October 13, 2025

October 7: Post-Threat Analysis

Key Insights:

- The anniversary of October 7 continues to serve as a rallying point for global hacktivists, transforming political symbolism into coordinated cyber campaigns.
- Groups like Sylhet Gang act less as direct attackers and more as propaganda orchestrators, leveraging Telegram and X (formerly Twitter) to amplify calls for action.
- The participation of NoName057(16), a pro-Russian hacktivist group, illustrates how actors from distinct geopolitical spheres unite around shared adversaries. This blurring of ideological lines enhances the resilience and reach of hacktivist campaigns.
- Despite the surge in claims, most attacks remained short-lived, focusing on high-visibility websites such as government portals, financial services and online commerce.

Over the past two years, the weeks surrounding October 7 have consistently marked a surge in hacktivist activity targeting Israel. As with previous years, this period has become a symbolic rallying point for pro-Palestinian and anti-Israeli hacktivist groups across the globe. In the days leading up to October 7, 2025, we observed renewed calls for coordinated cyber action against Israel. This included a notable mobilization message posted by the Sylhet Gang group on its Telegram channel.

On October 7 alone, more than 50 cyberattack claims against Israeli targets were recorded. The weekly average number of attacks claimed spiked to almost three times the average compared to the weeks preceding October 7. This sharp escalation underscores how hacktivist campaigns continue to use symbolic anniversaries to amplify their visibility and coordinate global action.

In this advisory, we will provide a brief overview of the main hacktivist groups that participated in this year's wave of cyberattacks, along with their tactics, preferred targets and observed narratives.

DDoS Attack Claims Targeting Israel

Following the hacktivist calls for coordinated cyber action against Israel, we observed a sharp rise in claimed DDoS activity between October 6 and October 8. The escalation began on October 6, when the number of claimed DDoS attacks jumped to 26, signaling the early stages of a coordinated campaign. Activity peaked on October 7, with 57 DDoS attack claims recorded in a single day. That is more than 14 times higher than the daily average observed throughout September 2025.

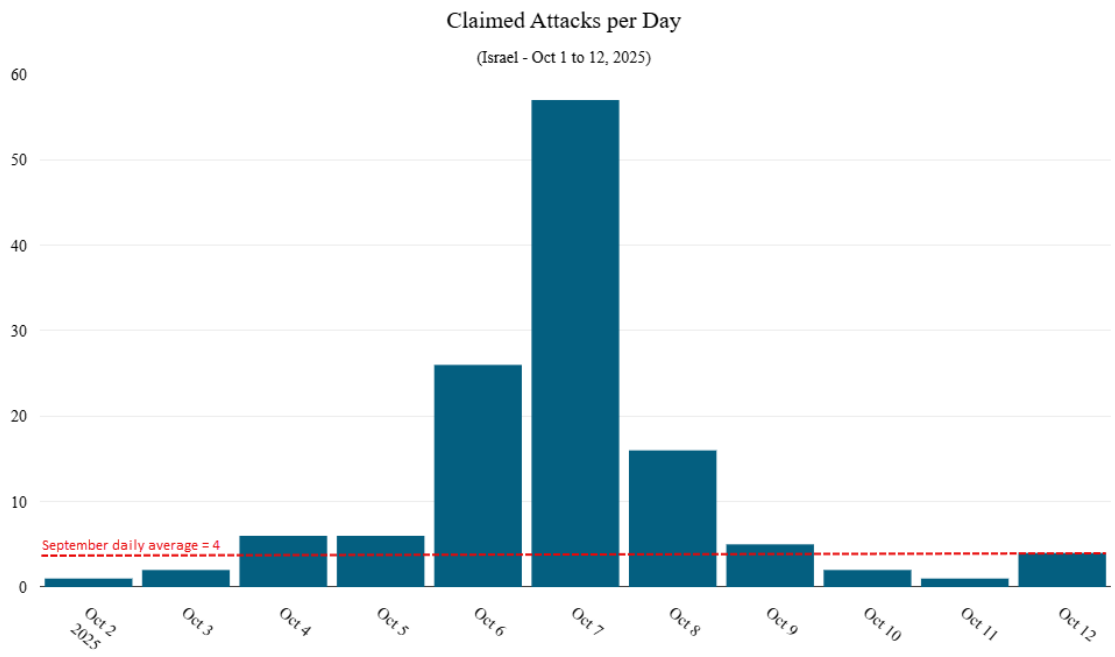

Figure 1: DDoS attack claims per day targeting Israel between October 1 and 12, 2025 (source: Radware)

Overall, the average number of attack claims per week increased by nearly 200% compared to the weeks preceding October 7.

