VNIS
Vnetwork Internet Security

Powered by
VNETWORK GROUP

REPORT

DDoS attack first half of 2025 in Vietnam

Table of contents

I Introduction 02

II What is a DDoS attack? 03

III Report 04

- Key figures 04
- Number of attacks in 2025 vs. same period 05
- DDoS attacks in Vietnam vs. Global figures 06
- DDoS attack types and intensity 07
- The rise of Ransom DDoS 09
- AI-Driven DDoS trends 10
- DDoS attack origins by country 11

IV Case study 12

V Trend & recommendations 16

VI Methodology & data sources 18

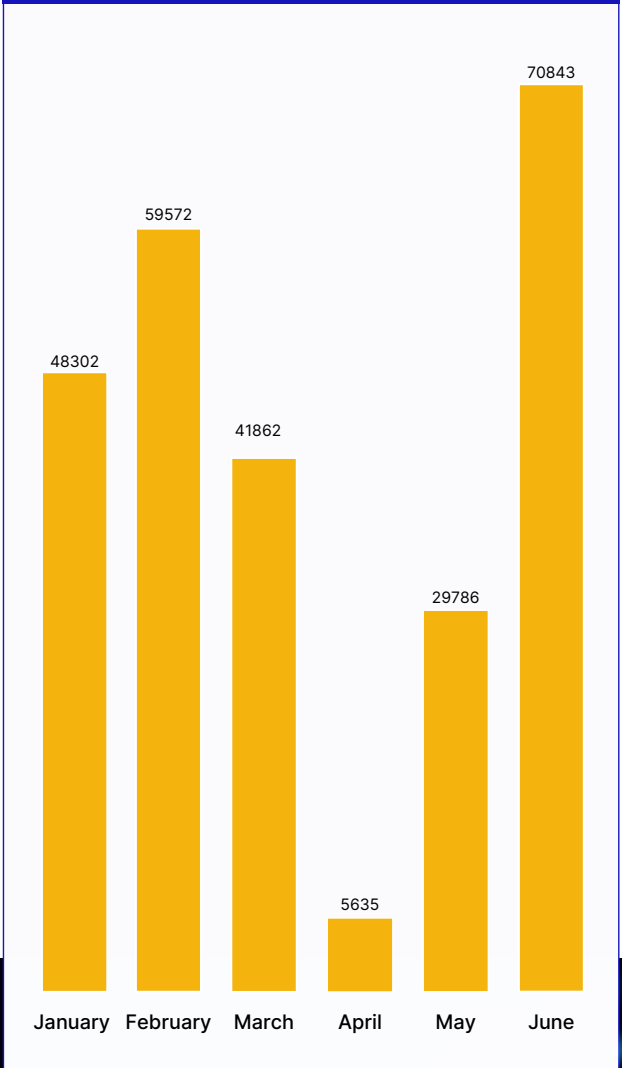
VII Contact 19

Introduction

In the context of rapid and extensive digital transformation, businesses are seizing opportunities to expand their markets and optimize operations, while also facing **increasingly complex** and l**arge-scale cyber threats** that are **harder to detect and control**.

Based on data analysis from the VNETWORK system, in the first half of 2025 alone, VNETWORK recorded a total of 1,178,591 cyberattacks. The most common and dangerous attack types included Zero-day, Credential Stuffing, SQL Injection, XSS, Brute-force, Account Takeover, and BEC (Business Email Compromise) through Email Phishing.

VNIS handled more than 256,000 DDoS attacks, equivalent to 0.7 percent of the 36 million attacks worldwide.



Notably, Distributed Denial of Service attacks remain persistent and damaging, with **256,000 incidents** recorded. Modern campaigns often combine multiple layers, using volumetric and protocol floods at **Layer 3/4** that strike the CDN and network edge, together with application layer attacks at **Layer 7** that target websites, applications, and APIs. These combinations disrupt services and payment flows, degrade performance, and can lead to operational and financial losses when traditional defenses are insufficient.

This report provides a detailed summary of VNIS data collected during the first half of 2025, compared with the same period in 2024 and aligned with global trends. The contents include analysis of attack scale, methods, affected industries, attack sources, and real case studies, along with practical recommendations to help organizations maintain safe and stable operations in a volatile digital environment.

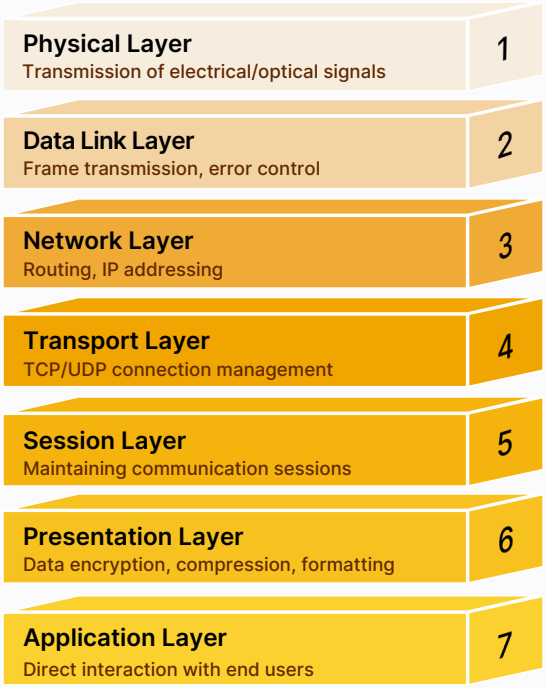
Disclaimer

This report aims solely to raise awareness and help businesses build stronger cybersecurity defenses. Any other claims or interpretations are not aligned with the intent of this publication.

