



**nic.br**

Núcleo de Informação  
e Coordenação do  
Ponto BR

**cgib.br**

Comitê Gestor da  
Internet no Brasil



**registro.br cert.br cetic.br ceptro.br ceweb.br ix.br**

nic.br cgi.br

ceptro.br

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is dense and covers the entire area.

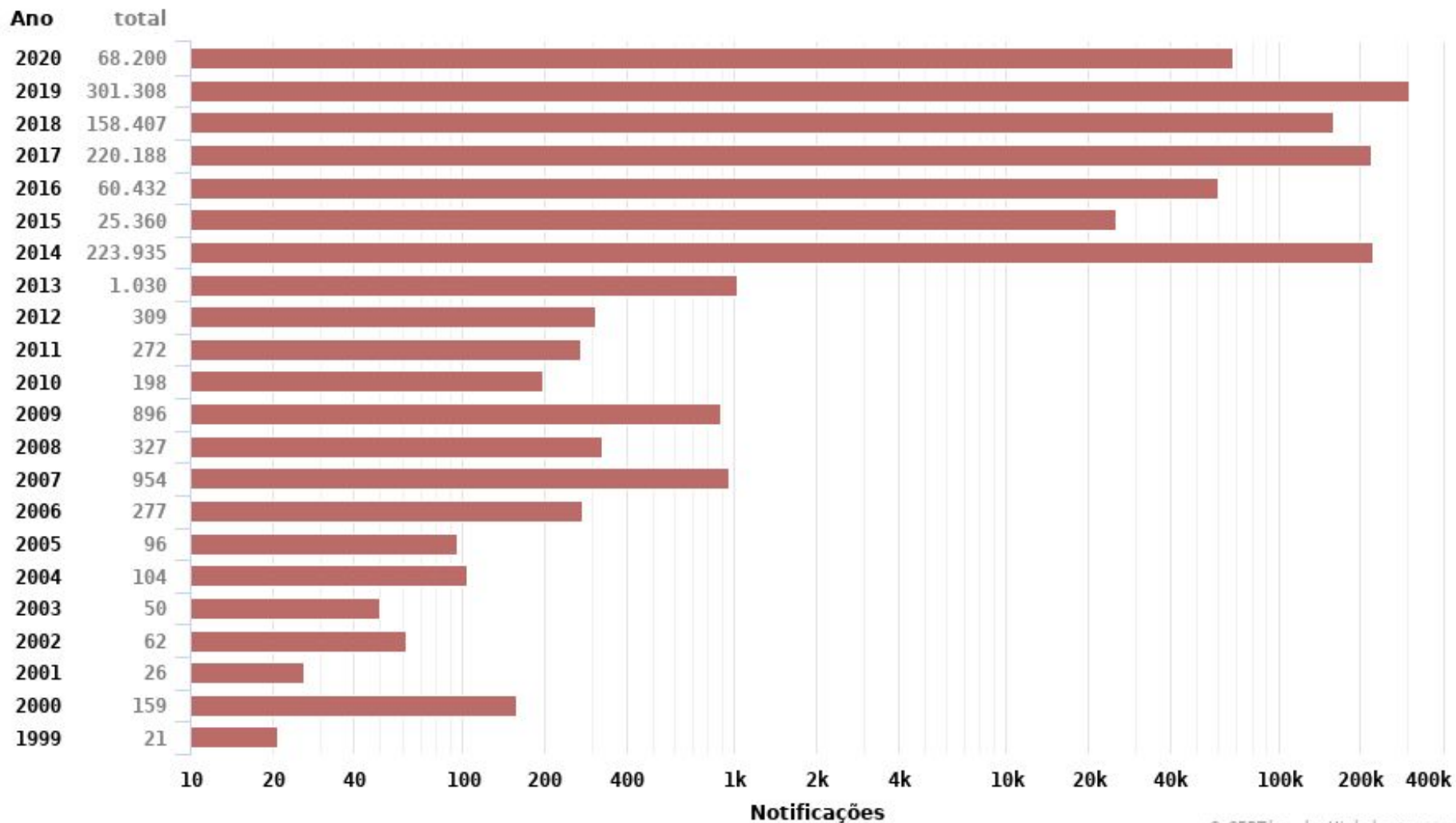
# MANRS

Mutually Agreed Norms for Routing  
Security

ceptro.br nic.br egi.br