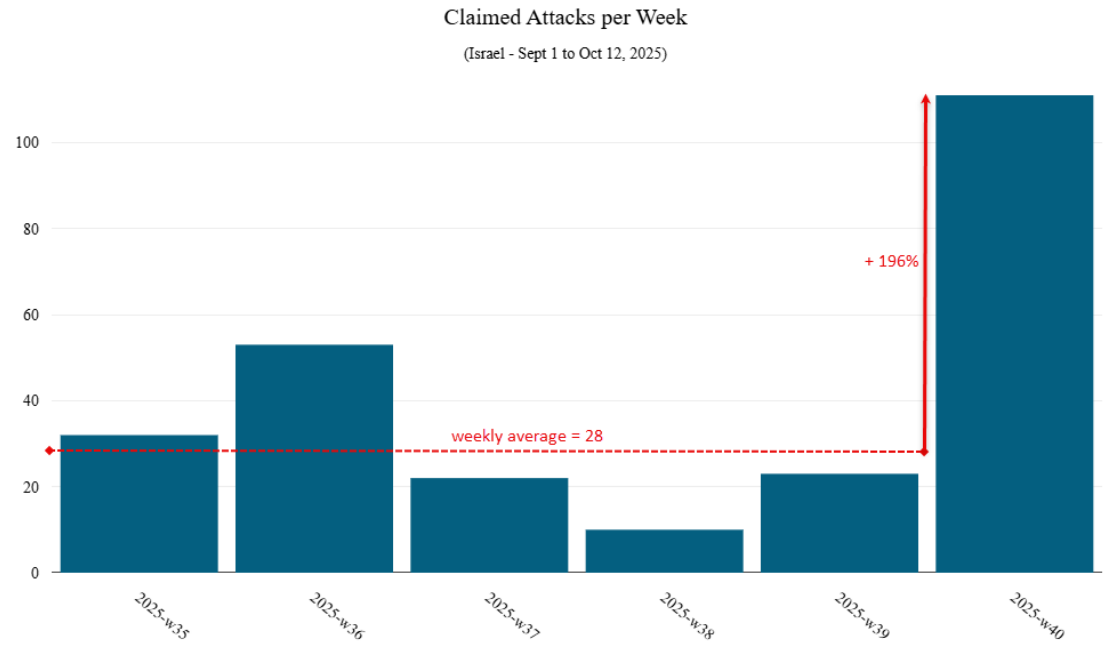

Figure 2: Total number of DDoS attack claims per week (source: Radware)

This surge highlights the increasing organization and responsiveness of hacktivist ecosystems, where Telegram channels serve as real-time coordination hubs. The temporal correlation between public calls for action and the subsequent wave of attack claims suggests a strong mobilization effect, consistent with similar patterns observed around symbolic or politically charged dates in previous years.

Threat Groups

Following the call to arms issued by Sylhet Gang, the group itself, as highlighted in our threat alert preceding October 7, proved once again to be more effective as a propaganda amplifier and mobilization hub than as an operational threat actor. Sylhet Gang primarily focuses on disseminating narratives, coordinating like-minded hacktivist groups and amplifying attack claims rather than executing attacks directly. Beyond a dozen unverifiable website defacements against Israeli domains, the group did not contribute any confirmed DDoS claims during the October 6–8 activity window.

