March 18, 2025

DieNet Activity Escalates Against US Organizations

Key Insights:

- DieNet is a new hacktivist threat group that emerged in March 2025
- DieNet leverages distributed denial of service (DDoS) attacks, sharing public proof-of-impact results via its Telegram channel(s)
- DieNet claimed 61 attacks against 19 U.S. organizations between March 11 and 17 and targeted several organizations in Iraq, Israel, the Netherlands and Egypt
- DieNet primarily targets critical infrastructure sectors, including finance, energy, transportation and telecommunications
- DieNet's campaigns are politically and ideologically driven, with consistent anti-US, anti-Trump and anti-Zionist messaging.
- Attacks are often framed as retaliation for perceived Western military actions, sanctions or political decisions.
- DieNet expressed alignment with Shiite militant groups in the Middle East, though Western European attacks reflect a broader anti-globalization narrative.

In a rapidly shifting world of hacktivism, DieNet surfaced in March 2025 as an especially bold and confrontational threat group. Known for their aggressive tactics and unapologetically brash tone, their communications are filled with threats, ridicule and taunts. Phrases like "we warned you" and "this is just the beginning" are common in their public statements.

Figure 1: First post on the newly created DieNet channel after the original channel got banned by Telegram (source: Telegram)

On March 12, only five days after their first ever message, DieNet's Telegram channel was banned. The group responded immediately by starting a new channel and threatening with more attack campaigns.

DieNet's campaigns are unmistakably political. They openly blame 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 its 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.

DieNet doesn't attack indiscriminately. Their targets are strategically selected to maximize visibility. They frequently go after critical infrastructure, including financial institutions, power grids, transportation systems and communication networks. Trump-affiliated businesses and prominent American corporations are also high on their list, chosen as symbols of the political grievances they aim to spotlight. By striking at recognizable names and vital services, DieNet seeks to generate headlines, instill fear and amplify their ideological message.

At their core, DieNet uses cyberattacks as a form of protest. Their objective is to challenge political leaders and governments through high-impact, highly publicized assaults. By focusing on high-profile targets, they ensure their defiance and demands are impossible to ignore on the global stage.

Figure 2: Messages by DieNet posted on March 16, 2025—during the peak of US-targeted claims—blaming President Trump for their actions. (source: Telegram)

Targeted Countries

DieNet's wave of cyberattacks began on March 7 when they launched their initial offensive against Meta.ai in the United States. Over the next two days, from March 7 to 8, they shifted their focus to Israel, striking both a university and a media outlet. These attacks were framed as retribution for Israeli government policies and were steeped in anti-Zionist and anti-Israel rhetoric, which DieNet used to justify their actions.

On March 9 and 10, the group turned its attention to Iraq, specifically targeting government and economic websites. In their claims, DieNet expressed solidarity with Shiite militant factions, leveraging the country's ongoing sectarian and political tensions as the backdrop for their cyber offensives.