# DDoS ao Longo do Tempo

## Notificações sobre equipamentos participando em ataques DoS



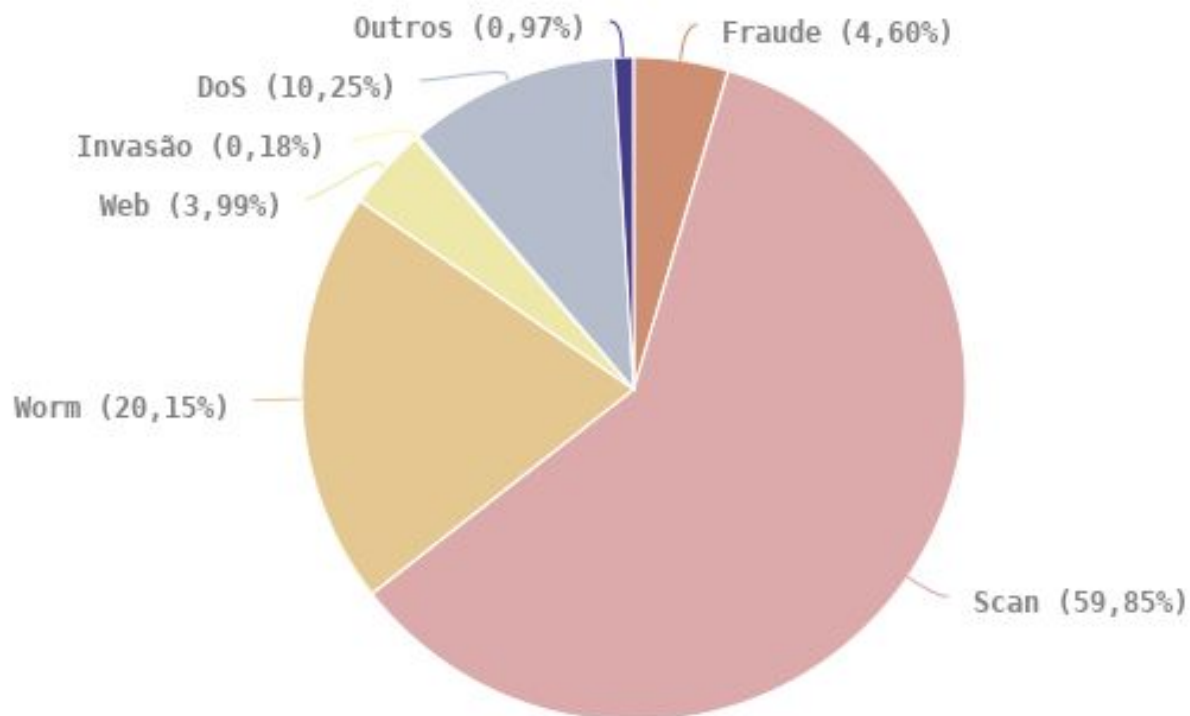
© CERT.br -- by Highcharts.com



# Características dos Ataques

**Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2020**

Tipos de ataque

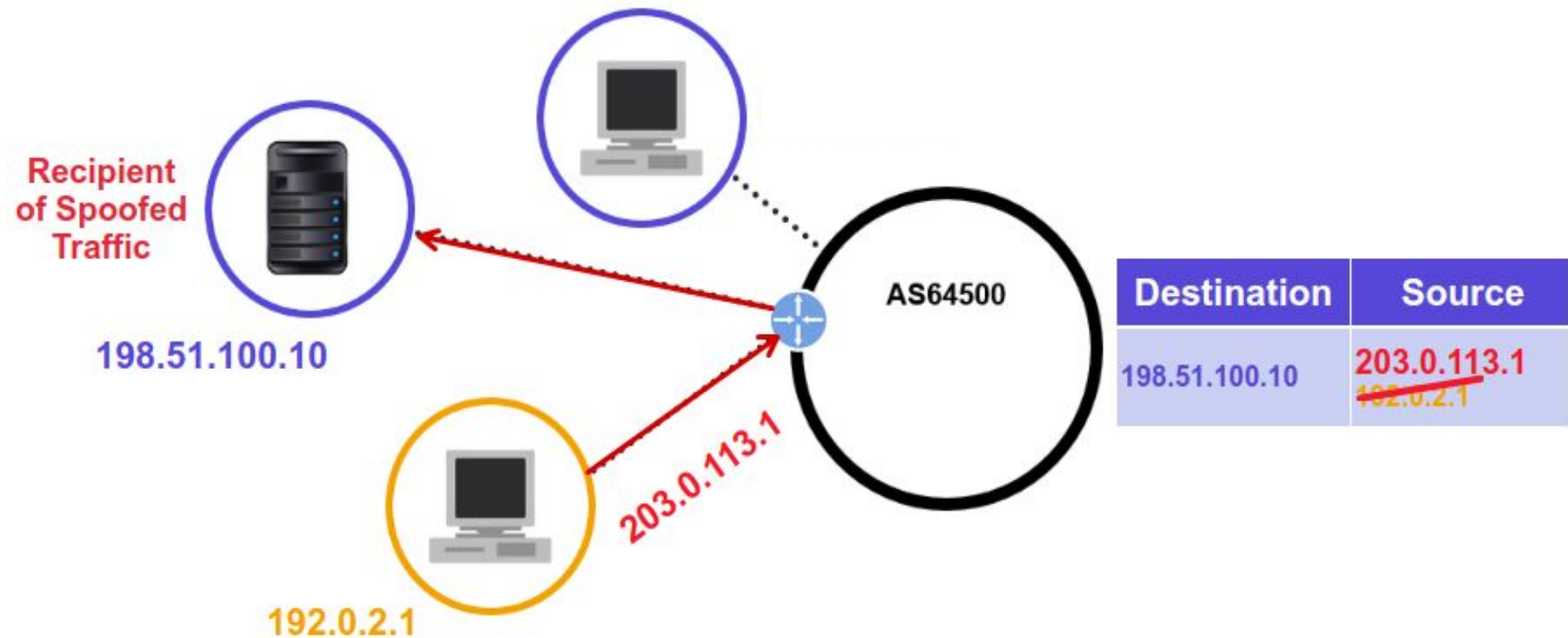


© CERT.br – by Highcharts.com

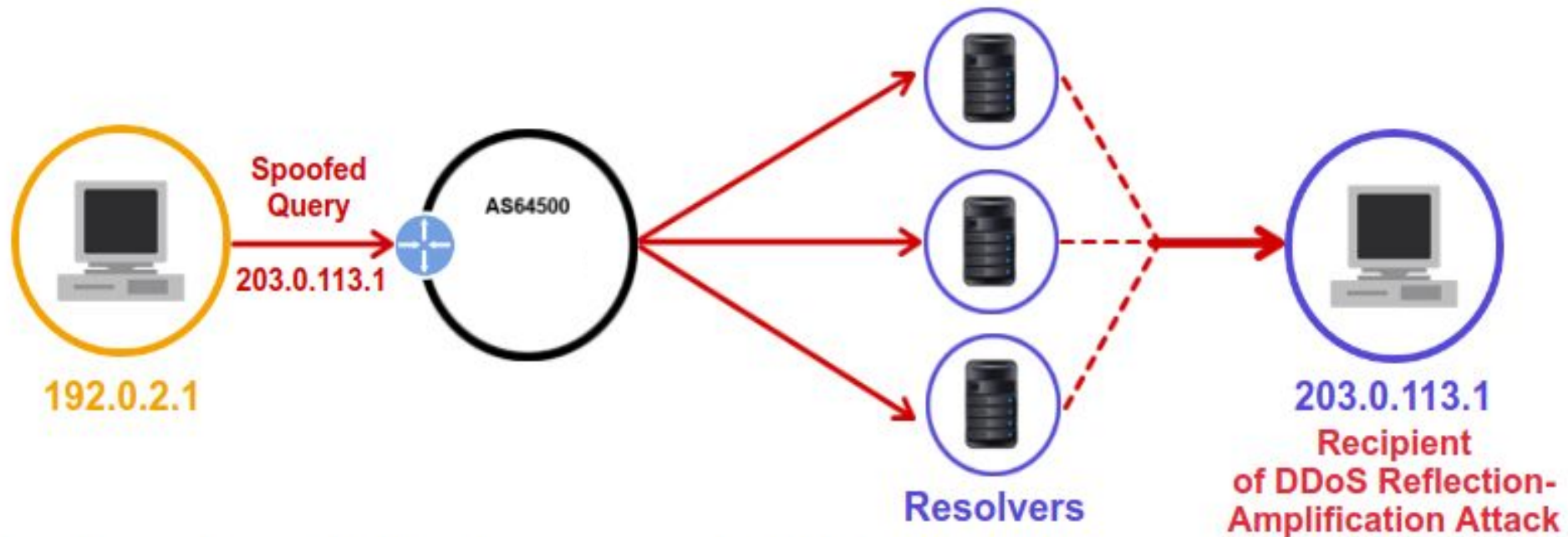
# O que é spoofing?

