April 3, 2024

OpIsrael 2024

Several hacktivist collectives have announced Sunday, April 7, as the kickoff date for this year's OpIsrael operation, coinciding with the 2013 inaugural OpIsrael attacks by Anonymous 11 years prior. This chosen date also reflects the six-month mark since the onset of hostilities between Israel and Hamas on October 7, 2023, during which Hamas launched attacks on communities along Gaza's southern border with Israel.

Background

OpIsrael was initiated by Anonymous in November 2012 as a reaction to the Israeli military operation named Pillar of Defense. This operation, which lasted for eight days starting on November 14, 2012, was the Israel Defense Force's response to the firing of 100 rockets at Israel from the Hamas-controlled Gaza Strip within a single day. Initially, OpIsrael served as an informal battle tag adopted by a collective of hacktivists from Anonymous to counteract the Israeli military action. The 2012 operations by Anonymous saw numerous Israeli websites suffer from data breaches, defacements and denial-of-service attacks, raising questions among security experts about whether this signified a new form of cyber warfare—and whether a group like Anonymous could be seen as an unconventional army.

In the subsequent year, Anonymous decided to formalize OpIsrael into an annual campaign aimed at Israel, marking its commencement on April 7, 2013, a date that coincided with Holocaust Remembrance Day. Their stated objective was to "erase Israel from the internet" by targeting Israeli networks and applications due to what Anonymous claimed were human rights abuses against Palestinians, with the broader aim of highlighting the Israeli-Palestinian conflict.

Almost a decade later, 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 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.

Building on OpsBedil's initial achievements, DragonForce Malaysia initiated OpsBedil Reloaded in 2022 amid escalating tensions in the Middle East during Ramadan. This time, their operations against Israeli targets included website defacements, denial-of-service attacks and data

breaches. Although OpsBedil did not achieve the same level of notoriety as OpIsrael, it introduced a significant risk to the region. Contrary to Anonymous, which had dwindled in capacity to target Israel effectively, DragonForce Malaysia and its allies possessed the time, resources and determination to introduce a substantial, albeit moderate, threat level to Israel, surpassing any recent activities reminiscent of OpIsrael.

In anticipation of OpIsrael's 10th anniversary in 2023, amidst a resurgence of hacktivism fueled by the conflict in Ukraine and escalating geopolitical strains involving Israel, numerous well-known groups declared their participation in the campaign. Earlier in the year, Mysterious Team Bangladesh and Anonymous Sudan initiated DDoS attacks against Australia as part of the operation OpAustralia. This collaboration between Sudanese and pro-Palestinian hackers, based primarily in India, shifted focus towards Israel in April. They were joined by other collectives from Southeast Asia, including the Vietnam Cyber Army, also known as Mr. Dempsey. Together, they orchestrated a series of DDoS attacks targeting a variety of organizations throughout Israel.

April 7, 2024

Several hacktivist groups declared Sunday, April 7, as the start date for this year's OpIsrael campaign, aligning with the date of the first OpIsrael attacks by Anonymous in 2013, 11 years earlier. This date also marks the six-month anniversary of the conflict between Israel and Hamas, which began on October 7, 2023, when Hamas attacked communities along Israel's southern border with Gaza. The Israel Defense Forces (IDF) retaliated with an operation named Operation Iron Swords. Concurrent with the ground conflict, there was a notable uptick in cyberattacks targeting Israeli entities, elevating Israel to one of the most targeted nations by hacktivists in 2023.

On the evening of April 2, 2024, Team Insane Pakistan expressed their pledge to join the OpIsrael campaign, specifically mentioning participating on Sunday, April 7. Soon after, a hacktivist collective known as Anonymous Global took to Telegram to initiate a countdown for OpIsrael, setting the stage for activities to begin on April 7. Additionally, earlier that day, AnonGhost and azzasec declared their support for OpIsrael, aligning themselves with the operation.

