Case Study: Cuộc tấn công DDoS vào GRANIX

Phân tích chi tiết cuộc tấn công DDoS vào nền tảng giao dịch OTC Crypto trong tháng 7/2025

Nguyễn An Hưng

09-13/07/2025
Thời gian diễn ra tấn công

30 triệu request/giờ
Tần suất tấn công trung bình

1.000 USD
Yêu cầu tiền chuộc

20-25%
Người dùng bị ảnh hưởng

Executive Summary

What happened

- **Thời gian:** 09-13/07/2025
- **Đối tượng:** Nền tảng OTC Crypto GRANIX
- **Tấn công:** DDoS liên tục
- **Quy mô:** **30M** request/giờ
- **Yêu cầu:** 1.000 USD tiền chuộc

How it was discovered

- **09/07 - 17:00:** Hệ thống có dấu hiệu giật lag
- **Quá trình điều tra:** Phân tích logs, traffic
- **Xác nhận:** Tấn công DDoS quy mô lớn
- **Nguồn tấn công:** Đa dạng IP từ nhiều quốc gia

Impact scope

- **Người dùng ảnh hưởng:** **20-25%**
- **Website:** Sập hoàn toàn trong 30 phút đầu tiên
- **Trải nghiệm người dùng:** Phải vượt CAPTCHA hoặc truy cập bị từ chối
- **Thời gian gián đoạn:** Liên tục trong 4 ngày

Current remediation status

- **Hệ thống:** Đã ổn định
- **Giải pháp:** Cloudflare và AWS bảo vệ nâng cao
- **Thiếu sót:** Không có kế hoạch phòng ngừa
- **Quy trình:** Chưa được ban lãnh đạo triển khai

Incident Timeline

Thời gian tấn công
4 ngày

Tần suất tấn công
30M req/h

Thời gian sập hoàn toàn
30 phút

09/07 - 17:00 — Khởi đầu
Hiệu suất hệ thống suy giảm đột ngột
Người dùng bắt đầu báo cáo về độ trễ và giật lag khi truy cập hệ thống

09/07 - 17:05
Phát hiện lưu lượng truy cập bất thường
Lưu lượng truy cập tăng đột biến vào NGINX ingress của cụm Kubernetes

09/07 - 17:10
Hệ thống cảnh báo
AWS WAF và phân tích của Cloudflare phát cảnh báo về tấn công DDoS

09/07 - 17:15
Triển khai xử lý ban đầu
Cô lập hệ thống gốc khỏi Internet để giảm thiểu tác động

09/07 - 17:30 — Đỉnh điểm
Website sập hoàn toàn
Website không thể truy cập được trong khoảng 30 phút đầu tiên của cuộc tấn công

09/07 - 18:00
Khôi phục truy cập
Bật CAPTCHA và rule chặn ngắn hạn trên Cloudflare, khôi phục truy cập cơ bản

09/07 - 20:00
Đợt tấn công thứ hai
Kẻ tấn công khởi phát đợt tấn công thứ hai với kỹ thuật tinh vi hơn

10/07 - 13/07
Chống trả các đợt tấn công
Sử dụng kết hợp rate-limit, WAF custom rule, challenge JS và phân tích hành vi

14/07 — Kết thúc
Trở lại bình thường
Lưu lượng truy cập trở lại bình thường, tiến hành tổng kết hậu sự cố

Sau sự cố
Phân tích và tổng kết
Không có kế hoạch phòng ngừa hay quy trình ứng phó nào được ban lãnh đạo triển khai

Systems Affected

Cuộc tấn công DDoS nhắm vào **lớp Ingress công khai** và **cơ sở hạ tầng bảo vệ**, gây ảnh hưởng đến truy cập người dùng nhưng không xâm phạm trực tiếp vào hệ thống backend.

Kubernetes Ingress Controller

Bị ảnh hưởng

k8s-granix-ingress / 10.0.2.11

Vai trò

Cổng Ingress công khai

Công nghệ

NGINX trên Kubernetes

Web frontend

API Gateway

Không phát hiện xâm phạm

Cloudflare Edge Network

Đã bảo vệ

cloudflare edge

Vai trò

CDN & lớp phòng thủ DDoS

Trạng thái

Đã kích hoạt bảo vệ nâng cao

Firewall | Challenge | Rate Limiting | Custom Rules

Root Cause Analysis

> *"Sự thật phũ phàng đã được phơi bày: GRANIX là một pháo đài với những bức tường giấy, và sự thiếu nhận thức của lãnh đạo đã để lộ những cánh cửa chính."*

Technical Weakness

- **Thiếu giới hạn request chi tiết** theo IP
- **Không có hệ thống giám sát** lưu lượng nền để phát hiện bất thường
- **Không có kịch bản phản ứng** sự cố sẵn sàng

Bằng chứng

Log ghi nhận hơn **15-30M** request/giờ đổ dồn vào các endpoint /api/*, từ nhiều IP có hành vi tương tự bot

