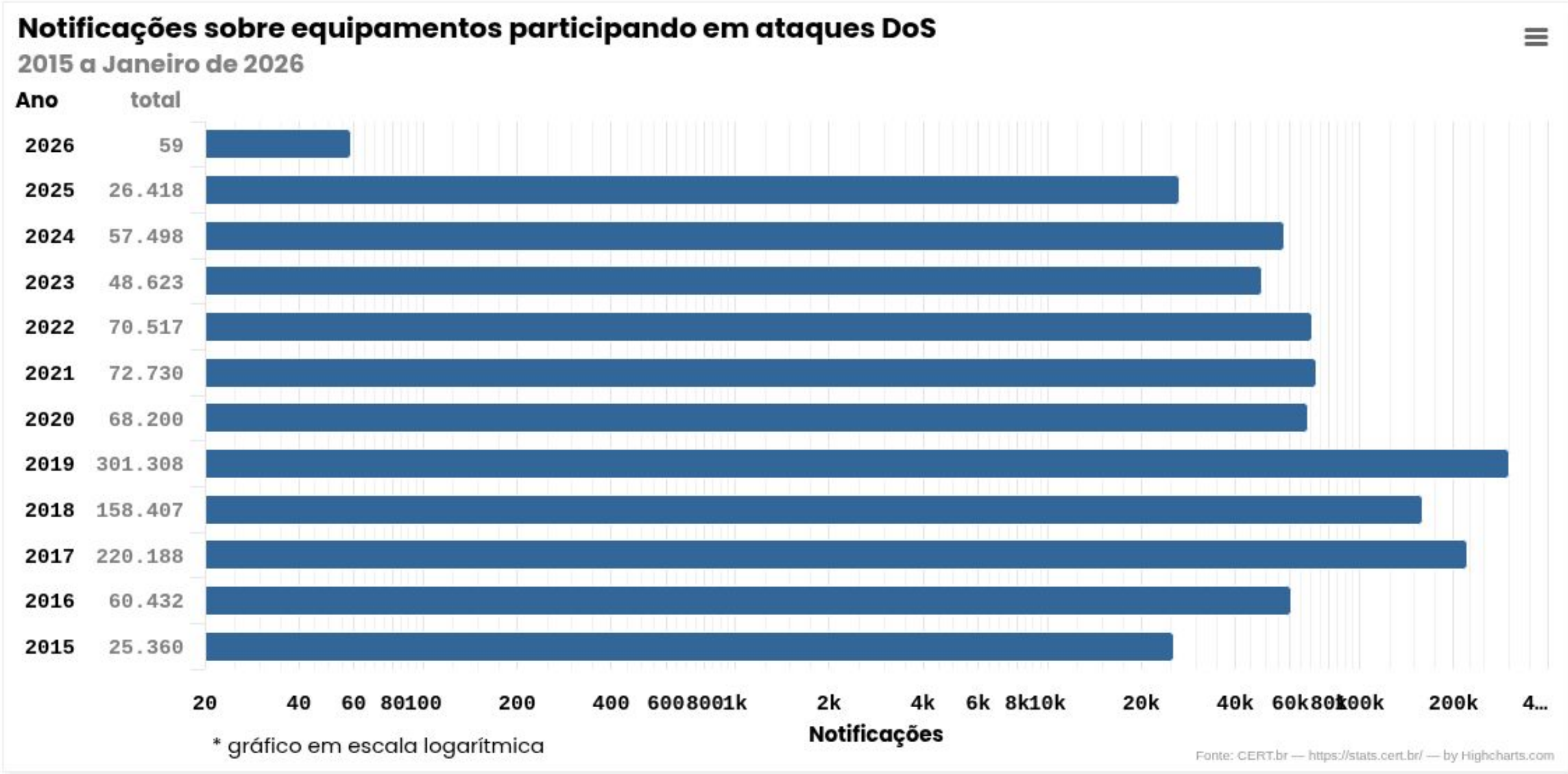
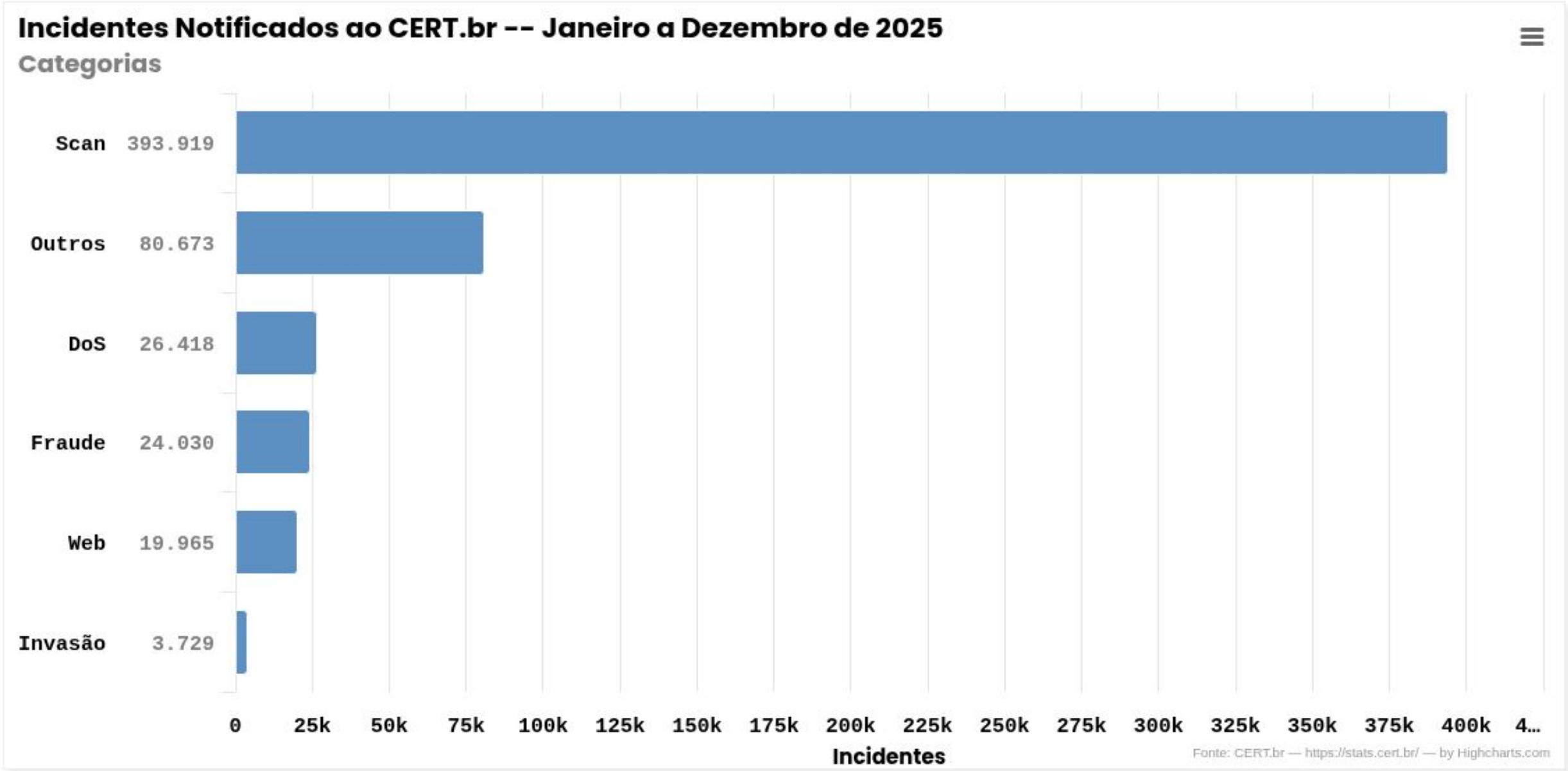
MANRS