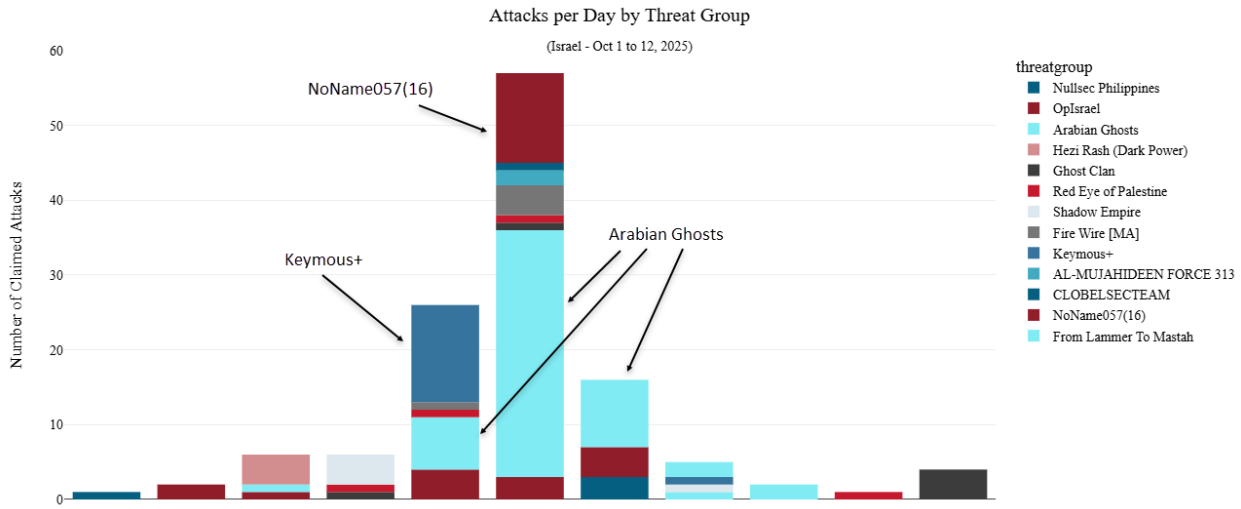

Figure 3: DDoS attack claims targeting Israel per day by threat group (source: Radware)

The most active group during this period was Arabian Ghosts, accounting for over 40% of all DDoS attack claims. They were followed, at a considerable distance, by Keymous+, NoName057(16) and OpIsrael, which registered 13, 12, and 11 claimed DDoS attacks, respectively. Notably, NoName057(16) stood out as the only Russian-aligned hacktivist collective to participate in this pro-Palestinian campaign, reaffirming its previously announced alliances with pro-Palestinian hacktivist groups.

