March 3, 2026

Retaliatory Hacktivist DDoS Activity Following Operation Epic Fury/Roaring Lion

Key Attack Insights:

- Following the onset of “Operation Epic Fury,” hacktivist groups mobilized within nine hours.
- The hacktivist threat in the Middle East is highly lopsided, with two groups, Keymous+ and DieNet, driving nearly 70% of all attack activity between February 28 and March 2.
- Hacktivists prioritized pillars of national infrastructure over random targets, directing 53% of all attacks toward government institutions.
- Despite regional tensions, the hacktivist offensive concentrates on a specific axis consisting of Kuwait, Israel and Jordan and collectively represents more than 76% of all attack claims.
- On March 2, the entry of pro-Russian NoName057(16) into the pro-Iranian/pro-Palestinian campaign signaled a broadening of the hacktivist threat.

Since late February 2026, the Middle East has experienced unprecedented kinetic warfare. Following the collapse of nuclear negotiations and a period of internal Iranian instability, a massive, coordinated military campaign dubbed Operation Epic Fury by the United States, also known as Operation Roaring Lion in Israel, was launched on February 28, 2026. This military offensive, which resulted in the death of Iran’s supreme leader and the destruction of over 2,000 strategic targets, has acted as a primary catalyst for global hacktivist mobilization. As the physical conflict expands across many countries in the region, pro-Iranian and allied "axis of resistance" hacktivist groups have pivoted from baseline activity to aggressive, retaliatory distributed denial of service (DDoS) campaigns targeting government and financial infrastructure across the Middle East.

Background and Timeline of Operations

Prelude to the Conflict (January – February 2026)

In January 2026, the internal instability in Iran intensified amid widespread anti-government protests. Concurrently, the United States began a major military buildup in the Middle East, deploying extensive assets, including the USS Gerald R. Ford carrier strike group.

By early February 2026, indirect nuclear negotiations between the U.S. and Iran had collapsed. The core disputes involve U.S. demands for an immediate end to Iranian nuclear enrichment and the dismantling of its ballistic missile programs.

Timeline of Operations

February 27, 2026: Authorization

U.S. President Donald Trump officially authorizes “Operation Epic Fury,” setting the stage for coordinated military action with Israel.

February 28, 2026: The Initial Strikes

At 6:30 am UTC (10:00 am Tehran time), the U.S. and Israel launch a massive, coordinated preemptive military assault on Iran to dismantle Iran's nuclear and missile capabilities, neutralize its military and induce regime change. The coalition utilizes over 100 American aircraft, naval vessels firing Tomahawk missiles and approximately 200 Israeli fighter jets. Strikes target the Pasteur Street district in Tehran, where the supreme leader's residence is located, as well as major command nodes, air defense and missile production sites and the Islamic Revolutionary Guard Corps (IRGC) Navy across major cities, including Tehran, Isfahan, Qom, and Kermanshah.

Iran immediately countered by launching hundreds of ballistic missiles and drones at Israel and U.S. military bases in the region and neighboring Gulf states, including the UAE, Qatar and Bahrain. Iran also threatens to close of the Strait of Hormuz.

March 1, 2026: Leadership Casualties and Air Superiority

Iranian state media and U.S. and Israeli officials confirm the death of Iran's Supreme Leader, Ayatollah Ali Khamenei, alongside other senior officials and military commanders, while Iran declares a 40-day mourning period.

The U.S. and Israel report striking over 2,000 targets within the first 48 hours, severely degrading Iranian air defenses and establishing air superiority over Iranian airspace.

The IRGC vows revenge and launches a second wave of strikes, while allied proxy groups, including Lebanese Hezbollah, begin firing rockets into Israel.

March 2, 2026: Regional Escalation

The conflict officially expands across at least nine countries in the Middle East as Iranian forces and proxies target regional oil infrastructure and U.S. military bases. Incidents include a drone boat exploding against an oil tanker in the Gulf of Oman and attacks near a British military base in Cyprus.

The International Atomic Energy Agency (IAEA) reports no confirmed damage to Iranian nuclear installations, despite ongoing, heavy bombardment in Tehran and other major cities.

The Iranian Red Crescent Society reported over 500 deaths in Iran, while U.S. and Israeli military estimates claim over 1,000 Iranian military personnel have been killed.

Ongoing Conflict

The joint U.S.-Israeli military campaigns and Iran's retaliatory regional strikes continue into their fourth day, severely disrupting regional stability and global markets.

Hacktivist Activity

The following sections analyze DDoS activity attributed to known hacktivist collectives on Telegram. Our methodology focuses exclusively on DDoS claims, as these serve as the most reliable indicator of operational intent. In contrast, website defacements and data breaches are excluded due to their frequent use as vehicles for disinformation and media manipulation. To ensure data integrity, each claim was cross-referenced with Check-Host.net reports to verify the target's resource, the uniqueness of the claim as well as its temporal accuracy.

We note that a report failure on Check-Host.net is not a sufficient indicator of target impact. Therefore, our analysis treats these claims as evidence of strategic interest and intent by the collectives, intentionally steering clear of performance or success metrics that may be skewed.

Timeline of Middle East Hacktivist Offensive (Feb 28 – March 2, 2026)

The three-day window between late February and early March 2026 was marked by an intense, highly coordinated series of cyberattacks. Driven by a lopsided threat landscape where a handful of groups made most claims. These collectives focused their efforts primarily on government and critical infrastructure targets across the Middle East and Europe.