Mutually Agreed Norms for Routing Security

ceptro.br nic.br cgi.br



https://stats.cert.br/incidentes/



https://stats.cert.br/incidentes/

MANRS

ceptro.br nic.br cgi.br

O que é MANRS?

- Mutually Agreed Norms for Routing Security
- É uma iniciativa global
- Suportada pela GCA (Global Cyber Alliance)
- **Consiste em 4 coisas básicas**
  - Filtros
  - Anti-Spoofing
  - Coordenação
  - Validação Global

MANRS

Roubo de prefixos

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

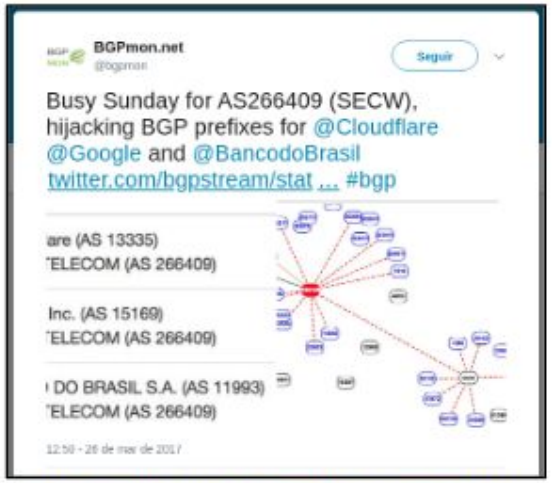
What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

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

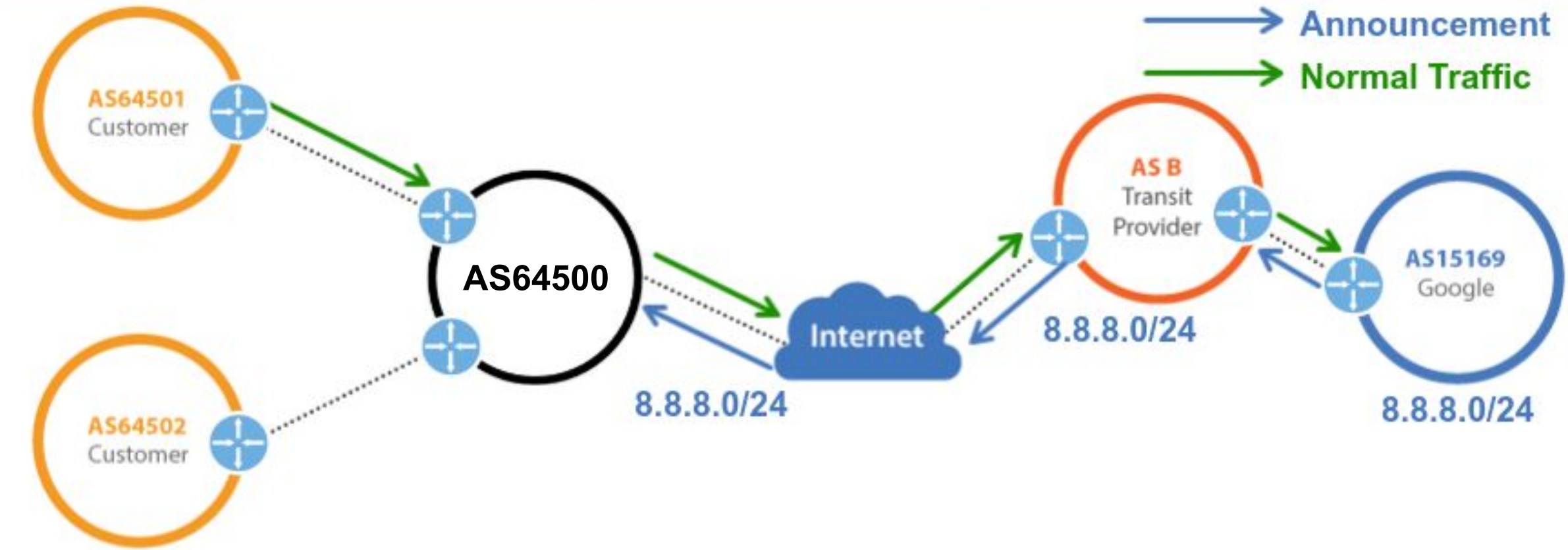
Mutually Agreed Norms for Routing Security (MANRS) 15 November 2018