What is a DDoS attack?

A DDoS (Distributed Denial of Service) attack is a type of cyberattack aimed at **disrupting** or **shutting down services** such as websites or applications. This is carried out by **overwhelming the target server** with **massive traffic** from multiple sources, making it **unable to process legitimate user requests.**

Why layers 3, 4, and 7?



These are the core weak spots. At **Layers 3 - 4**, attackers overwhelm bandwidth and connections with fake IP, TCP, or UDP packets, pushing network systems beyond their limits. **Layer 7**, on the other hand, deals directly with applications like websites, APIs, and DNS. When bombarded with requests, it rapidly drains CPU, memory, and database capacity, bringing services to a halt. **Other layers** are harder to reach remotely or have minimal direct impact, so they are rarely targeted.

Why are DDoS attacks dangerous?

Disruption and loss of revenue and reputation due to high recovery costs, missed customer opportunities, and reduced trust.

Low cost and ease of execution, since attackers can rent or purchase cheap DDoS tools on illegal marketplaces.

Difficult to detect and prevent, as they often use botnets, spoofed IPs, multi-vector, and multi-layer techniques.

Easily leveraged as a stepping stone for data exploitation or malware installation.

III Report

3.1 Key figures

256.000

Total number of attacks in the first half of 2025

Compared to the same period in 2024, the number of DDoS attacks in the first half of 2025 increased by 87.000, highlighting the escalating frequency and scale of attacks.

1.2 Tbps

Largest recorded DDoS attack traffic volume

A peak of 1.2 Tbps demonstrates the massive power of modern botnets. At this scale, most enterprise infrastructures could be taken down within minutes if lacking specialized defenses.

32%

Protocol attacks firmly lead the chart

59.572 attacks in six months. These attacks exploit vulnerabilities in network protocols or system resources, exhausting server CPU, memory, and connections without necessarily requiring high bandwidth.

34%

The finance sector remains the top target

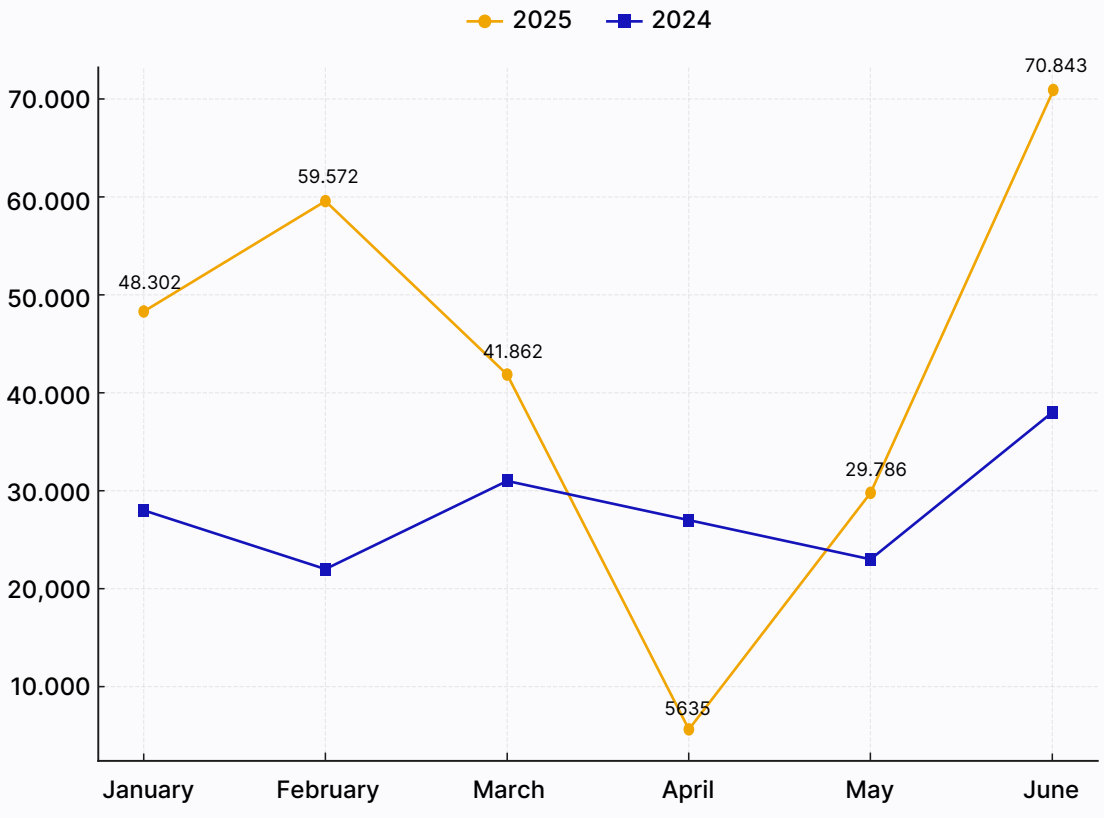
The financial sector remains the most targeted industry in 2024 and early 2025. Its reliance on online transactions and demand for continuous operations make it a “hot spot” for DDoS campaigns.

3.2 Number of attacks in 2025 vs. the same period

In **the first half of 2025**, the VNIS system recorded and mitigated a total of **256.000** DDoS attacks in **Vietnam**, averaging about **42.700** attacks per month. This marks a sharp increase compared to the same period in **2024**, when attacks totaled around **169.000**, averaging **28.200** per month. Overall, **attack intensity rose by approximately 51%**, and the monthly distribution showed much greater volatility compared to the previous year.