- Pacotes IP com endereços de origem incorretos
  - **Erro de configuração**
    - Problema de Software
  - **Teste e Simulação**
    - Teste de Performance
  - **Atitude maliciosa**
    - Esconder a identidade do atacante
    - Fingir ser outro computador na rede
- O spoofing pode ser usado em ataques de negação de serviço e é um problema sério na Internet

# Como funciona o ataque spoofing



# Como funciona o ataque reflexão-amplificação





# Fatores de amplificação

Protocolo	Fator de Amplificação	Comando Vulnerável
DNS	28 a 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
LDAP / CLDAP	46 a 70	Malformed request
SSDP	30.8	SEARCH request
Chargen	358.8	Character generation request

# Total de ASNs e IPs Notificados pelo CERT.br

Mês	DNS		SNMP		NTP		SSDP		Portmap		Ubiquiti	
	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2020-08	3.261	63.398	3.191	83.327	1.131	69.764	770	15.579	1.647	10.844	1.274	15.503
2020-09	3.193	54.958	3.172	81.526	1.143	70.447	720	15.395	1.627	12.073	1.208	12.596
2020-10	3.247	54.648	3.253	86.907	1.128	70.329	818	19.746	1.654	12.264	1.147	10.771
2020-11	3.268	52.582	3.231	83.917	1.161	72.123	803	20.592	1.635	11.907	1.104	9.440
2020-12	3.253	55.852	3.200	81.773	1.186	71.765	812	21.070	1.623	11.258	1.041	8.654
2021-01	3.243	61.129	3.206	80.996	1.194	70.290	785	19.191	1.642	11.438	1.034	8.187
2021-02	3.252	64.200	3.188	78.482	1.191	71.413	771	18.584	1.614	11.134	996	7.702
2021-03	3.225	63.207	3.252	80.335	1.220	69.490	773	22.095	1.626	9.724	937	7.181
2021-04	3.259	59.877	3.305	78.657	1.221	71.816	791	19.001	1.647	9.704	902	6.361
2021-05	3.241	62.856	3.345	80.922	1.239	71.958	773	20.064	1.612	9.312	886	6.458
2021-06	3.279	57.252	3.402	79.712	1.200	71.987	765	19.345	1.628	11.407	857	6.539
2021-07	3.214	46.520	3.372	76.858	1.222	73.758	739	17.893	1.640	9.681	873	6.528

# Ferramentas de Linha de Comando

## DNS

**DIG** – <https://www.isc.org/community/tools/>

- nativo em Linux, \*BSD, MacOS e parte do BIND para Windows
- versões *online*, ex: <http://www.geektools.com/digtool.php>

```
$ dig +bufsize=4096 @<ip-servidor-aberto> <domínio> ANY
```

## NTP

```
$ ntpdc -n -c monlist <ip-servidor-aberto>
```

```
$ ntpq -c rv <ip-servidor-aberto>
```

## SNMP

```
$ snmpget -v 2c -c public <ip-servidor-aberto> iso.3.6.1.2.1.1.1.0
```

```
$ snmpctl snmp get <ip-servidor-aberto> oid iso.3.6.1.2.1.1.1.0
```

```
$ snmpwalk -v 2c -c public <ip-servidor-aberto>
```

## SSDP

```
$ printf "M-SEARCH *
```

```
HTTP/1.1\r\nHost:239.255.255.250:1900\r\nST:upnp:rootdevice\r\nMan:\"ssdp:discover\"\r\nMX:3\r\n\r\n" | nc -u <ip-servidor-aberto> 1900
```

## Chargen

```
$ echo | nc -u <ip-servidor-aberto> 19
```

# O que é MANRS?

- Mutually Agreed Norms for Routing Security
- É uma iniciativa global
- Apoio da ISOC
- Consiste em 4 coisas básicas
  - Filtros
  - Anti-Spoofing
  - Coordenação
  - Validação Global

# Porque utilizar filtros? Roubo de prefixos

Mutually Agreed Norms for Routing Security (MANRS) 27 April 2018

EN ES

What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum

Cryptocurrency Wallets

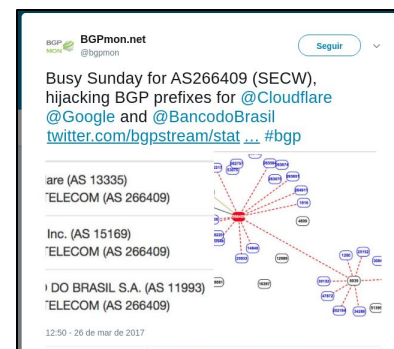
<https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>

Mutually Agreed Norms for Routing Security (MANRS) 28 August 2017

EN FR ES

Google leaked prefixes – and knocked Japan off the Internet

<https://www.internetsociety.org/blog/2017/08/google-leaked-prefixes-knocked-japan-off-internet/>



<https://twitter.com/bgpmon/status/846087079763177472>

Mutually Agreed Norms for Routing Security (MANRS) 15 November 2018

Route Leak Causes Major Google Outage

<https://www.internetsociety.org/blog/2018/11/route-leak-caused-a-major-google-outage/>