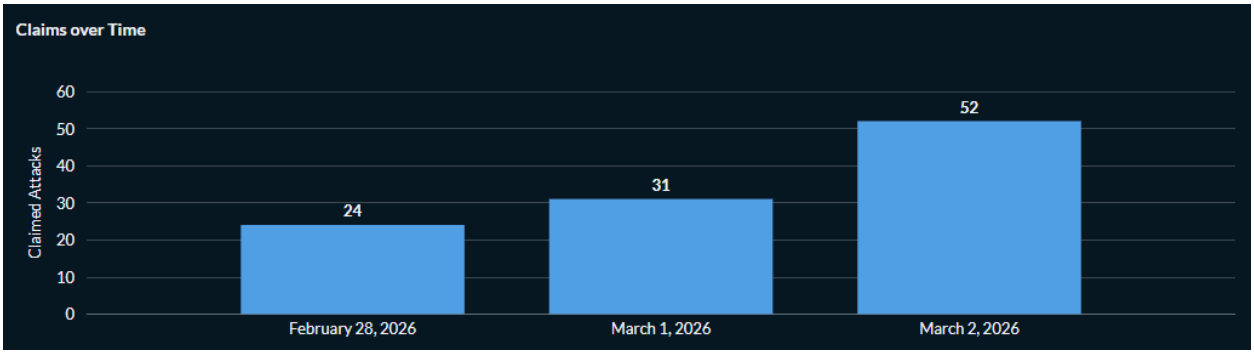

Figure 1: Hacktivist DDoS attack claims targeting the Middle East between February 28 and March 2 (source: Radware)

Below is a chronological breakdown of the major events as they unfolded.

Saturday, February 28: The Opening Salvo (24 Attack Claims)

- **10:00 am Tehran Time (6:30 am UTC):** Reports indicate the first kinetic strikes hit their targets, setting the stage for a potential digital offensive.

- **3:13 pm UTC (5:13 pm IST):** The hacktivist group **Hider Nex** (also known as Tunisian Maskers Cyber Force) launches the first retaliatory DDoS attack. Their first target is Bezeq, one of **Israel**'s largest telecommunications organizations. The group states its attack is a show of support for Iran against its enemies.

  Hider Nex is a pro-Palestinian and pro-Tunisian hacktivist collective that emerged in mid-2025. Operating from Tunisia and emerging in mid-2025 amid escalating cyber tensions with Morocco, it formed to support pro-Palestinian causes and counter perceived Moroccan cyber operations.

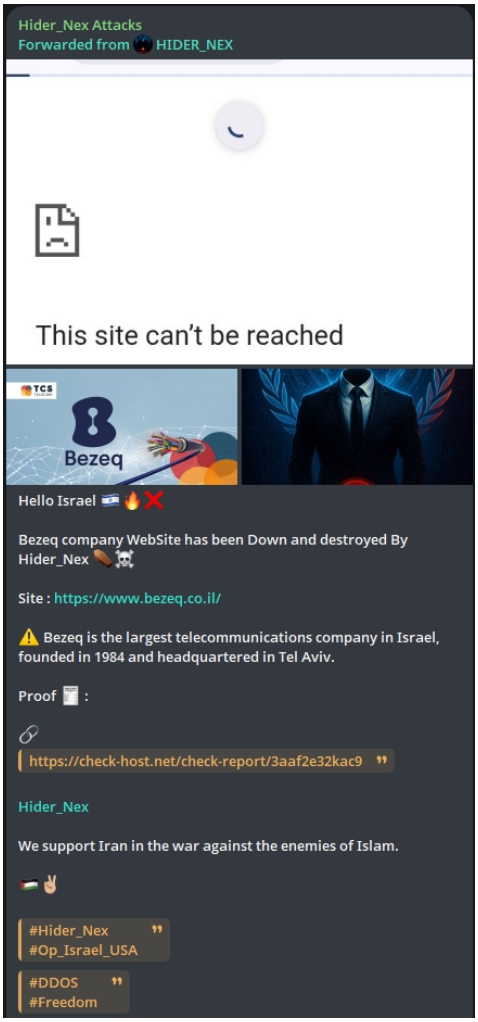

Figure 2: Hider Nex claiming the first DDoS attack on Telegram (source: Telegram)

- **4:47 pm UTC (6:47 pm IST):** Approximately an hour and a half after Hider Nex's strike, **DieNet** joins the fray by targeting a government website of **Qatar**.

  DieNet surfaced in March 2025 as an especially bold and confrontational threat group. DieNet's campaigns are unmistakably political. In March of 2025 they openly blamed U.S. President Donald Trump for fueling their motivation, claiming their cyber offensives are acts of retaliation against U.S. military interventions, economic sanctions and controversial government policies. Their rhetoric consistently targets Trump, portraying him as a symbol of American aggression and imperialism. The group positions itself as a force pushing back against U.S. dominance and global influence.

  Their operations are also often ideologically driven. When attacking Israeli organizations, they use anti-Zionist language. In Iraq, DieNet aligns itself with Shiite militant factions, boasting responsibility for cyberattacks on government institutions and banking systems. However, when they turn their focus toward European corporations, their messaging shifts. It's less about religion and more about opposing Western power structures and the spread of globalization.

- **Late Afternoon (UTC):** Within 30 minutes of hitting Qatar, **DieNet** expands its campaign to target government, transportation and infrastructure sites in **Bahrain** and the **UAE**. The group explicitly stated their actions were a protest against U.S. and Israeli policy, specifically citing their opposition to President Donald Trump.