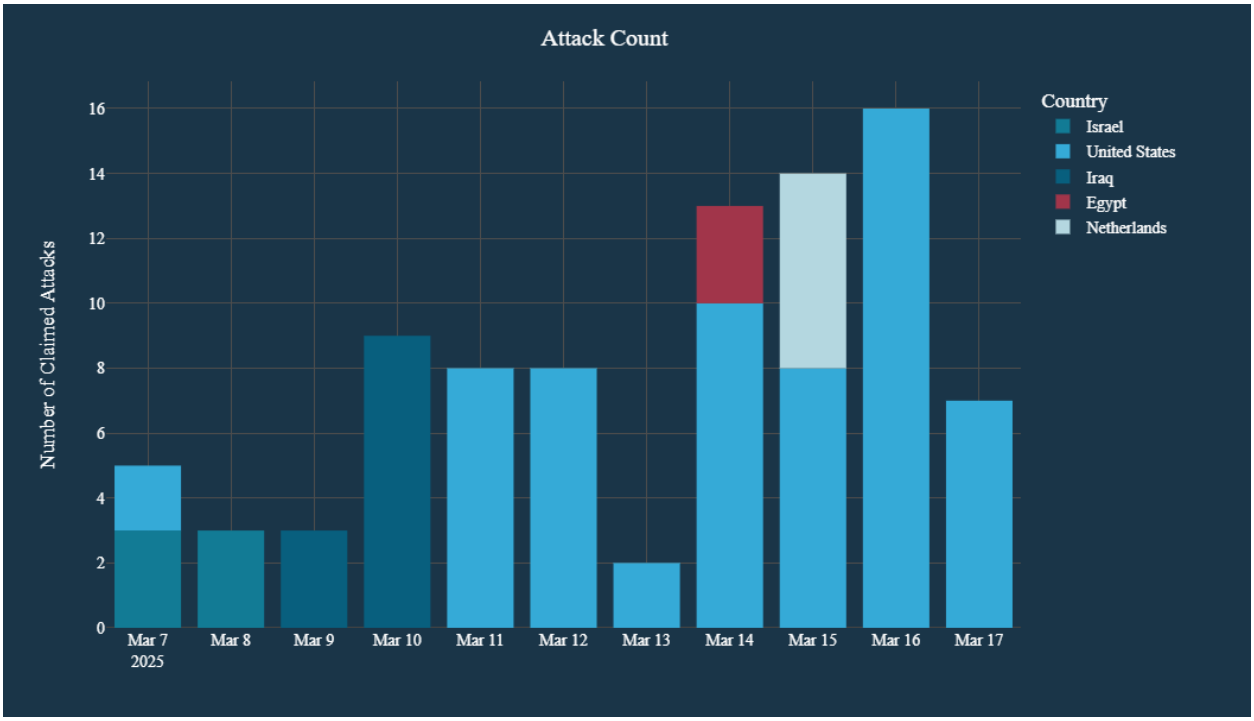

Figure 3: Attack claims, by DieNet, per country over time (source: Radware)

Between March 11 and March 17, DieNet escalated their campaign, taking responsibility for 61 attacks against 19 different U.S. organizations such as SpaceX, TikTok, Nasdaq, Amazon Pay, etc. Their targets spanned critical sectors, including finance, transportation, energy, media outlets and businesses linked to Donald Trump. Throughout their messaging, DieNet positioned the United States as their primary adversary, portraying their actions as direct retaliation for Trump's leadership and the country's military interventions. A broader anti-Western and anti-capitalist narrative underscored their rhetoric during this period.

On March 14, DieNet expanded their focus to Egypt, attacking a major telecommunications provider. They justified this breach with anti-Zionist language, accusing the company of collaborating with Israel and framing the assault as part of their larger ideological campaign.

The following day, March 15, DieNet targeted payment service providers in the Netherlands. Unlike previous attacks driven by ideological motivations, this operation appeared to be a calculated demonstration of their alleged ability to disrupt vital digital infrastructure within the European Union. They highlighted the Netherlands' dependence on digital systems, framing the attack as a warning of their reach and power rather than a purely ideological strike.