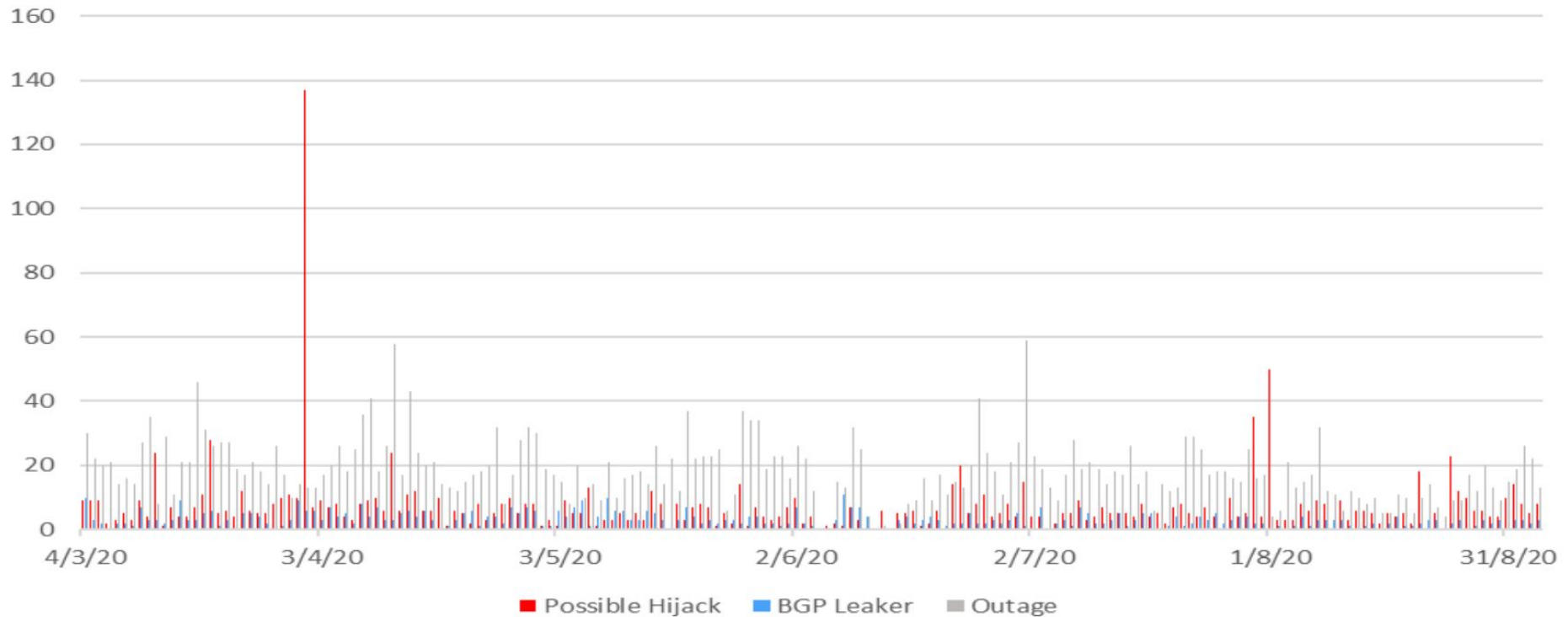


<https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/>

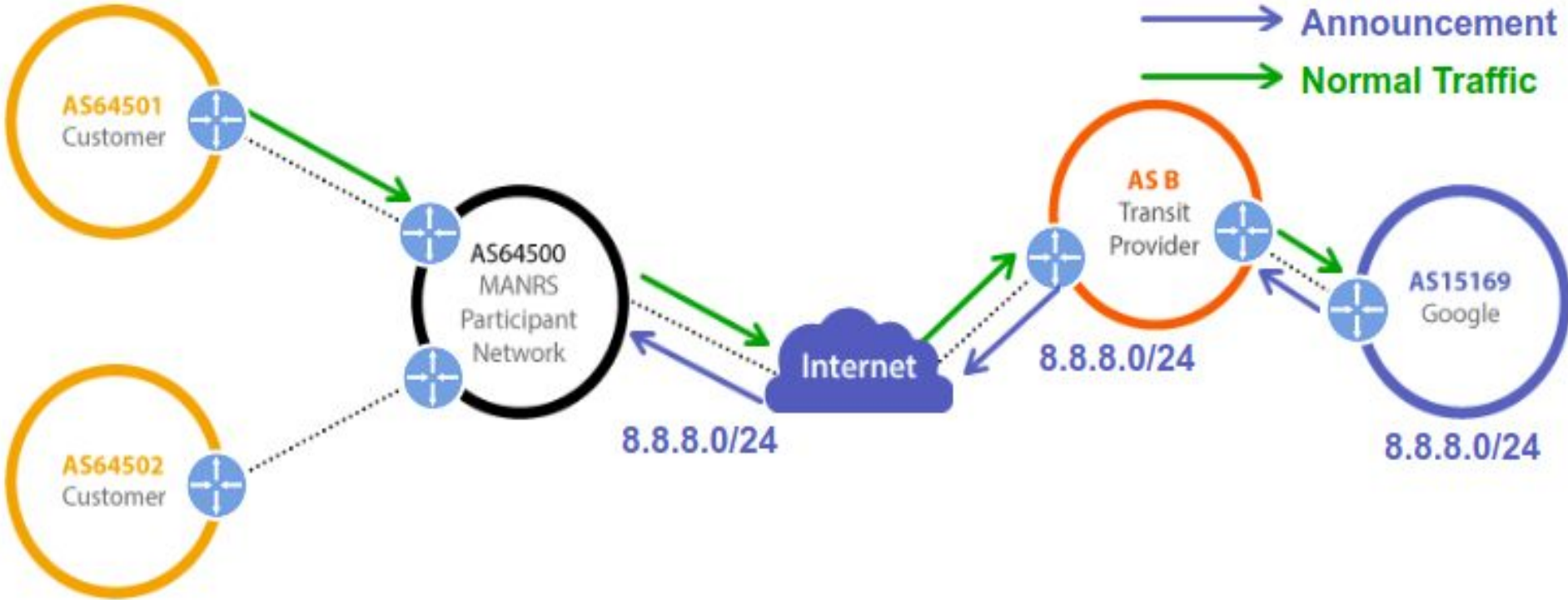


# Porque utilizar filtros? Roubo