

# Một số kỹ thuật giả dạng dữ liệu mạng của mã độc

Trần Minh Quảng

*Trưởng phòng Mã độc và khai thác lỗi*

*Công ty An ninh mạng Viettel*

1

# Nội dung

Giới thiệu

Botnet

Các giao thức điều khiển thường gặp

Một số kỹ thuật giả dạng dữ liệu mạng

Demo





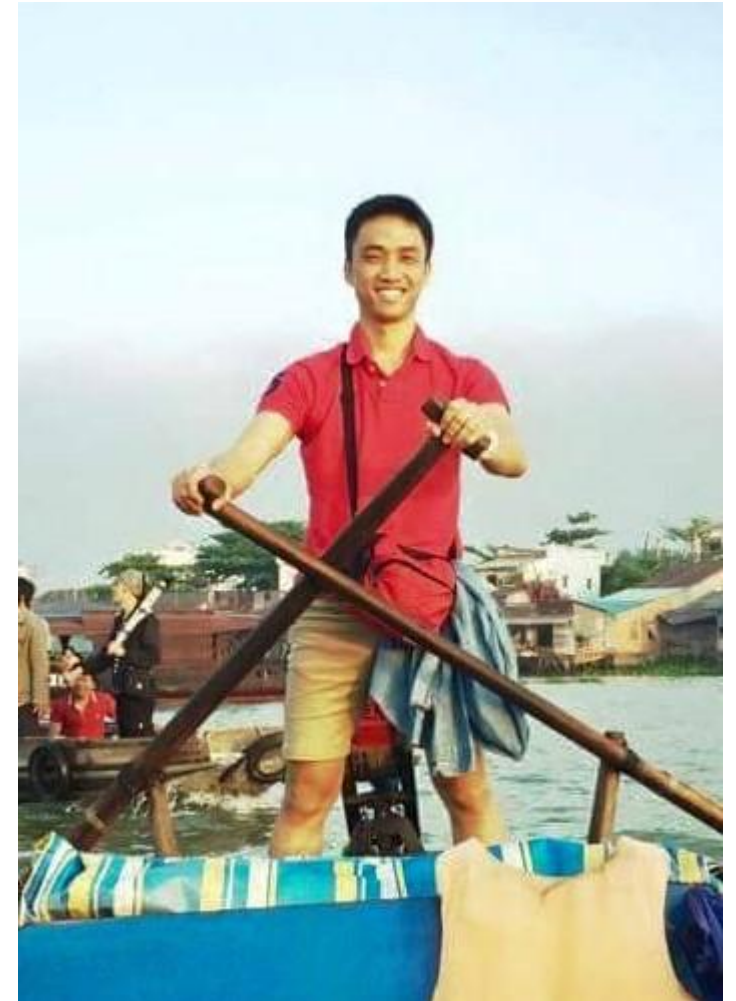
# Giới thiệu

**Một số kỹ thuật giả dạng dữ liệu mạng của mã độc**

Trần Minh Quảng - Công ty An ninh mạng Viettel

# Về tôi

- Nghiên cứu
  - Dịch ngược
  - Mã độc
- Trình bày hội thảo
  - #tradahacking
  - TetCon
  - Security BootCamp
  - ...
- Công ty An ninh mạng Viettel