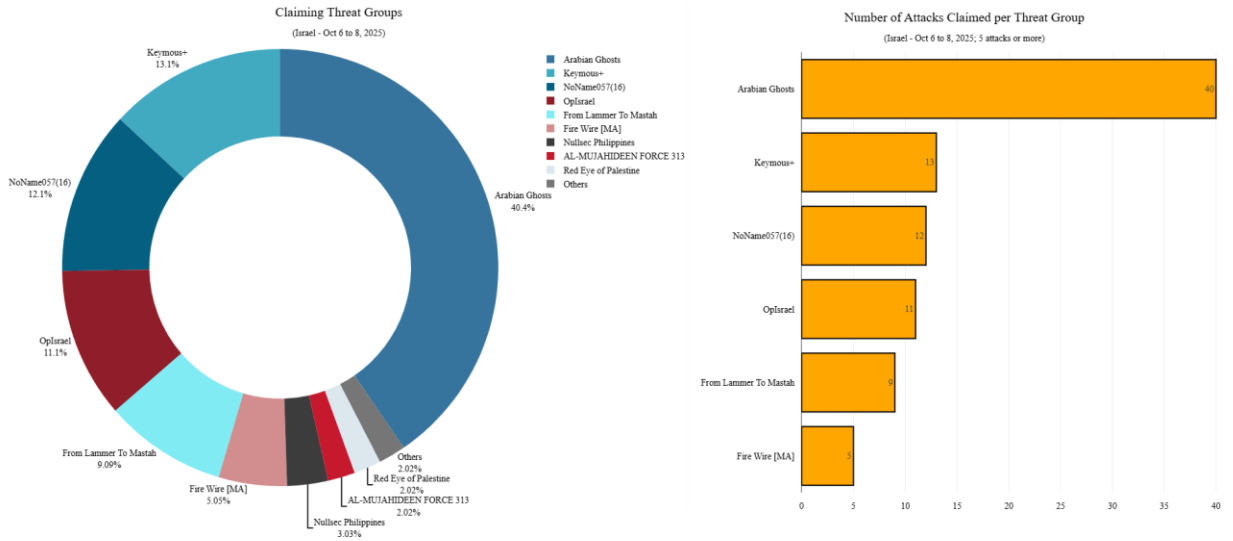

Figure 4: Top claiming threat groups targeting Israel between October 6 and 8 (source: Radware)

Targeted Industries

During the October 6-8 activity window, the government was the most frequently targeted Israeli sector, accounting for the largest share of claimed DDoS attacks. This was closely followed by business and e-commerce websites, reflecting the hacktivists' intent to disrupt both symbolic and high-visibility online services.

Beyond these primary targets, education, healthcare, manufacturing, retail and financial services each represented roughly 7% of the total attack claims. The relatively even distribution among these secondary sectors suggests that hacktivist campaigns were driven less by precise strategic intent and more by opportunistic target selection, leveraging publicly accessible online assets to maximize the perceived impact of their operations.

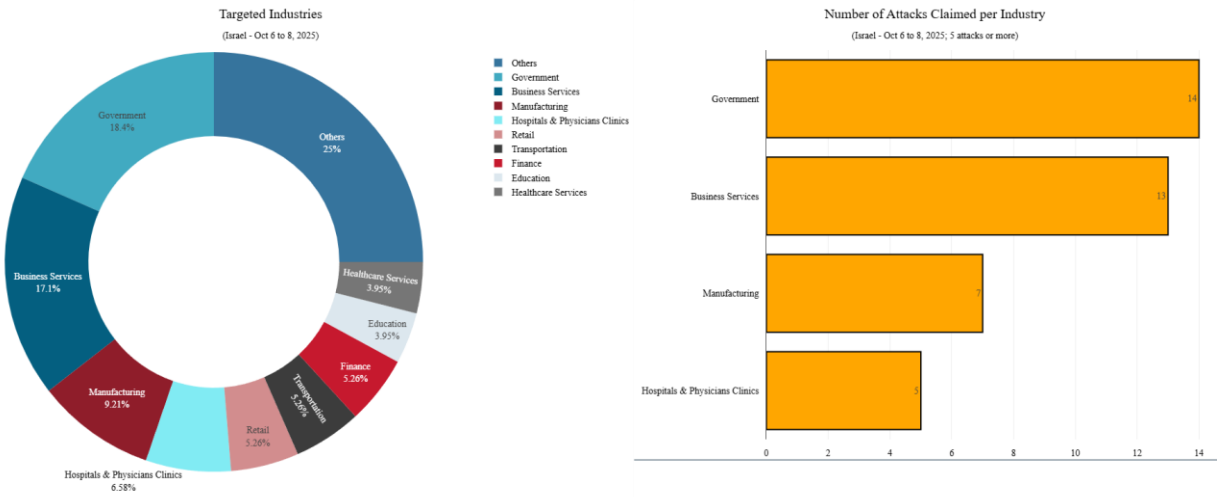

Figure 5: Top targeted Israeli industries between October 6 and 8 (source: Radware)

Key Participating Threat Groups

Sylhet Gang

The group we previously referenced, Sylhet Gang, was among the first to issue a call for action on October 7. On its X account, the group identifies itself as originating from Bengal, though its membership and operational links appear more geographically dispersed. In the lead-up to and during October 7, Sylhet Gang announced on its Telegram channel that it had compromised dozens of Israeli, American and European servers.

According to its own statements, the group claimed to have defaced several of these systems, uploaded proof-of-concept files, exfiltrated data and even installed malicious software on some of the affected servers. Following these announcements, the group published a small number of URLs allegedly associated with the targeted websites, though none of the claims could be independently verified.