de prefixos

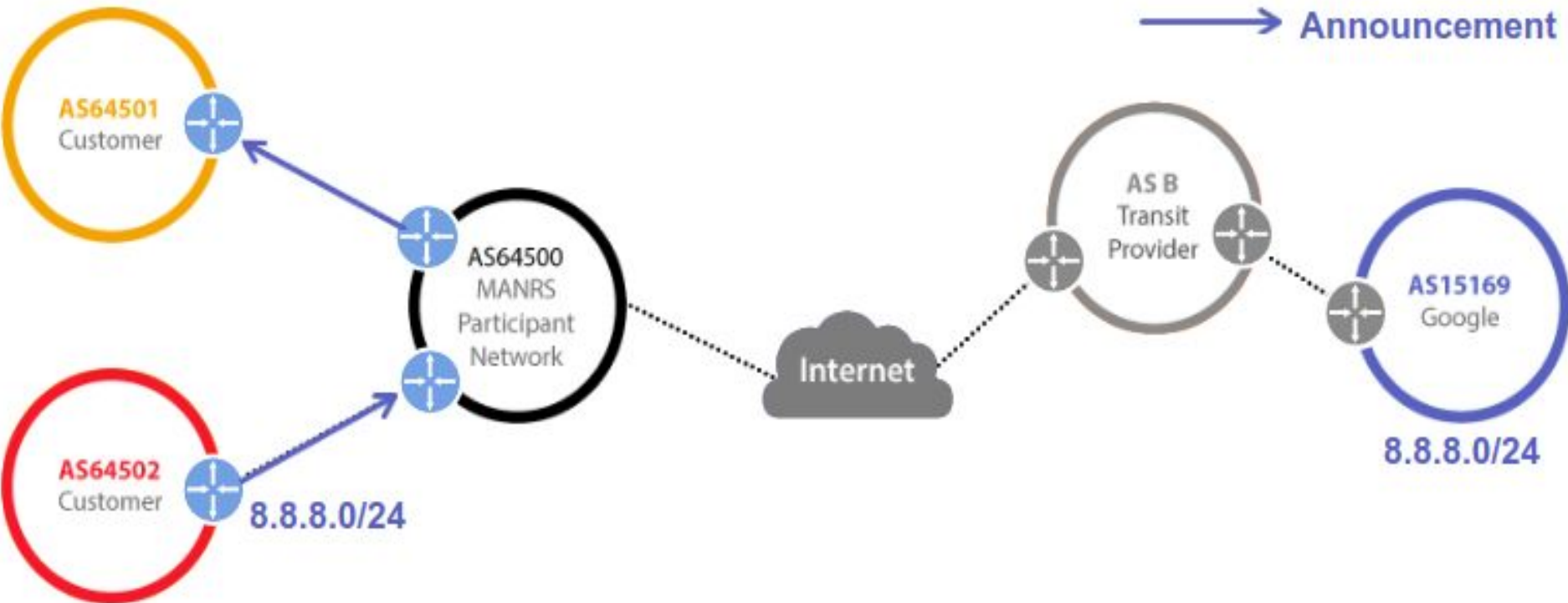
180 dias de atividades suspeitas



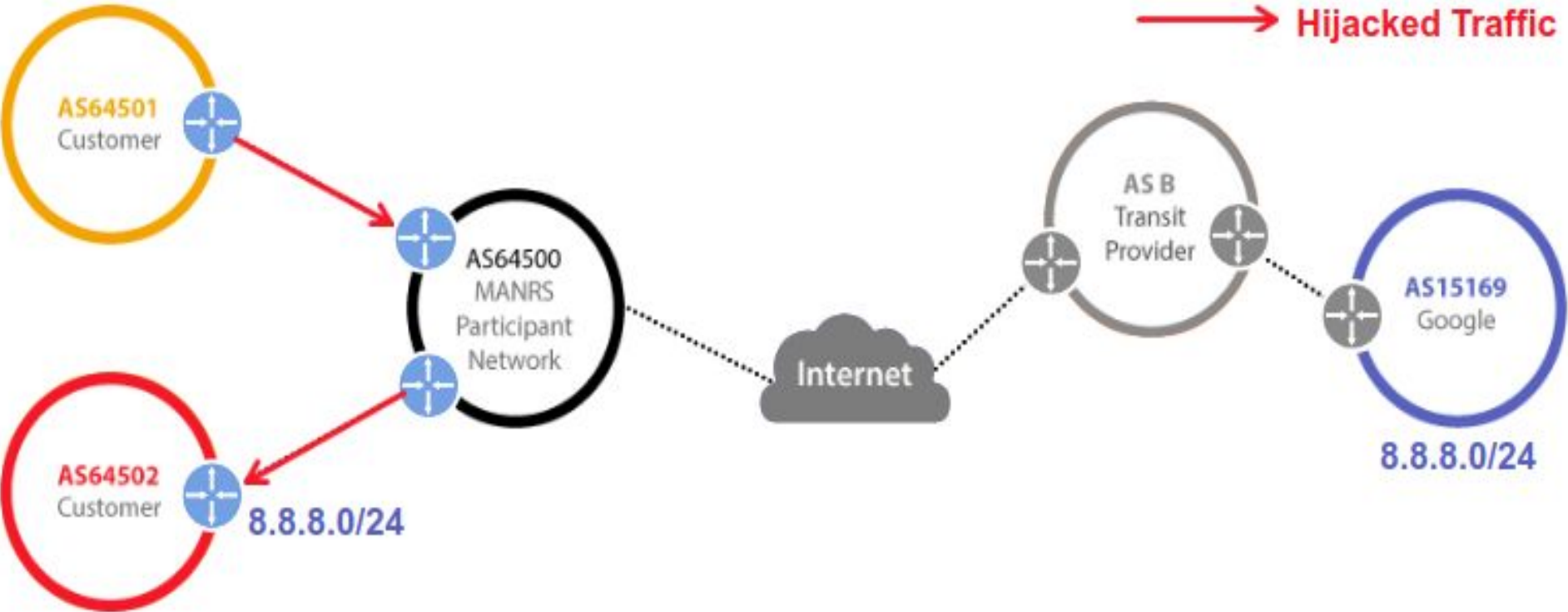
# Porque utilizar filtros? Roubo de prefixos