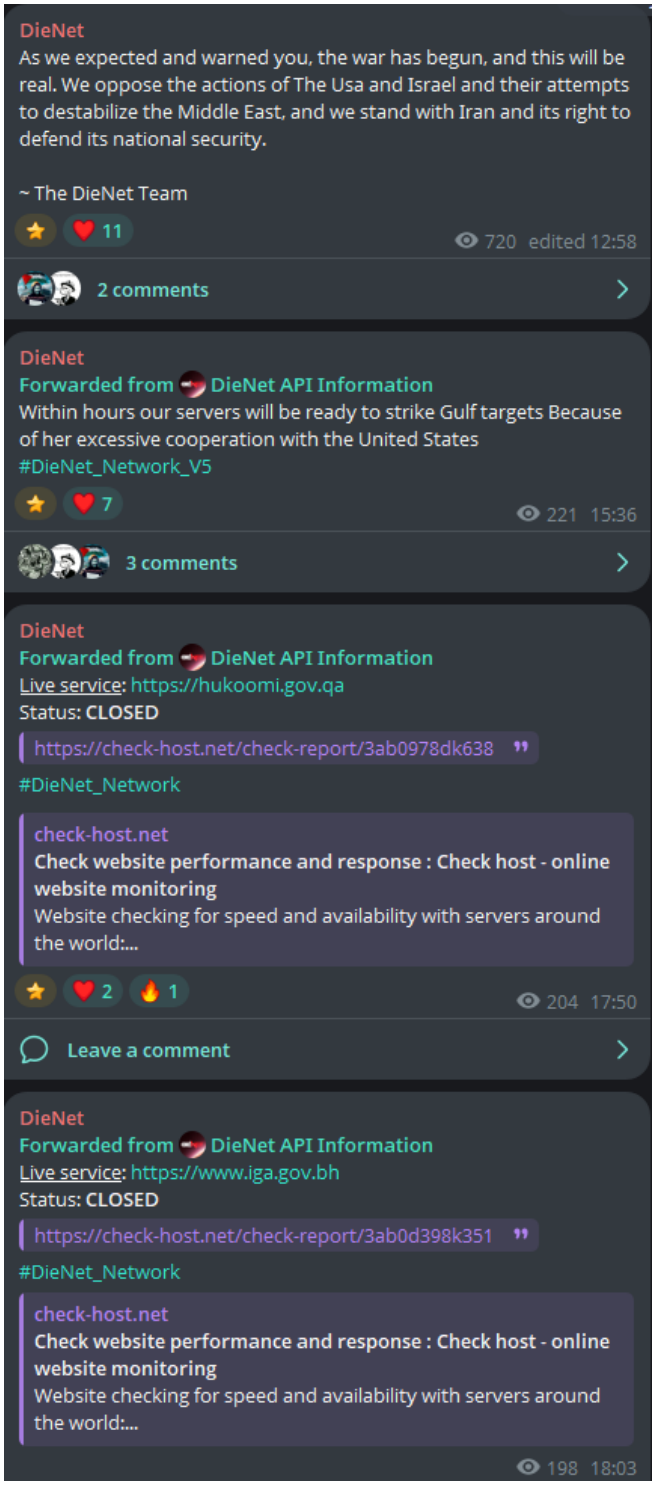

Figure 3: DieNet announcing imminent attacks on Gulf targets, followed by DDoS attack claims (source: Telegram)

- **7:31 pm UTC (8:31 pm IST): Nation of Saviors (NOS)** claims an attack against Israel's **Alon Group**, promising to hold the DDoS for over 20 hours.

  NOS is a pro-Palestinian and pro-Pakistan hacktivist collective that became highly active in 2024 and 2025. They are closely aligned with the Axis of Resistance and are part of a broader network of Southeast Asian and Middle Eastern hacker groups that coordinate large-scale campaigns against Western and Indian interests.

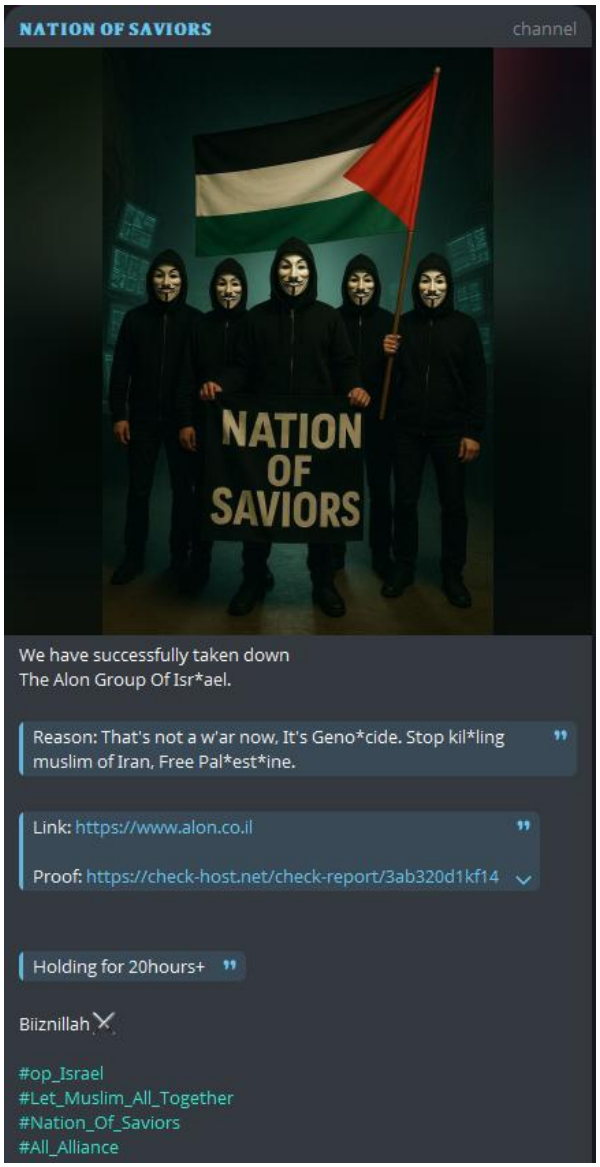

Figure 4: Nation of Saviors (NOS) claims attack against Israel's Alon Group (source: Telegram)

- **8:04 pm UTC: Keymous+** joins the campaign against **Israel**, claiming to have launched attacks targeting telecommunications providers and technology organizations, including Bezeq, Partner Communications, ITC, NCT, Advantech Wireless and Adagio Software.

  Keymous+ is a prominent hacktivist collective that emerged in late 2023 and significantly expanded its operations throughout 2025. The group, with probable origins in Algeria, identifies as "North African hackers" and is characterized by its high-volume DDoS attacks and its hybrid nature, blending ideological hacktivism with commercial cybercrime.

Figure 5: Keymous+ makes its first DDoS attack claim targeting organizations in Israel (source: Telegram)

Sunday, March 1: Expansion and Infrastructure Focus

The momentum continues into March 1 with 31 attack claims, as new groups enter the theater.

- **6:47 pm UTC:** The **Conquerors Electronic Army (CEA)** group officially joins the campaign. They focus their efforts on **Israel**'s retail and finance sectors, targeting **Terminal X**, an AI agent platform for investment managers, as part of what they call the "Battle of the Promise of the Hereafter."

