

# TRÀ ĐÁ #5 HACKING

29/09/2017 - DA NANG



TRẦN MINH QUẢNG

TRADAHACKING #5

XÂY DỰNG SINKHOLE  
ĐỂ XỬ LÝ MÃ ĐỘC APT

## ABOUT ME

- ▶ Reverser, Malware Analyst, Security Researcher, Programmer
- ▶ Thành viên [@PiggyBirdCTF](#)
- ▶ Sở thích: du lịch và thể thao
- ▶  quangking  quangtrm







by hackers - for hackers

# TRÀ ĐÁ #5 HACKING

29/09/2017 - DA NANG

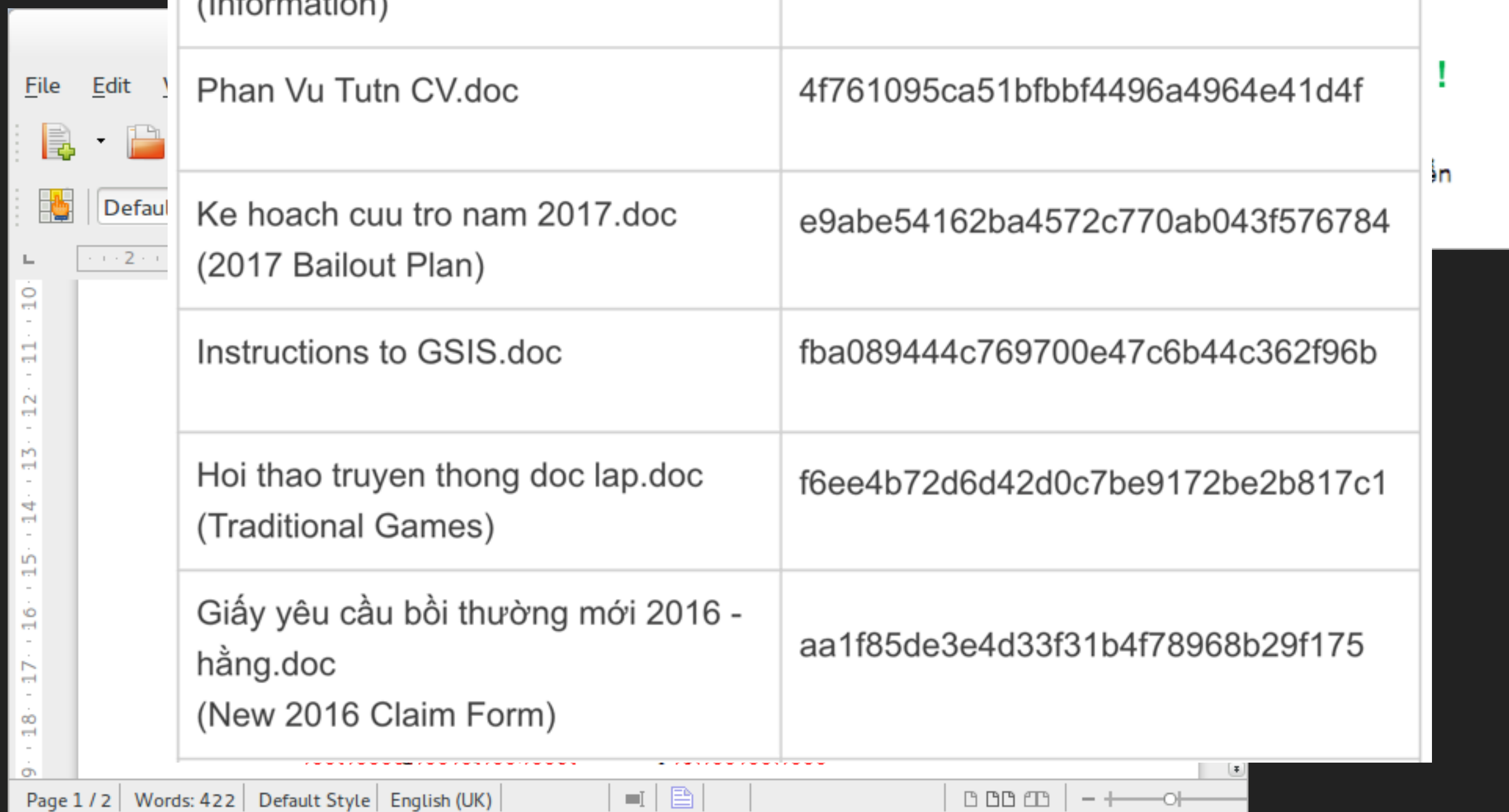
Organized By



<http://trada.vnsecurity.net>

# ADVANCE PERSISTENCE THREAT

## ADVANCE PERSISTENCE THREAT



Thong tin.doc (Information)	ce50e544430e7265a45fab5a1f31e529
Phan Vu Tutn CV.doc	4f761095ca51bfbbf4496a4964e41d4f
Ke hoạch cuu tro nam 2017.doc (2017 Bailout Plan)	e9abe54162ba4572c770ab043f576784
Instructions to GSIS.doc	fba089444c769700e47c6b44c362f96b
Hoi thao truyen thong doc lap.doc (Traditional Games)	f6ee4b72d6d42d0c7be9172be2b817c1
Giấy yêu cầu bồi thường mới 2016 - hăng.doc (New 2016 Claim Form)	aa1f85de3e4d33f31b4f78968b29f175

## CÁC GIẢI PHÁP GIÁM SÁT, PHÁT HIỆN MÃ ĐỘC APT

- ▶ **Network-based** anomaly detection - Network Sensor

- ▶ Phát hiện kết nối độc hại theo dấu hiệu cho trước

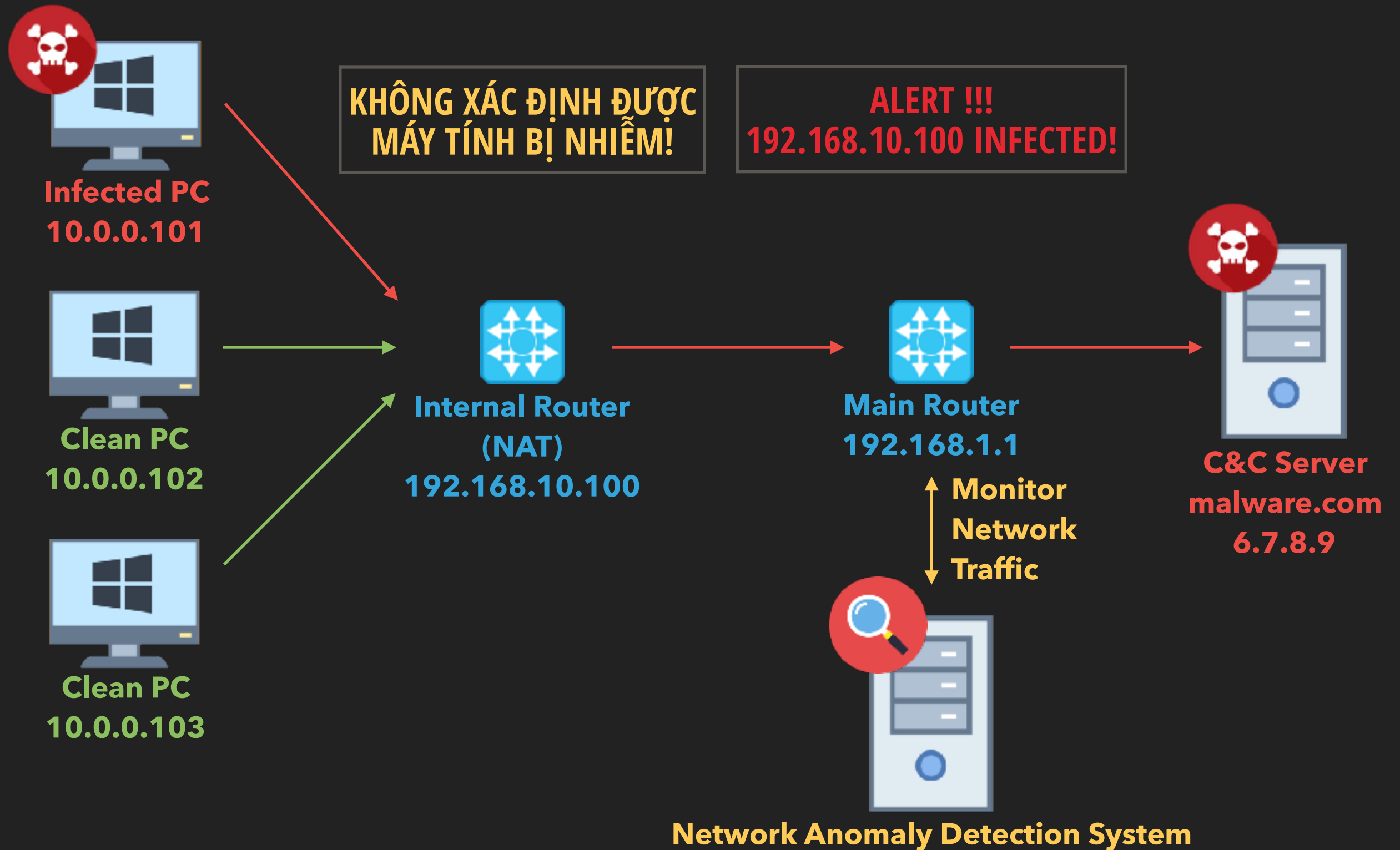
- ▶ **Vấn đề:** khó xác định chính xác máy tính bị nhiễm sau NAT

- ▶ **Host-based** anomaly detection - Security Endpoint

- ▶ Phát hiện chính xác máy tính bị nhiễm theo dấu hiệu cho trước

- ▶ **Vấn đề:** khó triển khai triệt để

## VẤN ĐỀ PHÁT HIỆN MÁY TÍNH BỊ NHIỄM SAU NAT







by hackers - for hackers

# TRÀ ĐÁ #5 HACKING

29/09/2017 - DA NANG

Organized By



<http://trada.vnsecurity.net>

# SINKHOLE

## MÁY CHỦ SINKHOLE

### ▶ Sinkhole

- ▶ Kỹ thuật chuyển hướng kết nối đến **máy chủ độc hại** sang **máy chủ sinkhole**

### ▶ Máy chủ sinkhole

- ▶ Giả lập giao thức mạng máy tính ma
- ▶ Thu thập thông tin về mạng máy tính ma
- ▶ **Phát hiện và xử lý máy tính bị nhiễm mã độc**



## MÁY CHỦ SINKHOLE

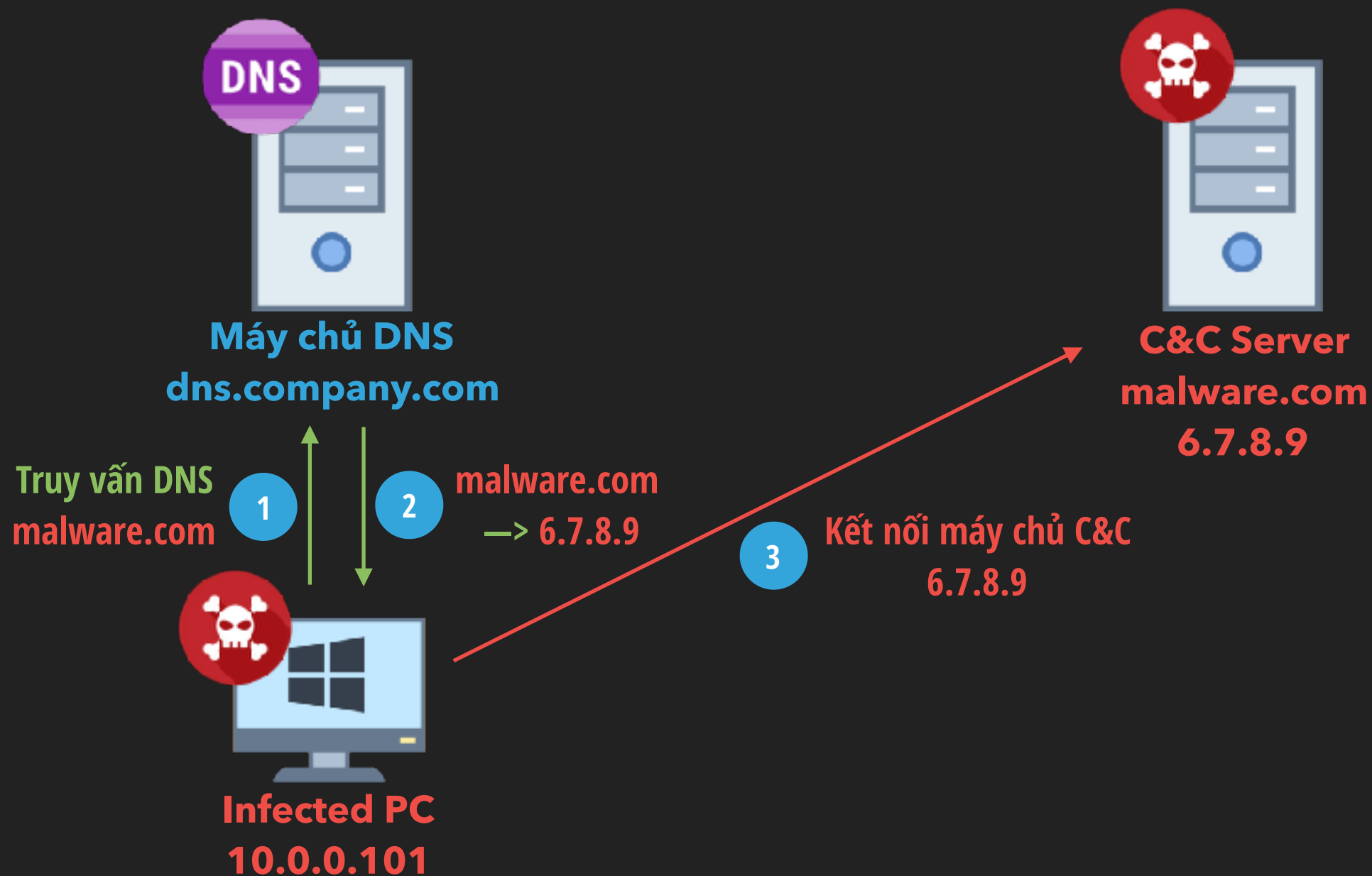
- ▶ Bài toán xây dựng máy chủ sinkhole
  - ▶ **Chuyển hướng** tên miền/IP độc hại
  - ▶ **Giả lập** máy chủ điều khiển
  - ▶ **Định danh** máy tính bị nhiễm
  - ▶ **Xử lý** gỡ bỏ mã độc

## CHUYỂN HƯỚNG TÊN MIỀN/IP ĐỘC HẠI

- ▶ 03 phương pháp chuyển hướng
  - ▶ Mã độc sử dụng **DNS mặc định**, kết nối **tên miền điều khiển**
  - ▶ Mã độc sử dụng **DNS quốc tế**, kết nối **tên miền điều khiển**
  - ▶ Mã độc kết nối **IP điều khiển**

## CHUYỂN HƯỚNG TÊN MIỀN/IP ĐỘC HẠI

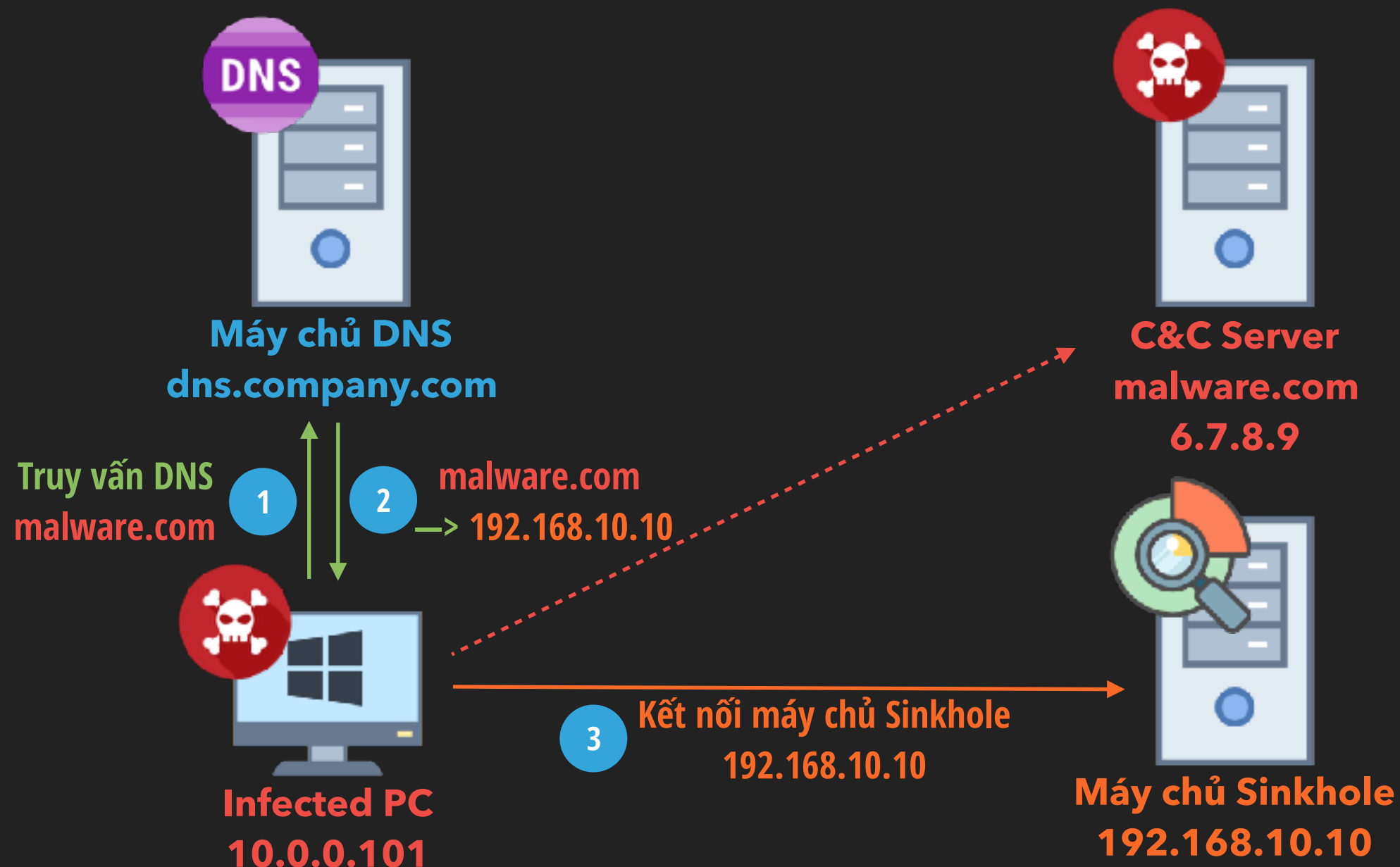
- ▶ Mã độc sử dụng **DNS mặc định**, kết nối **tên miền điều khiển**





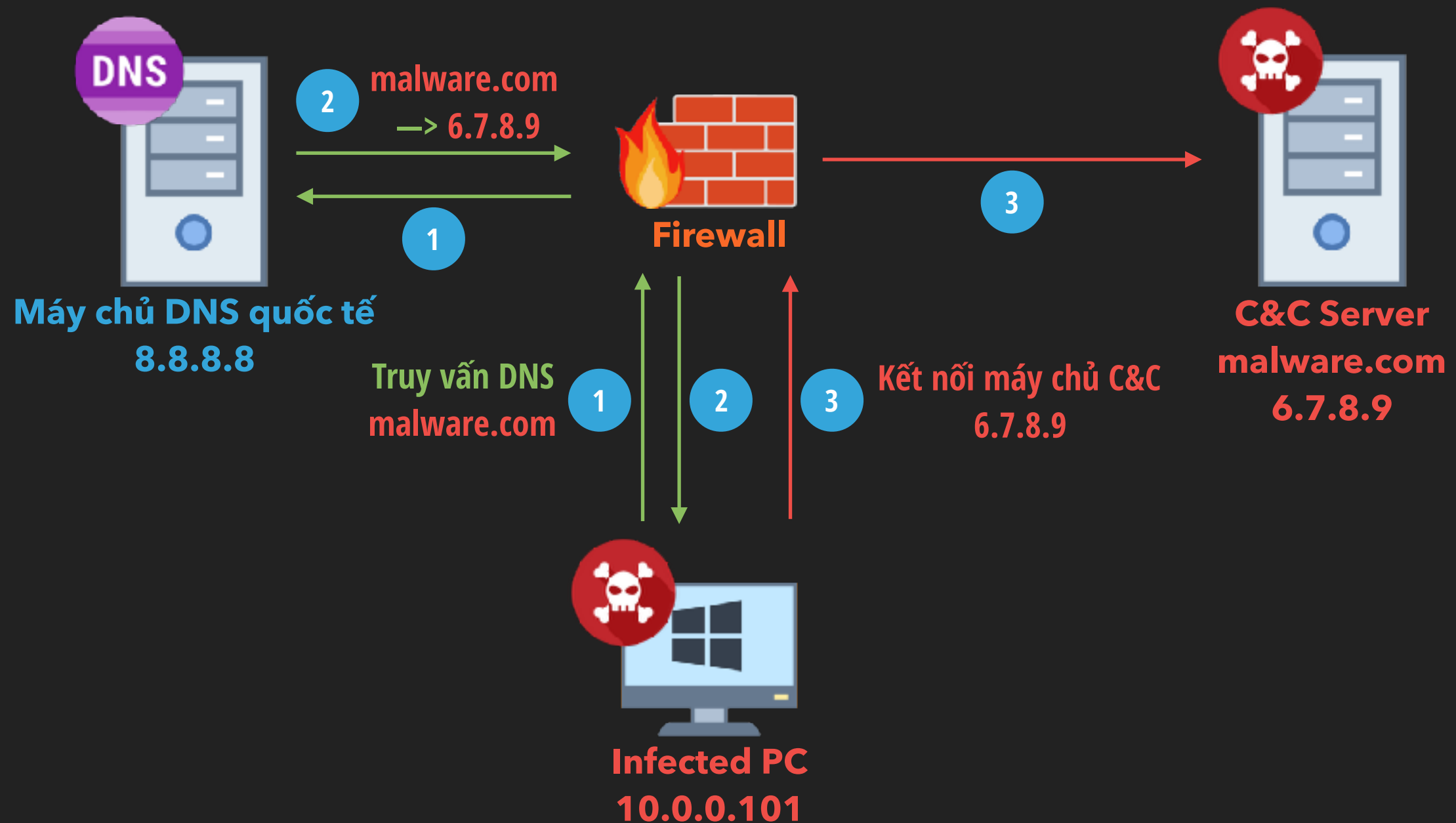
## CHUYỂN HƯỚNG TÊN MIỀN/IP ĐỘC HẠI

- ▶ Mã độc sử dụng **DNS mặc định**, kết nối **tên miền điều khiển**



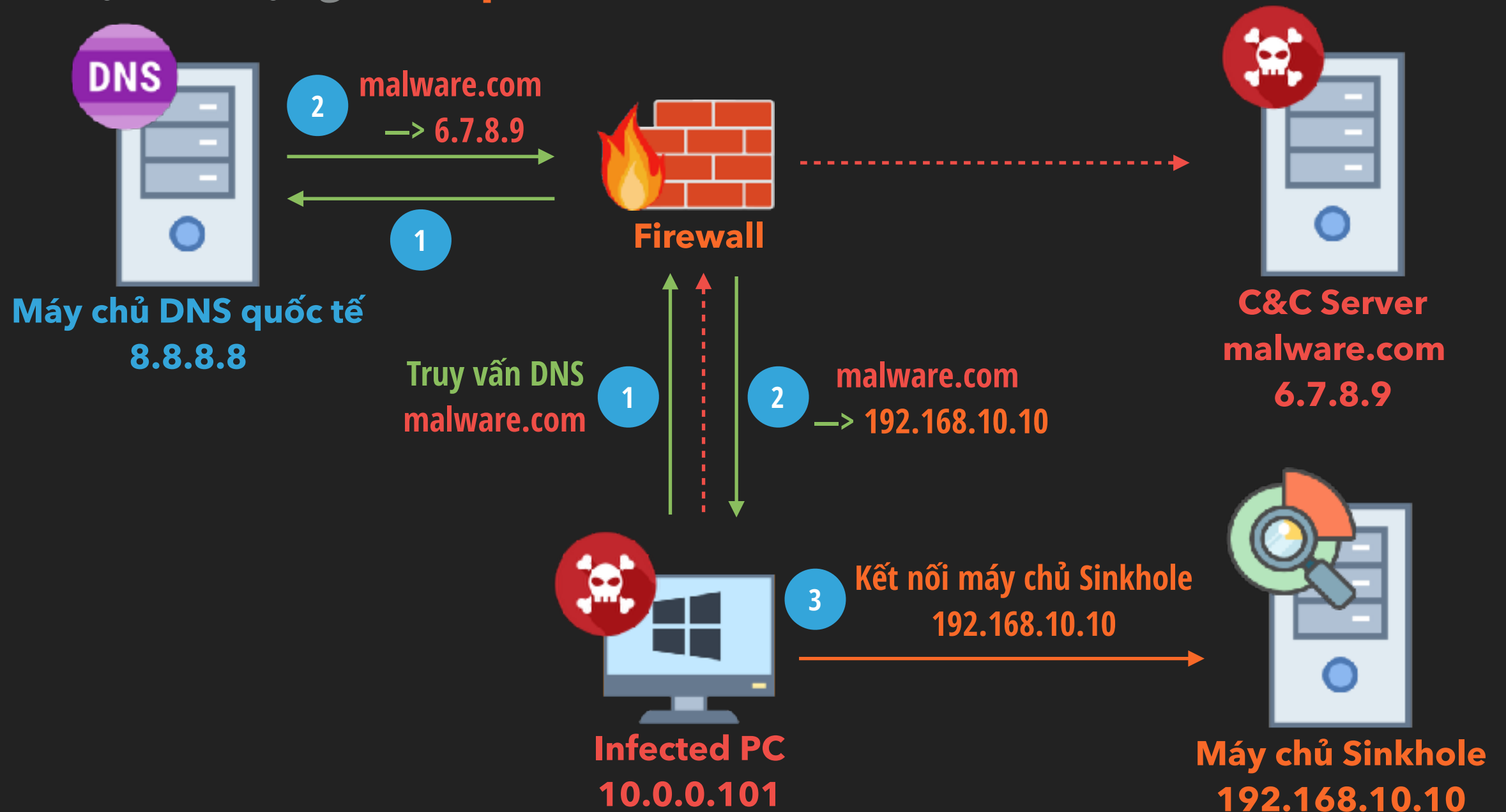
## CHUYỂN HƯỚNG TÊN MIỀN/IP ĐỘC HẠI

- ▶ Mã độc sử dụng **DNS quốc tế**, kết nối **tên miền điều khiển**



## CHUYỂN HƯỚNG TÊN MIỀN/IP ĐỘC HẠI

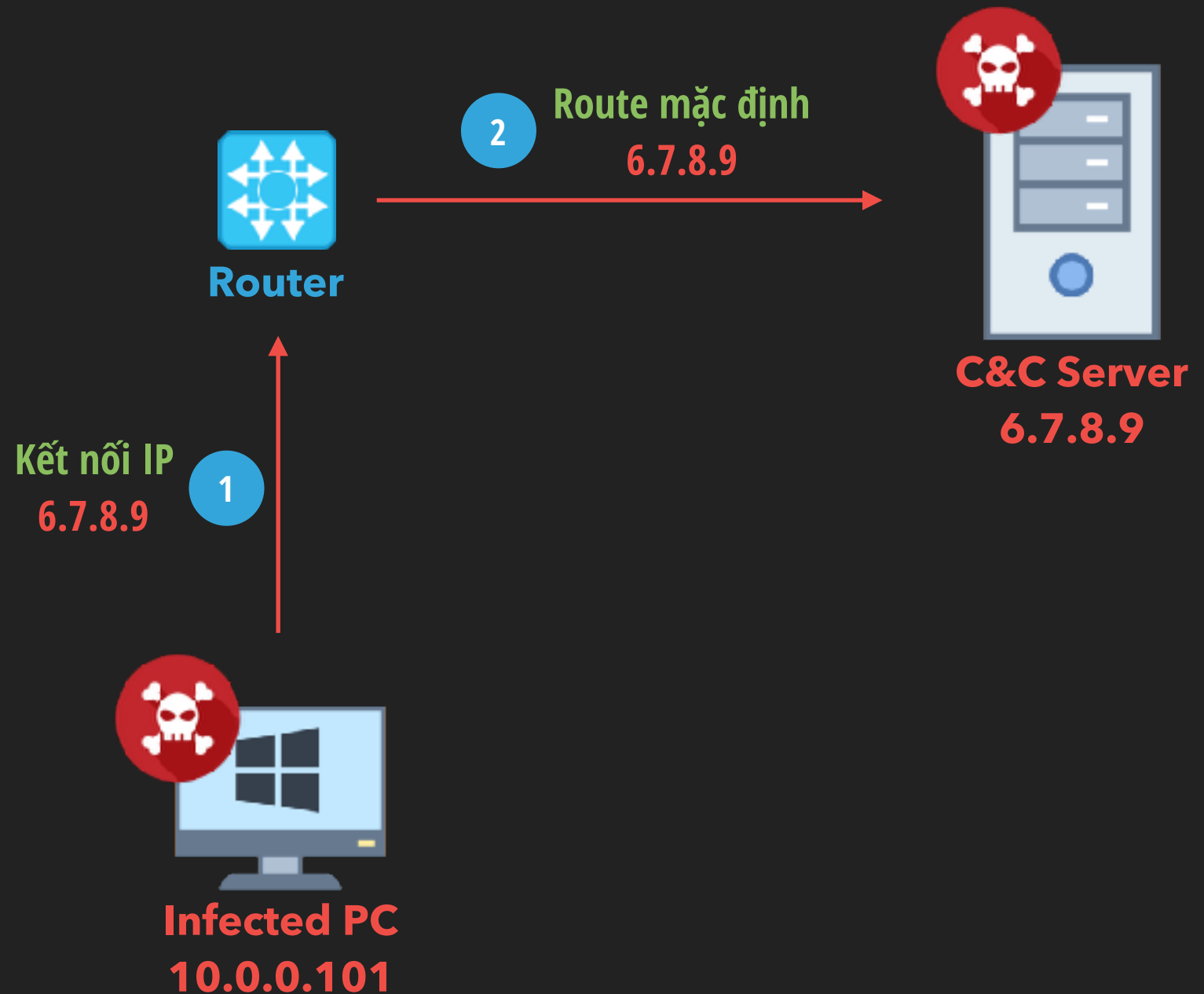
- ▶ Mã độc sử dụng **DNS quốc tế**, kết nối **tên miền điều khiển**





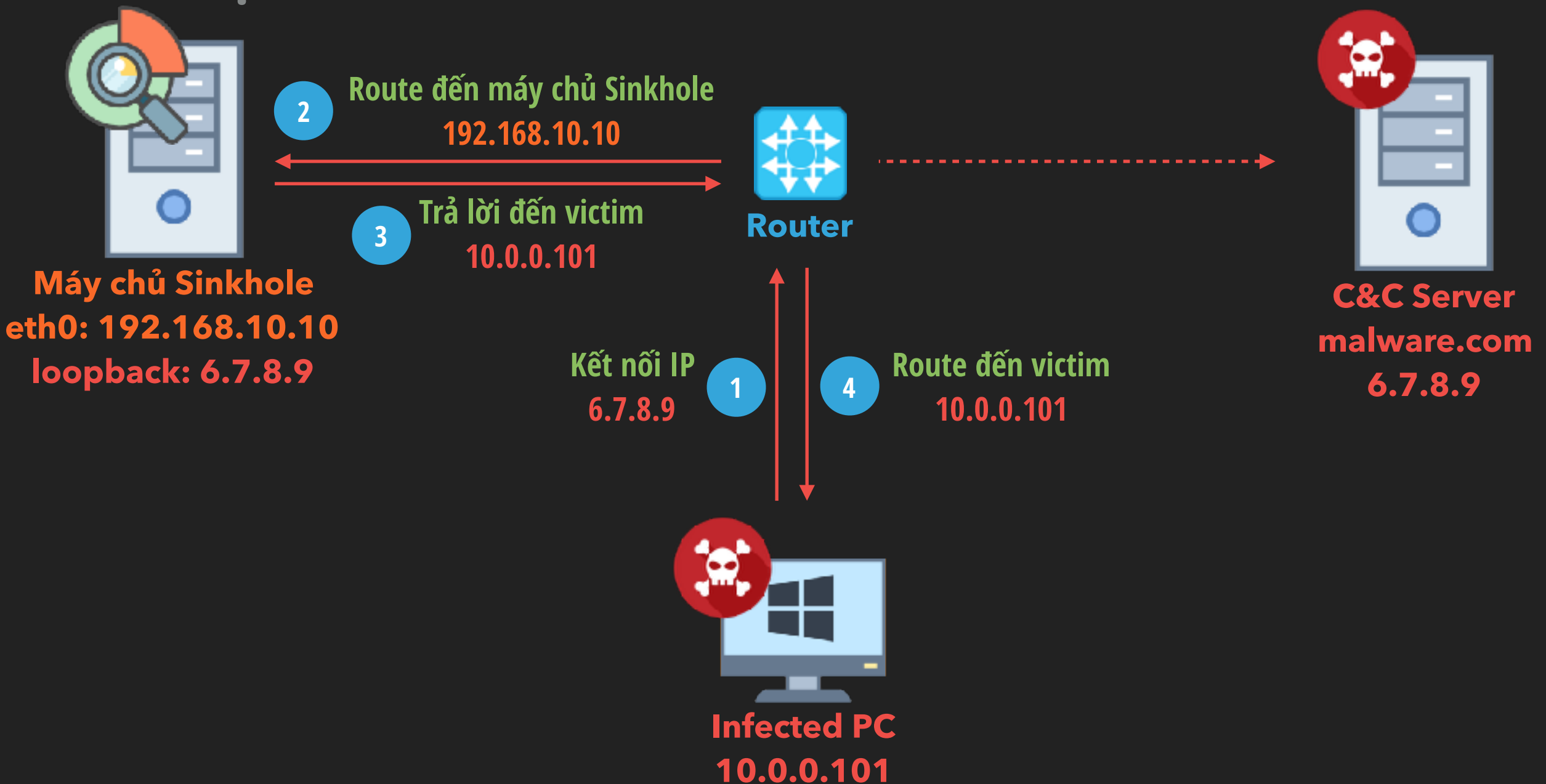
## CHUYỂN HƯỚNG TÊN MIỀN/IP ĐỘC HẠI

### ► Mã độc kết nối IP điều khiển



## CHUYỂN HƯỚNG TÊN MIỀN/IP ĐỘC HẠI

### ► Mã độc kết nối IP điều khiển



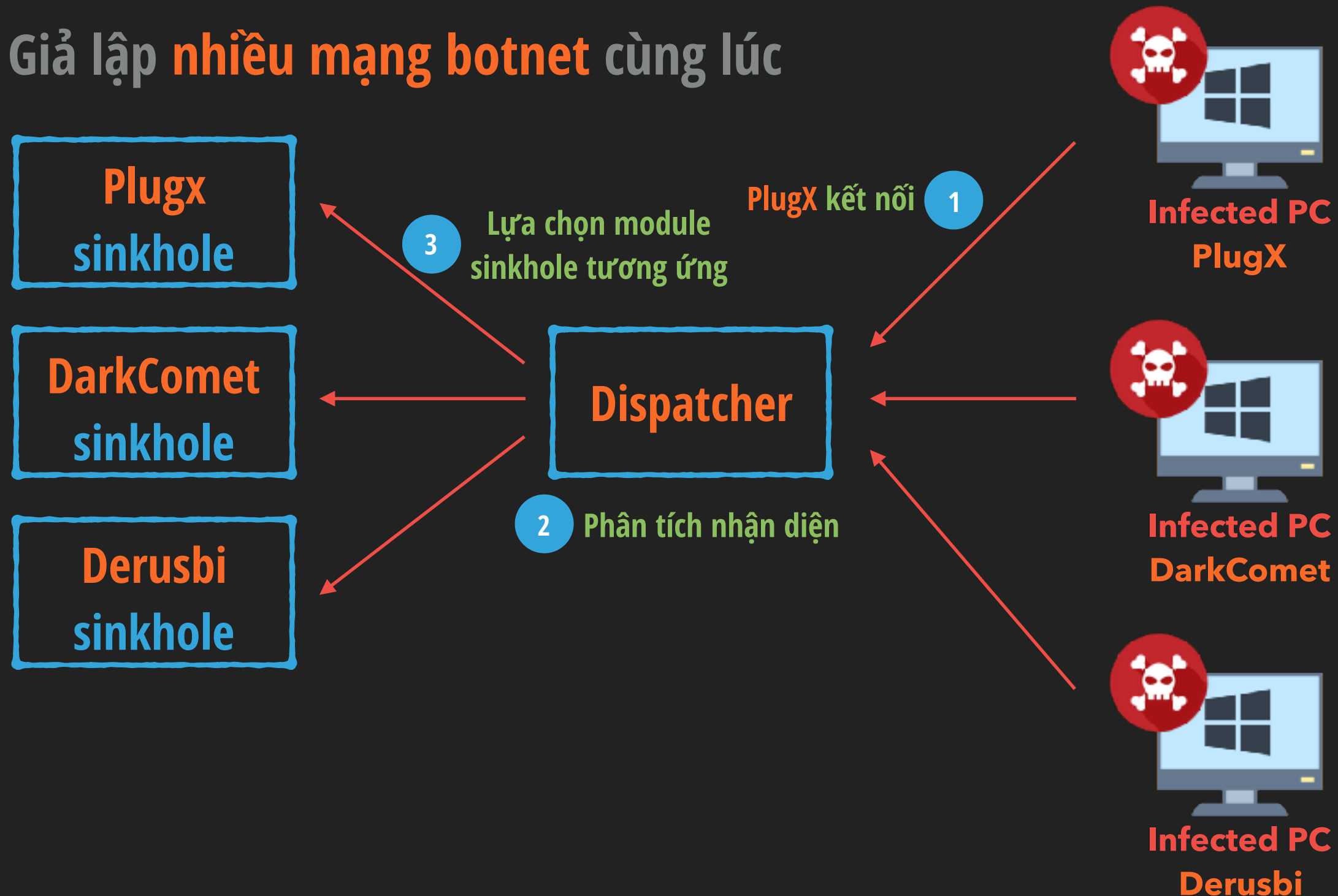
## MÁY CHỦ SINKHOLE

- ▶ **Giả lập** máy chủ điều khiển
  - ▶ **Unpack** mã độc (nếu cần)
  - ▶ **Dịch ngược** mã độc
  - ▶ Xây dựng **protocol** điều khiển



## MÁY CHỦ SINKHOLE

- ▶ Giả lập **nhiều mạng botnet** cùng lúc



## MÁY CHỦ SINKHOLE

- ▶ **Định danh** máy tính bị nhiễm
  - ▶ Sử dụng các lệnh điều khiển của mã độc
  - ▶ Một số lệnh hữu ích
    - ▶ **Lấy thông tin máy tính** (Computer Name, User name, RAM, CPU, IP Address, MAC...)
    - ▶ **Liệt kê thư mục** (Thư mục người dùng, nội dung các phân vùng...)
    - ▶ **Thực thi phần mềm** (hiển thị thông báo)

## MÁY CHỦ SINKHOLE

- ▶ **Xử lý** gỡ bỏ mã độc (1)
  - ▶ Sử dụng các lệnh điều khiển của mã độc
    - ▶ **Thực thi phần mềm** (công cụ gỡ bỏ mã độc)
    - ▶ **Update bản thân**



## MÁY CHỦ SINKHOLE

- ▶ **Xử lý** gỡ bỏ mã độc (2)
  - ▶ Lấy mẫu, cập nhật signature cho phần mềm diệt virus
    - ▶ Sử dụng các lệnh điều khiển của mã độc
      - ▶ **Upload file** (file thực thi của mã độc)
  - ▶ Helpdesk xử lý thủ công sau khi định danh được máy tính



by hackers - for hackers

# TRÀ ĐÁ #5 HACKING

29/09/2017 - DA NANG



Organized By



<http://trada.vnsecurity.net>

# PLUGX

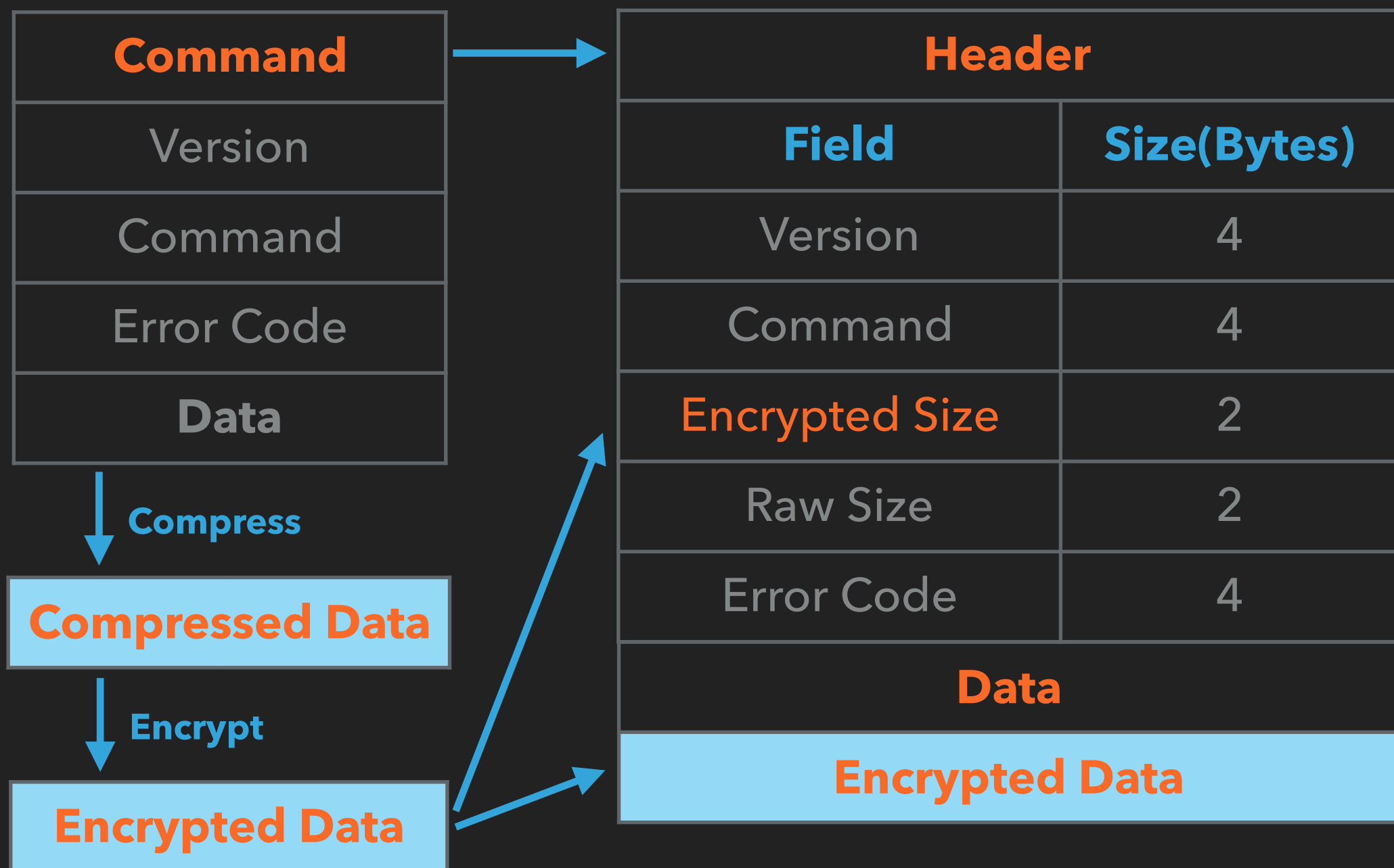
## MÃ ĐỘC PLUGX

### ▶ PlugX

- ▶ RAT (Remote Administration Tool)
- ▶ Nguồn gốc Trung Quốc
- ▶ Sử dụng phổ biến trong các cuộc tấn công có chủ đích nhắm vào Việt Nam

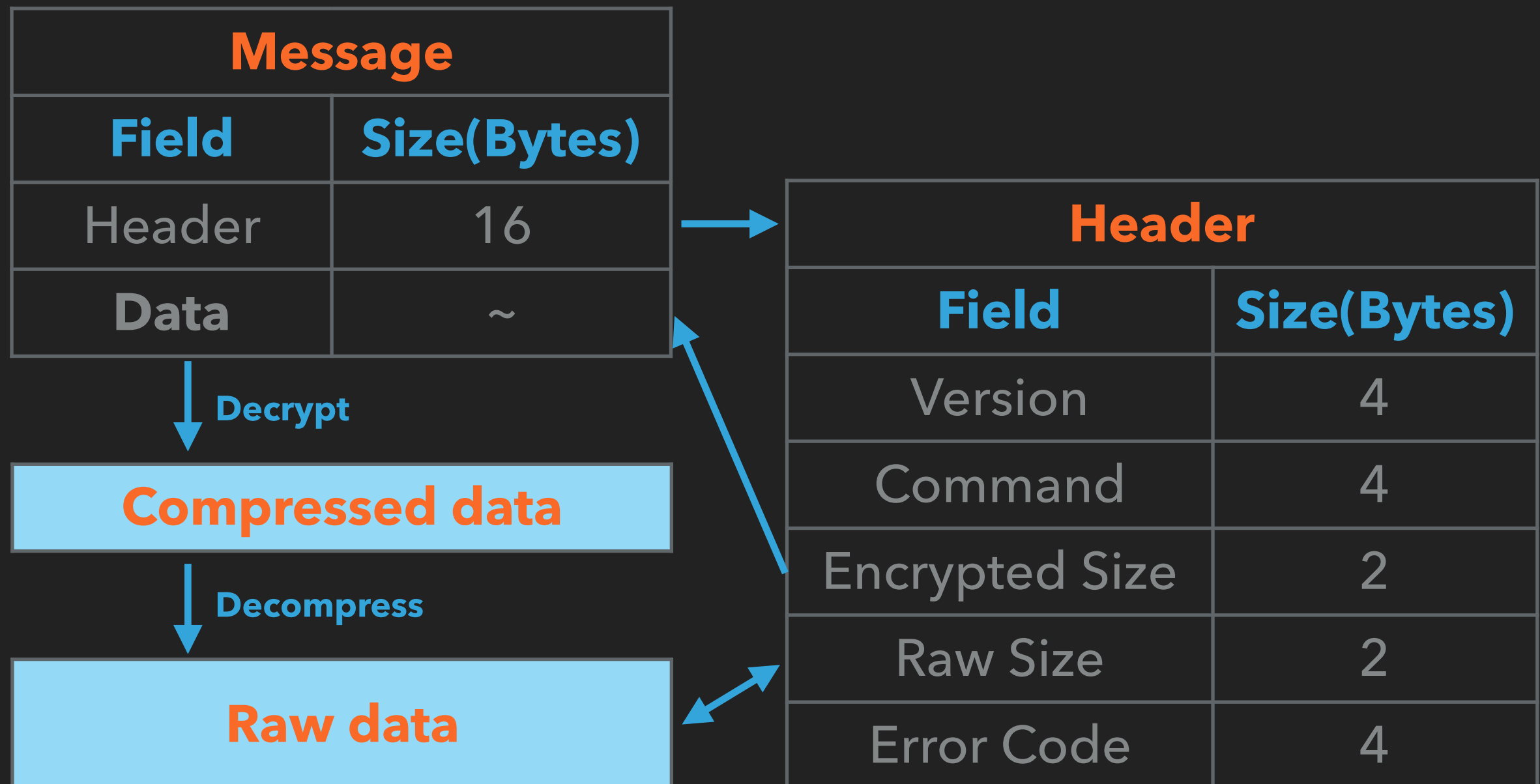
## MÃ ĐỘC PLUGX

### ► Protocol - Request đến mã độc



## MÃ ĐỘC PLUGX

### ► Protocol - Response từ mã độc



## MÃ ĐỘC PLUGX

### ▶ Protocol

- ▶ Thông tin về máy tính bị nhiễm
  - ▶ Tên máy tính
  - ▶ RAM, CPU
  - ▶ Username
  - ▶ Địa chỉ IP



## MÃ ĐỘC PLUGX

### ▶ **Commands**

#### ▶ Disk

- ▶ Lấy danh sách các ổ đĩa
- ▶ Liệt kê thư mục
- ▶ Tạo/sửa file
- ▶ Thực thi file
- ▶ Download/upload file

## MÃ ĐỘC PLUGX

- ▶ **Commands**

- ▶ Option

- ▶ Lock máy (Windows + L)
    - ▶ Logoff/Reboot/Shutdown
    - ▶ Hiển thị thông báo

## MÃ ĐỘC PLUGX

### ▶ **Commands**

- ▶ Keylog - Thu thập log gõ bàn phím
- ▶ Nethood - Thu thập thông tin về tài nguyên mạng
- ▶ Portmap - Tunnel kết nối
- ▶ Process - Quản lý các tiến trình
- ▶ Regedit - Quản lý regedit

## MÃ ĐỘC PLUGX

### ▶ **Commands**

- ▶ Screen - Chụp ảnh, theo dõi màn hình
- ▶ Service - Quản lý các service
- ▶ Shell - Command line
- ▶ SQL - Quản lý cơ sở dữ liệu SQL
- ▶ Telnet - Thực hiện telnet

## MÃ ĐỘC PLUGX

- ▶ Một số **tên miền điều khiển**
  - ▶ dubkill [.] com
  - ▶ phimnoi [.] org
  - ▶ dcsvn [.] org
  - ▶ anninhthoquoc [.] com
  - ▶ ...



by hackers - for hackers

# TRÀ ĐÁ #5 HACKING

29/09/2017 - DA NANG

Organized By



<http://trada.vnsecurity.net>

# DEMO





by hackers - for hackers

# TRÀ ĐÁ #5 HACKING

29/09/2017 - DA NANG

Organized By



<http://trada.vnsecurity.net>

# THANK YOU!