As with previous operations, Sylhet Gang's campaign illustrates its emphasis on propaganda and narrative amplification over verifiable technical impact. The group's communications appear primarily aimed at rallying support and amplifying visibility among ideologically aligned hacktivist networks, rather than executing sustained or technically sophisticated cyberattacks.

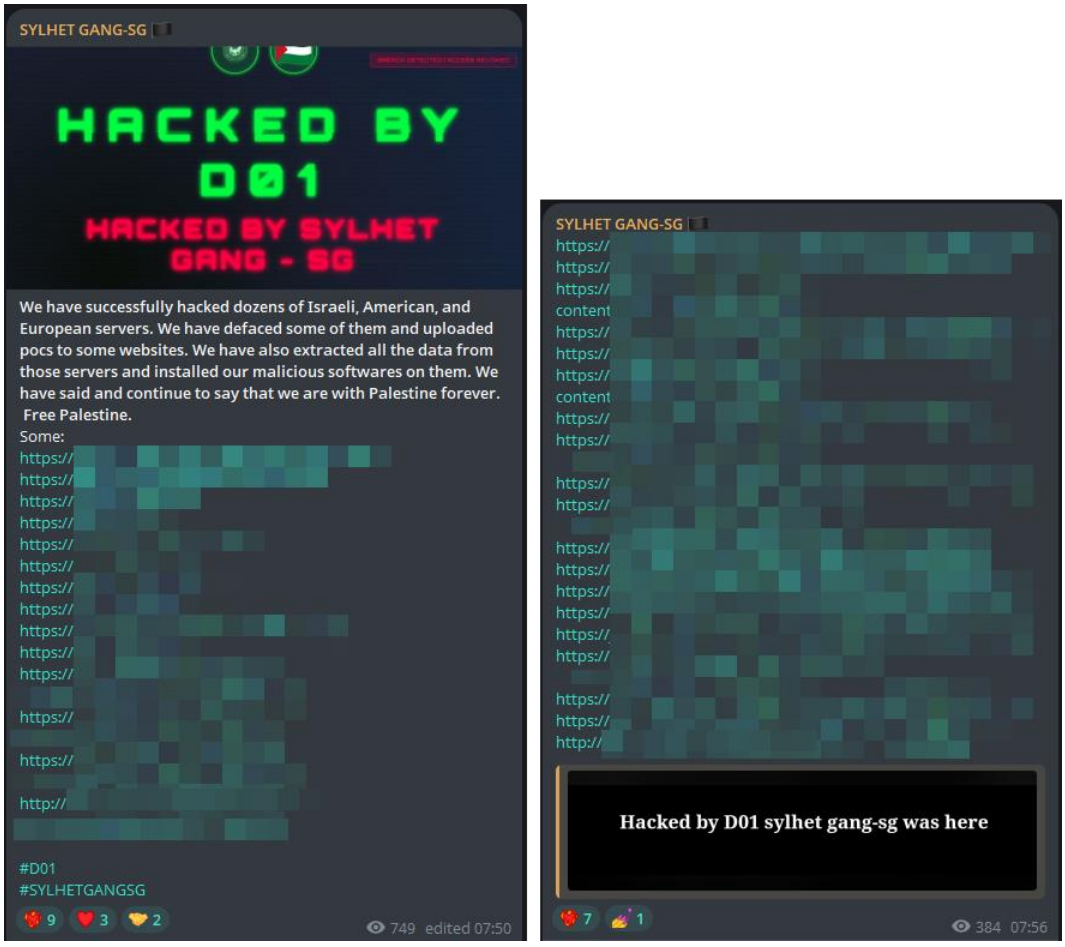

Figure 6: Sylhet Gang announcing the alleged hacking of dozens of Israeli, American and European servers (source: Telegram)

Keymous+

Keymous+ was among the most active groups participating in the October 7 campaign, claiming responsibility for DDoS attacks against more than a dozen Israeli websites. The group's primary focus appeared to be the financial sector, though additional targets included insurance, transportation and several other industries.