  The CEA is a pro-Iranian hacktivist collective that became prominent in late 2024 and 2025. Unlike the Sylhet Gang, which has roots in the Bengali-speaking community, the Conquerors Electronic Army is another part of the cluster of groups often referred to as the Axis of Resistance, which aligns their operations with Iranian and Hezbollah narratives.

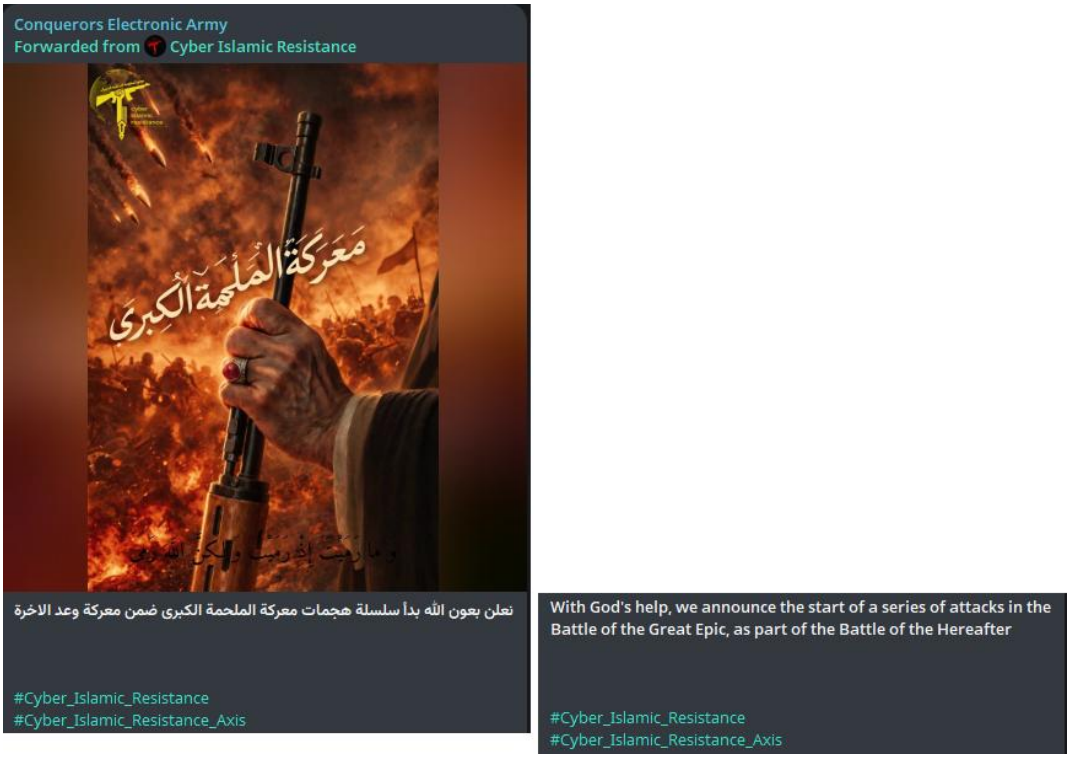

Figure 6: Conquerors Electronic Army announces the start of a series of attacks in support of Iran (source: Telegram)

Figure 7: Conquerors Electronic Army claims attack on Israel-based Terminal X (source: Telegram)

- **Sylhet Gang** enters the campaign later in the day. Their primary target is the **Saudi Arabian government**, specifically the Ministry of Home Affairs' HCM and Internal Management Systems. The group claims this is in retaliation for Saudi Arabia allowing the U.S. to use its bases and airspace.

  Sylhet Gang is a pro-Palestinian, Bengali-speaking hacktivist group that has conducted cyberattacks for political and ideological reasons since July 2023. The group's name is derived from Sylhet, a city and region in northeastern Bangladesh.

Figure 8: Sylhet Gang claims disruption of Saudi Ministry of Home Affairs' systems (source: Telegram)

Sylhet Gang also publicly rejects the condemnation of Iran by their own Bangladeshi Foreign Ministry. It is not uncommon for hacktivists to target or turn against their own governments. Ultimately, these individuals are activists first; their ideological motivations can drive them to challenge domestic policies just as readily as they target foreign entities.

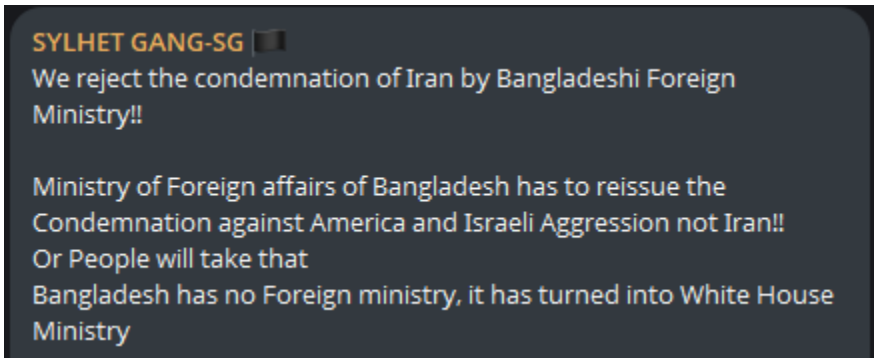

Figure 9: Sylhet Gang publicly rejects the condemnation of Iran by their own Foreign Ministry (source: Telegram)

Monday, March 2: The Pro-Russian Pivot

The final day of this concentrated window sees 52 attack claims, characterized by the entry of a powerful European-focused actor.

- **11:17 am UTC:** The pro-Russian hacktivist group **NoName057(16)** joins the pro-Palestinian alliance. They launch attacks targeting Israeli government, telecommunications and business targets.