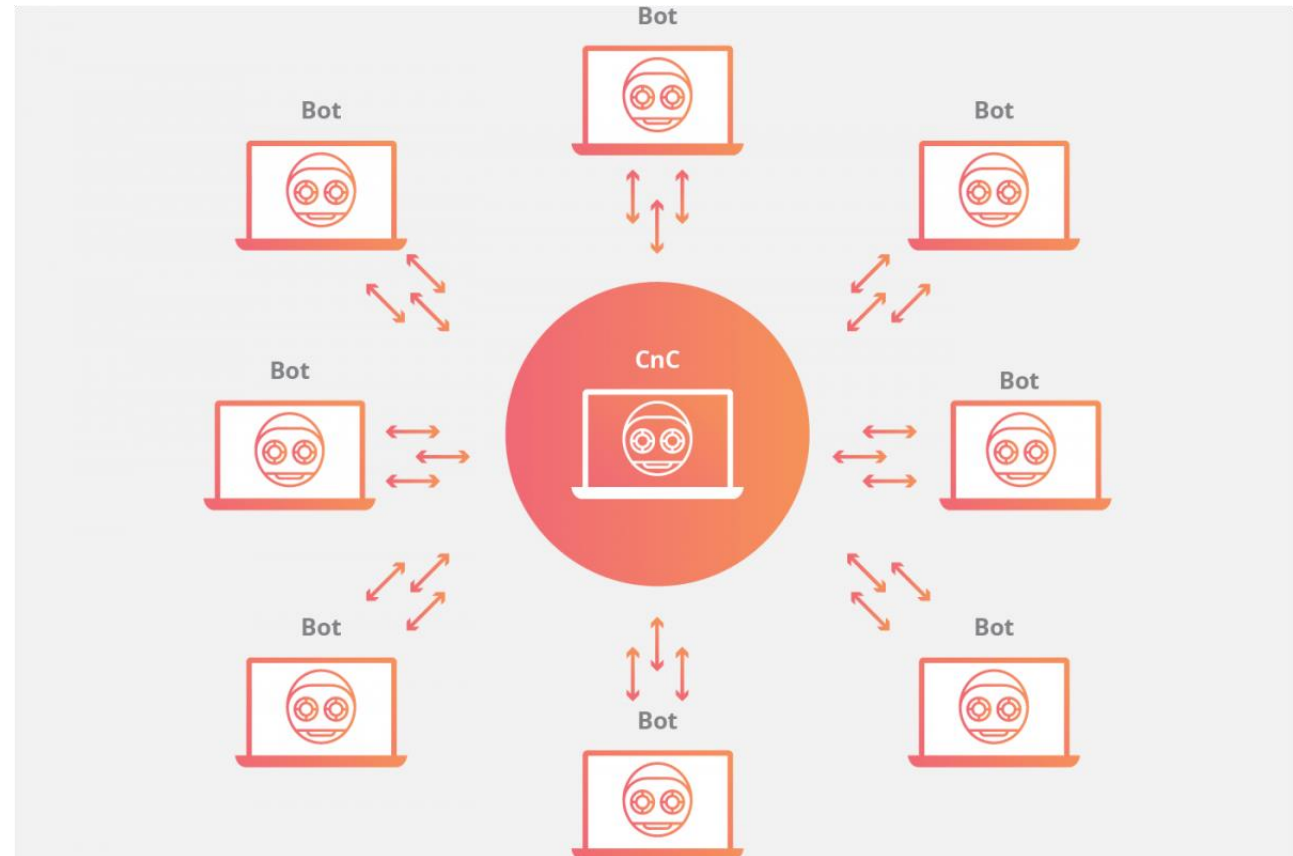
# Botnet

**Một số kỹ thuật giả dạng dữ liệu mạng của mã độc**

Trần Minh Quảng - Công ty An ninh mạng Viettel

# Một số khái niệm mã độc

- Botnet
  - Lay nhiễm trên nhiều máy tính
  - Kết nối về máy chủ điều khiển
  - Ra lệnh tập trung
- Máy chủ điều khiển (Command & Control Server - C&C/C2)
- Bot (zombie/victim)
  - Kết nối đến C&C nhận lệnh thực hiện





# Các giao thức điều khiển thường gặp

Một số kỹ thuật giả dạng dữ liệu mạng của mã độc

Trần Minh Quảng - Công ty An ninh mạng Viettel



# Các giao thức điều khiển thường gặp

- TCP (Transmission Control Protocol)
  - Hoạt động có trạng thái
    - Thiết lập kết nối
    - Truyền dữ liệu
    - Kết thúc kết nối
- UDP (User Datagram Protocol)
  - Phi trạng thái
  - Dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo
  - Nhanh hơn TCP
- Dữ liệu được truyền theo một định dạng thống nhất giữa **Bot** và **C&C server**





