VNIS
Vnetwork Internet Security

Được thực hiện bởi
**VNETWORK GROUP**

BÁO CÁO

# **Tấn công DDoS** 6 tháng đầu năm 2025 tại Việt Nam

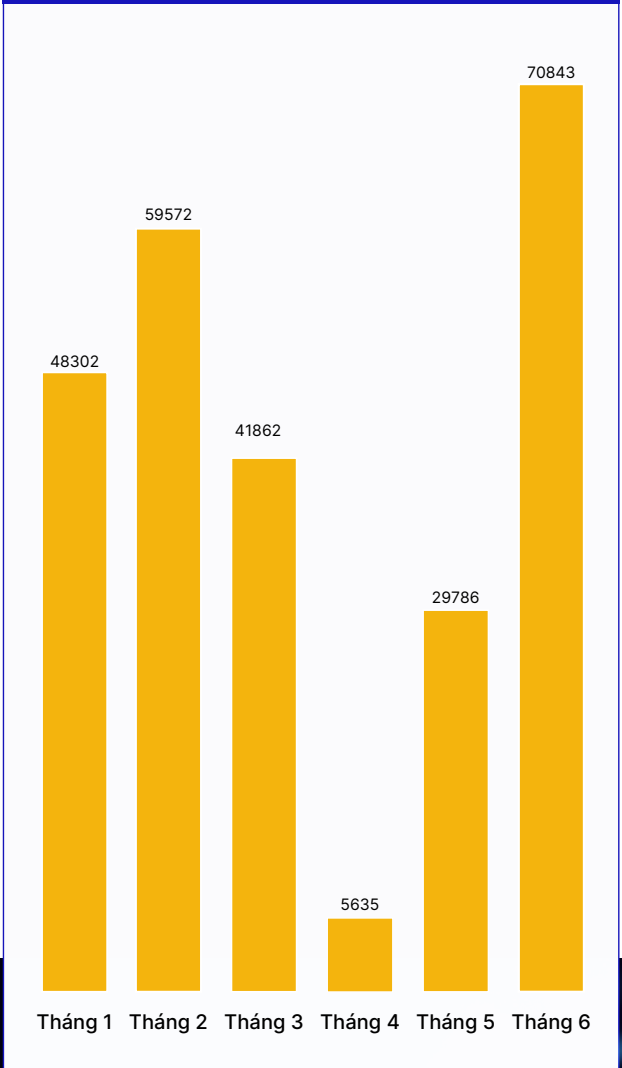
# Mục lục

# Giới thiệu báo cáo

Trong bối cảnh chuyển đổi số ngày càng sâu rộng, các doanh nghiệp đang đứng trước cơ hội mở rộng thị trường và tối ưu vận hành, **đồng thời đối diện với nguy cơ an ninh mạng ngày càng tinh vi, quy mô lớn** và **dễ dàng được thuê mướn**.

Thực tế này được phần nào phản ánh qua dữ liệu của VNETWORK. Chỉ riêng 6 tháng đầu năm 2025, hệ thống VNETWORK đã ghi nhận tổng cộng 1,178,591 cuộc tấn công mạng. Những hình thức tấn công phổ biến và nguy hiểm bao gồm Zero-day, Credential Stuffing, SQL Injection, XSS, Brute-force, Account Takeover, BEC (Business Email Compromise) và Email Phishing...

**VNIS đã xử lý hơn 256.000 cuộc tấn công DDoS, tương đương 0,7% trong tổng số 36 triệu cuộc tấn công toàn cầu.**




Đáng chú ý nhất, tấn công từ chối dịch vụ phân tán (DDoS) vẫn là mối đe dọa lớn, chiếm tới **256,000 cuộc**. Các chiến dịch DDoS hiện nay thường kết hợp tấn công đa tầng (**tầng 3/4 ở CDN** và **tầng 7 ở Web/App/API**), nhắm trực tiếp vào hạ tầng mạng, ứng dụng, API và hệ thống thanh toán. Mức độ phức tạp này giúp chúng dễ dàng vượt qua các biện pháp phòng thủ truyền thống, gây gián đoạn dịch vụ nghiêm trọng, ảnh hưởng trực tiếp đến hiệu năng, uy tín hệ thống và dẫn đến tổn thất tài chính đáng kể cho doanh nghiệp.

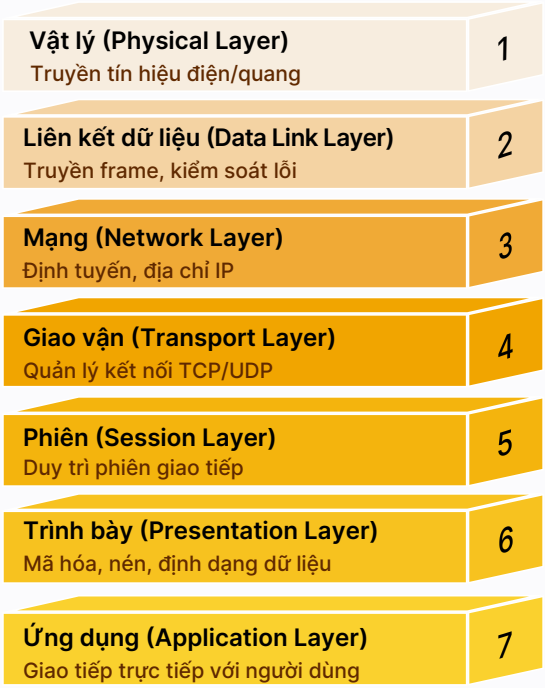
Báo cáo này tổng hợp chi tiết dữ liệu từ VNIS trong nửa đầu năm 2025, so sánh với cùng kỳ năm 2024 và xu hướng toàn cầu. Nội dung bao gồm quy mô, phương thức, các lĩnh vực chịu ảnh hưởng, nguồn tấn công, cùng những case study thực tế và khuyến nghị phòng thủ thiết thực, giúp doanh nghiệp duy trì hoạt động an toàn và ổn định trong môi trường số biến động.



# II Tấn công DDoS là gì?

Tấn công DDoS (Distributed Denial of Service) là hình thức tấn công mạng nhằm **làm gián đoạn** hoặc **ngừng cung cấp dịch vụ** như website, ứng dụng. Điều này được thực hiện bằng cách **làm quá tải máy chủ** mục tiêu **với lưu lượng truy cập cực lớn** từ nhiều nguồn khác nhau, khiến máy chủ **không thể xử lý các yêu cầu từ người dùng thật.**

## Tại sao tấn công DDoS lại tập trung ở tầng 3, 4 và 7?




Đây là những điểm dễ gây gián đoạn mạnh nhất. Ở **tầng 3–4**, kẻ tấn công có thể làm nghẽn băng thông và kết nối bằng các gói tin IP, TCP/UDP giả mạo, khiến hạ tầng mạng quá tải. Trong khi đó, **tầng 7** trực tiếp xử lý ứng dụng (web, API, DNS...), nên khi bị flood request sẽ nhanh chóng tiêu tốn CPU, RAM và cơ sở dữ liệu, dẫn đến dịch vụ ngừng hoạt động. Các **tầng khác** khó tiếp cận từ xa hoặc ít ảnh hưởng trực tiếp, do đó ít được nhắm đến.