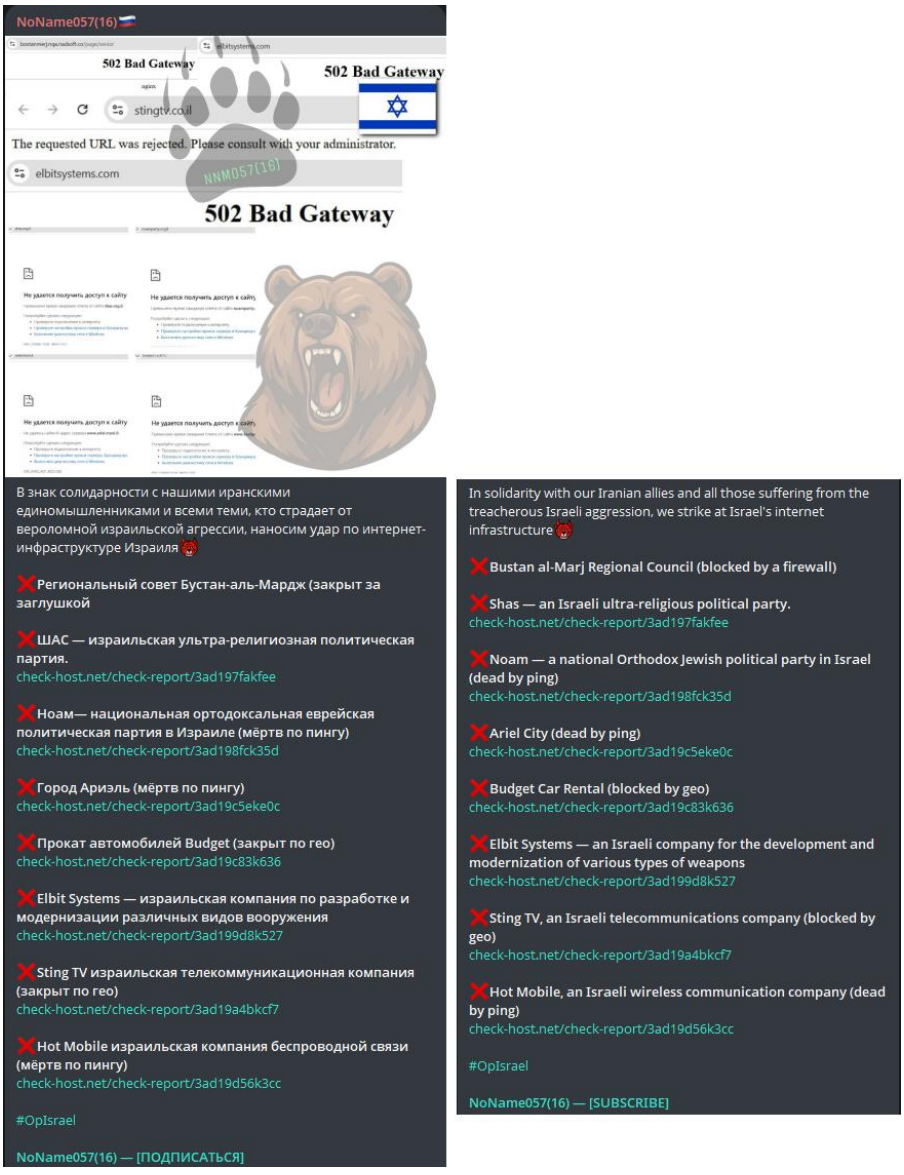

Figure 10: Russia-aligned hacktivist group NoName057(16) claims its first targets in the Middle East (source: Telegram)

The Middle East Cyber Surge (February 28 - March 2)

Between February 28 and March 2, the Middle Eastern digital landscape experienced a concentrated burst of hacktivist activity, characterized by DDoS attacks targeting critical infrastructure and government services. This period saw nine distinct hacktivist groups claim 107 attacks against 81 organizations across 8 different countries in the region.

