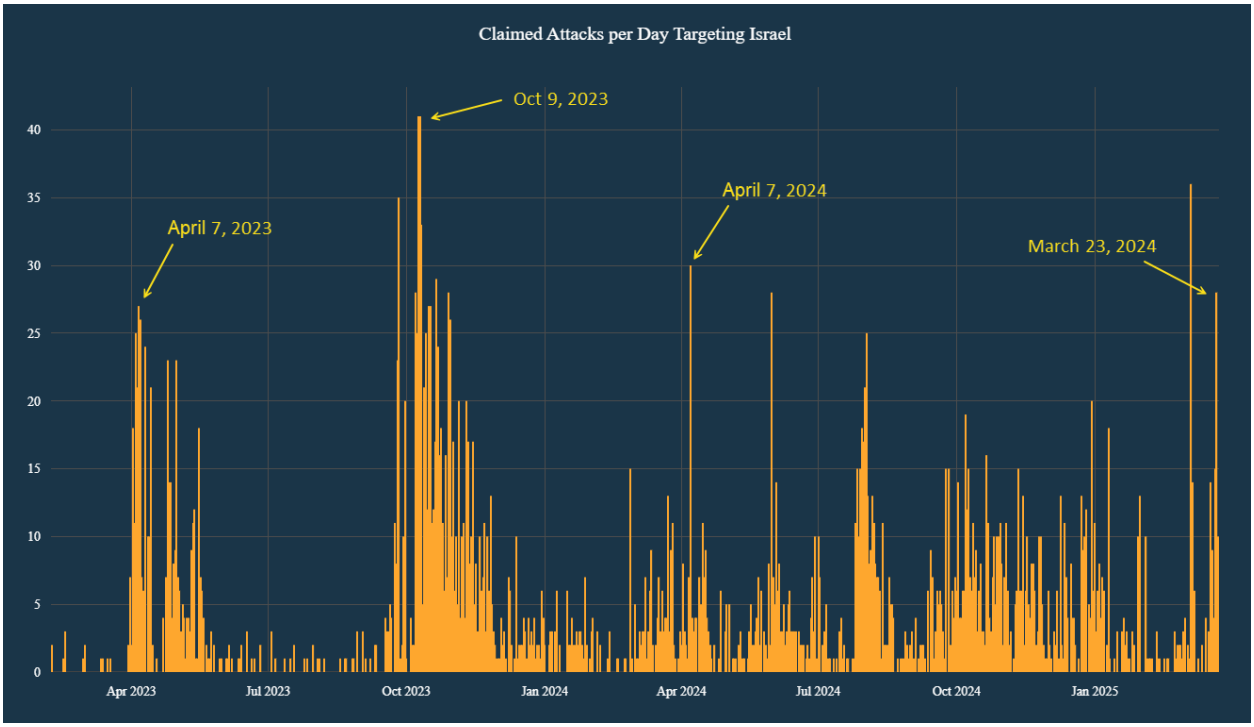

Figure 1: Claimed attacks targeting Israel (source: Radware)

OpIsrael 2025

On March 18 and 21, 2025, a private Telegram channel named ‘#OpIsrael’ disseminated a call to action across multiple hacktivist networks. The channel advocates for a global hacktivist campaign to express solidarity with the Palestinian people and to oppose Israeli policies, particularly those related to the occupation of Palestinian territories.

The message from ‘#OpIsrael’ emphasizes the campaign's focus extending beyond Israel alone:

> *"OpIsrael is not only about Israel—it seeks to highlight the role of international allies and entities that enable or support Israeli policies. This includes nations, such as the United States and the United Kingdom, that have historically been involved in shaping the geopolitical realities of the region."*

Figure 2: OpIsrael call to action by the private channel named '#OpIsrael' (source: Telegram)

OpIsrael Trends

Hashtags such as #OpIsrael, #OpJerusalem and #FreePalestine are strong indicators of increasing hacktivist activity targeting Israeli organizations, particularly from late March through mid-April. Since 2023, Radware has actively tracked hashtag usage on key Telegram channels linked to known threat actors.

Of these, #OpJerusalem saw minimal use—mostly limited to 2024—and accounted for just 0.2% of the total mentions compared to #OpIsrael, which became the primary focus of their analysis.