# Các giao thức điều khiển thường gặp

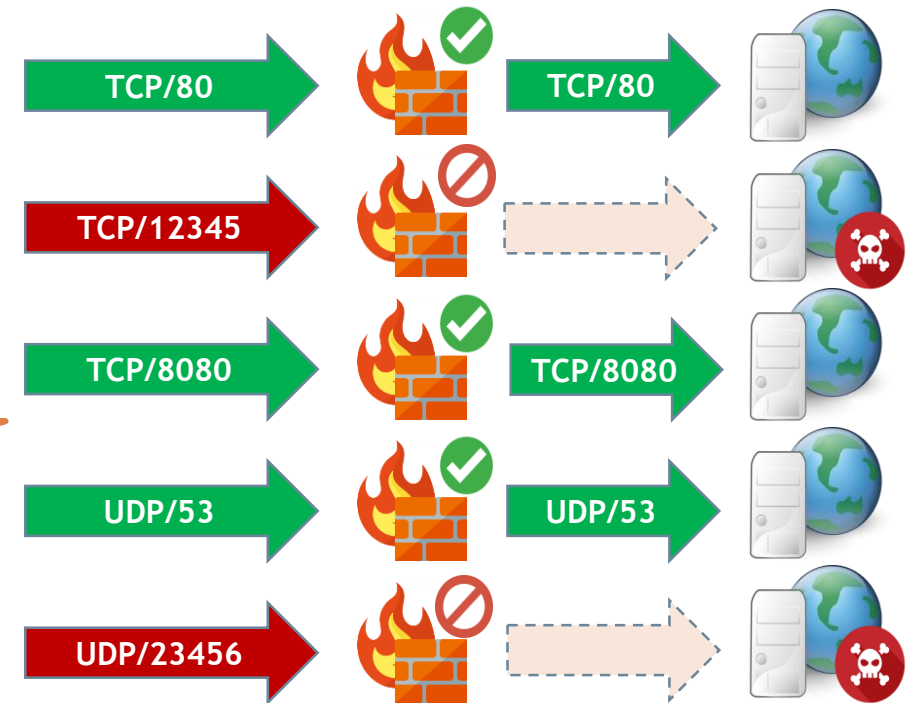
- **Cách thức phòng chống**

- Cấu hình tường lửa chỉ cho phép máy tính kết nối đến một số cổng xác định
- Kiểm soát nội dung dữ liệu phải phù hợp với cổng sử dụng

- **Cách thức vượt qua**

- Sử dụng các cổng phổ biến làm cổng giao tiếp (80/8080/443/53...)

▪ **Giả dạng các định dạng dữ liệu**



10

# Một số kỹ thuật giả dạng dữ liệu mạng

Một số kỹ thuật giả dạng dữ liệu mạng của mã độc  
Trần Minh Quảng - Công ty An ninh mạng Viettel

# Một số kỹ thuật giả dạng dữ liệu mạng

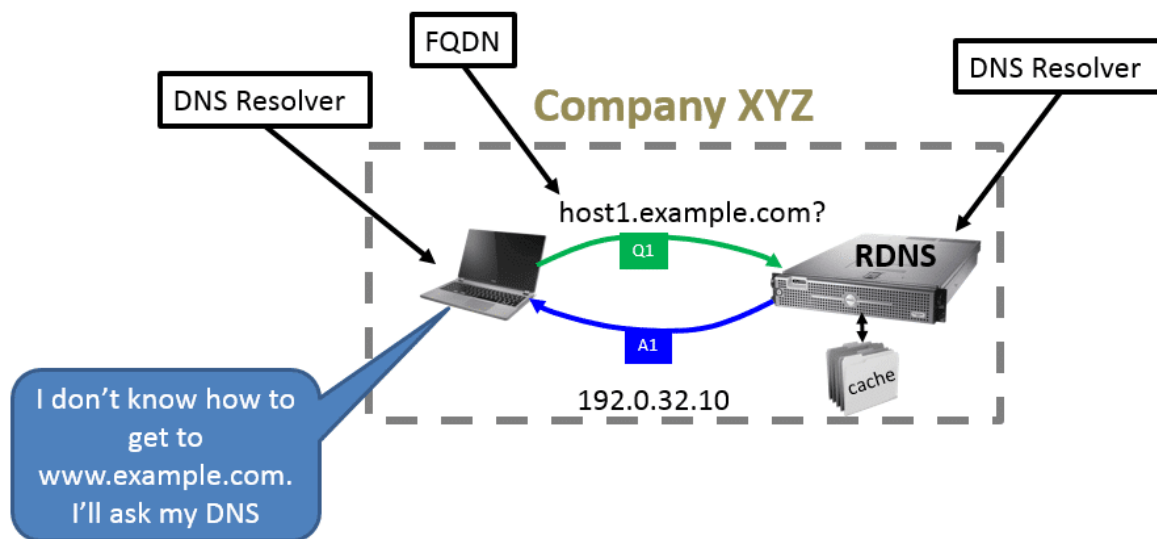
- Giả dạng HTTP
  - Giấu dữ liệu vào các thẻ html
  - VD: tự định nghĩa thẻ riêng <maldata>