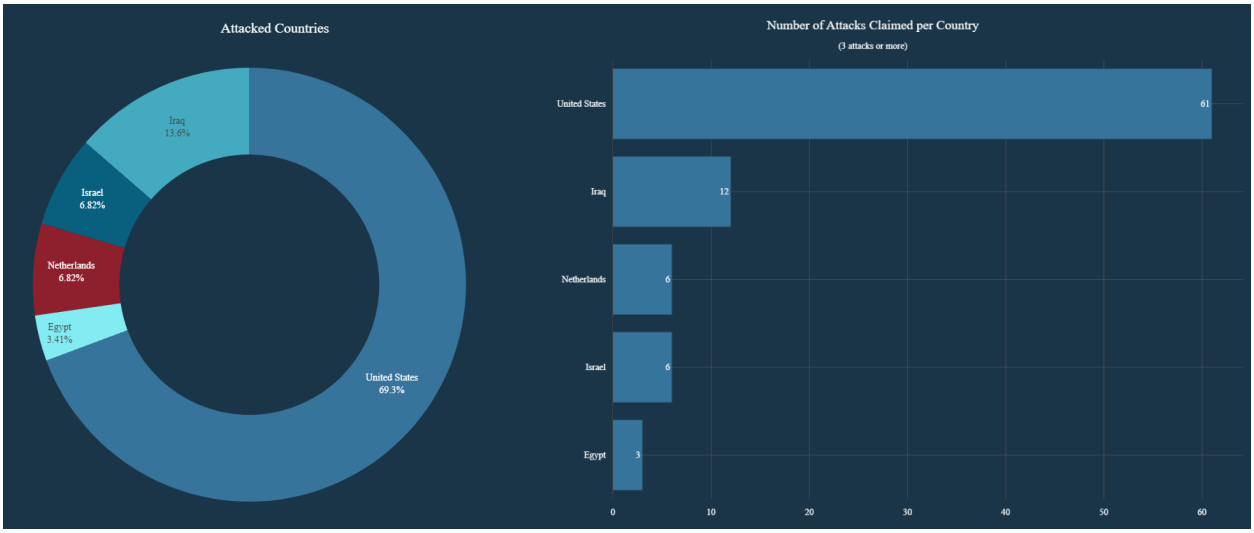

Figure 4: DieNet attack claims by country (source: Radware)

Targeted Industries

The financial sector is one of DieNet's primary battlegrounds. High-profile targets like Nasdaq, Amazon Pay and The Clearing House have been targeted as part of a broader campaign against American economic power. By targeting financial institutions, DieNet aims to destabilize global financial systems and deliver a potent anti-capitalist message, portraying these entities as tools of Western oppression.

Telecommunications providers have also been in DieNet's crosshairs. Attacks targeting Lumen Technologies and Orange Egypt reflect both anti-Western and anti-Zionist motives. DieNet's messaging casts these companies as complicit in the policies of Western powers and Israel, with a particular emphasis on disrupting communication networks to sow social instability.

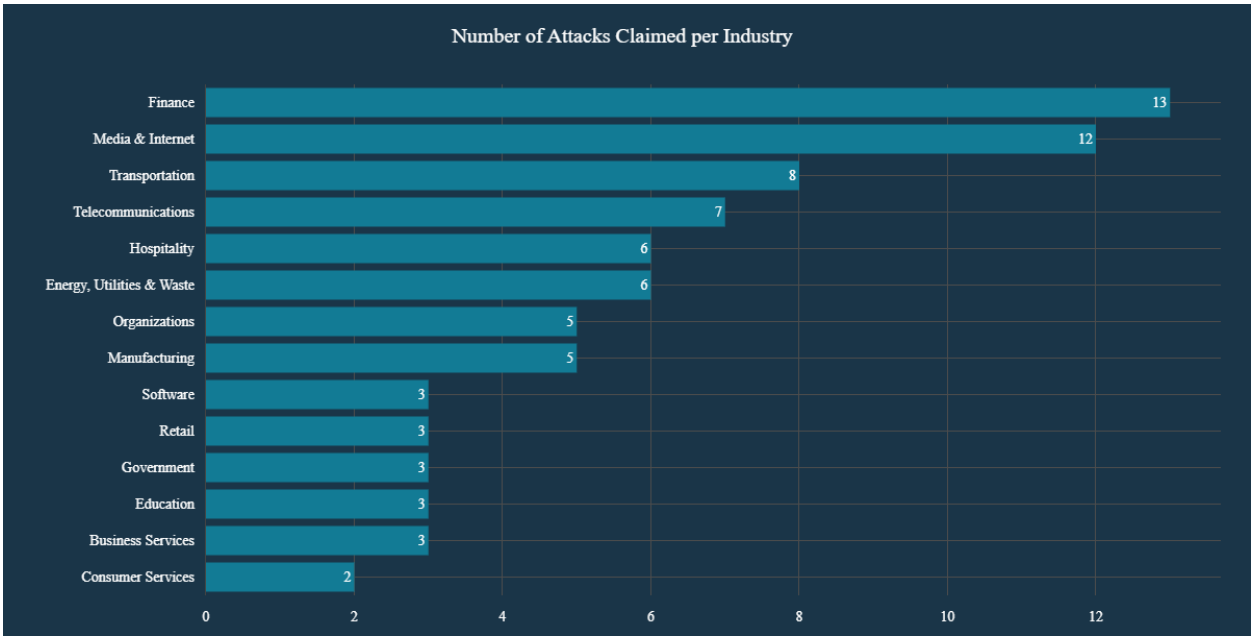

Figure 5: DieNet attack claims by industry (source: Radware)

The transportation sector hasn't been spared. From Lyft and the Port of Los Angeles to the Netherlands' OVpay and Chicago Transit Authority, DieNet's attacks demonstrate their ability to hinder daily life by targeting civilian infrastructure. Their actions are framed as indirect strikes on societal functionality, designed to paralyze economies and expose the fragility of Western infrastructure.

Energy and utilities are another critical focus area. DieNet's attacks on the PJM Interconnection and North American Electric Reliability Corporation (NERC) are presented as direct assaults on national security. By targeting energy systems that millions rely on, they aim to undermine public confidence, spread fear, and weaken civilian morale.

In a more personalized campaign, DieNet has also targeted Trump-branded properties, including the Trump International Beach Resort, Trump Winery, and Trump Golf. These attacks are deeply symbolic, representing a vendetta against Trump himself. By hitting his business empire, DieNet seeks to damage his political influence and retaliate for policies they oppose.

Beyond infrastructure, DieNet has focused on software and business services such as TradeStation, iDEAL, and Ideal Security. These attacks aim to disrupt financial transactions and erode trust in digital commerce, particularly in the US and the Netherlands. Their strategy underscores an intent to undermine Western financial dominance and create psychological pressure on businesses and consumers alike.

Media and internet platforms have been targeted as well. TikTok, Military.com, Snapchat, Meta, and The Jerusalem Post are accused by DieNet of perpetuating Western propaganda or censorship. Their attacks are framed as acts of resistance against media manipulation, portraying themselves as defenders of free information.

In Iraq, DieNet has launched attacks against government institutions like the Foreign Ministry and Central Bank. They claim solidarity with Shiite militant groups and frame these operations within broader regional conflicts, using cyberattacks to promote rebellion narratives and destabilize the Iraqi state.

DieNet's anti-Zionist agenda is also evident in their attacks on educational institutions, specifically Haifa University. By targeting this prominent Israeli university, they aim to strike a blow at the country's technological and academic leadership, furthering their ideological narrative against the Israeli state.