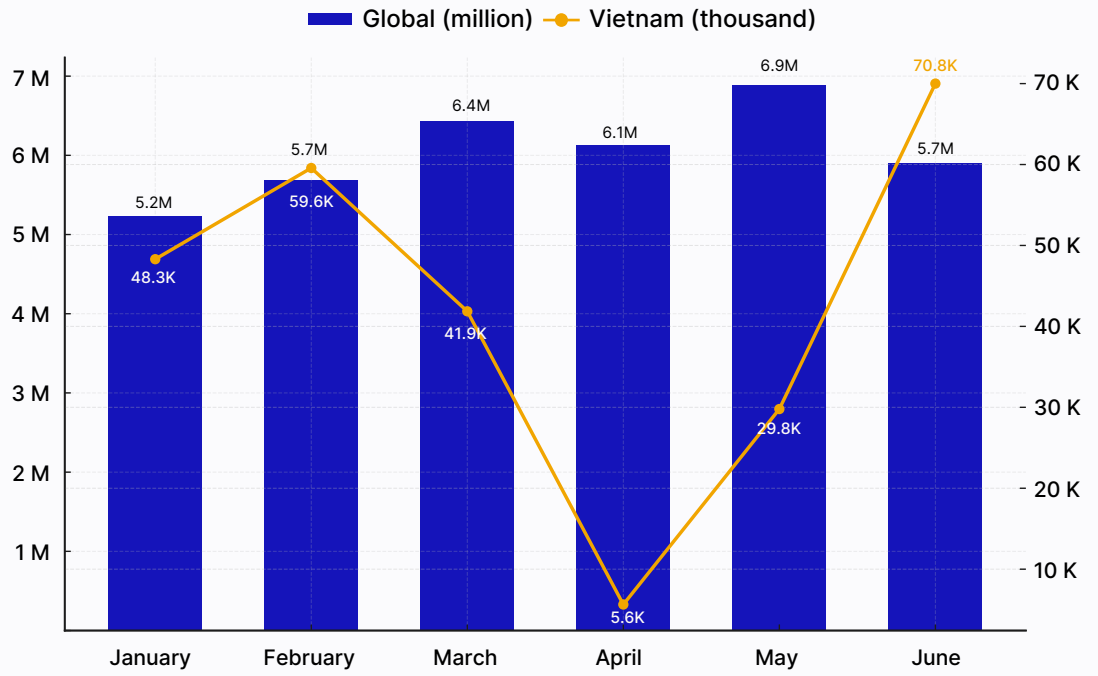
The trend in the first half of 2025 reflects a typical pattern of cyberattack campaigns: an initial surge (January–February with 48.302 and 59.572 incidents), followed by a sudden drop (April with only 5.635 incidents), and then a sharp resurgence (June with 70.843 incidents) - the peak of the period, nearly double the monthly average of the same timeframe in 2024.

Number of DDoS attacks recorded in the first half of 2025 vs. the same period in 2024



3.3 DDoS attacks in Vietnam vs. Global figures

VNIS recorded a total of 36.11 million DDoS attacks worldwide



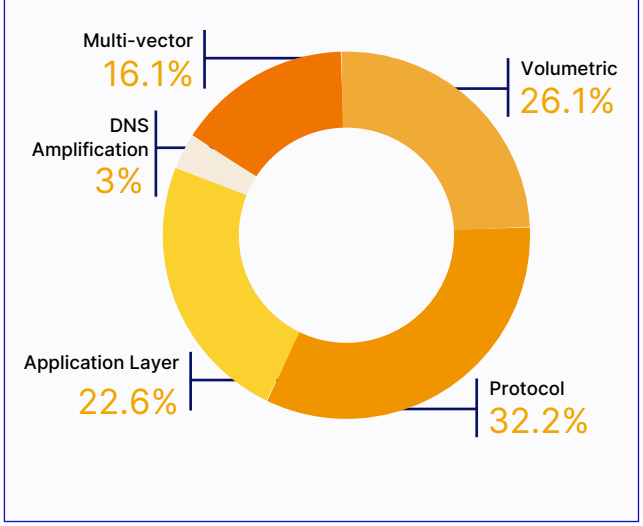
Viewed against the global landscape, Vietnam presents a clear contrast. **Worldwide DDoS activity stays consistently high** and relatively stable, fluctuating between 5.2 and 6.9 million attacks per month, with a total of **36.11 million incidents**. In Vietnam, however, attack patterns are far more erratic and cyclical. This indicates that **attackers in Vietnam are not only launching large-scale volume-based assaults** but are also **experimenting with diverse tactics** and constantly shifting attack vectors, which creates unpredictable pressure on defense systems.

These figures confirm that DDoS attacks in Vietnam are increasingly **cyclical and volatile**, yet growing in intensity, posing serious challenges to the IT infrastructure of enterprises.

It is crucial for organizations to adopt a multi-layered, real-time defense strategy that can **handle heavy traffic surges** during peak attacks while maintaining **early detection** and **adaptive protection**. At the same time, having a **detailed response playbook** allows the operations team to **react quickly whenever attackers shift their tactics**, helping ensure the system stays stable and accessible even during intense assaults.