Procedural Weakness

- **Không có tài liệu hoặc kịch bản** phòng chống DDoS
- **Nhân sự và ban lãnh đạo** không có nhận thức đúng về rủi ro từ các cuộc tấn công có đòi tiền chuộc
- **Không có kiểm thử khả năng** chịu tải từ trước

Lịch sử tương tự

Chiến dịch tương tự đã biết: Các cuộc tấn công có chủ đích nhằm vào nền tảng crypto tại Đông Nam Á trong năm 2023 với yêu cầu tống tiền tương tự

Indicators of Compromise (IoCs)

IP độc hại tiêu biểu

154.203.39.9
Nhật Bản

46.114.15.16
Đức

31.59.11.231
Nhật Bản

46.203.52.126
Nhật Bản

Các IP này có thể thay đổi hoặc sử dụng các kỹ thuật proxy/vpn để che giấu vị trí thực

Hành vi đáng ngờ

Flood các endpoint /, /api/..., /api/airdrop/... với tần suất cao

Giả lập User-Agent là trình duyệt di động để qua mặt filter

Tần suất tấn công lên đến 30 triệu request/giờ

Yêu cầu tiền chuộc 1.000 USD để dừng tấn công

Các hành vi này có thể thay đổi trong các cuộc tấn công tương lai, cần có hệ thống giám sát linh hoạt

Threat Intelligence Integration

MITRE ATT&CK Mapping

Tác động **T1498.001**

Network Denial of Service - Tấn công từ chối dịch vụ mạng

Quan sát

Flood dữ liệu vào gateway nhằm **đánh sập ingress** và làm **tê liệt cluster**

Impact

Network Denial of Service

Chiến dịch tương tự đã biết

Các cuộc tấn công crypto tại Đông Nam Á

Năm **2023**, các nền tảng crypto tại Đông Nam Á đã hứng chịu các cuộc tấn công tương tự với yêu cầu tống tiền như nhau

$ Mô hình tống tiền

Yêu cầu tiền chuộc **1.000 USD** để dừng tấn công, với chiến thuật tương tự

Kỹ thuật tấn công

Sử dụng **botnet** để tạo lưu lượng truy cập ảo với tần suất cao, nhắm vào các endpoint API quan trọng

Containment Actions

Các biện pháp **ngăn chặn ngay lập tức** đã được triển khai để chống lại cuộc tấn công DDoS, kết hợp các giải pháp từ Cloudflare, AWS và cấu hình NGINX.

1

Cloudflare Protection

Kích hoạt đầy đủ các tính năng bảo vệ DDoS trên Cloudflare

- Rate limiting
- Challenge JS
- OWASP Managed Rules

2

AWS WAF Configuration

Tùy chỉnh AWS WAF để lọc các yêu cầu độc hại

- Lọc theo header bất thường
- Chặn IP trong blacklist
- Chặn theo vùng địa lý

3

NGINX Optimization

Tối ưu lại cấu hình ingress NGINX để tăng khả năng chịu tải

- Giới hạn kết nối
- Tăng kích thước bộ đệm
- Tối ưu timeout

4

Autoscaling

Bật autoscale cho pod ingress và các dịch vụ ứng dụng

- Tăng số lượng pod
- Phân phối tải
- Hấp thụ lưu lượng tấn công

5

Rate Limiting

Giới hạn tốc độ yêu cầu trên NGINX Ingress Controller

- Giới hạn theo IP
- Giới hạn theo endpoint
- Burst rate limiting

6

Log Analysis

Phân tích nhật ký truy cập để xác định IP độc hại

- Xác định mẫu tấn công
- Chặn IP tự động
- Cập nhật blocklist

Remediation Steps

Các biện pháp **khắc phục dài hạn** đã được triển khai để tăng cường khả năng phòng thủ và phục hồi của hệ thống sau cuộc tấn công DDoS.

1

Blocklist Động

Triển khai blocklist động cập nhật bằng Lambda@Edge

- Cập nhật tự động
- Phản ứng tức thời

2

CAPTCHA & Challenge

Thêm CAPTCHA / challenge JS riêng cho các API trọng yếu

- Bảo vệ endpoint quan trọng
- Lọc bot tự động

3

Autoscale

Bật autoscale cho pod ingress và rule WAF bằng Terraform

- Mở rộng tự động
- Hấp thụ lưu lượng tấn công

4

Giám sát Thời gian thực

Kết nối Prometheus + Grafana để giám sát lưu lượng

- Phát hiện sớm
- Dashboard trực quan

5

Phân tích Log

Tập hợp log và gửi về hệ thống ELK để phân tích chuyên sâu

- Điều tra sự cố
- Phân tích mẫu tấn công

6

Tối ưu NGINX

Tối ưu hóa cấu hình NGINX Ingress Controller

- Xử lý hiệu quả hơn
- Giảm tác động tấn công

Lessons Learned

Lỗ hổng kỹ thuật

- **Chưa có autoscale** cho ingress và cấu hình rate-limit phù hợp
- **Cloudflare ở cấu hình mặc định**, chưa tối ưu cho ngành crypto
- **Thiếu chiến lược phòng thủ DDoS** chủ động