Meanwhile, #FreePalestine functions more as a symbolic battletag tied to broader campaigns surrounding the Israel-Hamas conflict. Mentions of this hashtag surged in October and have gradually declined since. In contrast, #OpIsrael hashtags more precisely reflect coordinated cyberattack campaigns against Israel, particularly in April and October, and have seen a noticeable rise in usage in recent weeks.

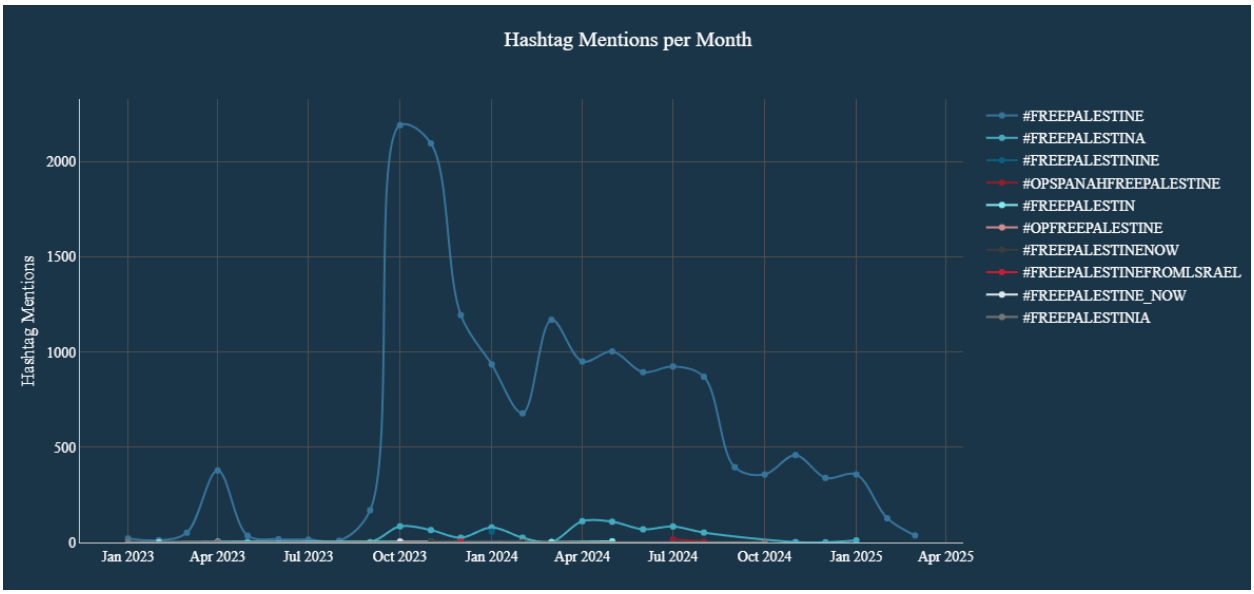

Figure 3: #FreePalestine hashtag mentions per month (source: Radware)