Figure 1: Telegram post by Team Insane PK on April 2 at 11pm Israel Time (source: Telegram)

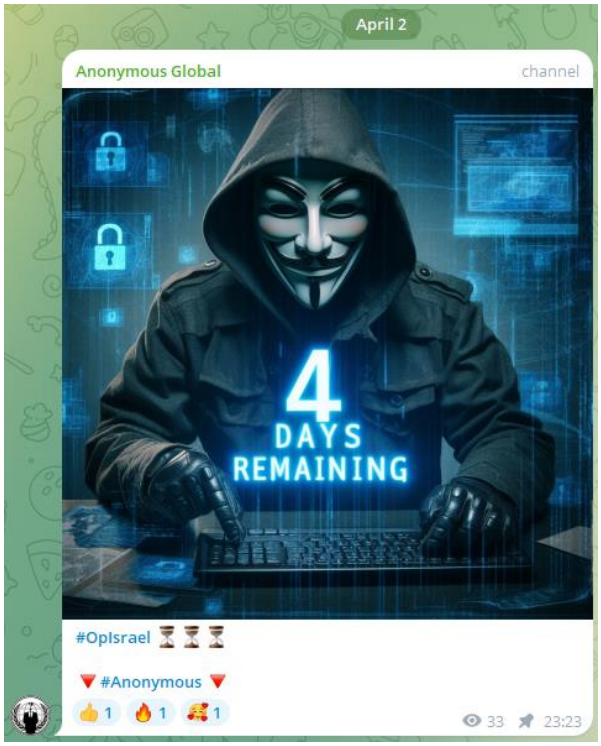

Figure 2: Telegram post by Anonymous Global on April 2 at 00:23 pm Israel Time (source: Telegram)

Figure 3: Telegram post by AnonGhost, announcing OpIsrael alliance with azzasec (source: Telegram)

Israel: Most Targeted Country by Hacktivists in 2023

In 2023, Israel emerged as the prime target for hacktivist activities. A reported 1,480 DDoS attacks make it the most attacked nation by such groups throughout the year. The onslaught began in the first half of the year, particularly from pro-Islamic hacktivist groups. These groups were inspired by the activities of pro-Russian hacktivists in 2022 and directed their efforts towards Israel during the annual OpIsrael campaign. From March 27 (the 13th week of the year) to April 16 (the 15th week), Israel faced a first wave of attacks reaching over 120 DDoS attacks in week 14. This heightened level of hacktivist activity persisted until the 20th week of the year, ending around May 21. For almost two months, Israel experienced a significant increase in hacktivist attacks, largely fueled by the momentum of the OpIsrael campaign.

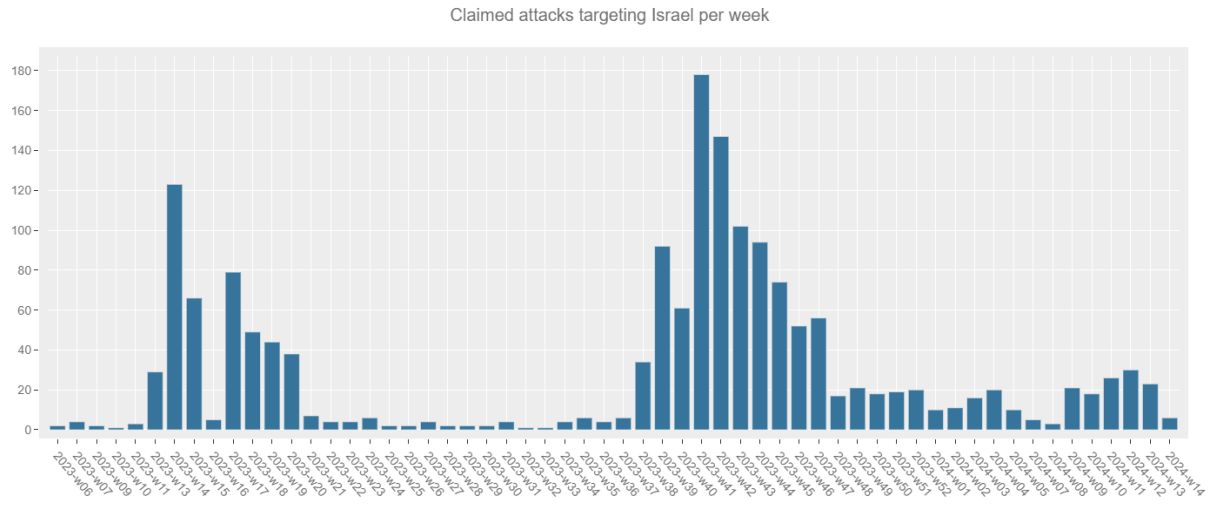

Figure 4: Number of DDoS attacks per week claimed by hacktivist groups on Telegram. Note that only two days were accounted in week 2024-14 (source: Radware)