## Vì sao tấn công DDoS lại nguy hiểm?

**Gián đoạn hoạt động làm mất doanh thu, uy tín** do chi phí xử lý lớn, mất cơ hội tiếp cận khách hàng, suy giảm niềm tin.

**Chi phí tấn công thấp và dễ thực thiện** do thuê hoặc mua công cụ DDoS giá rẻ trên trang giao dịch bất hợp pháp.

**Khó phát hiện & ngăn chặn** dùng botnet, IP giả mạo, đa phương thức, đa lớp.

**Dễ trở thành đòn bẩy** thực hiện tấn công khai thác dữ liệu hoặc cài mã độc.

# III Báo cáo

## 3.1 Số liệu nổi bật

256,000

### Tổng số cuộc tấn công trong nửa đầu năm 2025

So với cùng kỳ năm 2024, số cuộc tấn công DDoS trong nửa đầu năm 2025 tăng thêm 87,000 vụ, cho thấy tần suất và quy mô tấn công ngày càng leo thang.

1.2 Tbps

### Lưu lượng cuộc tấn công có quy mô lớn nhất

Mốc 1.2 Tbps phản ánh sức mạnh huy động từ các mạng botnet khổng lồ. Với lưu lượng này, hạ tầng của phần lớn doanh nghiệp có thể bị đánh sập chỉ trong vài phút nếu thiếu biện pháp phòng thủ chuyên dụng.

32%

### Tấn công Protocol chiếm tỷ trọng cao nhất

59,572 cuộc trong 6 tháng. Tấn công này khai thác lỗ hổng trong các giao thức mạng hoặc tài nguyên hệ thống, làm cạn kiệt CPU, bộ nhớ, kết nối trên server mà không nhất thiết phải dùng lượng băng thông lớn.

34%

### Ngành tài chính là mục tiêu hàng đầu

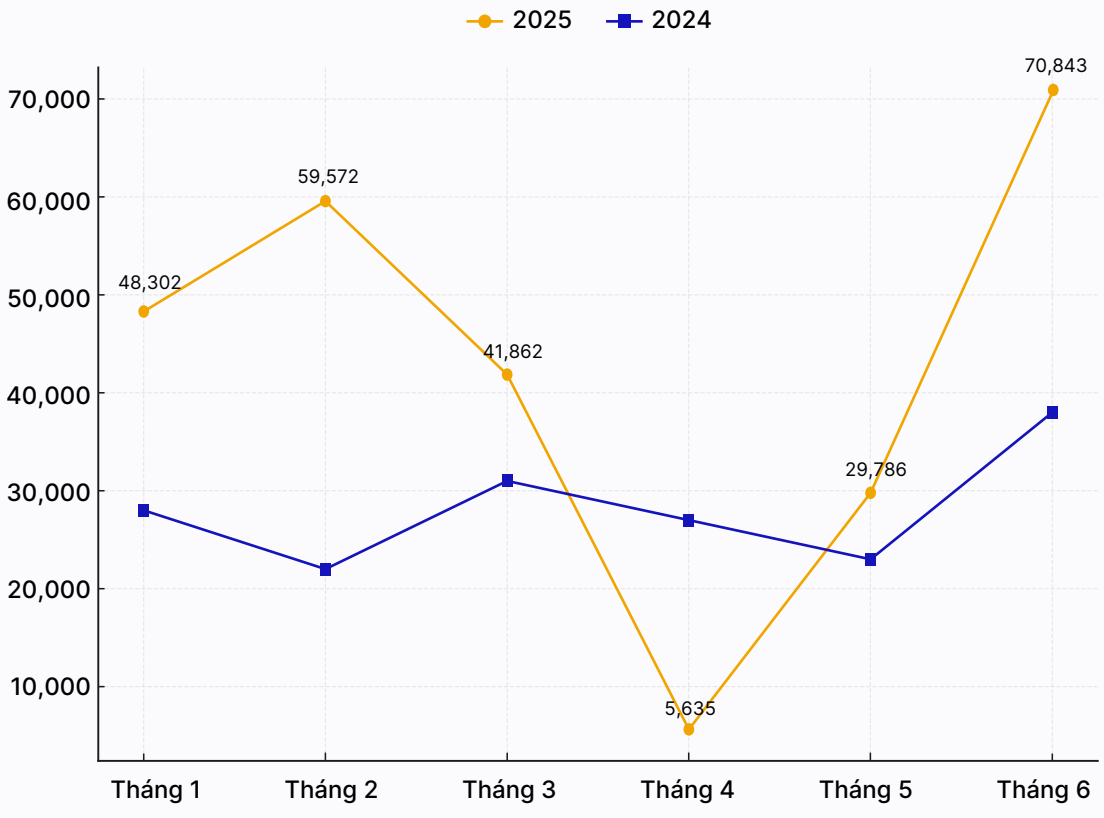
Ngành tài chính tiếp tục là lĩnh vực bị nhắm tới nhiều nhất trong năm 2024 và đầu năm 2025. Phụ thuộc vào giao dịch trực tuyến và yêu cầu hoạt động liên tục khiến ngành này trở thành "điểm nóng" của các chiến dịch DDoS.

# 3.2 Số lượng tấn công năm 2025 và cùng kỳ

Trong **6 tháng đầu năm 2025**, hệ thống VNIS đã ghi nhận và chặn lọc tổng cộng **256,000** cuộc tấn công DDoS tại **Việt Nam**, trung bình khoảng **42,700** cuộc mỗi tháng. Con số này tăng mạnh so với cùng kỳ năm **2024** khi số lượng tấn công chỉ đạt khoảng **169,000** cuộc, với trung bình **28,200** cuộc tấn công mỗi tháng. Như vậy, **cường độ tấn công đã tăng xấp xỉ 51%**, đồng thời sự phân bố theo từng tháng cũng cho thấy mức độ biến động lớn hơn hẳn so với năm trước.

