Cyber Insight

DieNET v2 Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources.
This information is analysis from a strictly cyber perspective.

The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

Credits Orange Cyberdefense

DieNet v2 Group

- **Creation date:**
  DieNET emerged on March 7, 2025, announcing its presence via a Telegram channel. The group's activity surged two days later, following the arrest of a Columbia University activist. DieNET-v2 was later referenced, indicating an evolution with expanded capabilities and membership.

- **Probable Origin**:
  DieNET's origins are unclear, but its Telegram activity and alliances suggest a decentralized, possibly international network. The group is supported by pro-Palestinian hacktivist groups, including some with pro-Russian sympathies, hinting at a Middle Eastern or Eastern European influence. No definitive evidence ties DieNET to a single country or region.

- **Main strategies:**
  DieNET-v2 primarily employs Distributed Denial of Service (DDoS) attacks, leveraging DDoS-as-a-service infrastructure for rapid, high-volume strikes. Attack vectors include TCP RST, DNS amplification, TCP SYN floods, and NTP amplification, often rotated for unpredictability. The group also claims website defacement and data breaches, though some claims, like a 247 GB data exfiltration, were exaggerated or unverified.

- **Geopolitical Motivation:**
  DieNET-v2's actions are driven by pro-Palestinian and anti-Trump ideologies, opposing U.S. and Israeli policies. The group has issued direct threats to the U.S. government, particularly in response to military actions like airstrikes in Yemen. Alliances with groups like LazaGrad Hack and Sylhet Gang-SG suggest broader anti-Zionist and anti-Western motives.

- **Targeted business sectors:** DieNET-v2 focuses on critical infrastructure, including energy, healthcare, and financial services. U.S. targets include the Port of Los Angeles and Chicago Transit Authority. The group also attacks digital platforms like NASDAQ and X for disruption. Healthcare providers, such as Epic Systems, are frequent targets.

Identification

DieNet initially emerged on Telegram in March 2025, announcing plans to target illegal sites and corrupt government platforms with DDoS attacks.
Just over a week later, DieNet-v2 was launched, representing a significant upgrade with larger botnets, more members, and enhanced attack capabilities.
While the group's core motivations, pro-Palestinian and anti-Trump sentiments, remained unchanged, DieNet-v2 marked a clear escalation in both resources and operational reach.

Credits Orange Cyberdefense

DieNet-v2 Group: Main collaborating

Mr Hamza

A pro-Palestinian hacktivist group with ties to pro-Russian and pro-Iranian entities.

Known for targeting Western government agencies, critical infrastructure, and private companies.

Promoted DieNET on March 7, 2025, indicating a possible alliance to enhance attack coordination.

LazaGrad Hack

A pro-Palestinian and pro-Russian hacktivist group.

Collaborates with DieNET, sharing ideological goals and possibly attack infrastructure.

Actively promoted DieNET’s emergence on Telegram in March 2025.

Sylhet Gang-SG

A hacktivist group that explicitly targets “allies of Zionist” entities.

Engages in DDoS attacks and has been linked to DieNET through mutual promotion and shared targets.

Supported DieNET’s launch and activities in early March 2025.

OverFlame

A group sharing DDoS-as-a-service infrastructure with DieNET, indicating technical collaboration.

Involved in similar ideologically driven attacks against critical infrastructure.

Attack traffic analysis shows overlapping infrastructure use with DieNET.