In the latter part of the year, following the conflict between Israel and Hamas, pro-Palestinian hacktivists intensified their cyberattacks against Israeli entities. Specifically, in the fortnight preceding October 7 (the 40th week), there was a marked escalation in the number of DDoS attacks aimed at Israeli institutions and organizations. Following the onset of the conflict, nearly 250 DDoS attacks were claimed by pro-Palestinian groups within two weeks. Although the frequency of these attacks gradually diminished over time, a significant uptick in cyberattacks against Israel was observed at the start of the Ramadan, signaling a buildup to the annual OpIsrael campaign for 2024. This resurgence of activity, as declared by various anonymous factions and pro-Palestinian hacktivists, was set to commence on April 7, 2024.

Coordination Among Hacktivist Groups

Hacktivists often use hashtags to name their operations, typically beginning with “#Op” to easily promote their attack campaigns and form temporary alliances. Consequently, it’s expected to observe a surge in hashtags related to OpIsrael in tandem with an uptick in claimed attack activities. This heightened discussion serves as a reliable indicator of global activity within the hacktivist community as they focus their efforts on specific nations or unite in campaigns aligned with shared goals.

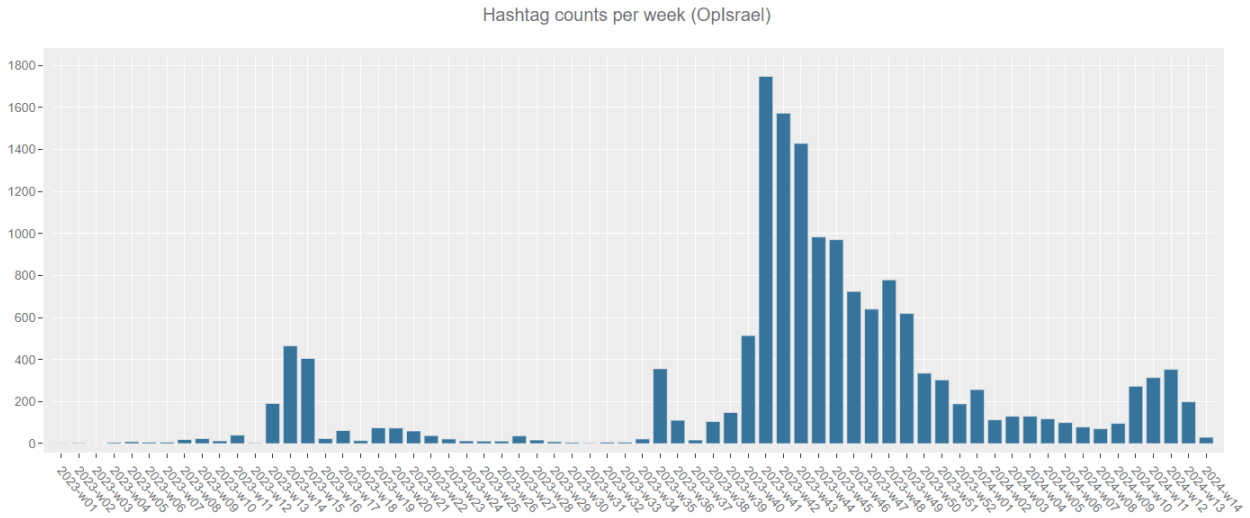

Figure 5: Weekly OpIsrael hashtag counts on Telegram. Note that only two days were accounted in week 2024-14 (source: Radware)

