

# PROJECT WHITEPAPER: PHANTOM GRID

## NEXT-GEN ACTIVE DEFENSE SYSTEM POWERED BY eBPF

Hạng mục	Chi tiết
Tên dự án	Phantom Grid
Phiên bản	1.0 (Public Release)
Phân loại	Technical Whitepaper
Ngày phát hành	27/12/2025
Tác giả	Mai Hải Đăng
Trạng thái	Draft / Final

# **MỤC LỤC**

1. TÓM TẮT ĐIỀU HÀNH (EXECUTIVE SUMMARY)
2. BỐI CẢNH VÀ THÁCH THỨC (PROBLEM STATEMENT)
  - o 2.1. Các điểm yếu cốt tử của hạ tầng hiện tại
  - o 2.2. Hạn chế của giải pháp truyền thống
3. GIẢI PHÁP CÔNG NGHỆ (CORE TECHNOLOGY)
  - o 3.1. Kiến trúc Module
    - A. The Mirage (Lớp ngụy trang chủ động)
    - B. The Phantom Protocol (Giao thức tàng hình - SPA)
    - C. The Portal (Cổng dịch chuyển không gian số)
  - o 3.2. Ngăn xếp kỹ thuật (Tech Stack)
4. TÍNH NĂNG VƯỢT TRỘI (KEY DIFFERENTIATORS)
5. TIỀM NĂNG THƯƠNG MẠI (MARKET & BUSINESS MODEL)
  - o 5.1. Khách hàng mục tiêu
  - o 5.2. Mô hình triển khai
6. LỘ TRÌNH PHÁT TRIỂN (ROADMAP)
7. KẾT LUẬN

# 1. TÓM TẮT ĐIỀU HÀNH (EXECUTIVE SUMMARY)

Trong kỷ nguyên của các cuộc tấn công mạng tinh vi (Advanced Persistent Threats - APT), tư duy phòng thủ truyền thống dựa trên "tường lửa" và "chữ ký" đã trở nên lỗi thời. Sự bất đối xứng trong an ninh mạng là quá lớn: Đội ngũ bảo mật phải đúng 100% thời gian, trong khi kẻ tấn công chỉ cần đúng một lần.

Phantom Grid là giải pháp Phòng thủ Chủ động (Active Defense) tiên phong, được xây dựng trên công nghệ eBPF (Extended Berkeley Packet Filter) hoạt động trực tiếp tại nhân (Kernel) hệ điều hành Linux. Thay vì thụ động chờ đợi tấn công, Phantom Grid biến hạ tầng mạng thành một "mê cung số", chủ động đánh lừa, phát hiện và cô lập kẻ tấn công trước khi thiệt hại xảy ra.

Điểm đột phá của Phantom Grid là việc tích hợp cơ chế Zero Trust Access thông qua giao thức Single Packet Authorization (SPA), giúp máy chủ hoàn toàn "tàng hình" trước mọi nỗ lực trinh sát của hacker.

## 2. BỐI CẢNH VÀ THÁCH THỨC (PROBLEM STATEMENT)

### 2.1. Các điểm yếu cốt tử của hạ tầng hiện tại

- Di chuyển ngang (Lateral Movement): Sau khi xâm nhập qua vành đai bảo mật, hacker thường tự do trinh sát mạng nội bộ. Các giải pháp hiện tại thiếu khả năng kiểm soát luồng giao thông Đông-Tây (East-West traffic) hiệu quả.
- Thời gian phát hiện chậm (Dwell Time): Trung bình hacker nằm vùng trong hệ thống 21 ngày trước khi bị phát hiện.
- Bề mặt tấn công rộng (Exposed Attack Surface): Các dịch vụ quản trị (SSH, Admin Panel) thường phải mở port, tạo cơ hội cho các cuộc tấn công Brute-force hoặc khai thác lỗ hổng Zero-day.