To substantiate their activity, Keymous+ shared check-host verification links as proof of their alleged disruptions. Each post was tagged with #OpIsrael and #RedEyeOnPalestine, signaling both ideological alignment with the broader pro-Palestinian cyber movement and participation in the coordinated online campaign.

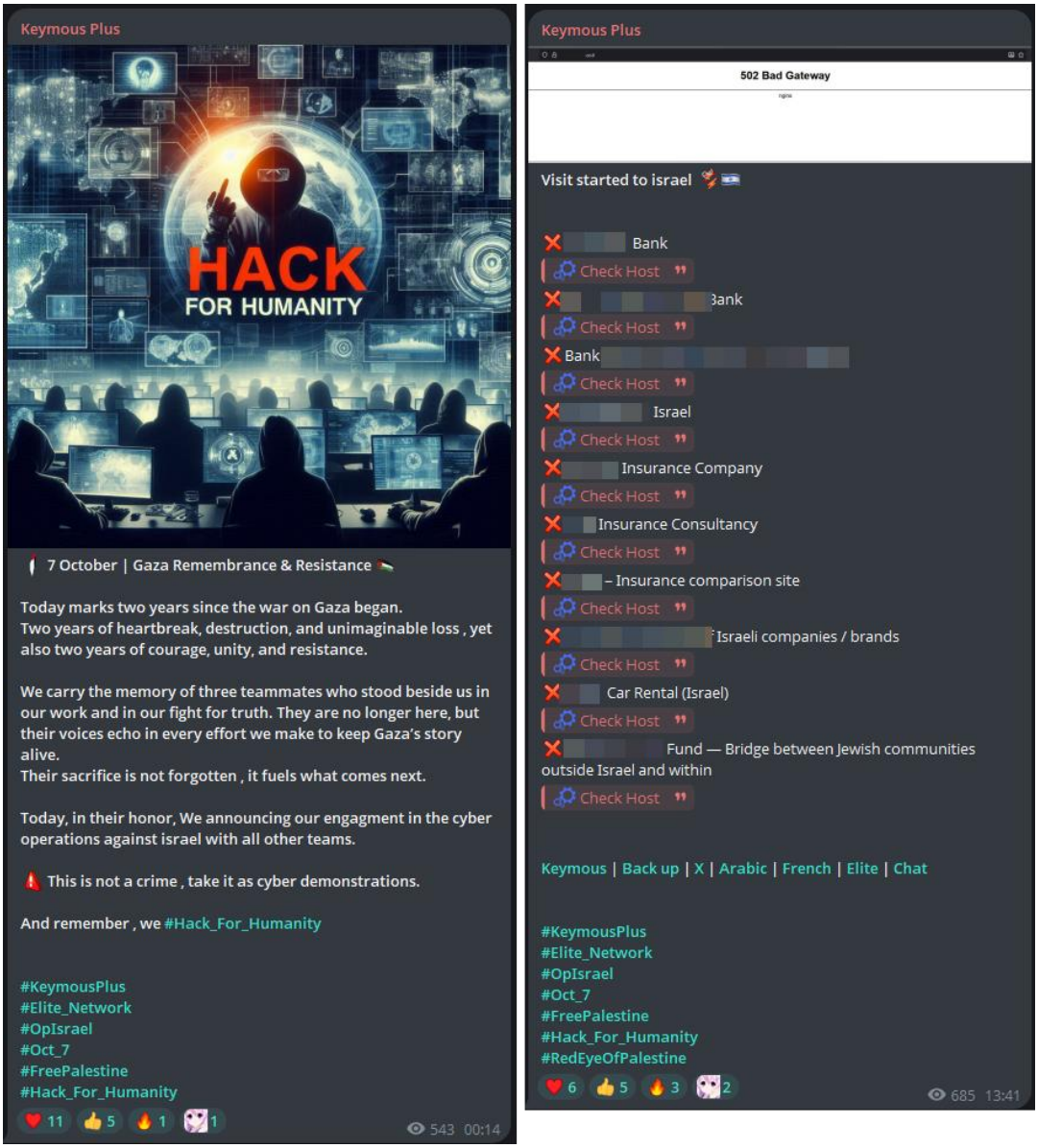

Figure 7: Keymous+ claiming attacks through check-host links (source: Telegram)