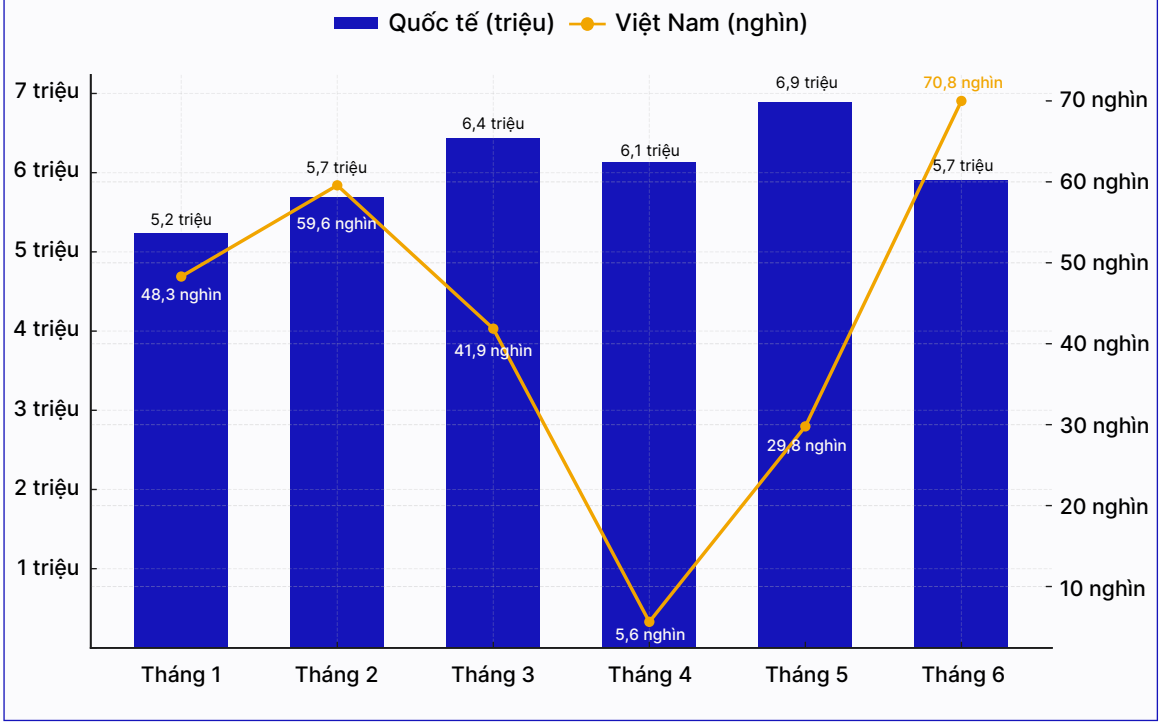
Diễn biến trong 6 tháng đầu năm 2025 phản ánh một bức tranh đặc trưng của các chiến dịch tấn công mạng: khởi đầu với sự leo thang mạnh mẽ (tháng 1–2 với 48,302 và 59,572 vụ), sau đó có giai đoạn hạ nhiệt đột ngột (tháng 4 chỉ còn 5,635 vụ), rồi bùng nổ trở lại (tháng 6 đạt 70,843 vụ), cao nhất trong kỳ và gần gấp đôi so với mức trung bình tháng của cùng kỳ năm 2024.

**Thống kê số lượng cuộc tấn công mạng trong 6 tháng đầu năm 2025 so sánh với cùng kỳ năm 2024**



# 3.3 Số lượng tấn công DDoS tại Việt Nam và quốc tế

**VNIS ghi nhận số lượng tấn công trên toàn cầu lên đến 36,110,000 cuộc tấn công**



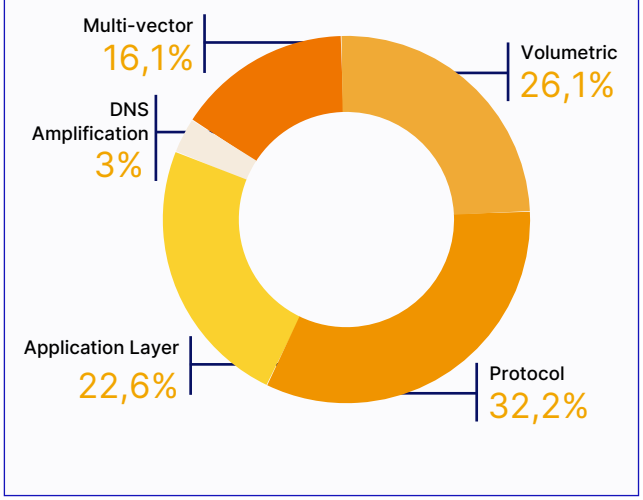

Khi đặt Việt Nam trong bức tranh toàn cầu, có thể thấy sự tương phản rõ rệt: trong khi **quốc tế duy trì mức rất cao** và tương đối ổn định, dao động từ 5.2 đến 6.9 triệu cuộc tấn công mỗi tháng, tổng cộng **36.11 triệu vụ**, thì Việt Nam lại thể hiện mức độ dao động bất thường và thất thường theo chu kỳ. Điều này cho thấy kẻ tấn công tại **Việt Nam không chỉ tập trung vào tấn công khối lượng lớn**, mà còn **thử nghiệm nhiều chiến thuật**, chuyển đổi vector liên tục tạo ra áp lực khó lường cho hệ thống phòng thủ.

Những con số này khẳng định rằng các cuộc tấn công DDoS tại Việt Nam đang ngày càng **có tính chất chu kỳ, biến động thất thường** nhưng cường độ ngày càng **lớn**, đặt ra thách thức nghiêm trọng đối với hạ tầng công nghệ thông tin của doanh nghiệp.

Do đó, cần thiết phải có một chiến lược phòng thủ đa lớp, vận hành theo thời gian thực, vừa có **khả năng hấp thụ lưu lượng khổng lồ** trong các đợt cao điểm, vừa có **năng lực cảnh báo sớm** và **điều chỉnh ngưỡng bảo mật** linh hoạt. Đồng thời, việc **xây dựng playbook ứng phó** tình huống chi tiết cho phép đội ngũ vận hành chuyển đổi **trạng thái phòng thủ kịp thời** khi kẻ tấn công thay đổi vector hoặc phương thức, từ đó duy trì tính ổn định và khả dụng của hệ thống ngay cả trong bối cảnh bị tấn công dữ dội.