Route Leak Causes Major Google Outage

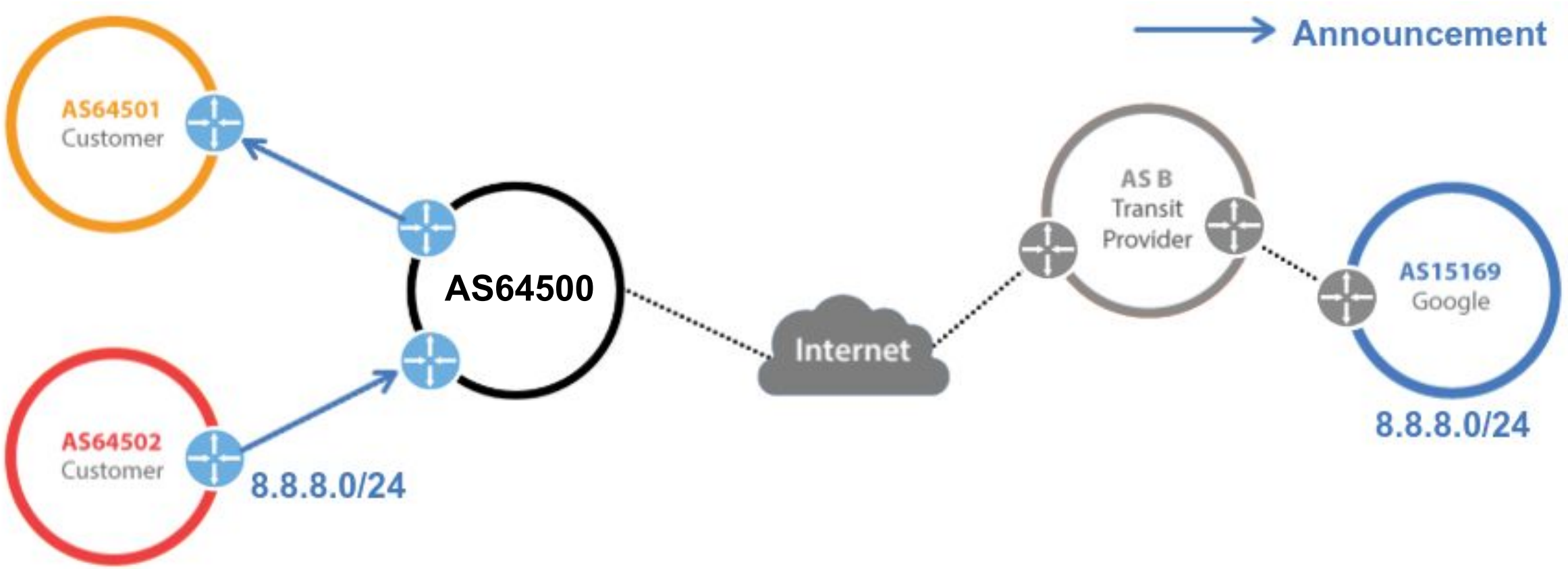
https://www.internetsociety.org/blog/2018/11/route-leak-caused-a-major-google-outage/

