October 1, 2024

Risk for Heightened Cyberthreats Leading to October 7

Key Insights:

- **October 7, 2023, Attacks Triggered Major Cyber Retaliation:** Israel's retaliation following the Hamas attack led to an unprecedented wave of DDoS attacks by pro-Palestinian hacktivists, marking a significant escalation in cyber conflict.
- **Longstanding Cyber Campaigns Against Israel:** OpIsrael, initiated by Anonymous in 2012, laid the groundwork for continued hacktivist operations, with campaigns like OpsBedil in 2021 and 2022 revitalizing efforts to target Israeli organizations.
- **Emergence of Patriotic Hacktivists:** The Ukraine war sparked a new wave of "patriotic hacktivists," who have remained active and increasingly sophisticated. This trend has expanded, with pro-Muslim and pro-Palestinian groups forming alliances to launch coordinated cyberattacks.
- **Evolving Hacktivist Tactics:** Hacktivists are leveraging social platforms like Telegram to coordinate and share attack tools, leading to more organized and destructive cyber campaigns.
- **Recent Regional Incidents Intensifying Cyberthreats**: Ongoing tensions and recent incidents in the region involving Israel have heightened the likelihood of more coordinated and international cyberattacks. These developments could further galvanize Israel opposing hacktivist groups to escalate their activities.
- **Heightened Cyberthreats Leading to October 7, 2024, Anniversary:** Hacktivists have become more skilled in executing prolonged, high-intensity DDoS attacks. Israeli and allied organizations should anticipate increased cyber activity around the first anniversary of the October 7 attacks.

On 7 October 2023, Hamas and several other Palestinian nationalist militant groups initiated coordinated armed incursions from the Gaza Strip into southern Israel's Gaza Envelope, marking the first invasion of Israeli territory since the 1948 Arab-Israeli War. The attack coincided with the Jewish holiday of Simchat Torah. Hamas and other Palestinian groups called the operation "Al-Aqsa Flood," while in Israel it has been referred to as "Black Sabbath" or the "Simchat Torah Massacre." Internationally, these events are often called the "7 October attacks."

As the sheer scale and brutality of the Hamas attack became clear over the following days, it was clear that Israel's response would be equally unprecedented in scale and intensity. Since then, we have seen the Israeli offensive in Gaza and a war of attrition on Israel's contested northern border.

The conflict did not go unnoticed by pro-Palestinian hacktivists. In response to Israel's retaliation, the country faced an unprecedented wave of DDoS attacks aimed at its organizations and institutions, reaching over 40 organizations targeted on both October 9 and October 10, 2023.

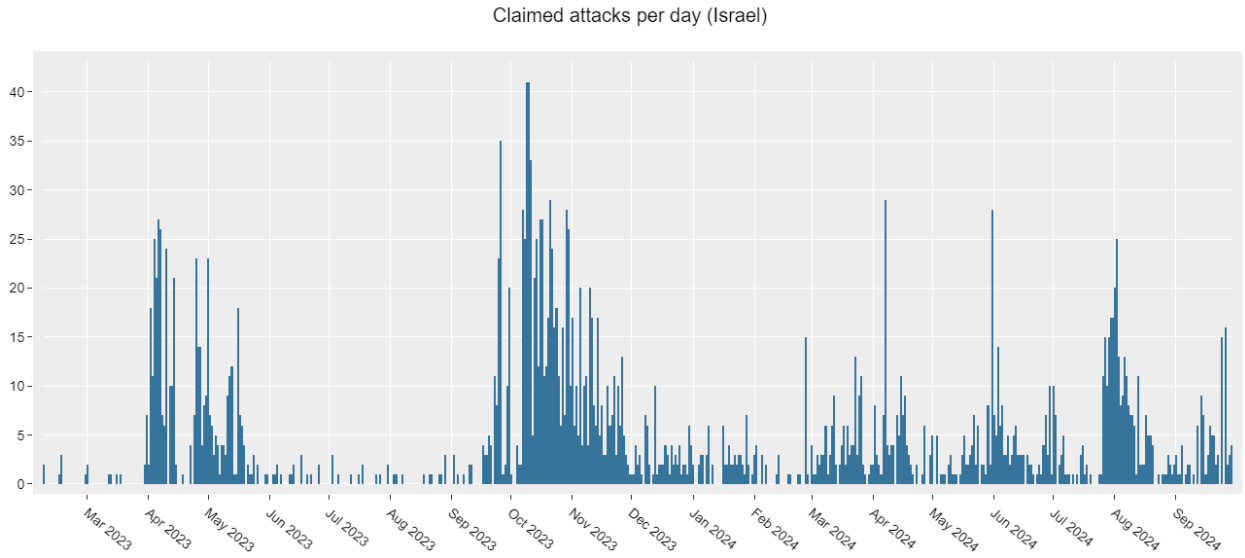

Figure 1: Hacktivist DDoS attack claims per day targeting organizations in Israel (source: Radware)

OpIsrael, Since November 2012

Israel is no stranger to cyber campaigns. 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.

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 Muslim-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. 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.

The New Hacktivists, Since February 2022

At the onset of the invasion of Ukraine, we saw the emergence of a new breed of hacktivist, aptly termed "patriotic hacktivists." Many expected their activity to quickly wane as they lost interest in targeting organizations and institutions worldwide and returned to their everyday lives. However, the opposite proved true. To this day, these new hacktivists have remained persistent, becoming increasingly skilled, sophisticated and organized with each passing year.

Patriotic hacktivists reignited the activity of religious hacktivists, and early in 2023, a pro-Muslim group called Anonymous Sudan made waves in Sweden, Denmark and Australia. Their actions quickly caught the attention of the pro-Russian patriotic hacktivist group Killnet. Recognizing a shared enemy, they officially welcomed Anonymous Sudan into the Killnet cluster. Throughout 2023, we witnessed a growing number of pro-Muslim hacktivists operating on Telegram. These individual groups began connecting on the platform, eventually forming ad-hoc alliances to target common enemies and coordinate attacks for more impactful campaigns.

After announcing its plans to pursue Hamas, the attention of pro-Muslim and pro-Palestinian groups quickly moved to Israel. In the aftermath of the events on October 7, pro-Palestinian hacktivists from Southeast Asia, along with pro-Russian and pro-Iranian groups, started numerous attack campaigns targeting organizations and institutions in Israel and its allied nations.

Public opinion following the 2023 Israel-Hamas war has been deeply divided, with significant differences both within individual countries and globally. Consequently, it wasn't long before various hacktivist groups in the West began targeting Israeli organizations in support of the Palestinian cause.

Reasons for Concern

With more than two and half years of experience performing DDoS attacks, building and sharing attack tools and forming alliances on social platforms such as Telegram, attacks from hacktivists have become more devastating and increasingly sophisticated to stop. See, for example, the Web DDoS attack campaign by a pro-Palestinion hacktivist that lasted six days, featured multiple attack waves amounting to a total of 100 hours of attack time, and peaked at 14.7 million requests per second. Learn about it here.

As October 7 nears, organizations and institutions in Israeli and allied countries need to prepare for a potential surge in DDoS activity targeting their networks and websites.

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.