# 3.4 Phân loại tấn công DDoS và cường độ

**Phân loại tấn công DDoS tại Việt Nam 6 tháng đầu năm**

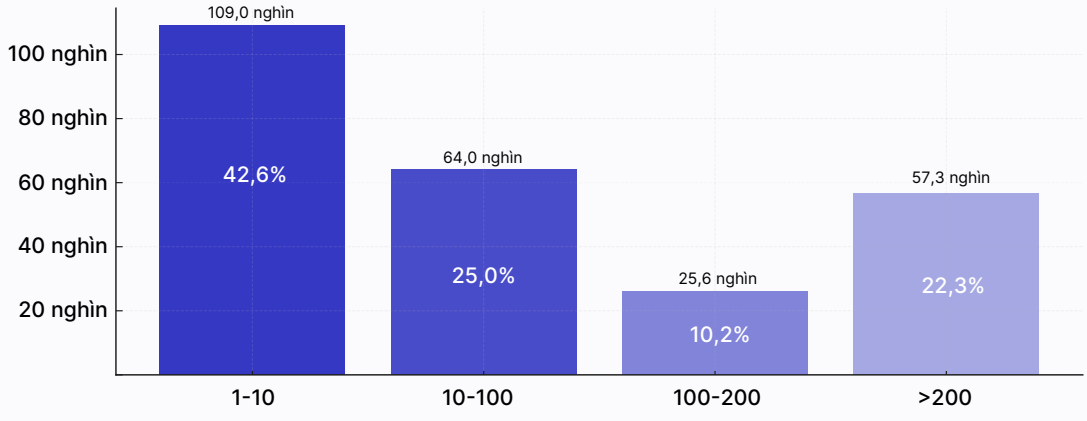



Tấn công **Volumetric** và **Protocol** vẫn chiếm tỷ trọng lớn trong các chiến dịch tấn công DDoS tại Việt Nam, nhưng sự **chuyển dịch mạnh sang các tấn công tầng ứng dụng** (Layer 7) và **Multi-vector** là tín hiệu cho thấy các phương thức tấn công ngày càng tinh vi và phức tạp hơn.

Điều này đòi hỏi các doanh nghiệp phải nhanh chóng nâng cấp hệ thống bảo mật để không chỉ phòng chống hiệu quả các cuộc tấn công volumetric truyền thống, mà còn chủ động bảo vệ API và ứng dụng web trước những mối đe dọa mới. Các biện pháp phòng thủ cần được triển khai theo hướng toàn diện và liên tục, thay vì chỉ dừng lại ở các lớp bảo vệ cơ bản. Chỉ khi đó doanh nghiệp mới có thể duy trì khả năng hoạt động ổn định trong bối cảnh môi trường mạng đầy biến động.

Với mức độ cường độ tấn công cao trên **200 Gbps** hơn **57,390** cuộc và sự thay đổi liên tục của chiến thuật tấn công, các tổ chức cần triển khai giải pháp phòng thủ đa lớp như **AI WAF, API protection, Multi-CDN,** cùng với khả năng giám sát thời gian thực và phản ứng nhanh. Các biện pháp bảo vệ chủ động và phát hiện sớm sẽ giúp giảm thiểu tác động và bảo vệ doanh nghiệp khỏi những tổn thất tài chính và uy tín đáng kể.

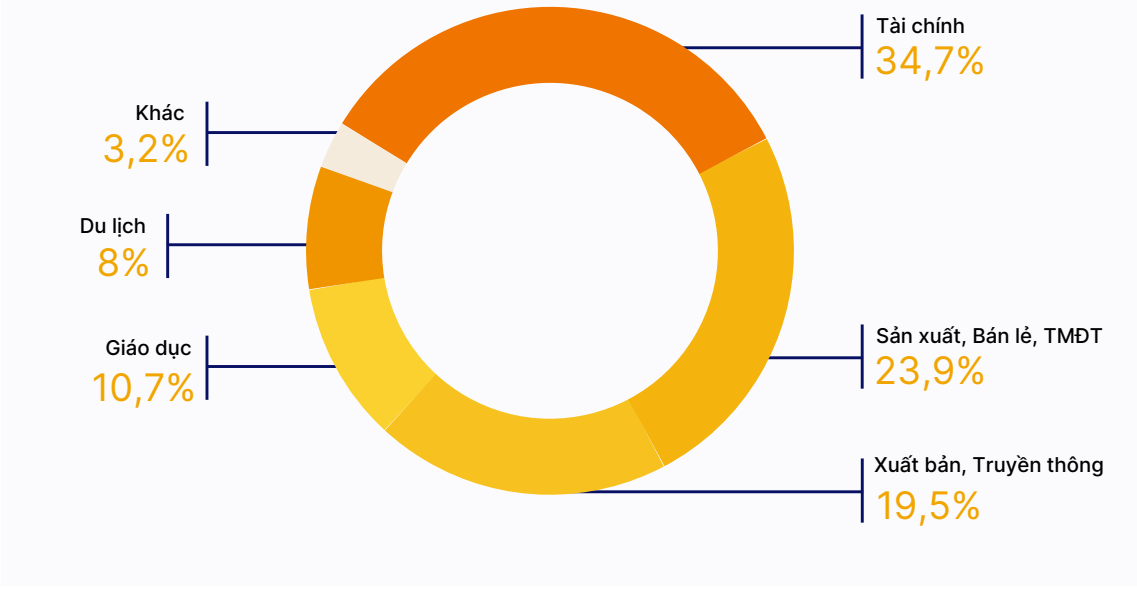
**Cường độ (Gbps) tấn công DDoS tại Việt Nam 6 tháng đầu năm**



# 3.4 Phân loại tấn công DDoS và cường độ

**Giải pháp chống tấn công VNIS** hiện đang bảo vệ nhiều doanh nghiệp thuộc **đa dạng lĩnh vực**, trong đó có 57% doanh nghiệp lớn và 43% doanh nghiệp vừa và nhỏ. Tỷ lệ phân bổ ngành nghề gồm: Tài chính (39%), Xuất bản & Truyền thông (26%), Sản xuất, Bán lẻ, Thương mại điện tử (23%), Du lịch (6%), Giáo dục (4%) và các lĩnh vực khác (2%).

## Tỉ lệ ngành nghề bị tấn công nhiều nhất




## [≈35%] Tài chính

88,713 vụ

Ghi nhận số lượng tấn công nhiều nhất (hơn 88,700 vụ), cho thấy đây vẫn là mục tiêu ưa thích của tội phạm mạng nhờ quy mô khách hàng lớn và giá trị tài sản cao. Tuy nhiên, tỷ trọng tấn công lại thấp hơn tỷ trọng khách hàng, phản ánh việc các tổ chức tài chính đã đầu tư nhiều vào hạ tầng bảo mật, khiến các cuộc tấn công khó xâm nhập hơn.