3.4 DDoS attack types and intensity

Types of DDoS attacks in Vietnam in the First Half of 2025

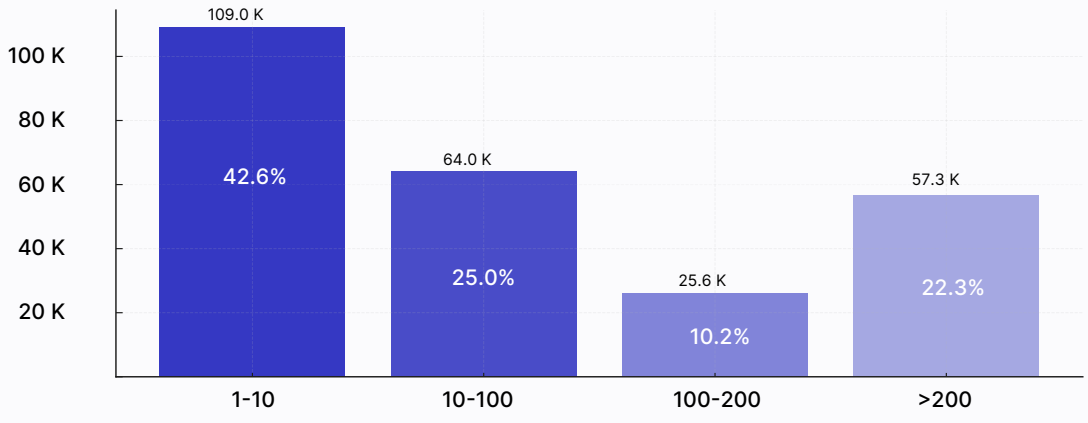


Volumetric and **Protocol attacks** still lead, but **the surge in Layer 7** and multi-vector assaults marks a new level of sophistication in DDoS tactics.

Enterprises must upgrade fast, securing not only against large-scale traffic floods but also protecting APIs and web apps from new threats. True resilience comes from continuous, all-layer defense. Basic protection alone cannot keep systems stable in today's unpredictable digital world.

More than **57.000** attacks reached intensities above **200 Gbps**, reflecting how quickly attack tactics are evolving. To stay resilient, organizations need a multi-layered defense that combines **AI WAF, API protection** and **Multi-CDN**, along with real-time monitoring and fast response. Early detection and proactive protection are essential to reduce damage and protect both financial stability and brand reputation.

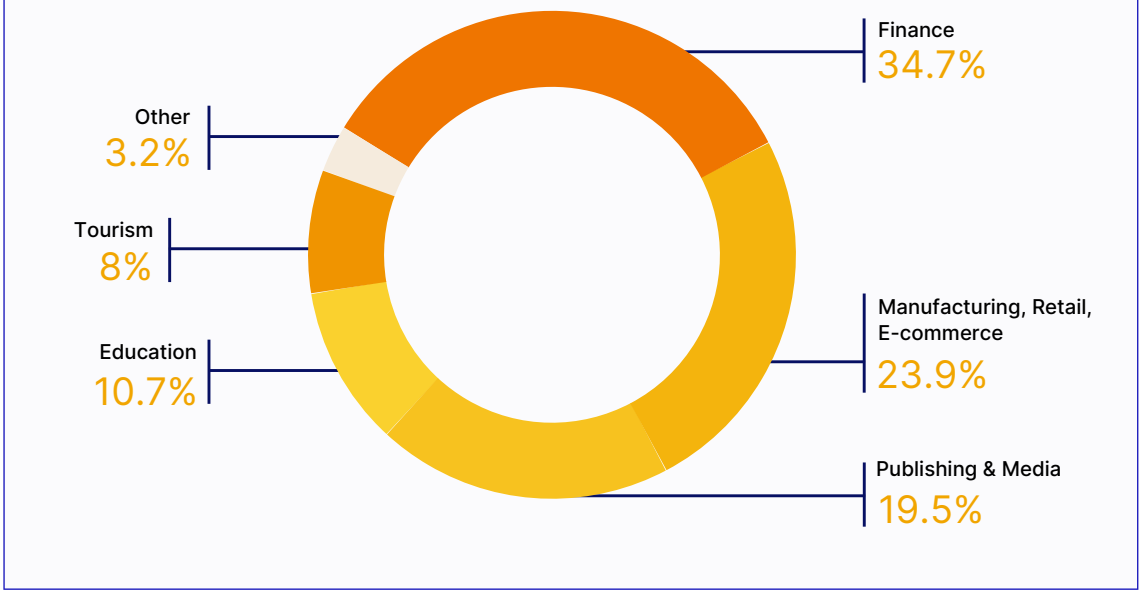
DDoS attack intensity (Gbps) in Vietnam in the first half of the year



3.4 DDoS attack types and intensity

VNIS - Secure and Speed up Web/App/API solution is currently protecting many businesses across diverse sectors, including **57% large** enterprises and **43% small and medium-sized** enterprises. The industry distribution includes: Finance (39%), Publishing & Media (26%), Manufacturing, Retail, E-commerce (23%), Tourism (6%), Education (4%), and other sectors (2%).

Most attacked industries



[≈35%] Finance

88.713 attacks

Over 88.700 attacks hit the financial sector, confirming it remains a prime target for cybercriminals due to its large customer base and valuable assets. However, the lower attack ratio suggests strong investments in security have made breaches much harder.