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

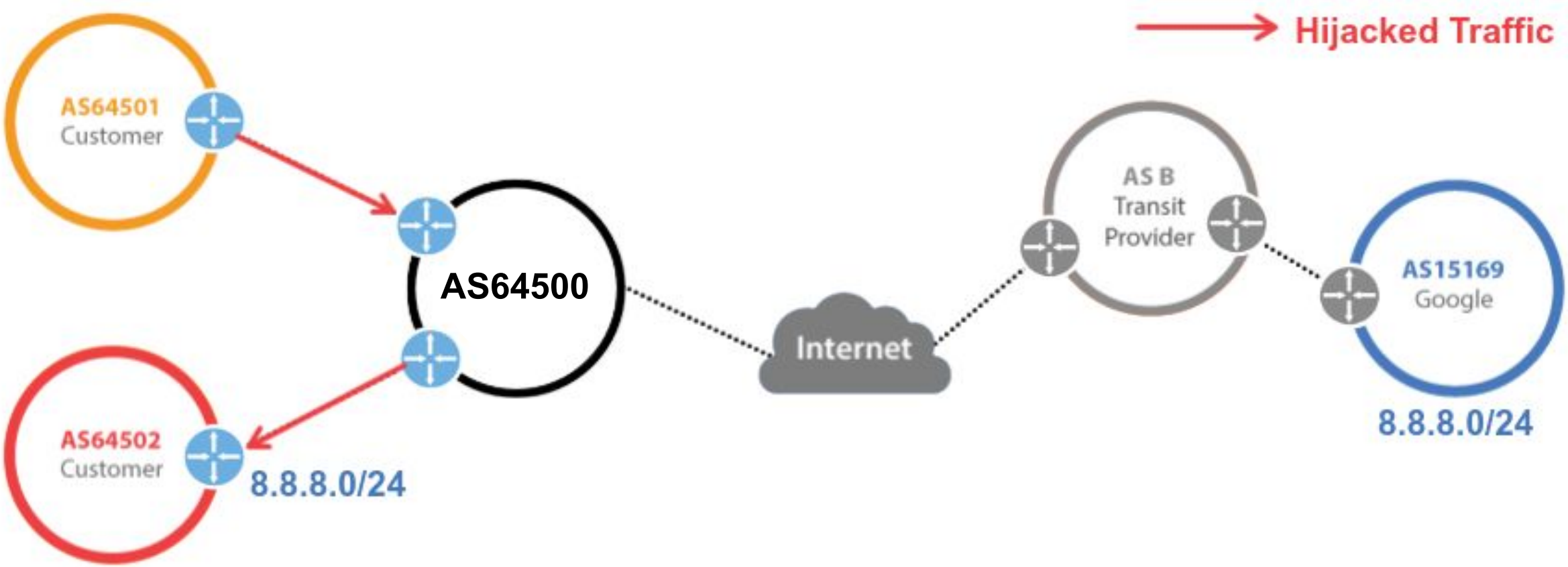
Roubo de prefixos



Roubo de prefixos



Roubo de prefixos



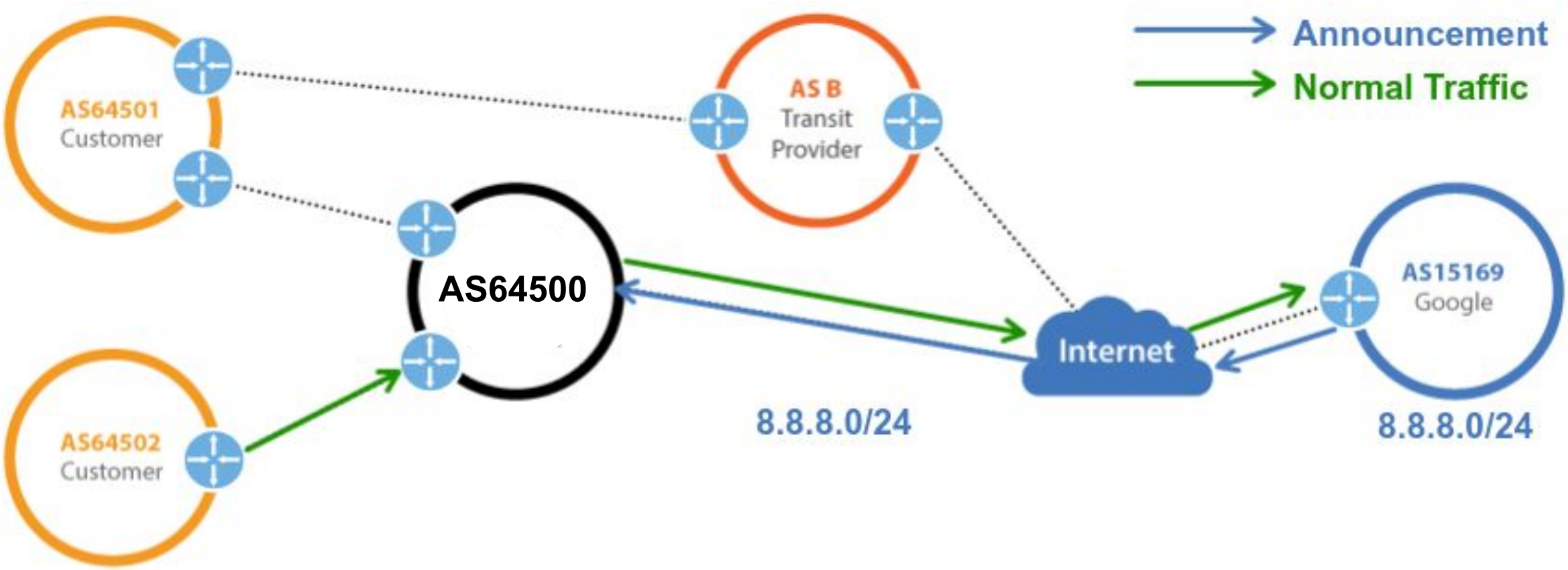
Roubo de prefixos

- **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

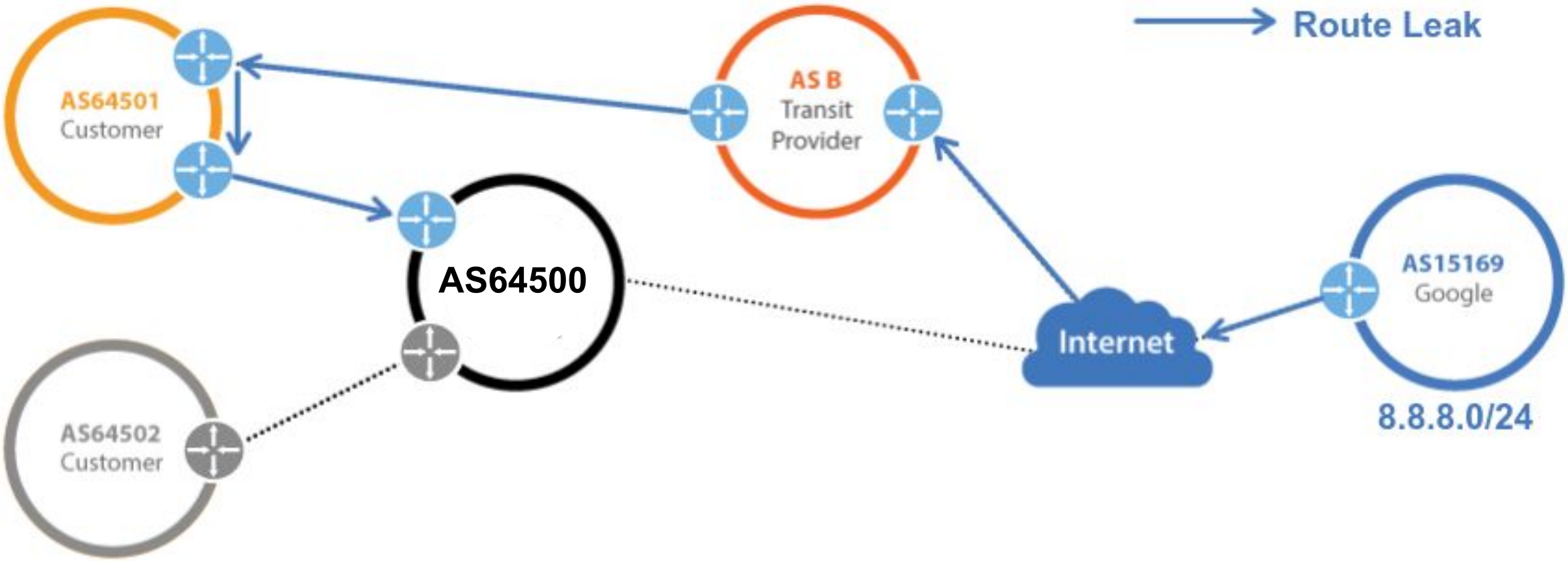
Roubo de prefixos

- 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**
      - telnet://lg.saopaulo.sp.ix.br
      - https://bgp.tools/
  - **Monitorar anúncios internos**

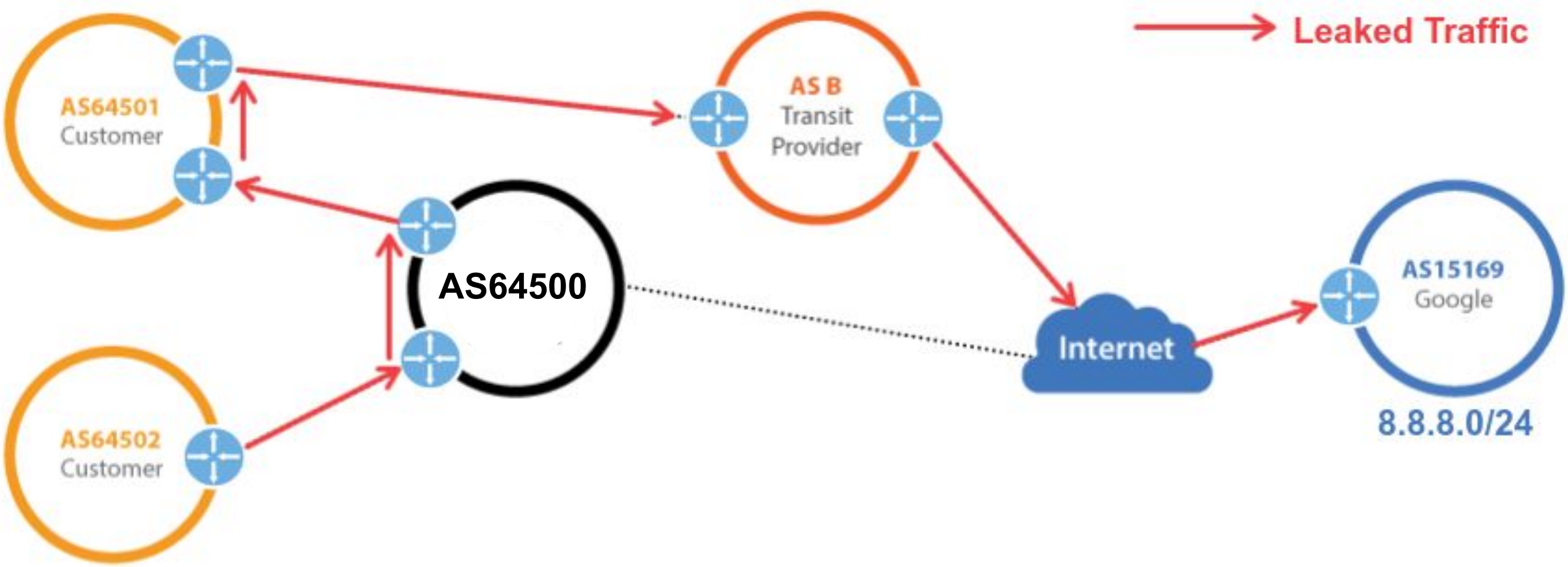
Vazamento de rotas



Vazamento de rotas



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.