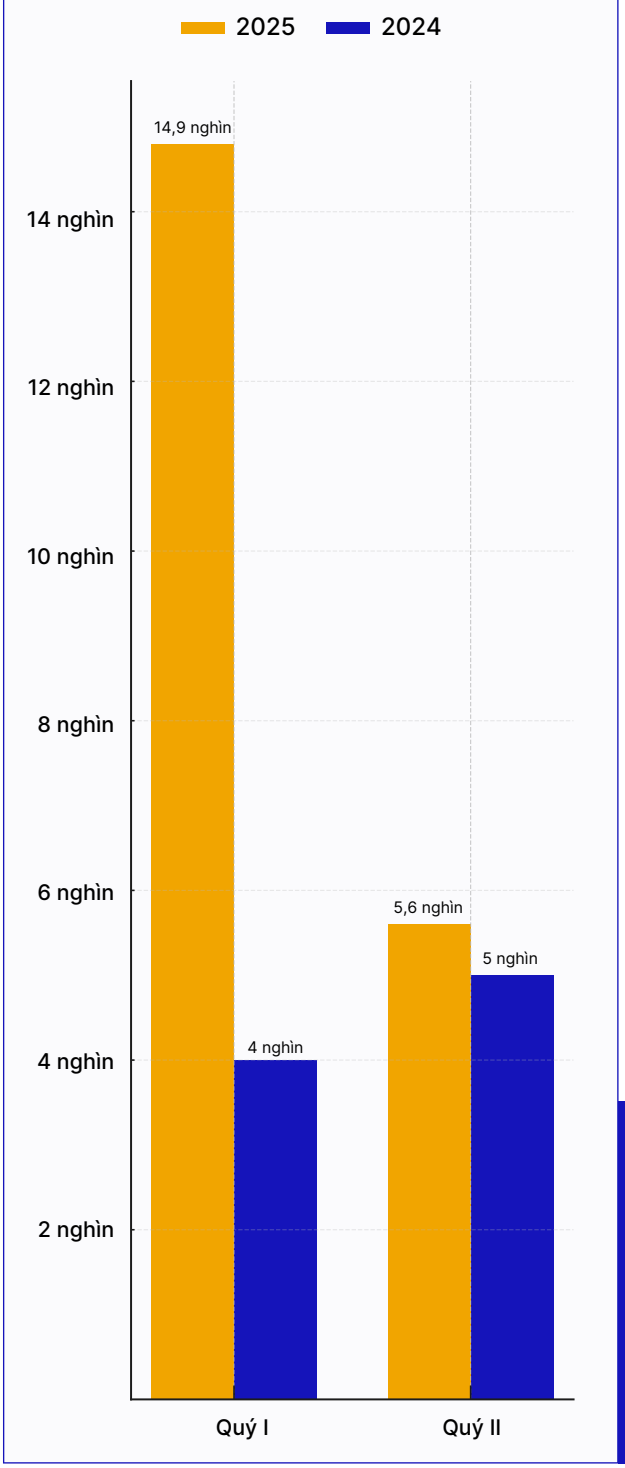
## [≈24%] Sản xuất, Bán lẻ, TMĐT

49,957 vụ

Ghi nhận gần 50,000 vụ, thấp hơn so với cơ cấu khách hàng. Tuy nhiên, các hệ thống thanh toán và giỏ hàng trực tuyến vẫn là mục tiêu giàu tiềm năng cho tấn công vào giờ cao điểm mua sắm. Việc tỷ trọng tấn công thấp hơn không đồng nghĩa an toàn, mà có thể phản ánh chiến thuật phân tán của kẻ tấn công.

# 3.5 Hiện trạng tấn công DDoS đòi tiền chuộc (Ransom DDoS)

**So sánh số vụ tấn công Ransom DDoS theo quý: 2025 vượt xa 2024**

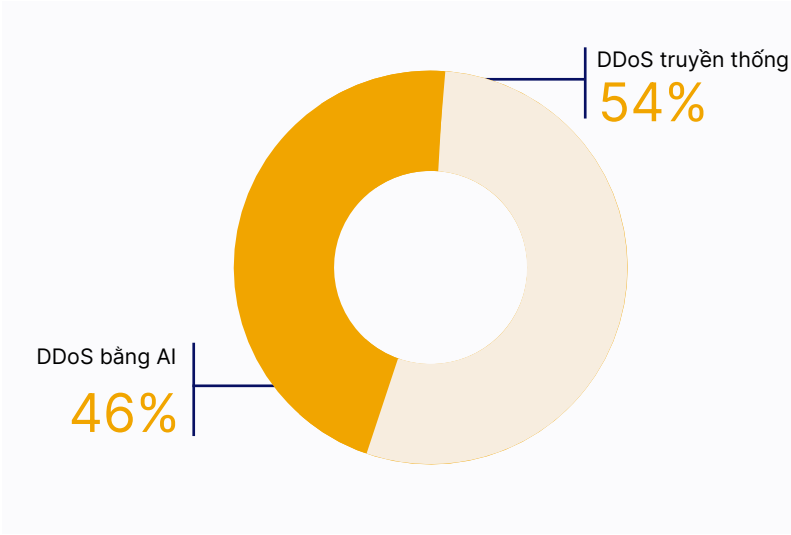



Trong **quý 1** năm 2025, số vụ tấn công Ransom DDoS đã tăng vọt lên **14,875 vụ**, cao gấp gần **3,7 lần** so với con số **4,000** vụ của cùng kỳ năm 2024. Đây là dấu hiệu cho thấy hacker tập trung khai thác giai đoạn đầu năm, thời điểm doanh nghiệp khởi động nhiều hoạt động số, phụ thuộc mạnh vào hệ thống trực tuyến để gây áp lực và ép trả tiền chuộc.

Sang **quý 2** năm 2025, số vụ tấn công ghi nhận **5,605**, tăng nhẹ 12% so với 5,000 vụ của quý 2 năm 2024. Mức tăng này không quá đột biến, cho thấy sau cú "sốc" ở quý 1, các tổ chức có thể đã tăng cường biện pháp phòng thủ, đồng thời tin tặc có thể tạm điều chỉnh chiến thuật nhằm tránh bị phát hiện hoặc chuẩn bị cho các đợt tấn công tiếp theo.

Ransom DDoS (RDoS) là hình thức tấn công từ chối dịch vụ phân tán (DDoS) kết hợp tống tiền: tin tặc đe dọa hoặc thực hiện tấn công làm gián đoạn dịch vụ trực tuyến và yêu cầu nạn nhân trả tiền chuộc để dừng tấn công.

# 3.6 Hiện trạng tấn công DDoS bằng AI




Hệ thống VNIS ghi nhận **117,760 cuộc tấn công DDoS** có sử dụng công nghệ AI, chiếm **46%** tổng số 256,000 cuộc tấn công tại Việt Nam. Với **cường độ tấn công trung bình hơn 322 Gbps** - một ngưỡng băng thông rất cao.