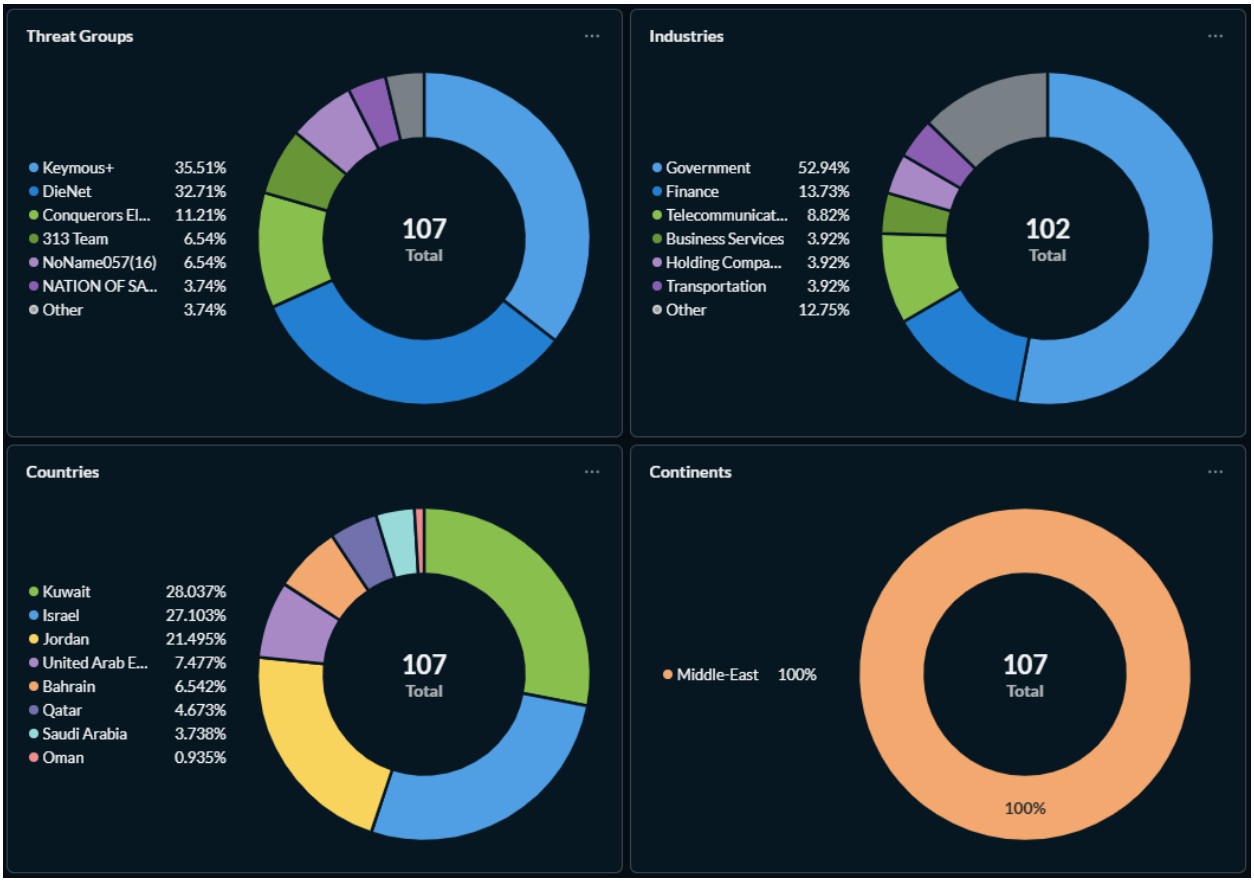

Figure 11: Claimed attack characteristics for threat groups targeting organizations in the Middle East region (source: Radware)

The data reveals a highly lopsided threat landscape, with a small number of groups responsible for the vast majority of the attack activity:

- Keymous+ emerged as the primary aggressor, accounting for 35.5% of all attack claims.
- DieNet followed as the second most active threat group, contributing to 32.7% of the total claims.
- Conquerors Electronic Army maintained a significant presence with 11.2% of the activity.

Other notable participants included 313 Team (6.5%), NoName057(16) (6.5%) and the Nation of Saviors (3.7%).

Target Sectors: Government Under Siege

The hacktivist groups focused their efforts on pillars of national stability, with the government sector bearing the brunt of the offensive. Government institutions were the target of almost 53% of all attacks, highlighting a clear intent to disrupt state functions and public messaging. Financial services ranked second at 13.7%, followed by telecommunications at 8.8%.

Geographical Distribution: The Kuwait-Israel-Jordan Focus

The distribution of attacks within the region was heavily concentrated in three specific nations: Kuwait, Israel and Jordan, with Kuwait accounting for 28%, Israel for 27.1% and Jordan for 21.5% of the total attack claims. The United Arab Emirates faced 7.5% of the activity, while Bahrain saw 6.5%. Remaining attacks were distributed among Qatar (4.7%), Saudi Arabia (3.7%) and Oman (1%).

The metrics suggest a coordinated effort by Keymous+, DieNet, CEA, 313 Team, NOS and Russia-aligned NoName057(16) to saturate the Middle Eastern digital space. By prioritizing government and financial targets in Kuwait, Israel and Jordan, the threat groups demonstrated a strategic focus on maximum visibility and civil disruption.

The Regional Divergence of Global Hacktivism (Feb 28 – March 2, 2026)

The turn of March 2026 saw a significant surge in coordinated digital aggression, with hacktivist collectives launching simultaneous campaigns across the Middle East and Europe. While both regions faced a high number of attacks, the data reveals two distinct threat personalities operating in these digital theaters.

1. The Middle Eastern Theater: A Consolidated Offensive

In the Middle East, the threat landscape was characterized by a lopsided distribution of power, where a small number of groups were responsible for the vast majority of disruptions.

- **Dominant Actors:** Keymous+ led the charge, claiming 35.5% of the 107 total attacks, closely followed by DieNet at 32.7%.
- **Target Concentration:** The offensive was focused on Kuwait, Israel and Jordan, which together accounted for 76.6% of all regional claims.
- **Sector Volatility:** The government sector was the primary target, accounting for more than half (53%) of targeted organizations.

2. The European Theater: The Dominance of NoName057(16)

While the Middle East faced a variety of groups, the European theater was dominated by a single entity. Between February 28 and March 2, five threat groups targeted 23 organizations in five European countries across 34 attack claims. European attacks peaked sharply on February 28 with 20 claims, before tapering off significantly to six and eight claims in the following two days.

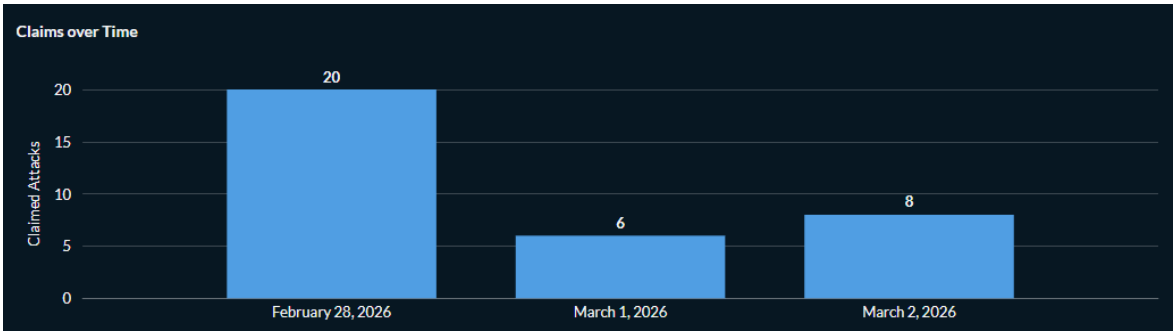

Figure 12: Hacktivist DDoS attack claims targeting Europe between February 28 and March 2 (source: Radware)

- **The NoName Hegemony:** The pro-Russian group NoName057(16) was responsible for 73.53% of all European attack claims. ServerKillers followed as a distant second at 17.65%.
- **Geographic Focus:** Denmark bore the brunt of this activity, receiving 55.9% of the regional attacks, while Germany and Spain each accounted for 17.65%.

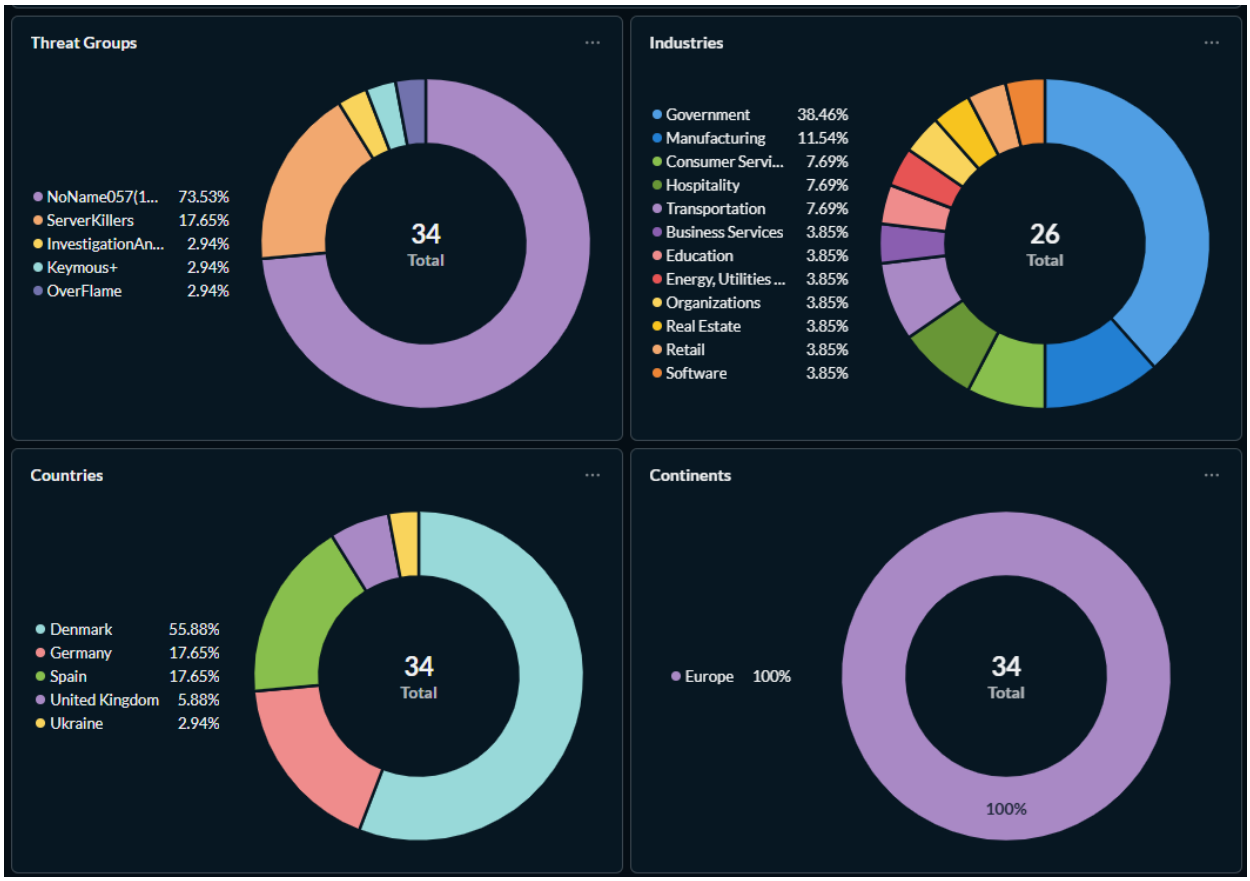

Figure 13: Claimed attack characteristics for threat groups targeting organizations in Europe (source: Radware)

Comparative Analysis: Industries at Risk

Despite different primary actors, both regions saw their government infrastructure as the most vulnerable point of entry.

Industry	Middle East Impact (%)	Europe Impact (%)
Government	52.94%	38.46%
Finance	13.73%	*Not in Top Tier*
Manufacturing	*Not in Top Tier*	11.54%
Telecommunications	8.82%	*Not in Top Tier*

The recent statistics for Europe are unsurprising, given the dominance of NoName057(16). As the group responsible for the vast majority of tracked DDoS activity, their strategic focus remains steadfastly on government institutions and public administration. Note that during late February to early March, Europe saw relatively routine hacktivist patterns. In contrast, the escalating conflict in the Middle East served as a catalyst that drove a surge in coordinated offensive actions from Iran-aligned collectives.

Global Hacktivist Activity

This section provides a consolidated view of the global hacktivist landscape between February 28 and March 2, 2026, combining the data from previous regional analyses to understand the global scale of the threat. The data covers unfiltered claims across the entire period.

Consolidated Activity and Major Players

Over these three days, a total of 149 attack claims were recorded targeting 110 distinct organizations across 16 countries. The activity was driven by 12 threat groups.

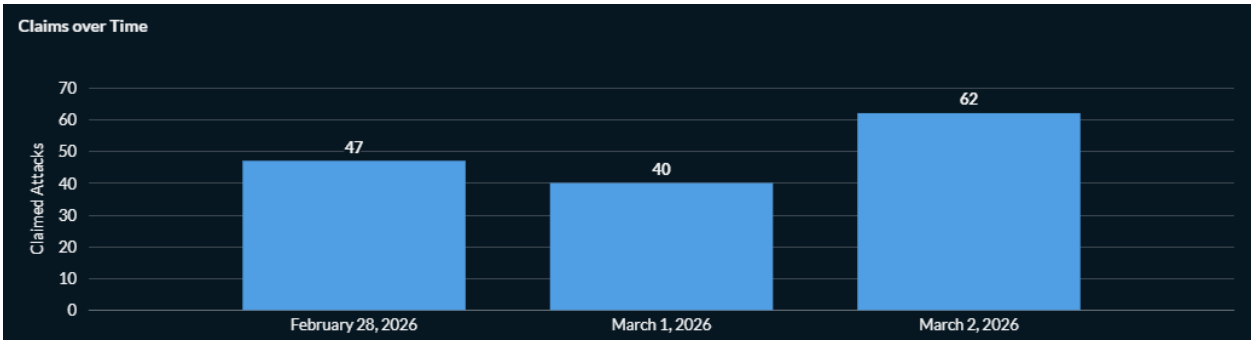

Figure 14: Global hacktivist DDoS attack claims between February 28 and March 2 (source: Radware)

A major characteristic of this period, as highlighted by other analyses, is a highly lopsided threat landscape where a very small number of groups were responsible for a staggering majority of all recorded global disruptions. The most dominant actors globally were those involved in the Middle East campaign:

- **Keymous+**: The most prolific group, responsible for 26.8% of all global claims.
- **DieNet**: A very strong secondary threat, accounting for 25.5% of the global total.
- **NoName057(16)**: Significantly contributing to the global hacktivist DDoS activity on the two major fronts, representing 22.2% of all global claims.