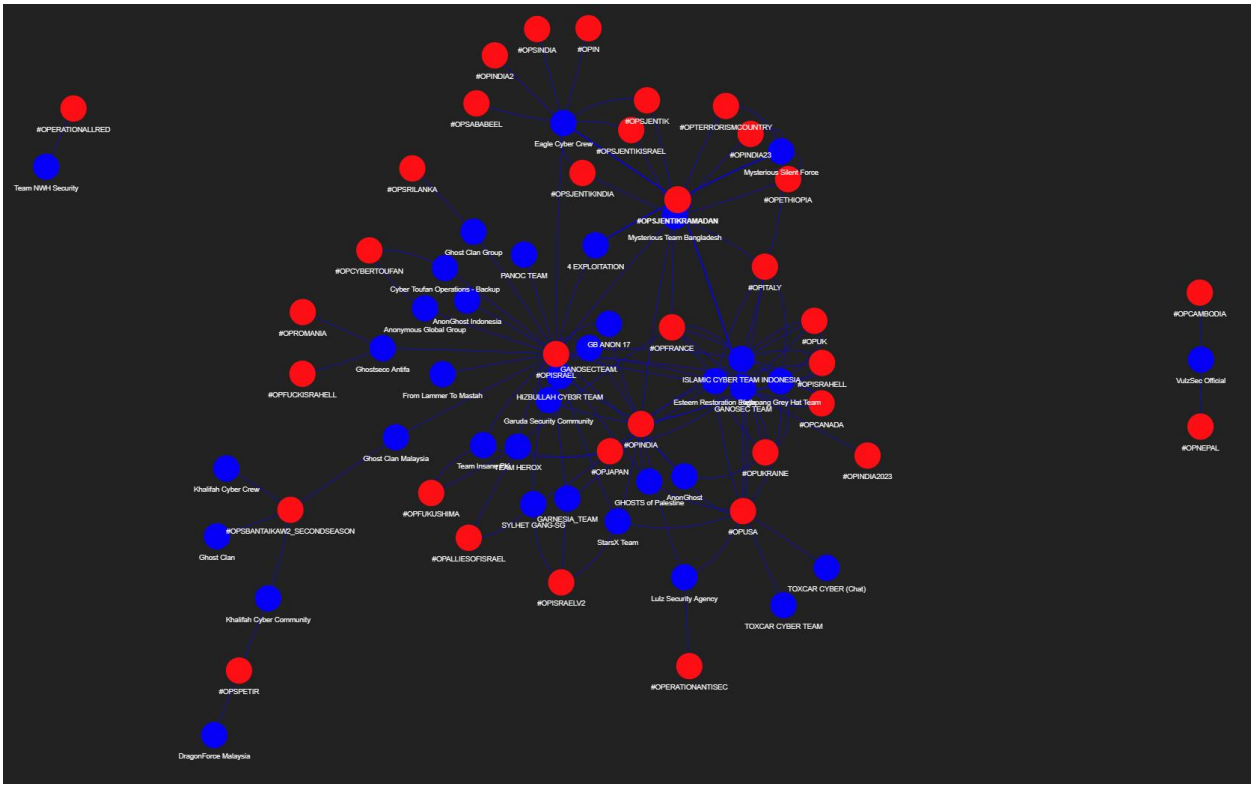

Figure 6: Graph linking Telegram channels (blue) and hashtags (red) over the period 2023/2024 (source: Radware)

Figure 6 displays a network graph highlighting connections between Telegram channels (depicted in blue) and hashtags (shown in red). A significant number of hacktivist groups linked

to the OpIsrael hashtag have also been involved in cyber campaigns targeting countries such as India, the UK, Italy, Ethiopia, Romania and France, among others. The onset of the conflict between Israel and Hamas served as a pivotal moment, influencing the involvement of various groups in cyberattacks aimed at Israel.

In the 2023 OpIsrael campaign, Anonymous Sudan, along with Mysterious Team Bangladesh and Team Insane PK, were among the most influential hacktivist groups.