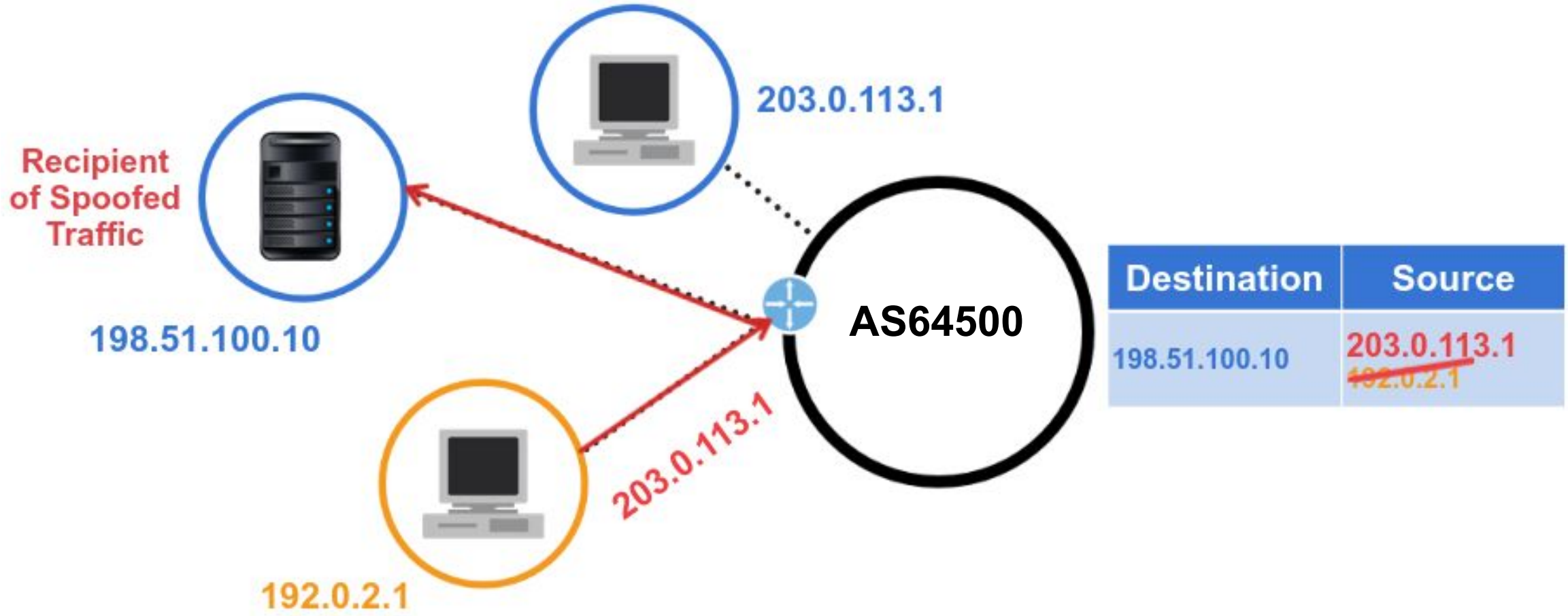
Anti-Spoofing

ceptro.br nic.br cgi.br

O que é spoofing?

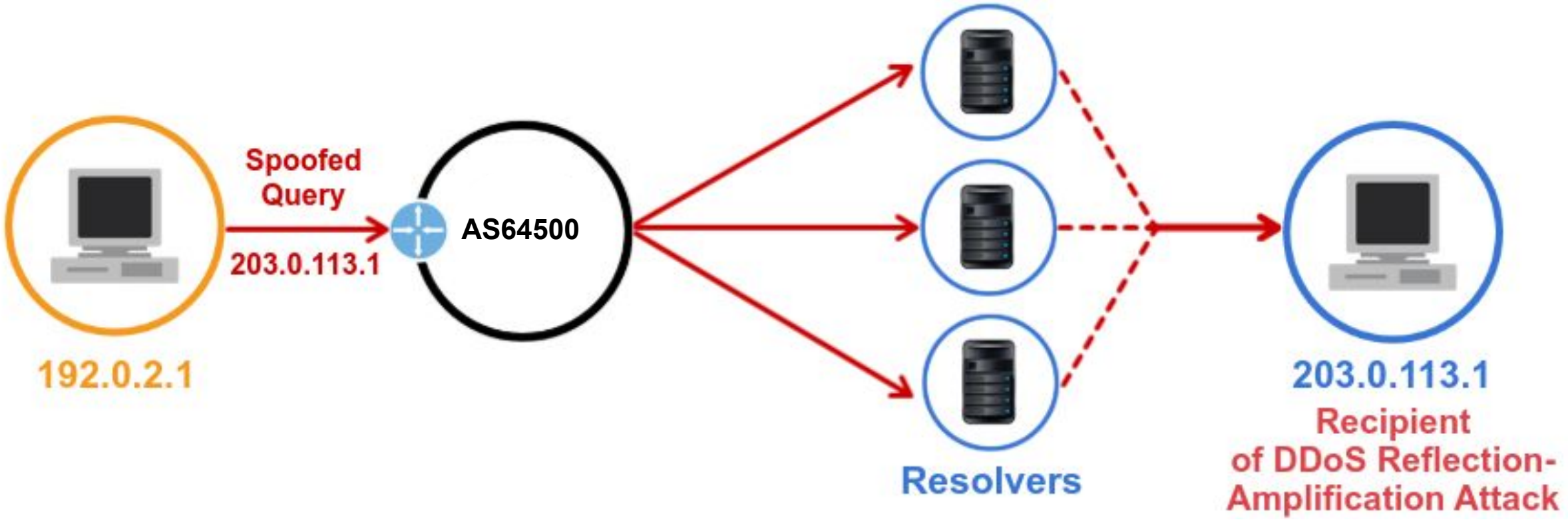
- Pacotes IP com endereços de origem incorretos
  - **Erro de configuração**
    - Problema de Software
  - **Teste e Simulação**
    - Teste de Performance
  - **Atitude maliciosa**
    - Esconder a identidade do atacante
    - Fingir ser outro computador na rede
- O spoofing pode ser usado em ataques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