Combined, these top three groups alone were responsible for 74.6% of the entire world's recorded attack claims during this window.

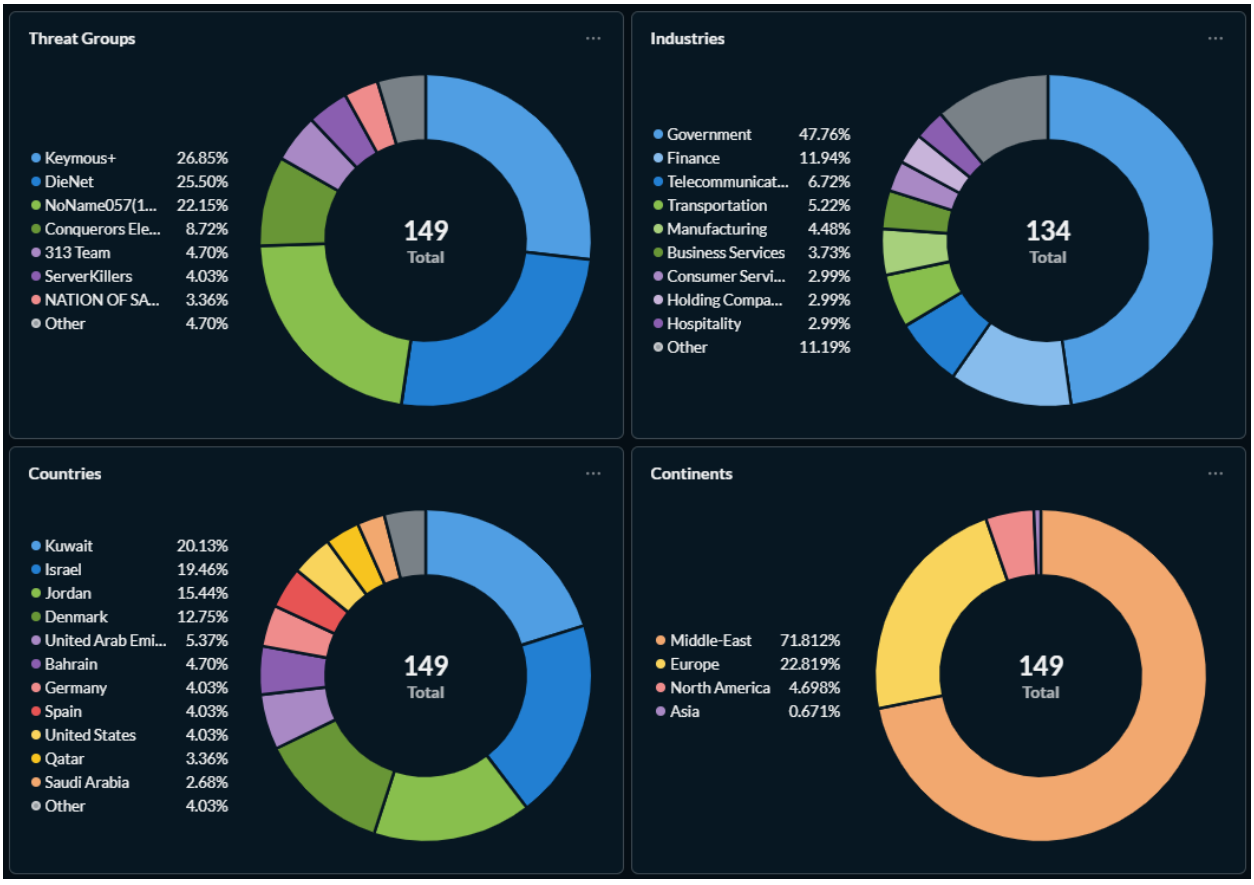

Figure 15: Claimed attack characteristics for the global hacktivist threat (source: Radware)

Global Targeting and Affected Industries

Global activity, biased largely by a majority of Middle East-targeted attacks (107 out of 149), concentrated disproportionately on public infrastructure and state-level targets, which are often

prioritized for maximum public disruption and political visibility. The government sector was the single most heavily targeted industry, accounting for 47.8% of all targeted organizations globally. Following as a secondary focus was finance at 11.9%, with telecommunications next at 6.7%. Other sectors that experienced DDoS attacks included transportation (5.2%), manufacturing (4.5%), business services (3.7%) as well as consumer services, holding companies and the hospitality sector (each around 3%).

Continental Distribution of Threat Activity

In terms of regional impact, one specific area was absorbing the majority of the aggression:

- **The Middle East** was the most targeted region, receiving 71.8% of all global attack claims.
- **Europe** followed as the next significant focal point, being the target of 22.8% of the total global activity during that limited period.

Activity in North America and Asia was significantly lower.

The countries experiencing the most intense pressure reflect these regional concentrations, with Kuwait, Israel and Jordan bearing the brunt at respectively 29.1%, 19.5% and 15.4% of global activity. Denmark followed at 12.8%, just before the United Arab Emirates that represented 5.4%.

Reasons for Concern

The digital front is expanding alongside the physical one in the region, with hacktivist groups simultaneously targeting more nations in the Middle East than ever before. Until Monday, we observed limited involvement of pro-Russian groups in the campaign, but as the conflict continues, we expect to see more groups from existing alliances with pro-Palestinian and pro-Iranian groups join the digital campaign.

Recommendations

While robust mitigation strategies can effectively neutralize DDoS attacks, unprotected infrastructure will almost certainly face significant disruption. Organizations should not wait for an active threat to implement defenses; in the current climate, a hacktivist strike is a matter of “when,” not “if.” Although government and financial sectors remain high priority targets, no industry is immune. By proactively hardening your environment, you ensure that a coordinated attack remains nothing more than an empty claim.

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.