## Hệ thống VNIS ghi nhận các đặc điểm nổi bật của các cuộc tấn công DDoS bằng AI, như sau:

- **Tự động thay đổi vector:** Nhanh chóng chuyển từ volumetric flood sang HTTP(S) flood, API flooding hay DNS amplification, khiến phòng thủ khó thích ứng.
- **Tối ưu hóa botnet theo thời gian thực:** Phân phối lưu lượng hợp lý, tránh bộ lọc truyền thống và duy trì áp lực liên tục.
- **Mô phỏng hành vi người dùng hợp lệ:** Tạo lưu lượng giả, gây khó khăn trong việc phân biệt truy cập chính thống và độc hại.
- **Gia tăng tính dai dẳng:** Duy trì nhiều ngày đến hàng tháng nhờ khả năng tự điều chỉnh chiến thuật tấn công.
- **Hạ thấp rào cản:** Tự động hóa việc thiết lập botnet và chọn vector tối ưu, giúp cả nhóm nhỏ hay cá nhân cũng có thể tấn công tinh vi với chi phí thấp.
- **Nhắm vào tầng ứng dụng và API:** Flood trực tiếp hệ thống xác thực, thanh toán hoặc dịch vụ số, gây thiệt hại lớn hơn so với nghẽn băng thông truyền thống.
- **Kết hợp tống tiền (RDoS):** Chọn thời điểm cao điểm để gia tăng sức ép, buộc nạn nhân trả tiền chuộc.
- **Mở rộng phạm vi toàn cầu:** Botnet IoT và proxy bị chiếm dụng, phân tán lưu lượng từ nhiều quốc gia, làm chặn theo IP hay địa lý kém hiệu quả.

Điều này phản ánh một sự dịch chuyển rõ rệt: từ những đợt **volumetric flood** đơn giản sang các chiến dịch **DDoS thông minh, đa tầng** và **dai dẳng** hơn. Với xu hướng này, **AI không chỉ đóng vai trò hỗ trợ mà đã trở thành "vũ khí chủ lực" của tin tặc**, buộc doanh nghiệp phải nâng cấp hệ thống phòng thủ theo hướng **AI đối phó AI** để bắt kịp tốc độ phát triển của mối đe dọa.

# 3.7 Nguồn gốc tấn công DDoS theo quốc gia

**VNIS ghi nhận Top 10 quốc gia có lưu lượng tấn công vào các doanh nghiệp Việt Nam lớn nhất**


Danh sách này phản ánh các nút botnet, proxy hoặc điểm cuối VPN nơi các cuộc tấn công DDoS xuất phát, chứ **không phải vị trí thực tế của các tác nhân đe dọa.**

Trong số các quốc gia hiện nay, những quốc gia có nền tảng công nghệ chưa phát triển mạnh như **Việt Nam, Ukraine, Mexico,** và **Indonesia** đang ngày càng trở thành những **nguồn phát tán chính của các cuộc tấn công DDoS**. Điều này cho thấy rằng tấn công mạng không chỉ đến từ các quốc gia phát triển với các cơ sở hạ tầng mạnh mẽ, mà còn **xuất phát từ những khu vực có cơ sở hạ tầng bảo mật yếu**, nơi các thiết bị IoT, máy chủ không bảo mật và các hệ thống chưa được bảo vệ đầy đủ dễ dàng bị lợi dụng để tạo ra botnet hoặc amplifier.

Mặc dù các quốc gia này chưa phải là điểm đến chính của các tác nhân đe dọa, nhưng chúng lại **đóng vai trò vị trí xuất phát cho các cuộc tấn công DDoS** do thiếu kiểm soát và bảo mật hạ tầng. Các tấn công này thường khó bị phát hiện và ngăn chặn vì chúng sử dụng địa chỉ IP giả mạo hoặc nút proxy từ các quốc gia không phải là nguồn gốc thực sự của cuộc tấn công. Điều này càng làm tăng thêm thách thức trong việc phát hiện và phòng chống tấn công DDoS.

# IV Case study


## Bối cảnh

Doanh nghiệp chỉ sử dụng tường lửa vật lý và các giải pháp chống tấn công cơ bản. Tuy nhiên, với quy mô tấn công cực lớn lên tới hơn 1,2 Tbps việc tự ứng phó gần như bất khả thi. Ngay cả khi tìm đến các nhà cung cấp khác, doanh nghiệp cũng không nhận được hỗ trợ hiệu quả do đặc thù hệ thống công nghệ thông tin khó tích hợp và  chưa đơn vị nào đủ năng lực xử lý lưu lượng này.

**VNIS ghi nhận lưu lượng lớn nhất vào hệ thống chứng khoán lên đến 1,2 Tbps**

## Quy mô tấn công

**Thời gian:**

Cuộc tấn công diễn ra **liên tục trong 4 ngày đầu** (trước khi VNIS được tích hợp) và vẫn **kéo dài hơn 1 tháng** sau đó. Đặc biệt nghiêm trọng trong khung giờ giao dịch cao điểm 9h00 – 11h00, 13h00 – 14h30 và 14h30 – 15h00 (ATC).

**Lưu lượng:**

Ghi nhận **Đỉnh tấn công đạt 1,2 Tbps** và **hơn 720,000 RPS** — mức quy mô **cực lớn** tại Việt Nam.

**Phương thức tấn công:**

Sử dụng nhiều kỹ thuật kết hợp:

- DDoS **đa lớp** Layer 3/4/7.
- API Flooding làm **nghẽn toàn bộ** cổng giao dịch.
- Khai thác SQL Injection và lỗ hổng, **hỗ trợ bởi AI**.

# IV Case study


## Tác động ban đầu

- Doanh thu từ phí giao dịch sụt giảm nghiêm trọng, chỉ **4 giờ downtime** đã gây thiệt hại ước tính hơn **200 tỷ đồng**, kéo theo **uy tín doanh nghiệp** bị ảnh hưởng.
- **Chi phí băng thông trả** cho nhà mạng đến **hàng trăm triệu** từ lưu lượng tấn công vượt ngưỡng mà không có biện pháp chặn lọc kịp thời.
- Hơn **86% lệnh thanh toán bị gián đoạn hoặc khớp chậm**, làm giảm thanh khoản thị trường và niềm tin nhà đầu tư.
- Nhà đầu tư không thể đặt, huỷ hoặc sửa lệnh trong hơn **5 giờ cao điểm mỗi ngày**, khiến hệ thống giao dịch bị tắc nghẽn.
- Đội ngũ IT **phải trực 24/7** xử lý khủng hoảng, nhưng vẫn không thể kiểm soát được lưu lượng tấn công.

## Giải pháp từ VNIS

### Tích hợp nhanh chóng

- Nhận được thông tin chuyên gia của VNETWORK đã triển khai chặn lọc tấn công ngay trong đêm.
- Đảm bảo khôi phục ổn định sau 5 phút tích hợp, dù hệ thống của doanh nghiệp chứng khoán có nhiều yêu cầu đặc thù.