Como funciona o ataque spoofing



Destination	Source
198.51.100.10	203.0.113.1 ~~192.0.2.1~~

Como funciona o ataque reflexão-amplificação



Fatores de amplificação

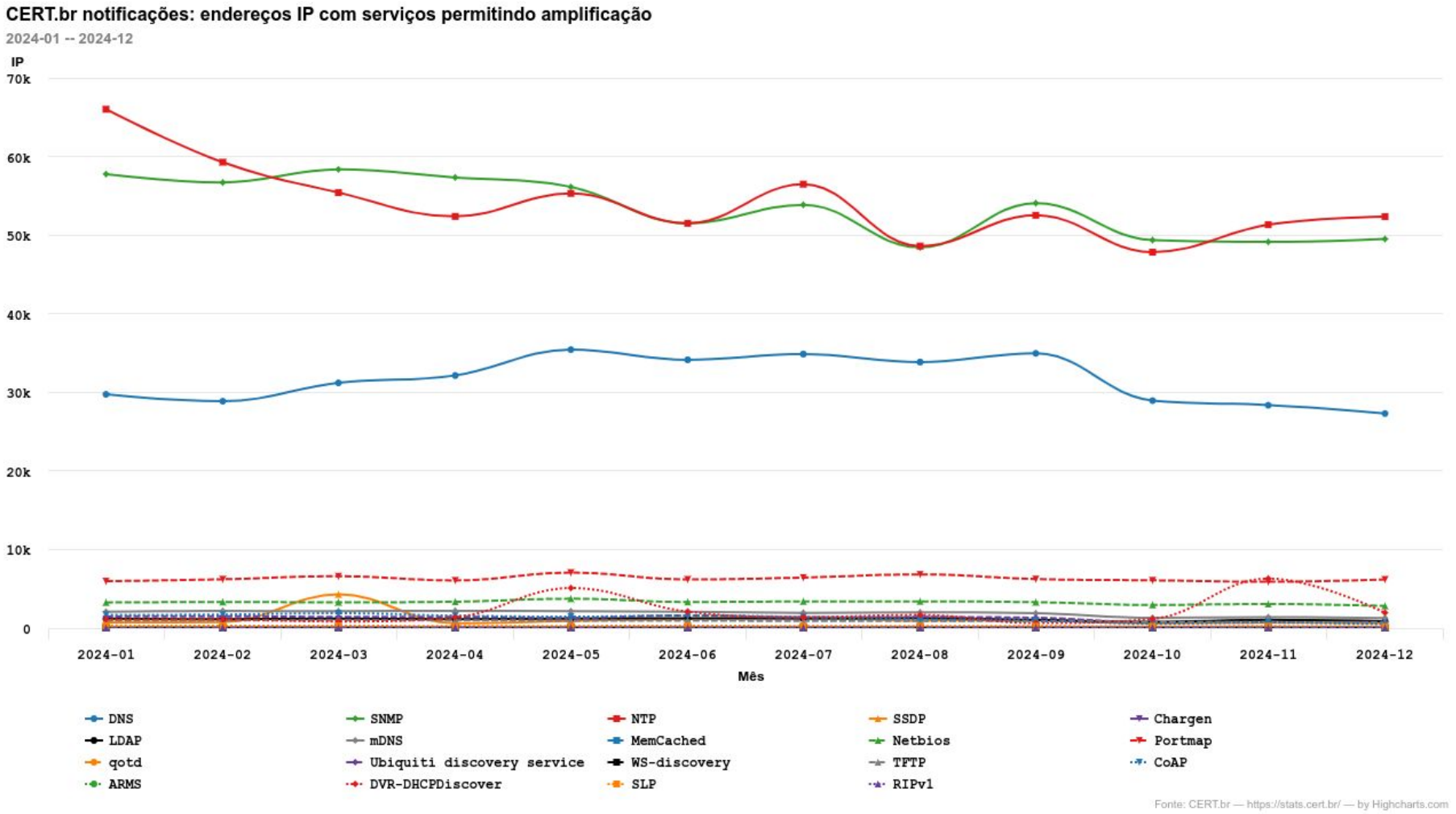
Protocolo	Fator de Amplificação	Comando Vulnerável
DNS	28 a 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
LDAP / CLDAP	46 a 70	Malformed request
SSDP	30.8	SEARCH request
Chargen	358.8	Character generation request

Total de ASNs e IPs Notificados pelo CERT.br

Serviços que permitem amplificação (com maior número de endereços IP no Brasil)

	DNS		SNMP		NTP		Portmap	
Mês	ASN	IP	ASN	IP	ASN	IP	ASN	IP
2024-01	2.937	29.754	3.539	57.760	1.174	66.012	1.333	5.964
2024-02	3.081	28.861	3.497	56.705	1.175	59.278	1.304	6.214
2024-03	3.104	31.210	3.537	58.352	1.176	55.404	1.300	6.593
2024-04	3.060	32.137	3.502	57.329	1.171	52.376	1.252	6.068
2024-05	3.119	35.435	3.497	56.128	1.160	55.305	1.254	7.056
2024-06	3.125	34.131	3.315	51.510	1.230	51.497	1.240	6.192
2024-07	3.156	34.863	3.480	53.841	1.162	56.477	1.319	6.428
2024-08	3.153	33.847	3.445	48.436	1.179	48.602	1.298	6.832
2024-09	3.106	34.968	3.562	54.068	1.161	52.522	1.260	6.238
2024-10	2.818	28.954	3.435	49.363	1.157	47.829	1.246	6.080
2024-11	2.954	28.382	3.448	49.138	1.155	51.325	1.276	5.894
2024-12	2.856	27.325	3.424	49.501	1.204	52.350	1.252	6.188

Total de ASNs e IPs Notificados pelo CERT.br



Ferramentas de Linha de Comando (teste na sua rede!)

- **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>`**

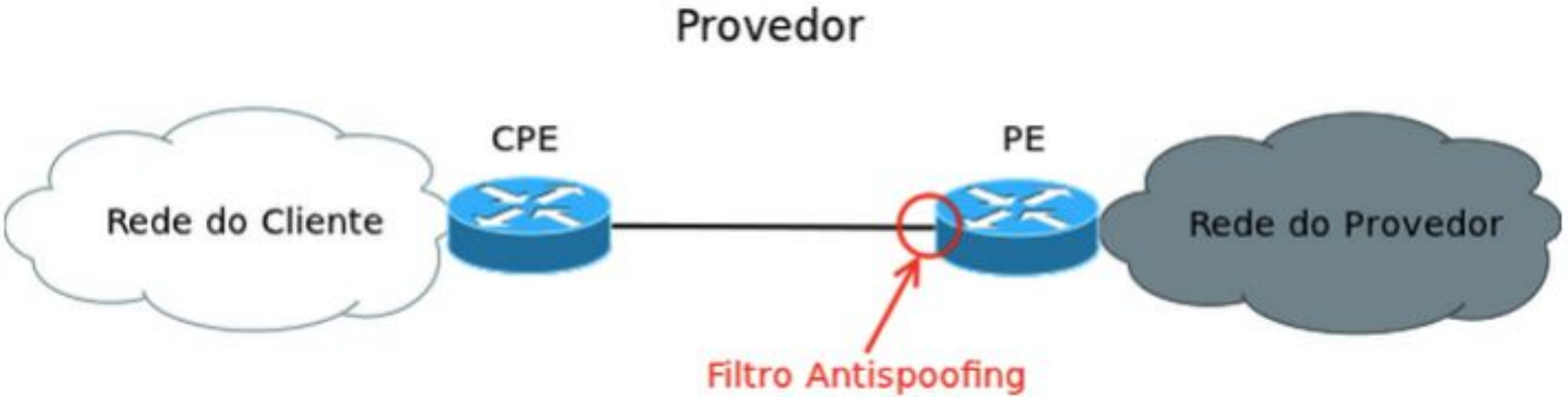
Ferramentas de Linha de Comando (teste na sua rede!)

- 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`

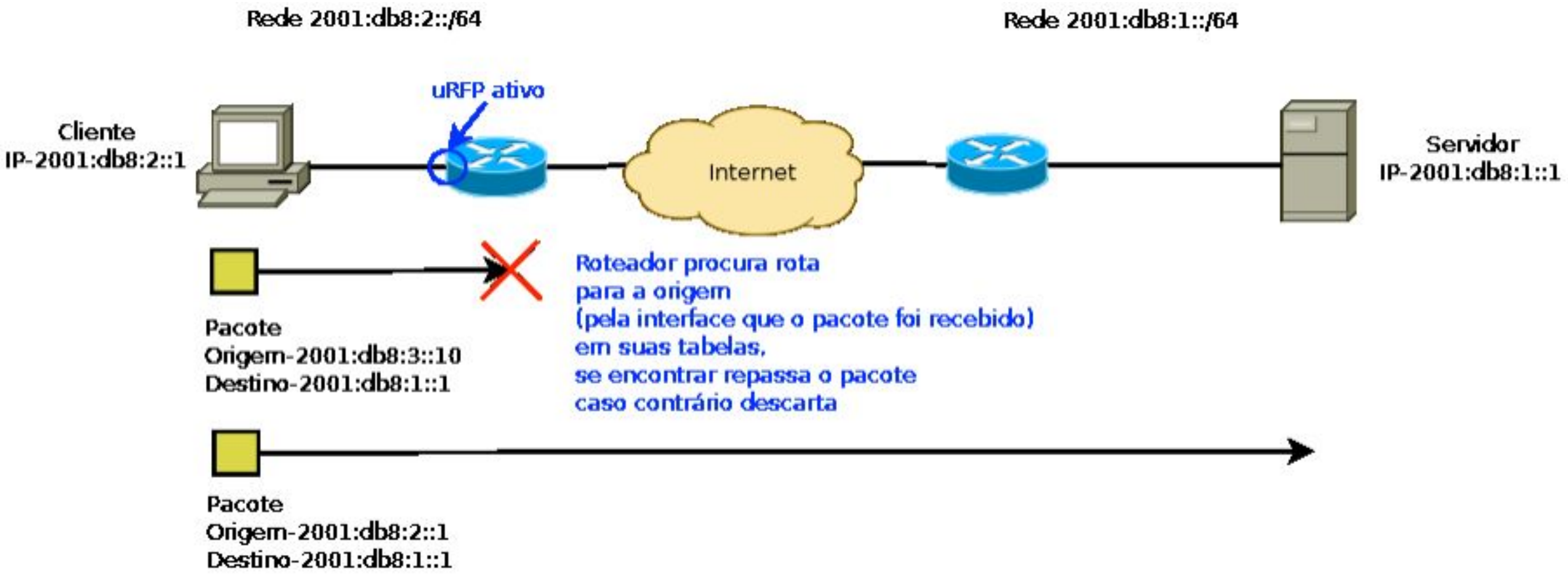
Soluções - Spoofing

- **BCP38**
  - http://www.bcp38.info
- **Ingress Access Lists**
  - Access Control List - ACLs
- **Unicast Reverse Path Forward (uRPF)**
  - Strict Mode
  - Loose Mode
- **Source Address Validation Improvement (SAVI)**
  - **RFC7039 - SAVI Framework**
    - https://datatracker.ietf.org/doc/html/rfc7039

Filtro anti-spoofing



uRPF - Funcionamento



Coordenação

ceptro.br nic.br cgi.br

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
  - Websites

Validação Global

ceptro.br nic.br cgi.br

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

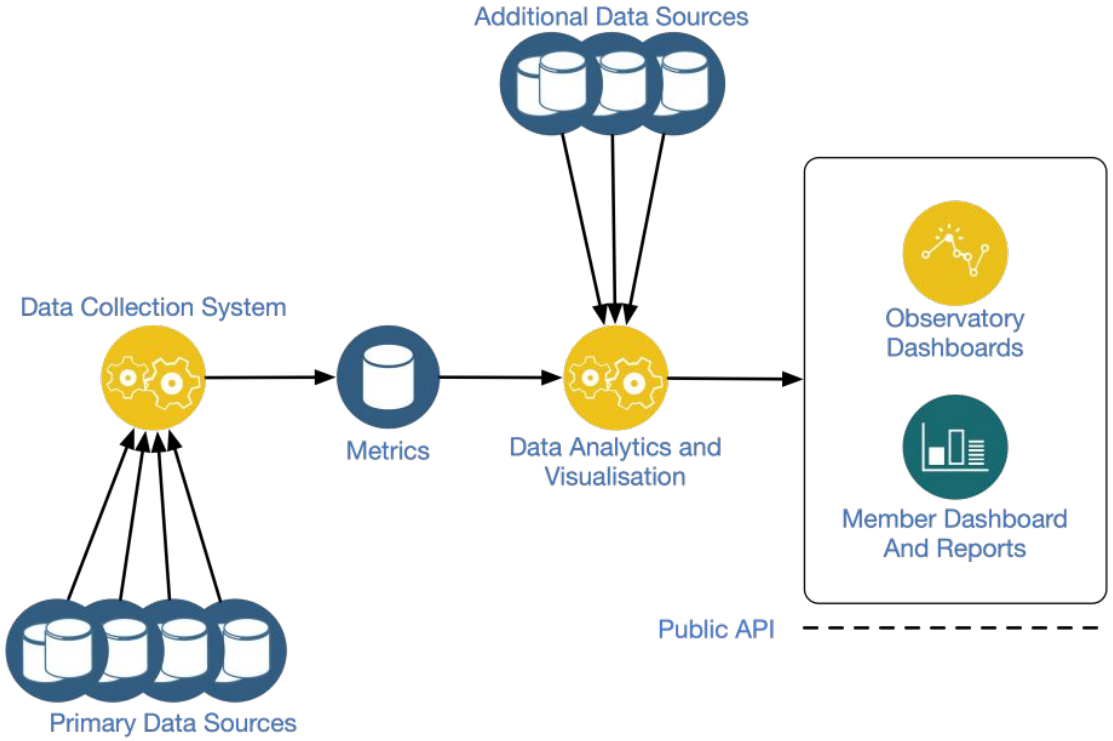
- **RADb**
  - http://www.radb.net/
- **NTTCOM**
  - https://www.us.ntt.net/support/policy/rr.cfm
- **TC IRR**
  - http://bgp.net.br/

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/

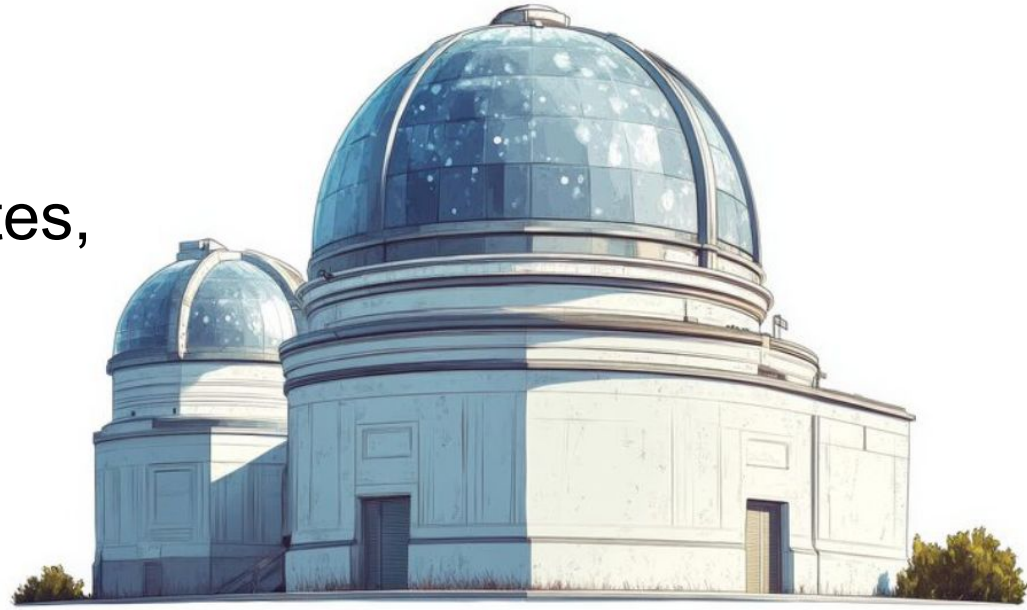
MANRS Observatory

- Monitora e avalia o nível de segurança do roteamento da Internet em escala global.
- Mede a chamada “**Alinhamento ao MANRS” (MANRS Readiness)**, indicando o quanto redes e operadores seguem boas práticas de segurança.

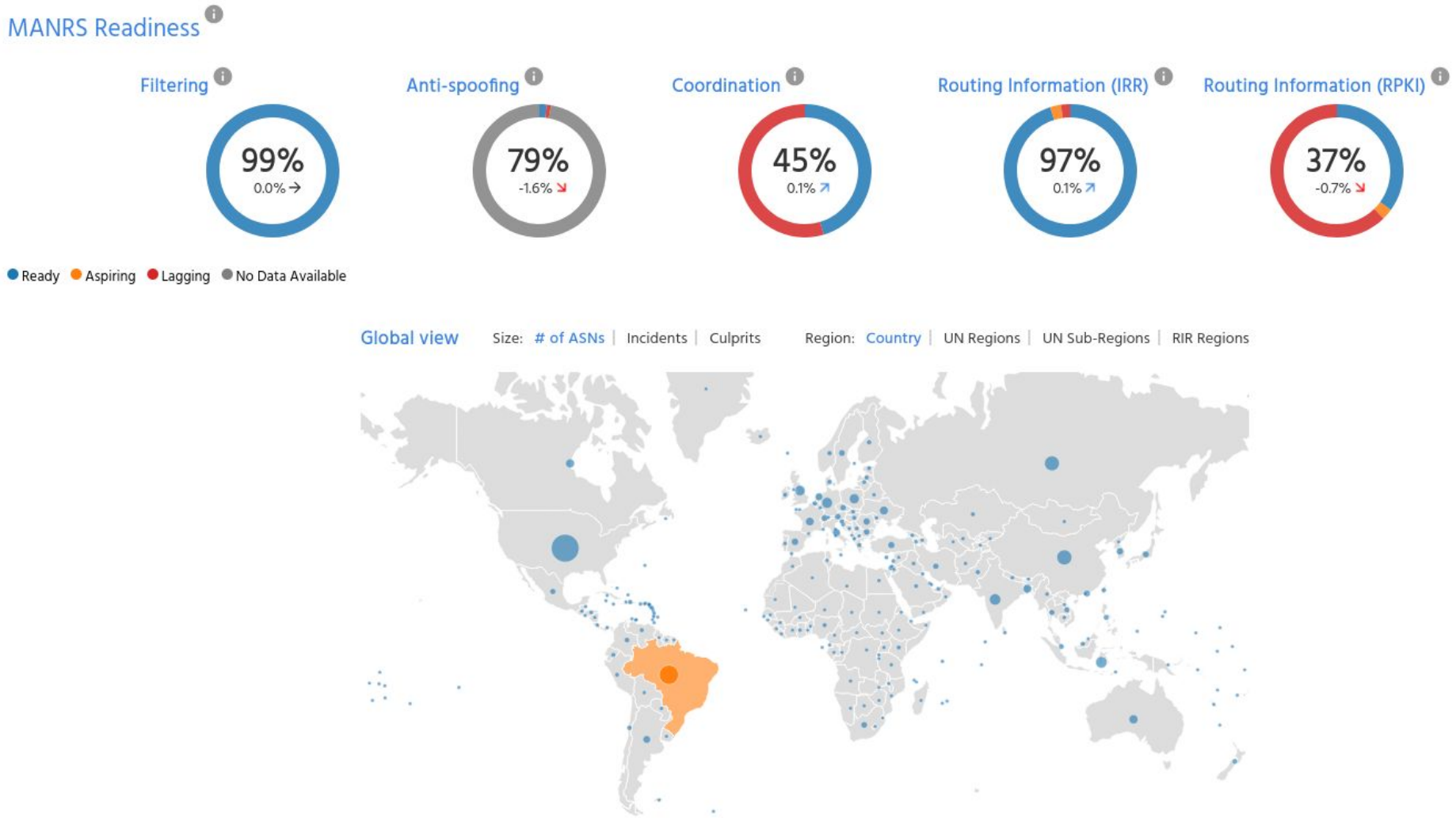


MANRS Observatory

- Agrega dados de diferentes fontes confiáveis para identificar problemas como:
  - Vazamentos de rotas (route leaks)
  - Sequestro de prefixos (BGP hijacks)
  - Falta de filtragem adequada
  - Ausência de medidas anti-spoofing
- Oferece uma visão detalhada para participantes, ajudando operadores a identificar falhas e melhorar suas práticas.



MANRS Observatory



Dúvidas?

Obrigado!

CEPTRO.br Cursos: cursosceptro@nic.br
CEPTRO.br IPv6: ipv6@nic.br

@comunicbr
@nicbr
@NICbrvideos

nic.br cgi.br

www.nic.br | www.cgi.br