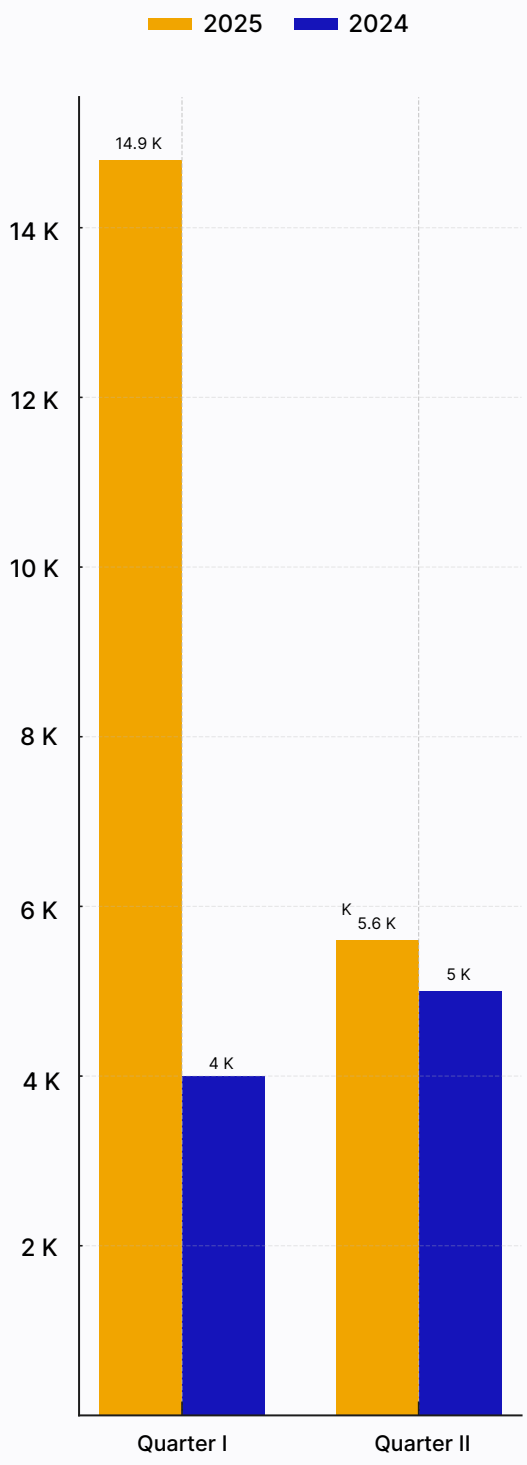
[≈24%] Manufacturing, retail, e-commerce

49.957 attacks

About 50.000 attacks hit the sector, fewer than expected by its size. Yet payment systems and online carts remain prime targets during peak hours. The lower ratio likely reflects dispersed attack strategies rather than true safety.

3.5 The rise of Ransom DDoS

Comparison of ransom DDoS incidents by quarter: 2025 far exceeds 2024

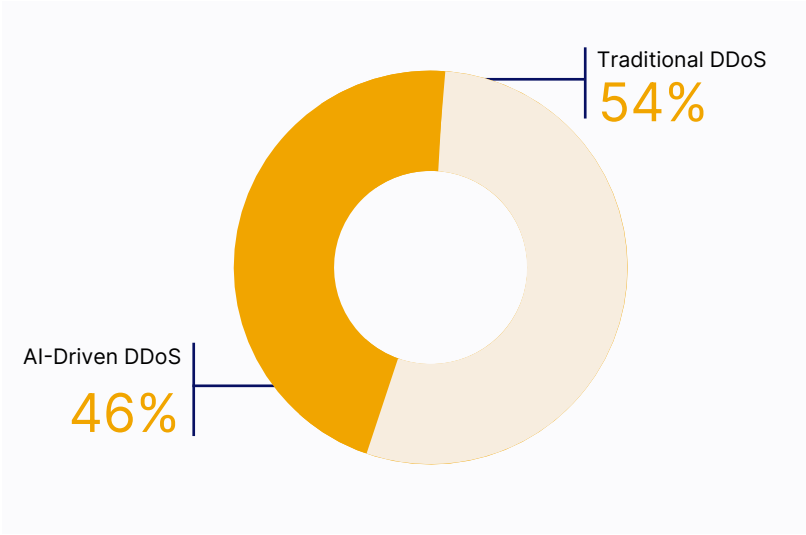


In Q1 2025, the number of ransom DDoS attacks surged to **14.875** incidents, nearly **3.7** times higher than the **4.000** incidents recorded in the same period of 2024. This indicates that hackers are focusing on exploiting the early part of the year-when businesses initiate many digital activities and heavily rely on online systems—to exert pressure and force ransom payments.

In **Q2** 2025, **5.605** incidents were recorded, a slight increase of 12% compared to 5.000 incidents in Q2 2024. This growth is not too drastic, suggesting that after the "shock" in Q1, organizations may have strengthened their defenses, while attackers may have temporarily adjusted their tactics to avoid detection or prepare for subsequent attack waves.

Ransom DDoS (RDoS) is a specific type of DDoS attack used for extortion, where hackers cripple or threaten online services to force victims to pay a ransom.

3.6 AI-driven DDoS trends



VNIS recorded **117.760 DDoS** attacks powered by AI, accounting for 46 percent of the total **256.000 attacks** in Vietnam. Average intensity **topped 322 Gbps**, an extremely high level of traffic.

VNIS - Secure and Speed up Web/App/API solution has identified the following key characteristics of AI-driven DDoS attackes:

- **Automatic vector shifting:** Rapidly switching from volumetric flood to HTTP(S) flood, API flooding, or DNS amplification, making defenses harder to adapt.
- **Real-time botnet optimization:** Distributing traffic intelligently to evade traditional filters and maintain continuous pressure.
- **Legitimate user behavior simulation:** Generating fake traffic that makes it difficult to distinguish between genuine and malicious requests.
- **Increased persistence:** Sustaining attacks for days to months thanks to the ability to self-adjust attack tactics.
- **Lowering the barrier:** Automating botnet setup and vector selection, enabling even small groups or individuals to launch sophisticated attacks at low cost.
- **Targeting application and API layers:** Flooding authentication, payment, or digital services, causing greater damage than bandwidth exhaustion.
- **Extortion integration (RDoS):** Timing attacks during peak hours to maximize pressure and force ransom payments.
- **Global expansion:** Using hijacked IoT botnets and proxies to distribute traffic across multiple countries, rendering IP or geolocation blocking less effective.