### 2.2. Hạn chế của giải pháp truyền thống

- Firewall/IPS: Dựa trên tập luật tinh, dễ bị qua mặt bởi mã hóa hoặc kỹ thuật giả mạo IP.
- Honeypot truyền thống: Tốn kém tài nguyên, độ trễ cao, dễ bị hacker phát hiện là môi trường giả lập (Fingerprinting).

### 3. GIẢI PHÁP CÔNG NGHỆ (CORE TECHNOLOGY)

Phantom Grid không chỉ là một công cụ, mà là một kiến trúc bảo mật toàn diện hoạt động ở tầng thấp nhất của hệ điều hành: XDP (eXpress Data Path) và Traffic Control (TC).

#### 3.1. Kiến trúc Module (Cơ chế Phối hợp)

Hệ thống phân chia không gian mạng thành hai vùng riêng biệt và áp dụng cơ chế xử lý khác nhau:

##### A. The Phantom Protocol (Cơ chế Tàng hình cho Tài sản Thực)

*Áp dụng cho các cổng dịch vụ quan trọng (Critical Assets) như SSH (22), Database, Admin Panel.*

- Nguyên lý: "Không thể tấn công thứ bạn không nhìn thấy."
- Cơ chế:
  - Mặc định, eBPF DROP toàn bộ gói tin đi vào các cổng này. Server hoàn toàn "chết" (Dead Host) dưới góc nhìn của hacker.
  - Single Packet Authorization (SPA): Để truy cập, Quản trị viên phải gửi một gói tin UDP đặc biệt (Magic Packet) chứa token mã hóa đến kernel.
  - Nếu xác thực thành công, tường lửa mở cửa sổ kết nối trong 30 giây *chỉ cho duy nhất IP của Admin*.

- Kết quả: Hacker quét mạng sẽ thấy các cổng này đóng hoàn toàn hoặc server không tồn tại. Tài sản thật được bảo vệ tuyệt đối.

## B. The Mirage (Cơ chế Giả lập trên Vùng Trống)

Áp dụng cho hàng nghìn cổng không sử dụng (Unused Ports) còn lại trên server.

- Nguyên lý: "Tạo nhiều loạn để che giấu tín hiệu thật."
- Cơ chế:
  - Thay vì trả về tín hiệu RST (tù chối) như server thông thường, eBPF XDP hook sẽ tự động sinh ra gói tin SYN-ACK giả mạo.
  - Hệ thống mô phỏng hàng loạt dịch vụ phổ biến (HTTP, FTP, Telnet) trên các cổng này.
- Kết quả:
  - Hacker quét IP sẽ thấy hàng ngàn cổng đang "Mở". Hắn sẽ bị choáng ngợp và mất phương hướng, không thể phân biệt đâu là thật, đâu là giả.
  - Mọi nỗ lực tấn công vào các cổng giả này đều vô hại và kích hoạt cảnh báo sớm.

## C. The Portal (Cổng dịch chuyển không gian số)

- **Công nghệ:** Transparent Redirection (DNAT không trạng thái).
- **Cơ chế:** Khi hacker cố gắng tương tác sâu hơn với một "Dịch vụ ma" (tạo ra bởi The Mirage), lưu lượng mạng bị âm thầm chuyển hướng sang môi trường cách ly (Container Honeypot) để thu thập hành vi.
- **Đặc điểm:** Quá trình chuyển hướng diễn ra trong suốt, không thay đổi địa chỉ IP đích

### 3.2. Ngăn xếp kỹ thuật (Tech Stack)

- Kernel Space: C (eBPF Programs), Clang/LLVM.
- User Space Agent: Golang (High-performance loading & Map management).
- Isolation Environment: Docker/Podman Containers.
- Control Center: ReactJS Dashboard (Real-time Threat Monitoring).

## 4. TÍNH NĂNG VƯỢT TRỘI (KEY DIFFERENTIATORS)

Tính năng	Mô tả kỹ thuật	Lợi ích doanh nghiệp
<b>Invisible Infrastructure</b>	Ứng dụng SPA (Single Packet Authorization) để ẩn hoàn toàn các port dịch vụ quan trọng.	Loại bỏ 100% rủi ro từ các cuộc tấn công quét lỗ hổng tự động.
<b>High-Fidelity Deception</b>	Tạo ra hàng nghìn "bẫy" giả lập (Fake Services) mà không tồn tại nguyên phần cứng.	Phát hiện hacker ngay từ giai đoạn trinh sát (Pre-attack phase).
<b>Kernel-Level Performance</b>	Xử lý gói tin tại tầng XDP (trước khi cấp phát bộ nhớ sk_buff của OS).	Độ trễ < 1ms, không ảnh hưởng đến hiệu năng server production.
<b>Real-time Forensics</b>	Ghi lại toàn bộ hành vi trong Honeypot (Keystrokes, File uploads).	Cung cấp bằng chứng số (Digital Forensics) chính xác để vá lỗ hổng.

## 5. TIỀM NĂNG THƯƠNG MẠI (MARKET & BUSINESS MODEL)

### 5.1. Khách hàng mục tiêu (Target Audience)

- **Critical Infrastructure:** Chính phủ, Điện lực, Viễn thông (Yêu cầu chống APT cao nhất).
- **BFSI Sector:** Ngân hàng, Tài chính, Bảo hiểm (Bảo vệ dữ liệu nhạy cảm).
- **Cloud Providers:** Các đơn vị cung cấp hạ tầng muốn tăng cường bảo mật cho khách hàng (Security-as-a-Service).

## 5.2. Mô hình triển khai

- **On-Premises Agent:** Cài đặt trực tiếp trên các máy chủ vật lý (Bare-metal).
- **Kubernetes Sidecar:** Triển khai như một DaemonSet để bảo vệ toàn bộ Cluster (Cloud-Native).

# 6. LỘ TRÌNH PHÁT TRIỂN (ROADMAP)

### Giai đoạn 1: Core Foundation (Đã hoàn thành)

- [x] Xây dựng nhân eBPF XDP/TC.
- [x] Hoàn thiện cơ chế "Giao thức tàng hình" (SPA).
- [x] Triển khai Agent quản lý bằng Golang.

### Giai đoạn 2: Intelligence & Integration (Quý 1-2/2026)

- **Adaptive Deception:** Sử dụng AI để học hành vi hacker và tự động thay đổi cấu hình bẫy (Dynamic Profiling).
- **SIEM Integration:** Tích hợp đầy log về Splunk/Elasticsearch.

### Giai đoạn 3: Ecosystem Expansion (Quý 3-4 2026)

- **Cloud-Native Security:** Đóng gói giải pháp chuyên dụng cho môi trường Kubernetes & Service Mesh (Istio/Linkerd).

- **Marketplace:** Cho phép cộng đồng đóng góp các mẫu "bẫy" (Honeypot templates) mới.

## 7. KẾT LUẬN

Phantom Grid đại diện cho sự chuyển dịch tất yếu của ngành an ninh mạng: Từ Phòng thủ thụ động sang Phòng thủ chủ động. Bằng cách làm chủ công nghệ lõi eBPF và triển khai kiến trúc Zero Trust thực thụ, Phantom Grid trao lại quyền kiểm soát chiến trường không gian mạng về tay người quản trị.

## TUYÊN BỐ MIỄN TRỪ TRÁCH NHIỆM (DISCLAIMER)

*Tài liệu này chưa thông tin về các kỹ thuật bảo mật nâng cao. Các công cụ và phương pháp được mô tả chỉ nhằm mục đích phòng thủ và nghiên cứu an ninh mạng hợp pháp. Tác giả không chịu trách nhiệm cho bất kỳ hành vi sử dụng sai mục đích nào gây ảnh hưởng đến hệ thống của bên thứ ba.*

## THÔNG TIN LIÊN HỆ

- **Author:** Mai Hải Đăng
- **Email:** maidang24112004@gmail.com
- **Repository:** <https://github.com/haidang24/phantom-grid>