Lỗ hổng quy trình

- **Không có playbook** hoặc kịch bản xử lý sự cố
- **Không có kế hoạch liên lạc**/ ứng phó khẩn cấp
- **Thiếu quy trình kiểm thử** khả năng chịu tải định kỳ

Yếu tố con người

- **Không có hỗ trợ** từ team hoặc quản lý cấp trên
- **Ban lãnh đạo không hành động** cải thiện sau sự cố
- **Thiếu nhận thức** về tầm quan trọng của an ninh mạng

Điểm cần cải thiện

- **Ma trận phản ứng sự cố**
- **Tabletop drill định kỳ**
- **Chiến lược phòng thủ chủ động**
- **Thay đổi văn hóa an ninh**

Recommendations

Các đề xuất được chia thành hai nhóm: **ngắn hạn** (tactical) để giải quyết các vấn đề cấp bách và **dài hạn** (strategic) để xây dựng nền tảng an ninh mạng vững chắc.

Ngắn hạn

Tactical (3-6 tháng)

Giới hạn truy cập

Giới hạn truy cập vào ingress theo burst rate/IP

Bảo vệ API quan trọng

CAPTCHA cố định trên trang login và giao dịch

Tối ưu hóa WAF

Tối ưu hóa liên tục các quy tắc Cloudflare WAF và AWS WAF

Giám sát nâng cao

Triển khai giải pháp giám sát lưu lượng mạng nâng cao

Dài hạn

Strategic (6-12 tháng)

Sổ tay ứng phó DDoS

Xây dựng và duy trì sổ tay ứng phó DDoS chi tiết

Threat modeling

Đưa tư duy threat modeling vào quy trình phát triển sản phẩm

Đào tạo nhận thức

Phát triển chương trình đào tạo nhận thức về an ninh mạng toàn diện

Nhóm ứng phó sự cố

Thành lập nhóm ứng phó sự cố chuyên trách hoặc thuê ngoài dịch vụ IR

Appendices

Log minh hoạ

```
[09/Jul/2025:17:15:23] 154.203.39.9 GET /api/v1/trade 429
[09/Jul/2025:17:15:23] 46.114.15.16 POST /api/v1/airdrop 429
[09/Jul/2025:17:15:24 31.59.11.231 GET /api/v1/balance 429
[09/Jul/2025:17:15:24 46.203.52.126 GET /api/v1/market 429
[09/Jul/2025:17:15:25 154.203.39.9 GET /api/v1/trade 429
```

So sánh cấu hình Cloudflare

Trước tấn công **Yếu**

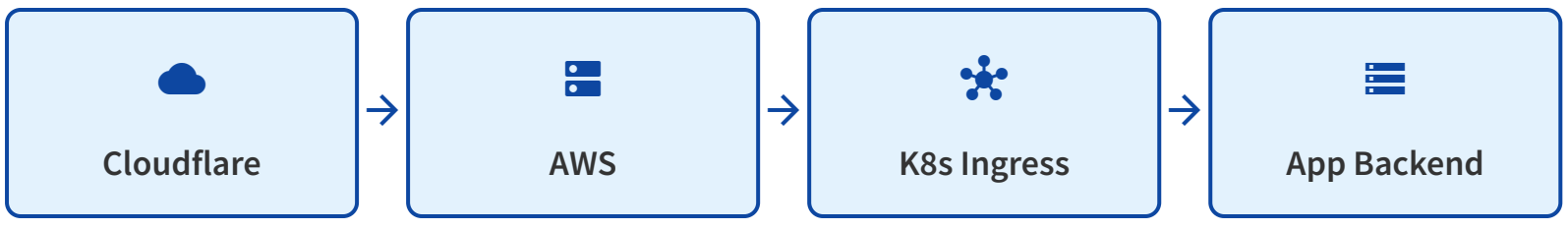
- Bật OWASP mặc định
- Chưa có rate limit
- Chưa có CAPTCHA

Sau tấn công **Tăng cường**

- Giới hạn **200 RPS/IP**
- Challenge toàn bộ **/api/***
- Yêu cầu trình duyệt hợp lệ

Sơ đồ kiến trúc

Luồng truy cập hệ thống



Ảnh chụp màn hình

Ghi nhận log từ Cloudflare

Spike CAPTCHA và lưu lượng truy cập bất thường trong thời gian tấn công

Lưu ý: Do điều khoản NDA, GRANIX là 1 cái tên bí danh được đặt ra, không phải tên công ty/trang web/dịch vụ thật.

Thank You

Nguyễn An Hưng

Người phòng thủ duy nhất trong trận chiến không đồng đội

Cuộc chiến này đã được chống đỡ và giành thắng lợi chỉ với một người.
Nhưng nếu không có sự thay đổi từ tổ chức, thì chiến thắng này chỉ là ***sống sót*** *– không phải là* ***thành công****.*

hungna.dev@gmail.com | blog.nguyenanhung.com | linkedin.com/in/nguyenanhung