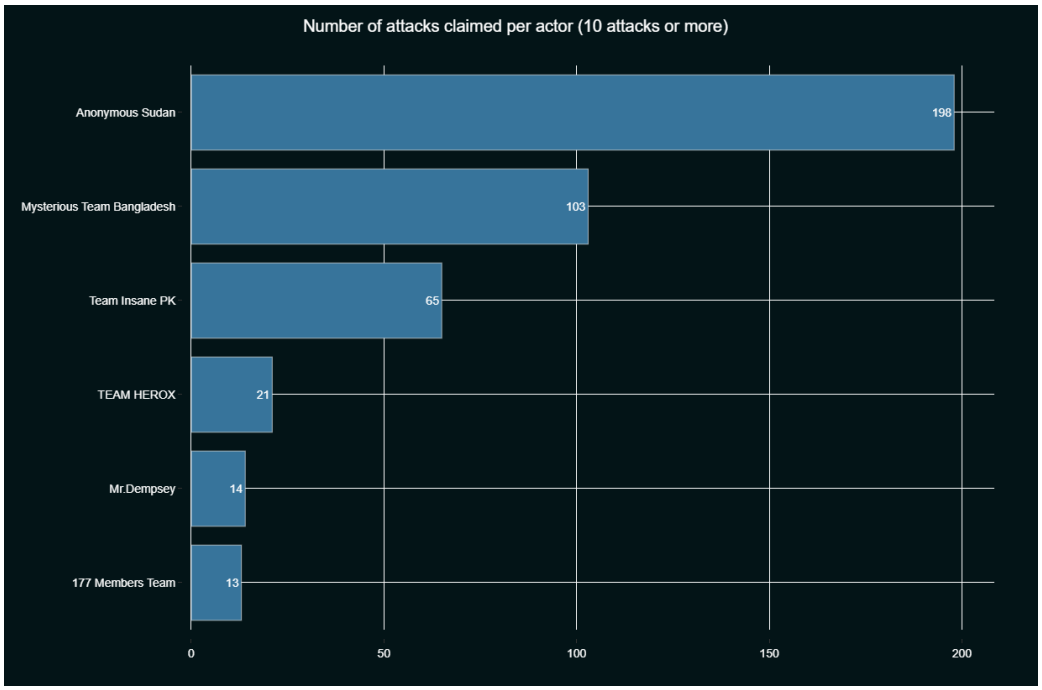

Figure 7: Most active hacktivists between January 1 and September 1, 2023 (source: Radware)

The conflict between Israel and Hamas drew a larger collective of hacktivists to the scene. One noticeable absence was Anonymous Sudan, who was engaged in different initiatives at the time. The activities were distributed among over two dozen groups, including StarsX team, Channel DDoS, Garnesia Team, Sylhet Gang, Dark Storm Team and Garuda, each claiming responsibility for more than 50 attacks.

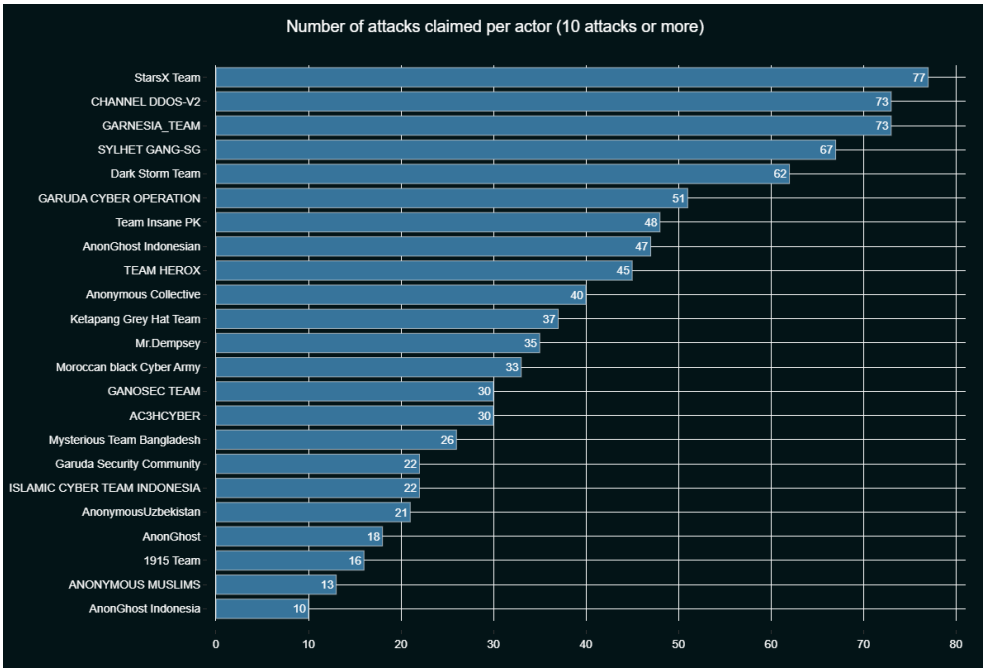

Figure 8: Most active hacktivists between September 1 and the end of 2023 (source: Radware)

In 2024, the landscape of hacktivist groups targeting Israel shifted with new leaders emerging to spearhead the initiatives. The Ketapang Grey Hat Team, Anonymous Collective, 1915 Team and Sylhet Gang were at the forefront of these assaults.