Arabian Ghosts

Arabian Ghosts emerged as the most active hacktivist group during the October 7 campaign, responsible for over 40% of the total DDoS attack claims observed during that period. Through its Telegram channel named MADGHOST, the group initially amplified messages and media posts from other hacktivist Telegram channels related to cyberattacks against Israel, effectively positioning itself as both a participant and an amplifier within the broader online mobilization.

As the campaign intensified, Arabian Ghosts began to publish their own attack claims, sharing links to targeted Israeli websites along with check-host verification results to support their assertions. Their reported operations included a mix of DDoS attacks and website defacements.

Each post was accompanied by the hashtags #OpIsrael and an Arabic tag translating to Al-Aqsa Flood. Al-Aqsa Flood is the codename used by Hamas and allied Palestinian armed groups for the October 7 attacks in 2023. By adopting this terminology, Arabian Ghosts sought to frame their cyber operations as part of a digital extension of the physical conflict, aligning themselves ideologically with the pro-Palestinian narrative and invoking historical continuity between kinetic and cyber forms of resistance.

Figure 8: DDoS attack claims posted by Arabian Ghosts on their Telegram channel MADGHOST (source: Telegram)

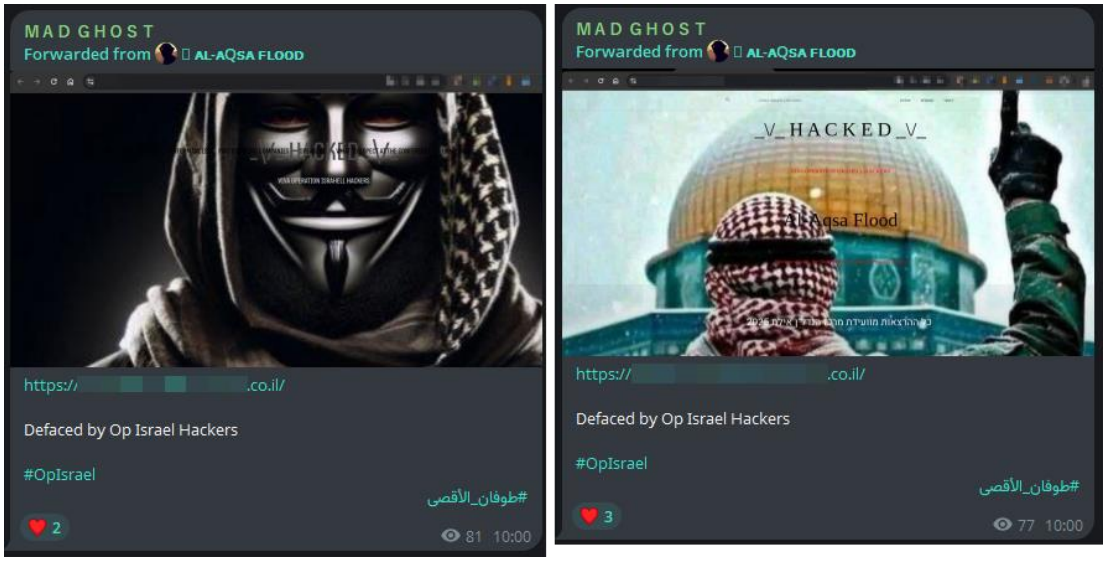

Figure 9: Defacement claims posted by Arabian Ghosts (source: Telegram)

NoName057(16)

The pro-Russian hacktivist collective NoName057(16) also took part in the October 7 cyber campaign. The group claimed a series of DDoS attacks targeting Israeli government assets, including websites of political parties and municipal administrations. Each attack claim was accompanied by a check-host link intended to validate the claim, consistent with the group's established pattern of public proof-sharing.