# Porque utilizar filtros? Roubo de prefixos



# Porque utilizar filtros? Roubo de prefixos



# Porque utilizar filtros? Roubo de prefixos

## **Períodos:**

variando de minutos a horas  
inicialmente à noite, escalando  
para feriados e finais de semana  
Início em março de 2017 e ainda  
está ocorrendo

## **Prefixos sequestrados:**

/24 de serviços Internet Banking  
/24 de provedores de nuvem

## **Equipamentos:**

roteadores de borda de pequenos e  
médios provedores  
1 caso via rede de gerência  
comprometidos via força bruta de  
senhas de administração

## **Levantados túneis GRE:**

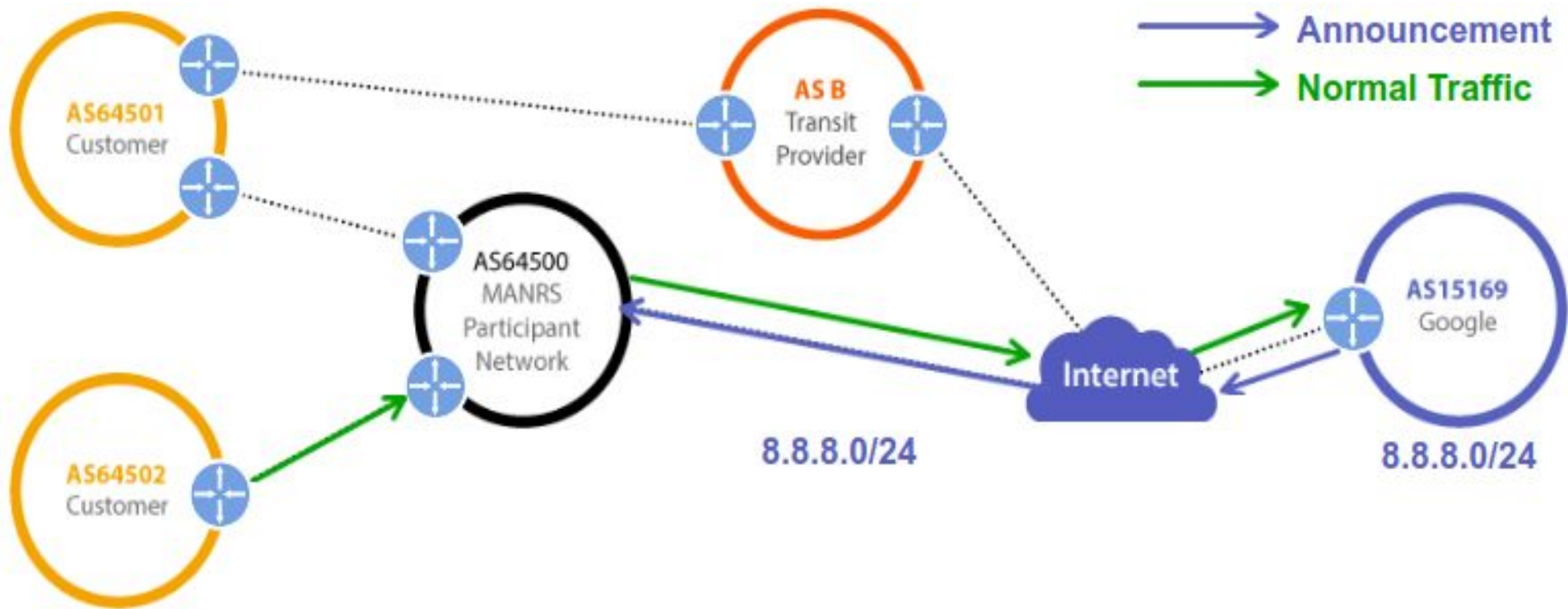
para destinos em provedores de  
hospedagem  
protocolos HTTP e DNS no destino



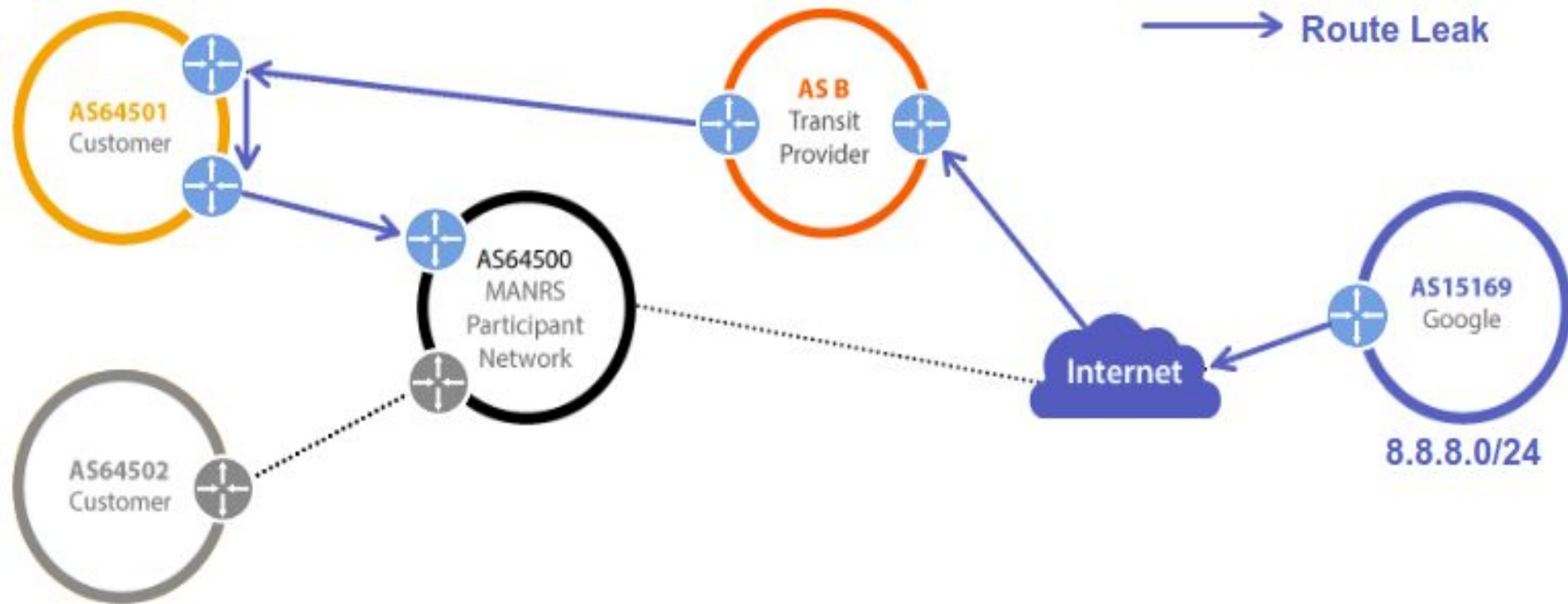
# Porque utilizar filtros? Roubo de prefixos