The shift is clear: from simple **volumetric floods** to **intelligent, multi-layered, persistent DDoS campaigns.** AI has become the **hackers' main weapon**, forcing businesses to **fight back with AI-powered defenses** to keep up with rising threats.

3.7 DDoS attack origins by country

Top 10 countries with the highest DDoS traffic targeting Vietnam recorded by VNIS

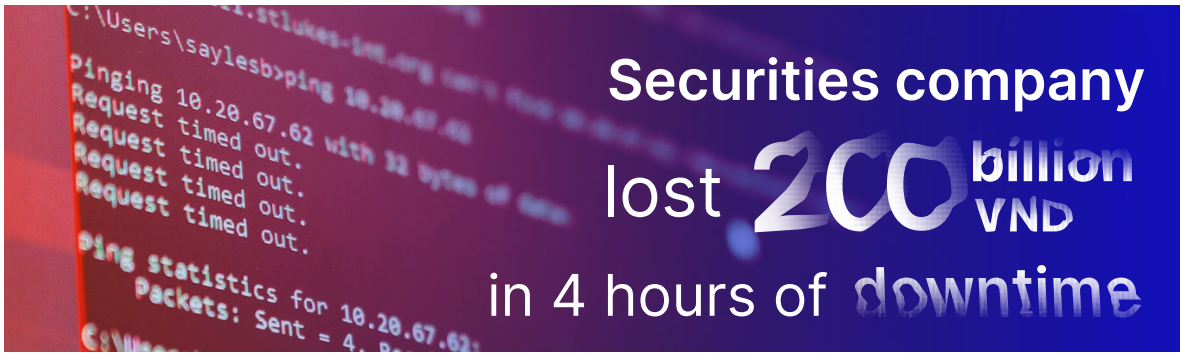
This list reflects botnet nodes, proxies, or VPN endpoints where DDoS attacks originate, **rather than the actual locations of threat actors.**

Nations with relatively weaker tech infrastructure, like **Vietnam, Ukraine, Mexico**, and **Indonesia**, are now **major sources of DDoS traffic**. Cyberattacks increasingly originate from places with **poor or insufficient security**, where vulnerable IoT devices and servers are hijacked to build global botnets.

Although these countries are not primary destinations for threat actors, they **serve as launch points for DDoS attacks** due to poor infrastructure control and security. Such attacks are often difficult to detect and mitigate because they leverage spoofed IP addresses or proxy nodes from countries that are not the true origin of the attack. This further increases the challenges in detecting and defending against DDoS threats.

These nations are not primary targets but **act as launchpads for DDoS attacks** due to poor infrastructure security. These attacks are difficult to trace or stop, as they often rely on spoofed IPs or proxy servers located in countries that are not the real origin of the attack. This makes the detection and prevention of DDoS threats even more challenging.

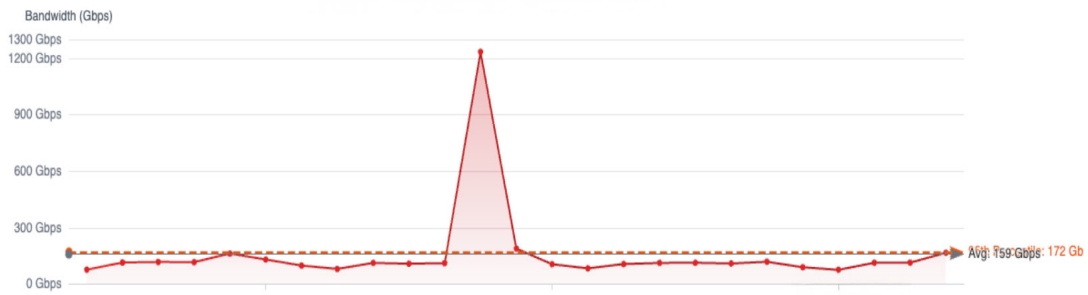
IV Case study



Case overview

The company only relied on physical firewalls and basic anti-attack solutions. However, with the massive attack scale of over 1.2 Tbps, self-defense was nearly impossible. Even when seeking help from other providers, the company did not receive effective support due to the complexity of its IT systems and the fact that no vendor had sufficient capacity to handle such traffic.

VNIS recorded peak traffic of 1.2 Tbps directed at a securities platform



Attack scale

Duration:

The attack persisted continuously during the first 4 days (before VNIS was integrated) and continued for more than a month afterward. It was particularly severe during peak trading hours: 9:00 – 11:00, 13:00 – 14:30, and 14:30 – 15:00 (ATC).

Traffic:

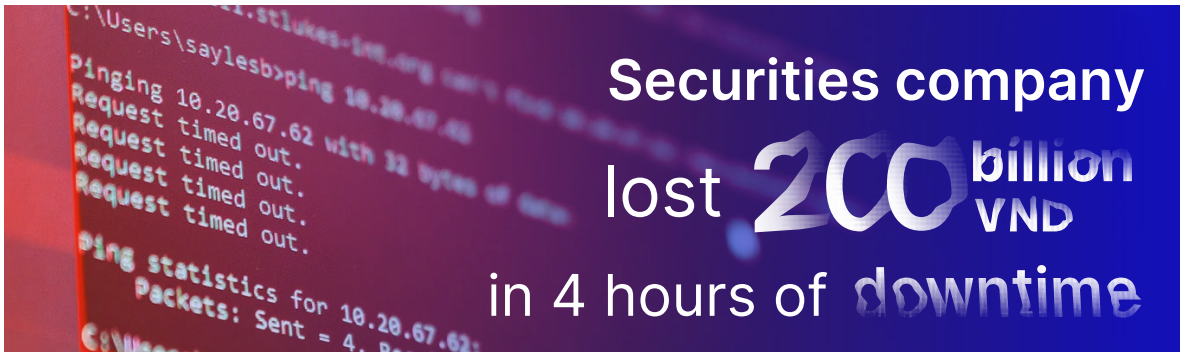
Peak attack reached 1.2 Tbps and over 720.000 RPS – an extremely large scale in Vietnam.