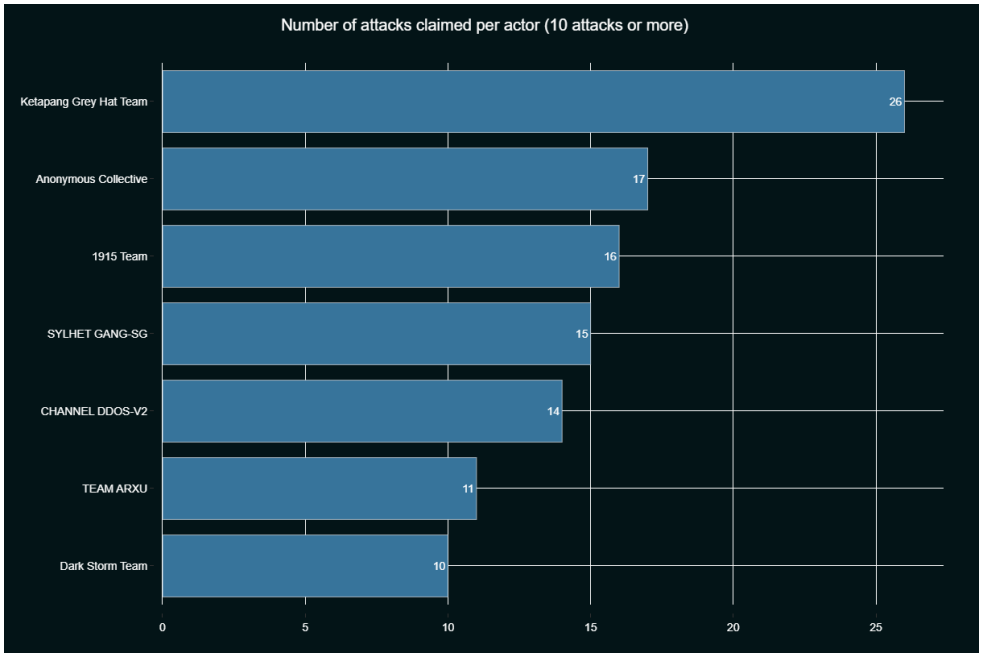

Figure 9: Most active hacktivists in 2024, until April 2 (source: Radware)

Iran’s Strategic Cyber Campaign Against Israel

Upon the outbreak of the conflict between Israel and Hamas on October 7, 2023, Iran rapidly escalated its support for Hamas, employing its sophisticated approach of integrating targeted cyberattacks with influence operations spread through social media, a strategy known as cyber-enabled influence operations. Initially, Iran's activities were reactive and took advantage of emerging opportunities. However, by the end of October, a concerted effort from Iran's major cyber and influence actors was directed at Israel, adopting a more focused, coordinated and damaging approach. This represented an exhaustive, all-in effort against Israel.

According to reporting from The New York Times, on April 1, Israeli air forces allegedly attacked a building next to the Iranian console in Syria during a top meeting of Iranian generals, killing 13 of them in the attack. Unlike previous airstrikes focused on Hezbollah, this one allegedly targeted high-seniority Iranian generals. On April 3, Iran sent a letter promising a "decisive response" that’s within the framework of international law. This might indicate a cyberattack as a means for revenge. It should also be noted that Friday, April 5, is the Iranian Jerusalem Day, the last Friday of Ramadan. Last year, there were many attacks on this date.

There is an increased risk of retaliation for government, fintech and finance organizations. Iran's former actions indicate it acts under the "eye-for-an-eye" principle, taking down government services and causing chaos. Iran is mainly interested in disturbing the way of life of as many Israelis as possible to create a deterrence equation that will stop Israel from this type of attack in the future. Attacking financial services used by Israelis can directly impact the public discourse.

The Threat of Hacktivism

Hacktivism represents a multifaceted form of activism motivated by various factors, including political and religious beliefs. It leverages technology to promote causes and confront perceived injustices, employing a range of tactics that evolve alongside emerging technologies. Despite the legal and ethical questions surrounding some methods, hacktivists contend they aim to foster social or political change and hold influential entities accountable.

Key tactics include denial-of-service (DDoS) attacks, used to shut down websites of opposed organizations or governments; website defacements, altering website content to express dissent or highlight issues; data breaches, stealing sensitive information to support their causes; and media campaigns, utilizing social media and other platforms to spread messages and engage broader audiences.