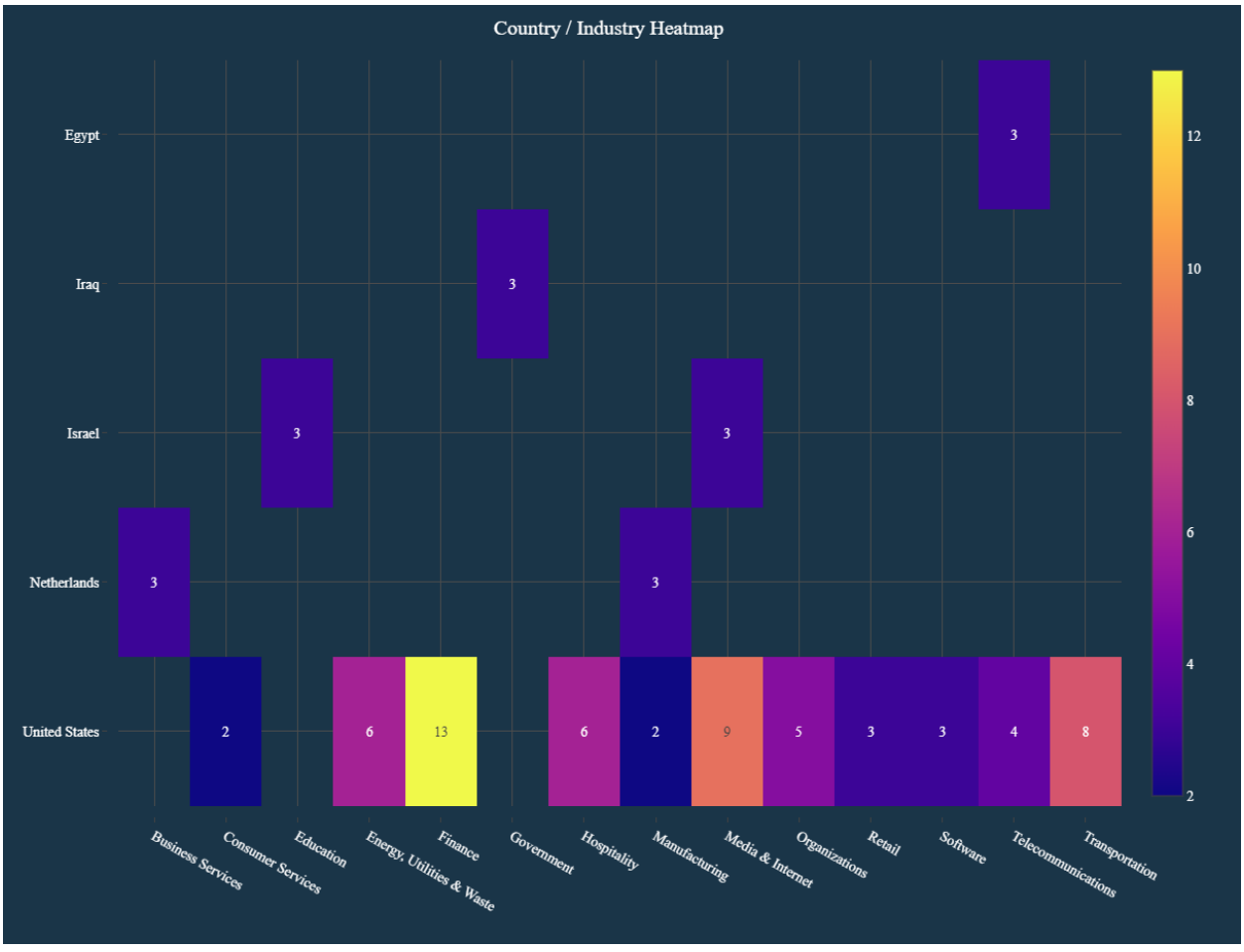

Figure 6: Country and industry heatmap of DieNet claimed attacks (source: Radware)

Reasons for Concern

DieNet's activities highlight several important risks. First, their focus on critical infrastructure—such as financial systems, energy providers, transportation and communications—means their attacks have a potential to cause real-world disruptions. These sectors are essential for day-to-day operations, and successful attacks can lead to service outages, economic impacts, and public uncertainty.

Second, DieNet's ability to coordinate widespread campaigns against high-profile targets shows a level of organization and persistence that is worth noting. While their messages are often aggressive and provocative, the technical aspects of their operations indicate a focused and sustained effort.

Third, their motivation appears to be both political and ideological. They position themselves in opposition to certain governments and policies, which suggests their campaigns could continue or escalate, depending on global events. Their support for specific groups and causes may also lead them to expand their list of targets.

Summary

DieNet is an emerging threat group that targeted critical services and high-profile companies in their first month on the hacktivist scene, often using aggressive messaging to amplify its impact. Their actions are politically driven, particularly against the United States and its allies, and they show ideological alignment with certain regional groups. While their communications are provocative, the underlying campaigns demonstrate serious intent. Ongoing vigilance and preparedness are essential to defend against these types of threats.

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.