NoName057(16) also extended its operations beyond Israel, conducting DDoS attacks against German websites. The group described Germany as pro-Israeli in its messaging. This cross-targeting pattern reflects NoName057(16)'s broader information warfare agenda, in which geopolitical alignment often dictates target selection. By attacking both Israeli and Western European infrastructure, the group positioned itself as part of a coalition of anti-Western and anti-Israeli actors, echoing narratives of solidarity it had previously expressed toward other hacktivist alliances.

Historically known for its DDOSIA volunteer network and crowdsourced DDoS operations, NoName057(16) continues to blend political opportunism with technical persistence, leveraging major geopolitical flashpoints, such as the October 7 anniversary, to amplify visibility and reinforce its ideological messaging.

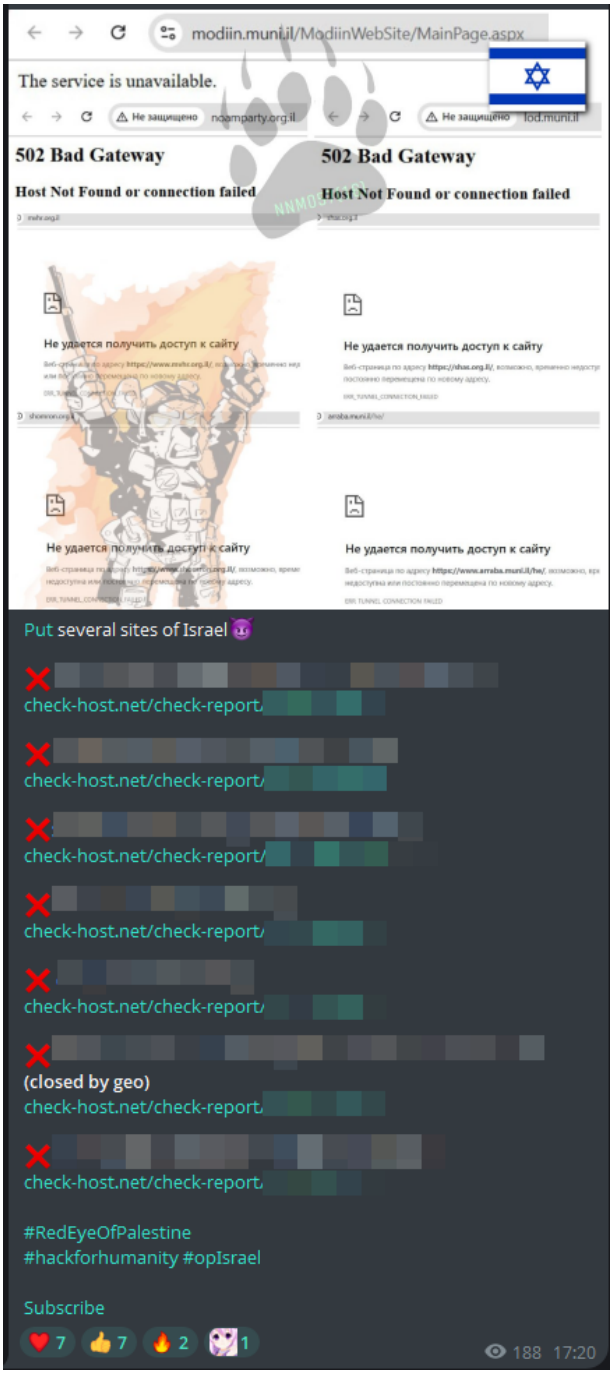

Figure 10: DDoS attack claims targeting Israel posted by NoName057(16) (source: Telegram)

Summary

The October 7 anniversary once again served as a catalyst for a surge in hacktivist activity targeting Israel, echoing similar mobilizations observed in previous years. The renewed calls for cyber action, amplified by groups such as Sylhet Gang, triggered a significant increase in DDoS and defacement claims across multiple sectors. Between October 6 and 8, the number of claimed DDoS attacks rose sharply, over 14 times the daily average of September 2025. Overall, the average number of attack claims per week nearly tripled compared to the preceding weeks, highlighting the enduring symbolic power of October 7 within hacktivist circles.

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.