In the context of the ongoing conflict between Israel and Hamas, and Iran's subsequent support for Hamas through cyber-enabled influence operations, hacktivism plays a critical role. Iran's integrated strategy of combining targeted cyberattacks with widespread influence operations on social media exemplifies the advanced and coordinated approach hacktivists are capable of.

This highlights the evolving threat landscape, where hacktivism not only poses challenges for national security but also underscores the need for comprehensive cybersecurity measures to counteract these sophisticated campaigns.

Evolution of Hacktivist Web DDoS Attack Techniques

The evolution of hacktivist strategies to leverage Layer 7 (L7) web application attacks underscores a significant shift in cyber activism tactics, reflecting both technological advancements and changing geopolitical landscapes. Initially, hacktivist groups relied on the sheer manpower of volunteers manually refreshing browser pages to overload web servers. This method, while straightforward, showcased the collective power of grassroots activism aimed at disrupting targeted websites.

The transition from manual efforts to sophisticated, automated attacks marks a notable evolution in hacktivist capabilities. Following the invasion of Ukraine, entities such as the IT Army of Ukraine and various pro-Russian groups demonstrated the power of crowd-sourced botnets. By distributing easy-to-use attack tools among volunteers, these groups could automate attacks and dynamically update target lists, massively scaling their impact without requiring advanced technical skills from their participants.

A key innovation in this domain has been the introduction of advanced reconnaissance techniques by groups like NoName057(16). By meticulously analyzing target websites to identify pages that would cause the most significant server strain, these hacktivists have refined their attacks to be indistinguishable from legitimate web traffic. This approach not only maximizes the disruption to the targeted infrastructure but also complicates defense efforts, as distinguishing between genuine users and attack traffic becomes increasingly challenging.

The focus on Web DDoS attacks, particularly in 2023, highlights a strategic pivot in hacktivist operations. While traditional volumetric and Layer 4 attacks remain prevalent, the emphasis on Web DDoS attacks signifies a nuanced understanding of web application vulnerabilities and the value of subverting these systems. The ability to cause significant operational disruption with minimal resource expenditure aligns closely with hacktivist objectives, leveraging digital means for protest or to signal dissent.

This evolution also signals to organizations the critical need for robust L7 DDoS protection. As attack methodologies become more refined and harder to detect, ensuring the security and availability of web applications is paramount. The rise of Web DDoS attacks not only poses a technical challenge but also necessitates a strategic response to safeguard against increasingly sophisticated and politically motivated cyber threats.

Reasons for Concern

Given the agitated year of hacktivist activity targeting Israel and the significant increase in activity since the start of the war with Hamas, this year's OpIsrael might attract a significant number of pro-Palestinian hacktivists.

The evolving landscape of cyberactivism, particularly through the lens of OpIsrael and associated operations, underscores a growing concern in the digital security domain. The notable shift in the hacktivist community towards a broadening array of groups engaging in cyberattacks against Israel signals an escalation in the scope and sophistication of these operations. The emergence of new leading actors, such as the Ketapang Grey Hat Team, Anonymous Collective, 1915 Team and Sylhet Gang in 2024, alongside the persistent involvement of groups like Anonymous Sudan, Mysterious Team Bangladesh, and Team Insane PK in previous campaigns, highlights the dynamic nature of hacktivist threats.

The increased coordination among hacktivist groups, leveraging hashtags for organization and rallying, further complicates the cyberthreat landscape. This coordination not only amplifies the impact of their campaigns but also facilitates the formation of temporary alliances, broadening the scope of their attacks. The interconnectedness illustrated between Telegram channels and hashtags reveals the sophisticated organizational structures underpinning these campaigns.

The evolving dynamics of hacktivist operations, marked by the emergence of new actors, increased coordination, improved Web DDoS techniques, and a broadening array of targets, present a complex and multifaceted threat landscape. Particularly, Israel stands at a critical juncture, potentially facing a renewed and intensified wave of targeting by hacktivists beginning April 7, 2024. This prospect underscores the need for heightened security measures and strategic preparedness to mitigate the impacts of such cyber operations. The anticipated escalation in hacktivist activities, aligned with historical campaigns and the emergence of new, more aggressive groups, emphasizes the continuous and evolving threat to Israel's cyber infrastructure.

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.