DenBots Proof

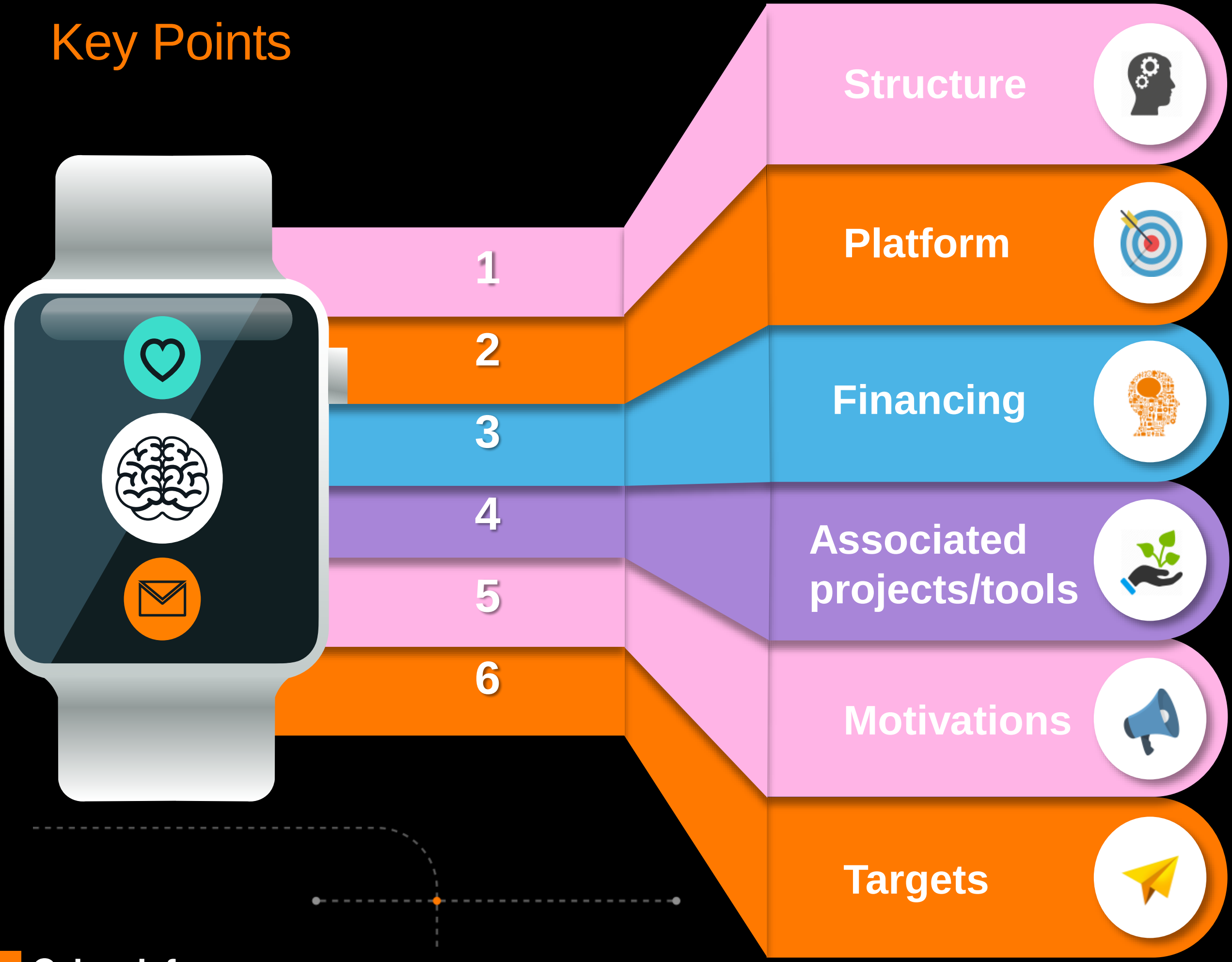
Another group utilizing the same DDoS-as-a-service infrastructure as DieNET.

Likely collaborates through shared tools and attack vectors to amplify disruption.

Identified in attack source analysis alongside DieNET and OverFlame.

Credits Orange Cyberdefense

Key Points



1 **Structure**

DieNet functions as a decentralized hacktivist group. Especially in its V2 phase, the group has seen a growing membership and embraces an autonomous structure through decentralized Telegram channels

2 **Platform**

The group primarily communicates and claims responsibility for attacks via Telegram channels, quickly re-establishing new channels when banned to maintain their presence and spread their aggressive messaging

3 **Financing**

There’s no clear evidence of direct funding; DieNet relies on alliances and rented DDoS-as-a-service tools, favoring shared or purchased attack capabilities over its own botnets.

4 **Associated projects/tools**

DieNET uses DDoS-as-a-service tools and leverages network-based attack techniques, often operating through shared infrastructure with allied groups such as OverFlame and DenBots Proof.

5 **Motivations**

DieNET is motivated by pro-Palestinian and anti-Western ideologies, targeting U.S. and Israeli entities, as well as European countries, in response to geopolitical events such as military actions and policy decisions.

6 **Targets**

DieNet targets critical infrastructure sectors such as finance, energy, transportation, telecommunications, healthcare, and digital commerce.

Credits Orange Cyberdefense

Vectors of Influence

1 Strategic Timing

The group's activities intensify in direct response to specific geopolitical events. This strategic timing is designed to maximize media coverage and amplify its political message by linking its actions to broader ideological causes.

2 Symbolic Targeting

Symbolic Targeting of Critical Infrastructure (CNI): DieNET-v2 deliberately targets critical infrastructure sectors such as energy, healthcare, and finance, to expose their vulnerabilities.

3 Building a Narrative

The group aligns its actions with strong ideological causes, particularly pro-Palestinian convictions and strong opposition to the U.S. administration, to gain support from like-minded hacktivist groups and individuals.

4 "Rebel Hacker" Myth

DieNET-v2 actively construct a "rebel hacker" myth to facilitate online indoctrination and mobilize potential new recruits.

5 Media Staging

Each operation is publicized to maximize visibility, often accompanied by statements detailing the targets and motivations. This approach is intended to intimidate adversaries and strengthen their image as an influential group.

orange Cyberdefense

Credits Orange Cyberdefense

Emotional Intelligence

1 Applying the SWITCH framework (Social Influence, Willpower, Incentives, Triggers, Context, Habits) to DieNET reveals their strategic approach.