# Một số kỹ thuật giả dạng dữ liệu mạng

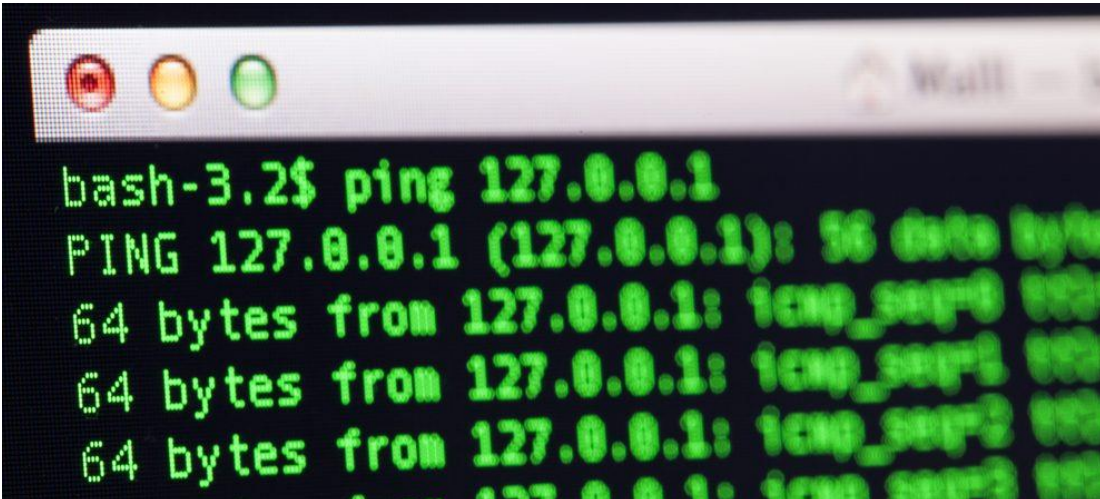
- **Giả dạng DNS**

- Sử dụng loại truy vấn TXT
- Giấu dữ liệu vào trường **question** và **answer** trong giao thức truy vấn DNS



# Một số kỹ thuật giả dạng dữ liệu mạng

- Giả dạng ICMP (Ping)
  - Giấu dữ liệu vào phần “Ping data”

A terminal window with a dark background and green text. The window title bar shows standard macOS window controls (red, yellow, green buttons) and a title "Wall - 3". The terminal text shows a user running a ping command: "bash-3.2\$ ping 127.0.0.1". The output shows "PING 127.0.0.1 (127.0.0.1): 36 data bytes" followed by three lines of "64 bytes from 127.0.0.1: icmp\_seq=0 0.000ms", "64 bytes from 127.0.0.1: icmp\_seq=1 0.000ms", and "64 bytes from 127.0.0.1: icmp\_seq=2 0.000ms".

```
bash-3.2$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 36 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 0.000ms
64 bytes from 127.0.0.1: icmp_seq=1 0.000ms
64 bytes from 127.0.0.1: icmp_seq=2 0.000ms
```