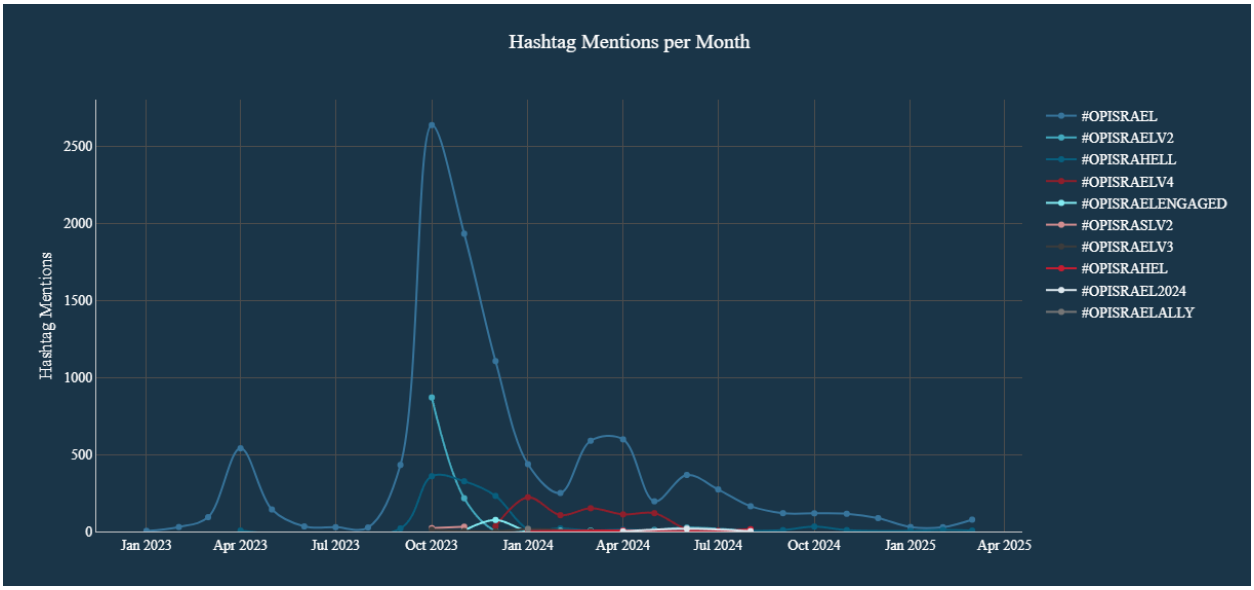

Figure 4: #OpIsrael mentions per month (source: Radware)

As shown in Figure 5, there is a noticeable spike in the use of #OpIsrael-related hashtags during April 2023, April 2024, and a significant rise beginning March 23, 2025.

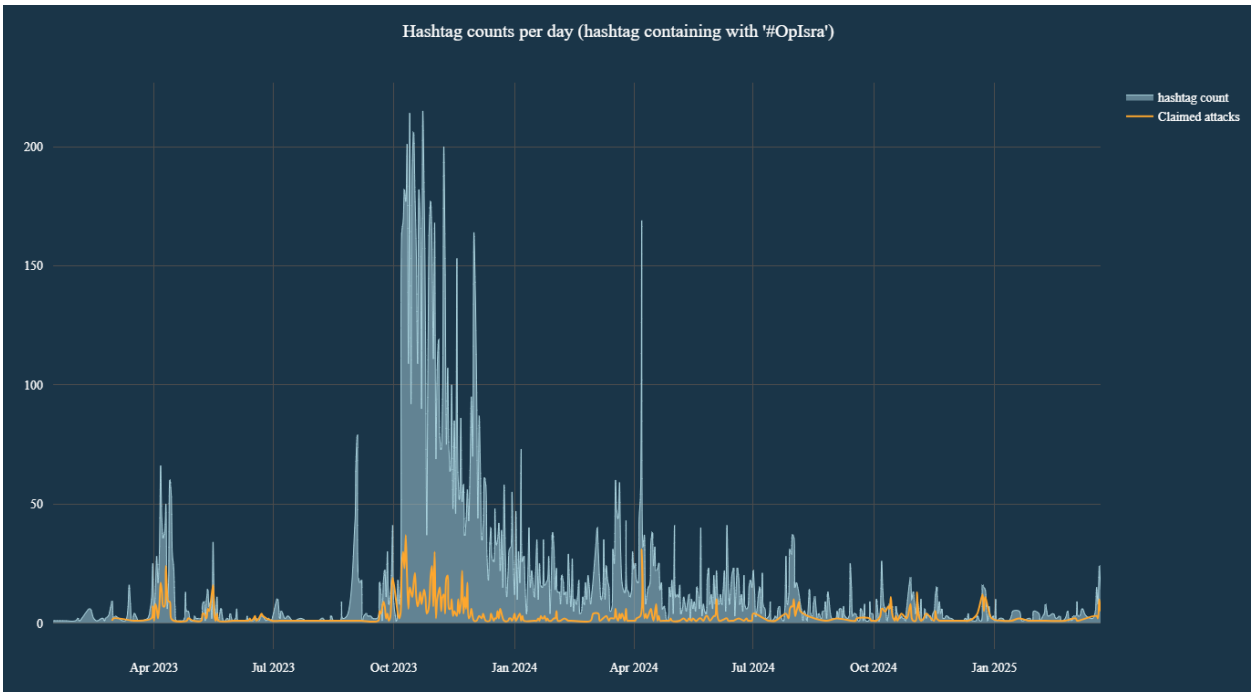

Figure 5: '#OpIsra…' hashtag counts and claimed attacks mentioning '#OpIsra…' hashtag per day (source: Telegram)

The surge in #OpIsrael mentions closely followed Israel's response to the Hamas attacks on October 7, 2023. This escalation led to sustained attention from hacktivist groups, resulting in a prolonged period of heightened activity that extended into the annual April 7, 2024, #OpIsrael campaign.