### Nhận định & phân tích lưu lượng

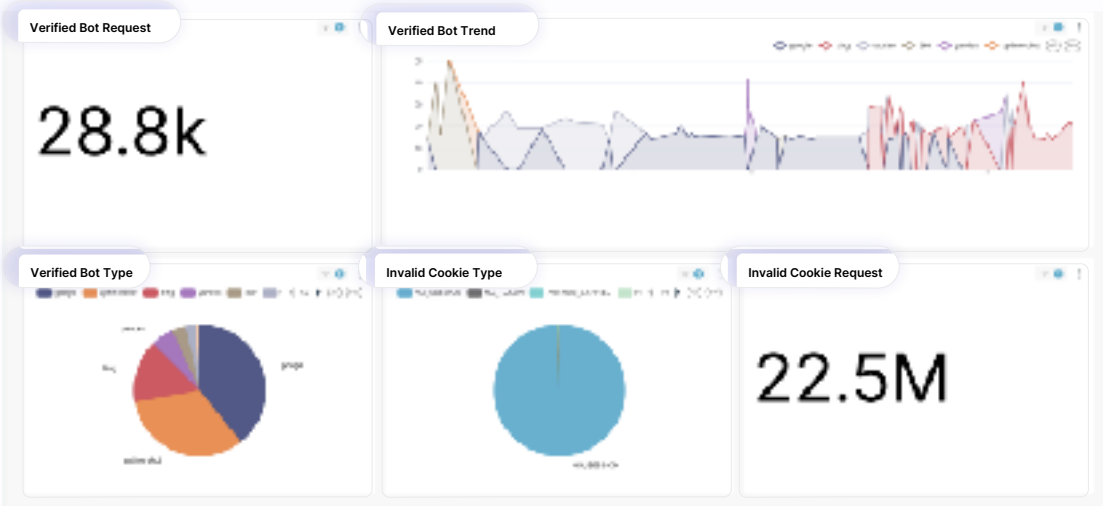
- SOC 24/7 giám sát realtime, nhanh chóng xác định nguồn gốc và vector tấn công (Layer 3/4/7, API Flooding, SQL Injection).
- AI WAF sử dụng Machine Learning để học từ kho dữ liệu tấn công khổng lồ của VNIS kết hợp tình hình thực tế, từ đó tự động nhận diện mẫu hành vi bất thường và phân biệt rõ giữa yêu cầu hợp lệ với lưu lượng độc hại.

# IV Case study

## Giải pháp từ VNIS

### Chặn lọc & xử lý đa lớp

- **Multi-CDN + AI Smart Load Balancing:** mở rộng hạ tầng trên toàn cầu ở 146 quốc gia với hơn 2,600 Tbps, giúp duy trì tính ổn định, giảm áp lực máy chủ gốc, phân tán lưu lượng DDoS Layer 3/4.
- **AI WAF:** tự động chặn DDoS Layer 7, SQL Injection, XSS, Zero-day và toàn bộ lỗ hổng theo danh sách OWASP Top 10.
- **API Protection chuyên sâu:** bảo vệ endpoint đặt lệnh, huỷ lệnh, thanh toán khỏi API Flooding và rò rỉ dữ liệu.
- **Rate Limiting & CAPTCHA thông minh:** loại bỏ botnet và truy vấn giả mạo, giữ nguyên vẹn giao dịch hợp lệ.




VNIS ghi nhận và phân tích tấn công realtime

### Giám sát & tối ưu liên tục


- SOC & chuyên gia VNIS đồng hành **24/7** cùng **hệ thống AI cập nhật rule** theo thời gian thực để đối phó các chiến thuật tấn công thay đổi.
- Hệ thống **báo cáo định kỳ**, tối ưu hiệu năng và bảo mật, đảm bảo giao dịch **mượt ngay cả trong giờ cao điểm**.

# IV Case study

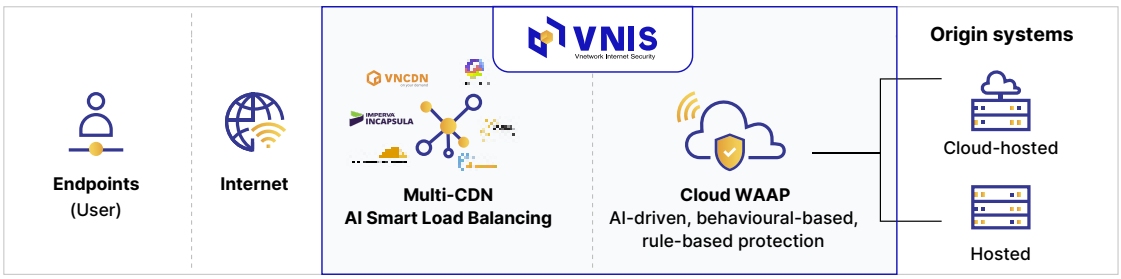
## Kết quả đạt được

- Hệ thống khôi phục giao dịch chỉ sau **5 phút** sau khi VNIS được tích hợp.
- Loại bỏ **99,997%** lưu lượng độc hại, giữ nguyên vẹn lệnh hợp lệ của nhà đầu tư.
- Thanh khoản thị trường được **khôi phục**, niềm tin khách hàng lấy lại, uy tín doanh nghiệp được bảo vệ.
- Doanh nghiệp thoát khỏi khủng hoảng, chuyển sang vận hành **ổn định** và **sẵn sàng tăng trưởng bền vững**.

# Về VNIS

Giải pháp VNIS WAAP (Web Application & API Protection) bảo mật được **kiến tạo từ AI**. Nơi AI không chỉ là công cụ hỗ trợ, mà đóng vai trò trung tâm trong việc **xây dựng giải pháp, dự báo, nhận diện** và **phòng chống** các cuộc **tấn công** mạng ngày càng tinh vi.

**Mô hình hoạt động kết hợp Multi-CDN và Cloud WAAP ứng dụng AI giúp chống tấn công DDoS toàn diện ở tầng 3/4/7**




## Với VNIS doanh nghiệp có thể:

**Bảo vệ Web/App/API** khỏi các tấn công theo thời gian thực: DDoS layer 3/4/7, bot attack, khai thác lỗ hổng bảo mật, zero-day, crawlers/malware...

**Phát hiện và ngăn chặn** mối đe dọa ngay từ giai đoạn đầu mà không làm ảnh hưởng đến trải nghiệm người dùng và hiệu suất hệ thống.