Attack methods:

Multiple techniques combined:

- Multi-layer DDoS at Layer 3/4/7
- API Flooding that completely clogged the trading gateway
- SQL Injection and vulnerability exploitation, enhanced by AI

IV Case study



Initial impact

- Revenue from transaction fees dropped sharply, with just **4 hours of downtime** causing estimated losses of more than **200 billion VND**, while also damaging the **company's reputation.**
- **Bandwidth costs paid** to the ISP reached **hundreds of millions of VND** due to attack traffic exceeding thresholds without timely filtering measures.
- More than **86% of payment orders were disrupted or delayed**, reducing market liquidity and investor confidence.
- Investors were unable to place, cancel, or modify orders during **over 5 peak trading hours per day**, leading to severe transaction congestion.
- The IT team had to **stay on duty 24/7** to handle the crisis but was still unable to control the attack traffic.

VNIS solution

Vietnam Internet Security

Rapid integration

- Upon receiving the report, VNETWORK experts immediately deployed attack mitigation overnight.
- The system was restored to stable operation within 5 minutes of integration, despite the securities enterprise having many unique technical requirements.

Traffic assessment & analysis

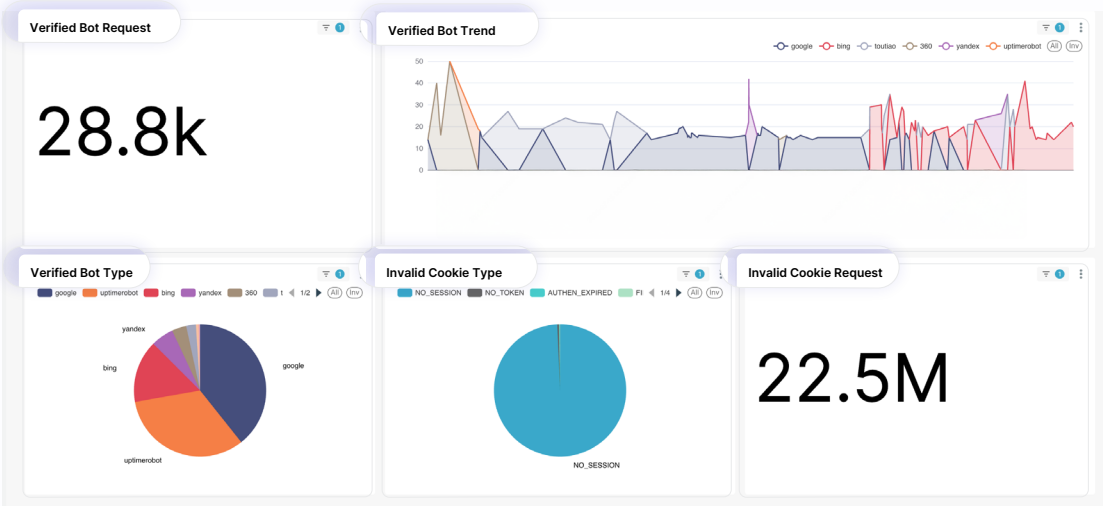
- The 24/7 SOC team monitored in real time, quickly identifying the origin and attack vectors (Layer 3/4/7, API Flooding, SQL Injection).
- AI WAF applied Machine Learning trained on VNIS's massive attack dataset, combined with live traffic data, to automatically recognize abnormal patterns and clearly distinguish between legitimate requests and malicious traffic.

IV Case study

VNIS solution

Multi-layer mitigation & filtering

- **Multi-CDN + AI Smart Load Balancing:** Expands infrastructure globally across 146 countries with over 2.600 Tbps capacity, ensuring stability, reducing pressure on origin servers, and dispersing Layer 3/4 DDoS traffic.
- **AI WAF:** Automatically blocks Layer 7 DDoS, SQL Injection, XSS, Zero-day, and all vulnerabilities listed in the OWASP Top 10.
- **Advanced API Protection:** Safeguards order placement, cancellation, and payment endpoints against API Flooding and data leakage.
- **Intelligent Rate Limiting & CAPTCHA:** Eliminates botnets and fake requests while preserving legitimate transactions.



VNIS recorded and analyzed attacks in real time

Continuous monitoring & optimization

- The SOC and VNIS experts worked side by **side 24/7**, with the **AI system updating rules** in real time to counter evolving attack tactics.
- **Regular reporting**, performance tuning, and security enhancements ensured smooth transactions even **during peak trading hours**.