As illustrated in Figure 6, the overall level of activity related to OpIsrael was several orders of magnitude higher in 2024 compared to both 2023 and 2025—noting the differing scales across the graphs. Activity levels during the early months of 2023 and 2025 remained relatively low and comparable. However, in the lead-up to this year's OpIsrael anniversary, a notable uptick has been observed since March 20, 2025, aligning with the typical pre-campaign activity patterns seen in the year prior to 2024.

As illustrated in Figure 7, the main campaign battletag, #OpIsrael, shows a clear increase in use across channels in April 2023. The first months of 2024 show a more stochastic and dramatic pattern leading up into April caused by the longtail of the October 7 campaigns, but still an observable, marked increase in March and April 2024. The first months of 2025 correspond to what was observed in 2023, with an escalating use of the main campaign hashtag as we progress closer to April 7, 2025.

The primary campaign hashtag, #OpIsrael, saw a clear surge in usage across various channels during April 2023. In contrast, the early months of 2024 exhibited a more stochastic and intense pattern, yet still showed a distinct rise in activity throughout March and April. Similarly, the initial months of 2025 reflect the trend observed in 2023, with a steadily increasing use of the main campaign hashtag as we get closer to April 7, 2025.

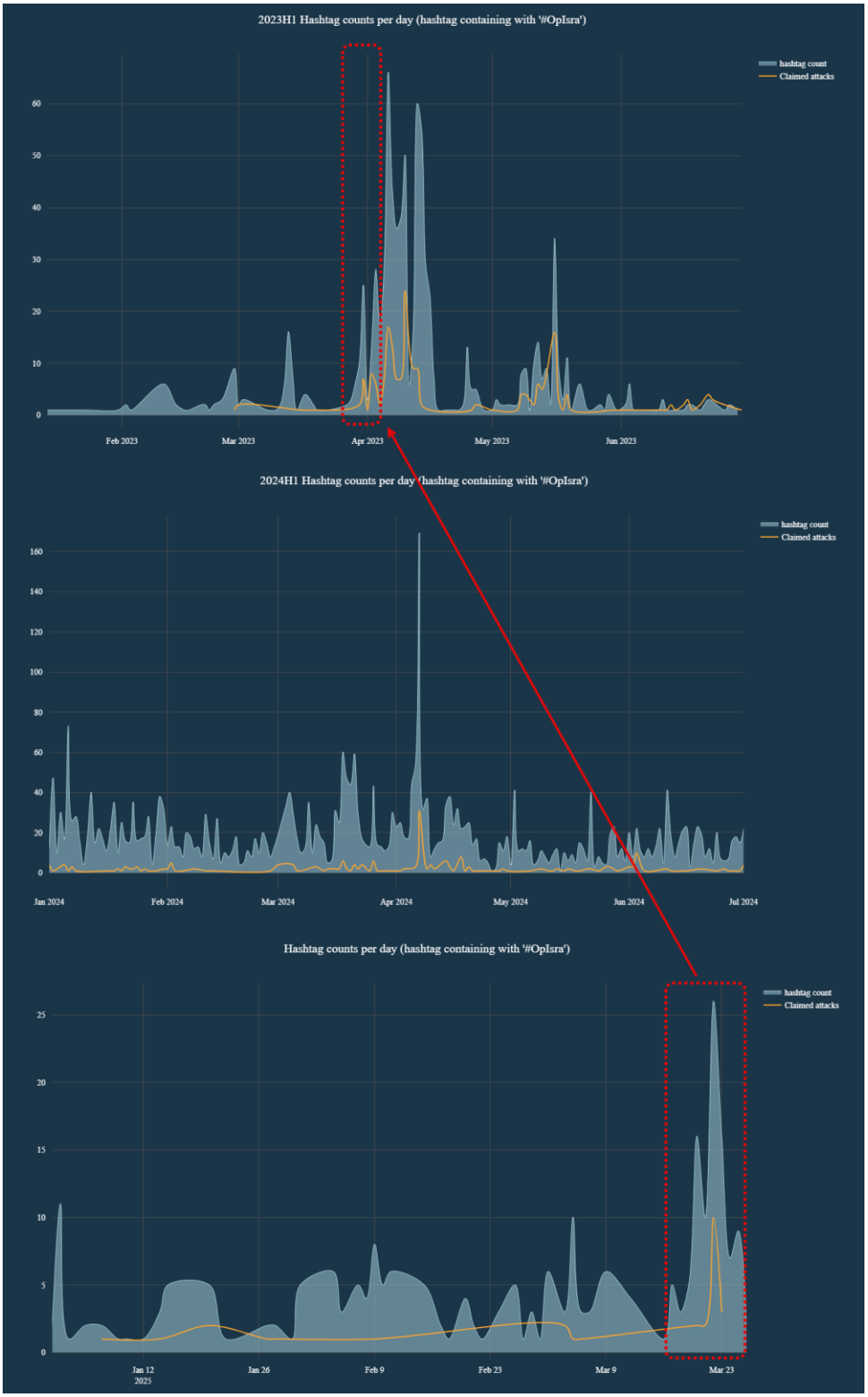

Figure 6: Hashtag counts for first half of 2023, 2024 and 2025 (source: Radware)

Figure 7: Evolution over time of OpIsrael-related hashtags (source: Radware)

Threat Groups

The following hacktivist groups were mentioned in the call to action circulated via the private Telegram channel named '#OpIsrael,' also illustrated in Figure 2. Close to 50 groups were tagged.

Arabian Ghosts	JoKeiR 07x	LulzSec Black	Fedayeen
Team 1945	Falcon Unit	Al Sham Electronic Corps	Shadow Hunter
DCA	Cyberjund	Sylhet Gang	MTB
Akatsuki	Muslim Cyber Soldier	Anonymous KSA	DieNet
Decay Stresser	Keymous	Sword of Justice	Cyber Toufan
Anon Pioneers	Holy League	Esteem Restoration Eagle	Cyber Islamic Resistance
Sector16	Laneh	Spider-X	Coup Team
FAD Team	FastAttacker1877	Islamic Hacker Army	Team Insane Pakistan
313 Team	Cyber Fatah Team	Advanced Cyber Tech	TH3 EL1T3 GH0ST
The Resistance	Im check mate	GhostSec	GhostClan Malaysia
The Returnees	Vortex	Team BD Cyber Ninja	Don Road
Anonymous VNLBN	7thDay	Wolf Cyber Army	Rabbit Cyber Team

Some groups primarily focus on website defacements, data leaks, or breaches, while others are classified by Radware as persistent threat actors known for consistently claiming cyberattacks—either specifically targeting Israel or operating on a global scale.

Figure 8 shows a list of the most active DDoS-focused hacktivist groups, based on claimed attacks against Israeli organizations and institutions over the past 8 weeks. In that same period, a total of 27 hacktivist groups have claimed 204 attacks against 140 unique hosts across 72 organizations and institutions in Israel.

The OpIsrael threat landscape extends beyond the groups explicitly mentioned in the call to action or illustrated in Figure 8. In 2024, numerous hacktivist threat groups formed alliances. Initially, these partnerships were primarily forged between like-minded actors who shared similar national identities and ideological goals. However, over the past year, we've seen a significant shift where alliances are increasingly emerging between groups of diverse nationalities and differing motivations, united by common perceived adversaries. These groups not only coordinate attacks on shared targets but also actively support each other's campaigns.

One particularly notable collective relevant to pro-Palestinian motivated cyber activity is the Holy League, which exemplifies this trend of cross-border, cooperative hacktivist operations. Members of the Holy League engage in a mix of DDoS attacks, website defacements and the leakage of sensitive data—tactics aimed at spreading fear and disruption through high-profile data breaches. Their motivations are deeply rooted in geopolitical tensions, with a strong emphasis on support for Palestine and outspoken opposition to Western entities such as NATO. Their rhetoric leans

heavily on religious and moral narratives, portraying themselves as champions of the oppressed and defenders of justice.

The group has also demonstrated a strategic use of visual propaganda to strengthen its identity and broaden its appeal. Their imagery is marked by dystopian cityscapes, religious iconography, and apocalyptic, fiery themes, all designed to create a striking and memorable visual signature. This aesthetic not only reinforces their ideological stance but also serves as a recruitment tool—targeting sympathetic audiences and drawing in new members from ideologically aligned hacktivist communities.

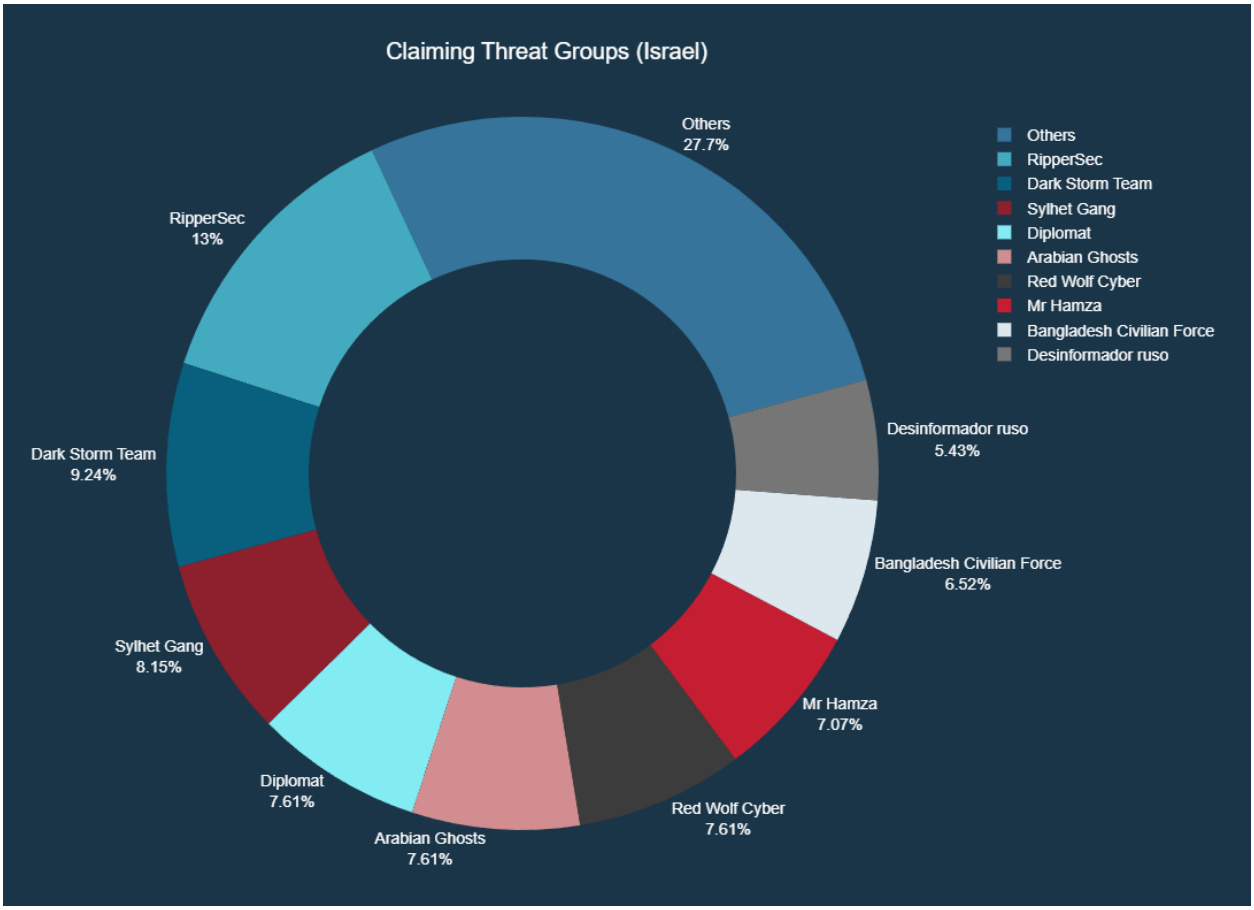

Figure 8: Threat groups claiming DDoS attacks targeting Israel between February and April 2025 (Radware)

Staying Ahead

Over the past three years, the Israel National Cyber Directorate (INCD) has consistently issued warnings to organizations in Israel regarding potential cyberthreats associated with campaigns like OpIsrael and OpJerusalem. These alerts are typically disseminated ahead of significant dates, such as Iran's Jerusalem Day, when cyberattacks against Israeli entities are anticipated.

In addition to the INCD's efforts, the Bank of Israel has also taken proactive measures. For instance, in November 2024, the Bank of Israel alerted financial institutions about a planned Iranian cyberattack targeting the nation's economic infrastructure.

In today's increasingly interconnected and active cyber hacktivist threat environment, the coordinated alerts issued by the INCD and the Bank of Israel are more crucial than ever. While the impact of previous hacktivist campaigns has generally been limited, this is largely due to the timely warnings and proactive defensive measures taken in response. As threat groups become more organized and collaborative, these early alerts continue to play a vital role in minimizing potential damage.

Recommendations

In the last few years, DDoS threat groups shifted tactics from network-based DDoS attacks to a combination of network and application layer attacks. Layer 7 Web DDoS attacks, as noted in the Radware 2025 Global Threat Analysis Report, escalated significantly in 2024, increasing almost 550% year-over-year compared to 2023. The intensity of these attacks grew exponentially during the first half of 2024 and plateaued at high levels during the second half, reflecting a sustained and aggressive threat environment. Use of advanced Layer 7 DDoS attacks has become a prominent tactic, leveraging vulnerabilities such as the HTTP/2 Rapid Reset and Continuation Flood to target online applications with increasing sophistication.

Network-based DDoS protection solutions are ineffective at detecting and mitigating Layer 7 DDoS attacks due to their inability to decrypt attack traffic and inspect Layer 7 headers in detail. As a result, these attacks often bypass traditional network defenses. Similarly, while on-premises or cloud-based web application firewalls (WAFs) are effective against standard web-based threats, they fall short in defending against modern Web DDoS attacks for several reasons:

- Scale: The volume of Layer 7 attacks, measured in requests per second (RPS), has reached unprecedented levels. In the past year, multiple third-party reports disclosed attacks exceeding millions of RPS. The sheer scale of these attacks overwhelms the capacity of traditional on-premises solutions.
- Attack Sophistication: These attacks mimic legitimate traffic, constantly randomizing requests to evade detection. Without predefined signatures or rule-based mechanisms to identify malicious behavior, traditional defenses are ineffective. Detecting and mitigating such traffic requires behavioral-based algorithms with self-learning and auto-tuning capabilities.
- Morphing Attacks: Modern Layer 7 threats are dynamic, frequently evolving and sustaining changes over extended periods. Standard WAF solutions lack the adaptability to respond in real time to these rapidly shifting attack patterns, leaving organizations vulnerable.

- Human Factor: The complexity of these attacks demands skilled security teams to maintain effective protection. Limited resources, personnel and budgets often hinder self-managed teams from addressing 24/7 attack campaigns. Additionally, on-premises tools rely on manual rule definitions, which are insufficient for the pace and sophistication of these threats.

Radware's cloud DDoS protection services stop network-layer and application-layer attacks with advanced behavioral-based algorithms capable of identifying and mitigating unknown malicious requests at scale in real time. Unlike volumetric approaches that fail to distinguish legitimate traffic surges from malicious activity, Radware's solution accurately identifies and blocks malicious traffic while ensuring legitimate users are not impacted.

The system provides comprehensive protection against a wide range of network and application layer threats, including sophisticated, randomized attacks, newly developed tools and high-scale Web DDoS campaigns. Radware's adaptive technology continuously analyzes threats and their variants, dynamically responding to evolving attack patterns without generating false positives. By automating the detection and mitigation process, Radware ensures robust, real-time protection tailored to the complexity and scale of modern DDoS attacks.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.