- Rotas anunciadas
  - Monitorar todos os anúncios com origem em seu ASN
    - BGPmon
      - <https://bgpmon.net>
    - BGPStream
      - <https://twitter.com/bgpstream>
      - <http://bgpstream.caida.org>
    - Via scripts de consulta a servidores looking glass
      - Ex: <telnet://lg.saopaulo.sp.ix.br>
  - Monitorar anúncios internos

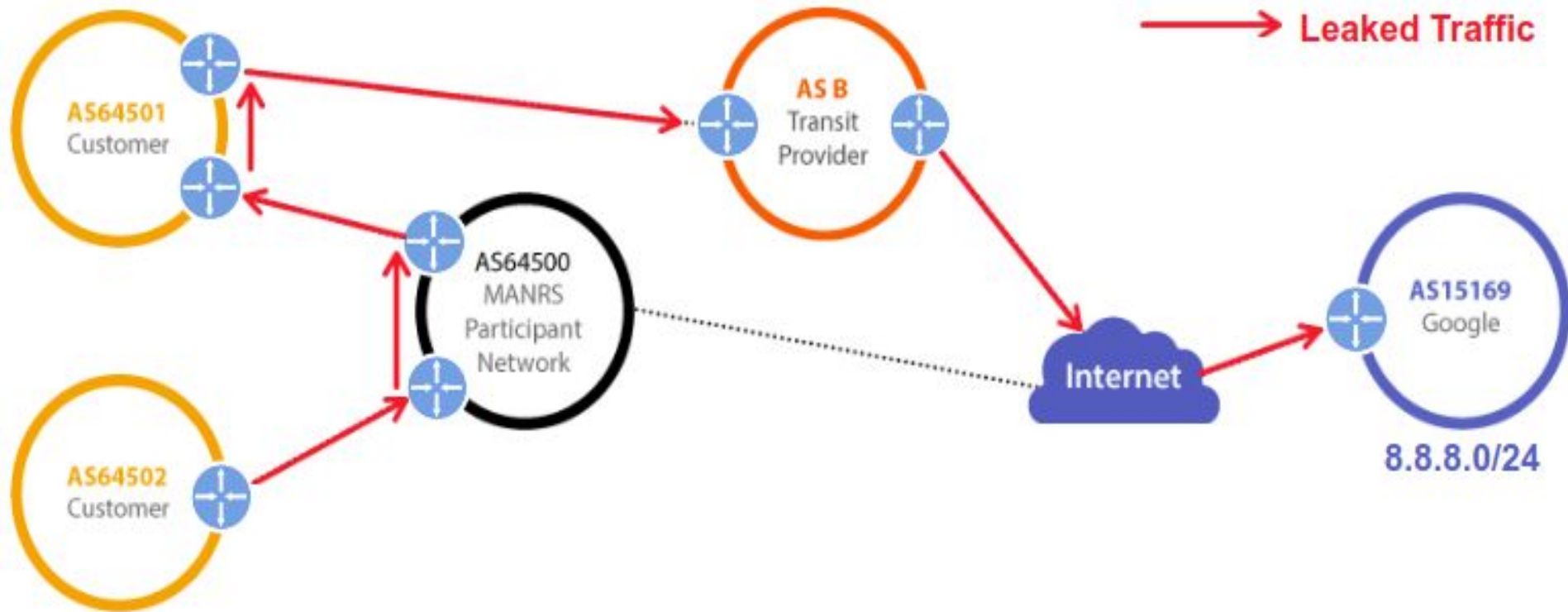
# Porque utilizar filtros? Vazamento de rotas