**Duy trì hiệu suất** vượt trội, kể cả trong những tình huống tải lưu lượng truy cập tăng cao hoặc tấn công có chủ đích.

# V Xu hướng & khuyến nghị

## Dự đoán xu hướng

**1) Gia tăng khoảng 32% cuộc tấn công DDoS trong 6 tháng cuối năm**

Số lượng thiết bị IoT ngày càng nhiều và kém bảo mật tạo ra botnet lớn; tin tặc ứng dụng AI để tự động hóa và che giấu lưu lượng; dịch vụ DDoS-for-hire giá rẻ giúp nhiều đối tượng dễ dàng tham gia; quá trình chuyển đổi số mở rộng bề mặt tấn công; chiến thuật đa vector nhắm vào tầng ứng dụng và API khiến các hệ thống phòng thủ khó đối phó.

**2) Xu hướng theo mùa và sự kiện: cao điểm DDoS có thể tái diễn vào Quý 4**

Hoạt động khuyến mại, IPO và sự kiện công cộng thường thu hút lưu lượng người dùng cao, tạo điều kiện để tin tặc lợi dụng. Chúng chọn đúng thời điểm cao điểm để tối đa hóa gián đoạn và gia tăng sức ép tài chính, kể cả tấn công tống tiền.

**3) Cường độ "siêu lớn" (>1 Tbps) trở thành kịch bản thường xuyên**

Botnet phân tán toàn cầu (IoT và proxy server) giúp tin tặc dễ tạo ra lưu lượng cực lớn. Doanh nghiệp thiếu Anycast CDN và Scrubbing đa vùng sẽ khó hấp thụ được các đợt tấn công cường độ cao.

**4) Tấn công nhắm API và hệ thống thanh toán tiếp tục gia tăng**

API ngày càng giữ vai trò trung tâm trong giao dịch số, trở thành mục tiêu ưa thích của DDoS tống tiền. Tin tặc tập trung flood tầng ứng dụng để làm nghẽn hệ thống xác thực, thanh toán hoặc dịch vụ khách hàng.

**5) Nguồn tấn công phân tán và khó dự đoán hơn**

Lưu lượng DDoS ngày càng đến từ nhiều quốc gia và ASN (là số hiệu hệ thống tự trị một mã định danh duy nhất được gán cho mỗi Autonomous System trong Internet.) khác nhau, phản ánh sự lan rộng của botnet toàn cầu. Hacker cũng tận dụng hạ tầng proxy và cloud bị lạm dụng để ẩn danh, khiến biện pháp chặn theo địa chỉ IP hoặc quốc gia kém hiệu quả.

**6) Tổ chức và cơ quan nhà nước trở thành mục tiêu, dữ liệu bị rao bán tràn lan**

Trong nửa đầu tháng 9/2025 đã ghi nhận các vụ tấn công mạng nhắm vào các doanh nghiệp lớn và cơ quan nhà nước, với dữ liệu nhạy cảm bị rò rỉ và rao bán công khai trên các diễn đàn ngầm. Dự báo từ nay đến cuối năm, tình hình sẽ còn diễn biến phức tạp hơn, khi xu hướng tấn công không chỉ dừng ở DDoS mà còn kết hợp với việc đánh cắp và khai thác dữ liệu để gây sức ép hoặc trục lợi tài chính.

# V Xu hướng & khuyến nghị

## Khuyến nghị cho doanh nghiệp, tổ chức

### Công nghệ & Giải pháp kỹ thuật

- Đầu tư giải pháp chống DDoS chuyên dụng đa lớp (Layer 3/4 và Layer 7) để bảo vệ toàn diện từ volumetric flood đến HTTP(S) flood.
- Bảo vệ DNS và API bằng multi-DNS, DNSSEC, API Gateway với mTLS/OAuth2, quota & schema validation.
- Tách tải động – tĩnh và chế độ degraded mode để giảm áp lực lên backend và duy trì trải nghiệm cơ bản khi bị tấn công.
- Chiến lược multi-cloud/multi-region cho dịch vụ trọng yếu để tránh "điểm nghẽn đơn lẻ" khiến toàn bộ hệ thống bị tê liệt khi một nơi gặp sự cố.

### Giám sát & Phát hiện sớm

- Thiết lập giám sát lưu lượng thời gian thực (SOC/IDS) để phát hiện sớm dấu hiệu bất thường trong lưu lượng truy cập.
- Định kỳ kiểm thử & diễn tập kịch bản DDoS để đánh giá khả năng phản ứng và tối ưu cảnh báo.

### Ứng phó & Quy trình vận hành

- Xây dựng kế hoạch ứng phó sự cố DDoS với mục tiêu khôi phục nhanh (RTO ≤ 10 phút), diễn tập định kỳ để SOC/IT luôn sẵn sàng.
- Chuẩn bị kịch bản Ransom DDoS (RDoS): có quy trình xử lý khi nhận đe dọa, không trả tiền chuộc, báo cáo cơ quan chức năng.
- Hợp tác với đơn vị an ninh mạng uy tín để được hỗ trợ 24/7 khi xảy ra tấn công quy mô lớn.

### Quản trị & Tài chính

- Dự toán chi phí DDoS (FinOps): bao gồm egress, scrubbing, WAF request, đồng thời thiết lập ngưỡng shed load tự động để kiểm soát tài chính.
- Đưa DDoS vào quản trị rủi ro cấp chiến lược, giúp lãnh đạo thấy đây là rủi ro kinh doanh, không chỉ là sự cố kỹ thuật.

# VI Phương pháp & nguồn dữ liệu

**Nguồn dữ liệu:**

Thu thập từ VNIS - giải pháp bảo mật Web/App/API của VNETWORK, qua hệ thống chống tấn công DDoS.

**Phương pháp thu thập:**

- Giám sát liên tục và ghi nhận sự kiện bảo mật.
- Sử dụng công cụ phân tích định lượng và định tính.

**Phạm vi:**

Số liệu tổng hợp từ hệ thống bảo mật VNIS của khách hàng tại Việt Nam và trên toàn cầu.

**Thời gian ghi nhận:**

Từ ngày 1/1/2025 đến 30/6/2025.

## Giải pháp bảo mật Web/App/API từ VNETWORK GROUP

VNIS mang đến sự bảo chứng vững chắc: hạ tầng an ninh mạng quy mô lớn, công nghệ phòng thủ tiên tiến và đội ngũ chuyên gia luôn sẵn sàng ứng cứu. Đây chính là nền tảng để doanh nghiệp yên tâm tập trung vào tăng trưởng, trong khi VNIS bảo vệ hệ thống số và thương hiệu.

Liên hệ ngay

Tìm hiểu thêm

## Liên hệ


**Việt Nam**
Tòa nhà UOA Tower,
số 6 Tân Trào, phường
Tân Mỹ, TP. Hồ Chí Minh

**Singapore**
111 North Bridge Road
#17-06 Peninsula Plaza

+84 (28) 7306 8789

contact@vnetwork.vn