IV Case study

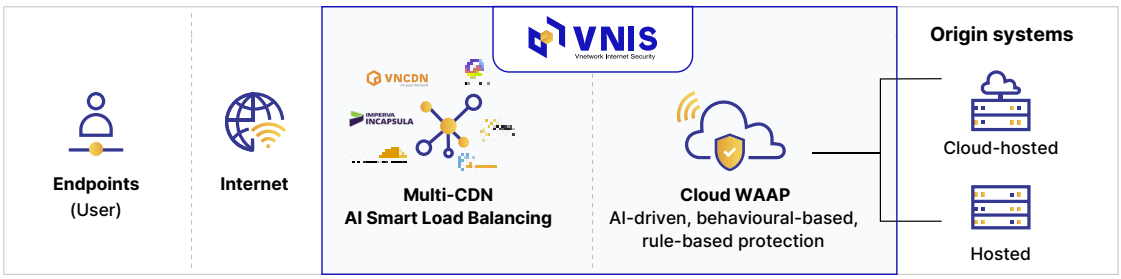
Results

- Trading system was restored within just **5 minutes** after VNIS integration.
- Eliminated **99.997%** of malicious traffic while preserving legitimate investor orders.
- Market liquidity was **recovered**, customer confidence restored, and enterprise reputation protected.
- The company overcame the crisis, moving to **stable** operations and readiness for **sustainable growth**.

About VNIS

VNIS WAAP (Web Application & API Protection) is an **AI-driven** security platform where artificial intelligence is not just an add-on, but the very **foundation of the solution** - empowering it to **predict, detect,** and **defend** against today's most advanced cyber threats.

An integrated Multi-CDN and AI-powered Cloud WAAP model delivers comprehensive DDoS protection across Layers 3/4/7.



VNIS empowers businesses to:

Protect Web/App/API against real-time attacks, including Layer 3/4/7 DDoS, bot attacks, vulnerability exploitation, zero-day threats, crawlers, and malware.

Detect and block threats at the earliest stage without impacting user experience or system performance.

Maintain consistently superior performance even under high traffic loads or targeted attack scenarios.

V Trends & recommendations

Trend forecast

1) DDoS attacks projected to rise 32% in H2 2025

The surge is driven by the proliferation of poorly secured IoT devices fueling massive botnets; attackers leveraging AI to automate and obfuscate traffic; cheap DDoS-for-hire services lowering entry barriers; digital transformation expanding attack surfaces; and multi-vector strategies targeting application and API layers that overwhelm traditional defenses.

2) Seasonal and event-driven spikes: DDoS peaks may recur in Q4

Promotions, IPOs, and public events attract high user traffic, creating opportunities for attackers. They strike at peak times to maximize disruption and financial pressure, including ransom-based attacks.

3) "Hyper-scale" attacks (>1 Tbps) becoming the norm

Globally distributed botnets (IoT and proxy servers) enable attackers to generate massive traffic volumes. Enterprises lacking Anycast CDN and multi-region scrubbing capacity will struggle to absorb such high-intensity waves.

4) API and payment system attacks will keep growing

As APIs become the backbone of digital transactions, they are increasingly prime targets for ransom-driven DDoS. Attackers flood the application layer to cripple authentication, payment, or customer service systems.

5) Attack sources more distributed and unpredictable

DDoS traffic is now spread across more countries and ASNs (Autonomous System Numbers), reflecting the global expansion of botnets. Hackers also abuse proxy and cloud infrastructure to stay anonymous, rendering IP- or country-based blocking far less effective.

6) Government agencies and organizations become prime targets as leaked data spreads widely

In early September 2025, attacks on major enterprises and state agencies were recorded, with sensitive data leaked and openly sold on underground forums. From now until year-end, the situation is expected to escalate, as attacks combine DDoS with data theft and exploitation for extortion or financial gain.

V Trends & recommendations

Key recommendations

Technology & technical solutions

- Invest in multi-layer DDoS mitigation (Layer 3/4 and Layer 7) to ensure comprehensive protection against volumetric floods and HTTP(S) floods.
- Safeguard DNS and APIs with multi-DNS, DNSSEC, and API Gateway equipped with mTLS/OAuth2, quota enforcement, and schema validation.
- Separate dynamic vs. static load and apply degraded mode to reduce backend pressure and maintain basic user experience during attacks.
- Adopt a multi-cloud/multi-region strategy for critical services to avoid “single points of failure” that could paralyze the entire system.

Early detection & monitoring

- mplement real-time traffic monitoring (SOC/IDS) to detect anomalies at the earliest stage.
- Regularly conduct DDoS simulations and stress tests to evaluate response readiness and optimize alerting mechanisms.

Response & operations

- Build a DDoS incident response plan with fast recovery objectives (RTO ≤ 10 minutes), and run regular drills to keep SOC/IT teams prepared.
- Prepare for Ransom DDoS (RDoS) scenarios: establish clear handling procedures upon receiving threats, avoid paying ransom, and report incidents to authorities.
- Partner with reliable and trusted cybersecurity providers for 24/7 support during large-scale attacks.

Governance & financial planning

- Forecast DDoS-related costs (FinOps), including egress, scrubbing, and WAF requests, while configuring automatic load shedding thresholds to control expenses.
- Elevate DDoS risk to a strategic risk management level so leadership understands it as a business risk, not just a technical incident.

VI Methods & Data sources

Data source:
Collected from VNIS – VNETWORK's Web/App/API secure & speed up solution, through the DDoS attack mitigation system.

Data collection method:
- Continuous monitoring and recording of security events.
- Use of both quantitative and qualitative analysis tools.

Scope:
Aggregated data from VNIS security systems of customers in Vietnam and globally.

Data recording period:
From January 1, 2025 to June 30, 2025.

Web/App/API security solutions

from VNETWORK GROUP

VNIS stands as a trusted shield with powerful infrastructure, advanced defense technology, and an expert team on standby. It lets businesses focus on growth while VNIS protects their digital assets and brand.

Contact us

More infomation

Contact

Vietnam
23-06, 23rd floor, UOA Tower, 6 Tan Trao Street, Tan My Ward, Ho Chi Minh City.

Singapore
111 North Bridge Road
#17-06 Peninsula Plaza

+84 (28) 7306 8789

contact@vnetwork.vn