# Porque utilizar filtros? Vazamento de rotas



# Porque utilizar filtros? Vazamento de rotas



# Filtros

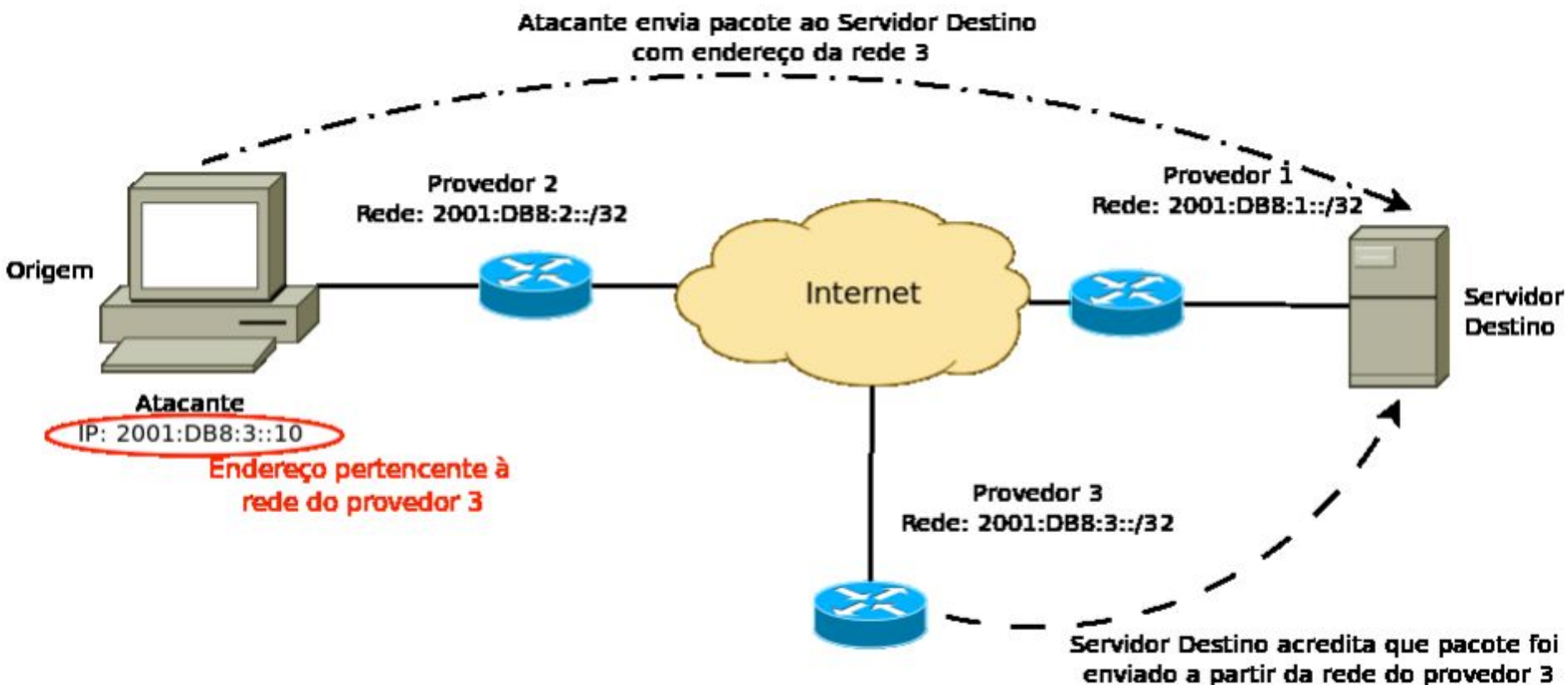
- Garanta que os seus anúncios BGP estejam corretos.
  - Publique suas informações de roteamento.
- Garanta que os anúncios BGP dos seus clientes estejam corretos.
  - Exija que eles publiquem suas informações de roteamento.
  - Aplique filtros de acordo com as informações publicadas por eles.
- Utilize WHOIS, IRR, RPKI e site da instituição para publicar e encontrar dados de roteamento.



# Filtros

- Filtro de prefixos
  - Entrada: Só receba os prefixos que foram acordados previamente com o seu cliente.
  - Entrada: Em casos de peering (como ATM do PTT) aplique filtro de bogons.
  - Saída: Só envie os seus prefixos e de seus downstream.
- Filtro de AS-Path
  - Só receba as rotas que o seu cliente possui e dos downstreams dele.

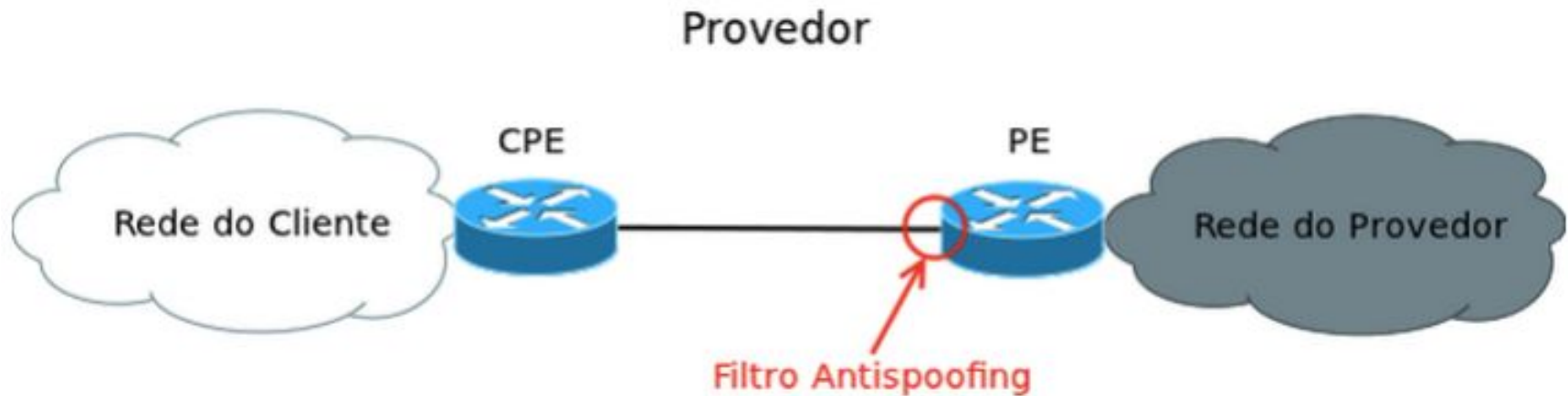
# Ataque usando spoofing



# Soluções propostas - Spoofing

- **Ingress Access Lists**
  - **Access Control List - ACLs**
- **Unicast Reverse Path Forward (uRPF)**
  - **Strict Mode**
  - **Loose Mode**
- **Source Address Validation Improvement (SAVI)**

# Filtro antispoofing



# uRPF





# Coordenação

- Ataques podem ser mitigados se tiver uma ação global e cooperativa
- Mantenha atualizada suas informações de contato
  - Administrativo
  - Técnico (NOC)
  - Abuso
- Publique sua informações
  - RIRs - Whois
  - IRRs
  - PeeringDB
  - Website

# Validação Global

- Publique suas informações de Roteamento
  - Seu sistema autônomo
  - Suas políticas de roteamento
  - As rotas dos seus clientes
- Peça que seus clientes e seus upstreams também publique suas informações de roteamento
- Utilize ferramentas
  - RPKI
  - IRR

# IRRs

- RADb
  - <http://www.radb.net/>
- NTTCOM
  - <https://www.us.ntt.net/support/policy/rr.cfm>
- TC IRR
  - <http://bgp.net.br/>

# Projeto MANRS

- Site do Projeto
  - <https://www.manrs.org/>
- Você pode assinar o projeto.
- Solicite que seus clientes e upstreams também assinem o projeto
  - <https://www.manrs.org/participants/>
- Faça o tutorial
  - <https://www.manrs.org/tutorials/>



# Dúvidas?



# Patrocínio Super Like



# Apoio de Mídia





**Obrigado !!!**

**nic.br egi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)