2 DieNET strengthens its legitimacy and expands its reach by partnering with groups like Sylhet Gang-SG. By amplifying shared narratives and supporting each other's campaigns, DieNET increases its visibility and influence within these circles, making their movement appear larger and more coordinated.

3 Symbolic victories and media attention are DieNet's main incentives, motivating members even when tangible results are limited. These public displays of impact help sustain engagement and attract new participants who are drawn to the group's visibility and perceived influence.

4 Geopolitical events, such as activist arrests or military actions, serve as catalysts, prompting DieNet to launch rapid attack responses. These timely reactions allow the group to capitalize on heightened emotions and media attention, maximizing the impact of their operations.

5 Their messaging uses NLP-style techniques, including emotionally charged language and strategic framing, like labeling opponents as "Zionist allies", to sway followers and provoke strong reactions. This approach aligns with NLP's emphasis on subconscious persuasion and influence.

6 DieNet's approach follows a logic of cognitive manipulation. The group plans its actions based on the psychological impact on its targets. They exploit reasoning flaws and information overload to sow doubt and confusion.

orange Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

Finance

Energy

Transportation

Telecommunications

Healthcare

Government

Digital commerce

Media and internet platforms

Software and business services

Critical Infrastructure

Private Companies

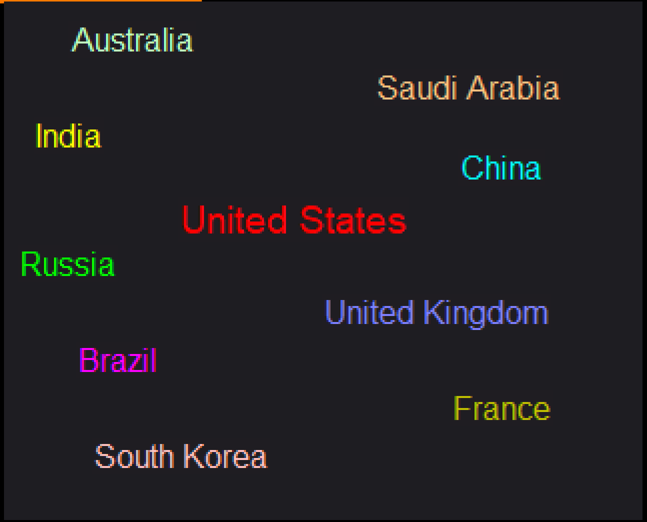
Political Institutions

Note on Surveillance Countermeasures

To counter DieNET-v2, monitor their Telegram channels to gather actionable intelligence. Equip your employees with counter-narratives to weaken the group’s ideological influence. Anticipate escalation during geopolitical flashpoints, and reinforce defenses for critical infrastructure sectors like energy and transportation.

Credits Orange Cyberdefense

Targeted Countries



Australia

Saudi Arabia

India

China

United States

Russia

United Kingdom

Brazil

France

South Korea

Credits Orange Cyberdefense

Most Likely Hypothesis

Strategic Targeting:

DieNet will likely continue to focus on critical infrastructure sectors such as energy, health, and financial services. Their primary goal remains to expose vulnerabilities within these essential services and cause significant disruption. This strategic targeting aims to mobilize public opinion against Western governments and erode trust in institutions.

Hybrid Attack Methods:

The group is expected to evolve beyond their current reliance on simple DDoS attacks. A likely future tactic involves the transition to combined attack methods, such as DDoS coupled with ransomware and stealers. They may also intensify their efforts in data breaches and website defacements to amplify their impact and public visibility.

Systemic Impacts:

Future attacks could cause more than temporary service interruptions, potentially leading to prolonged outages or even physical damage. By targeting critical infrastructure, DieNet seeks to create widespread societal impacts and destabilize public confidence in essential systems. This escalation would represent a shift towards causing significant national harm beyond mere disruption

Credits Orange Cyberdefense

The most dangerous hypothesis

Feared Scenario:
DieNet-v2 could coordinate a large-scale, multi-vector cyberattack against critical infrastructure in the United States or allied countries. This attack could be synchronized with major geopolitical events to maximize chaos and media coverage. The group may leverage alliances with other hacktivist collectives to amplify the impact and reach of the operation.

Primary Targets:
Their primary targets would likely include energy grids, transportation systems, financial networks, and healthcare providers. By disrupting these essential services, DieNet aims to create widespread societal and economic instability.

Methodologies:
DieNet could combine massive DDoS attacks with data breaches and coordinated misinformation campaigns. The group is expected to use DDoS-as-a-service platforms, rented botnets, and possibly exploit vulnerabilities in third-party providers. These hybrid tactics would make detection, attribution, and mitigation much more difficult for defenders.

Potential Consequences:
Such an attack could result in prolonged outages, financial losses, and disruption of emergency services, potentially endangering lives. If successful, this scenario could embolden other hacktivist groups and escalate the overall threat landscape.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense