O maior inimigo pode ser você!

DNS + SSDP + NTP

Prevenção é a melhor solução !

GTER40 - São Paulo – SP

Grupo de Trabalho de Engenharia e Operação de Redes
Dezembro/2015

Network Education

Apresentação

Pacheco Tecnologia

Telecom
CONSULTORIA E TREINAMENTO

Elizandro Pacheco

(Network Education)

Consultor em Redes há 13 anos

Ubiquiti® Certified Trainer

Network Education®

Network Education

UBIQUITI NETWORKS
AUTHORIZED
TRAINING PARTNER

Motivação

Estudar métodos de ataque e defesa de um assunto que é discutido diariamente em grupos e redes sociais.

Fazer um levantamento diferenciado, com números de dispositivos realmente vulneráveis a nível de Brasil.

Método de Análise

Fonte de ASNs:
ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-latest

Foram filtrados todos blocos IPv4 delegados ao BR .

Scan com script próprio em python desenvolvidos com ajuda de Uesley Corrêa (Telecom Treinamentos em Consultoria – RJ) com auxílio de ferramentas adicionais.

SSDP – Simple Service Discovery Protocol

O SSDP é o protocolo base do uPNP (Universal Plug and Play), que tem por objetivo simplificar a implementação de redes em casas e escritórios através da descoberta automática de serviços e dispositivos na rede.

Mais informações:

http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf

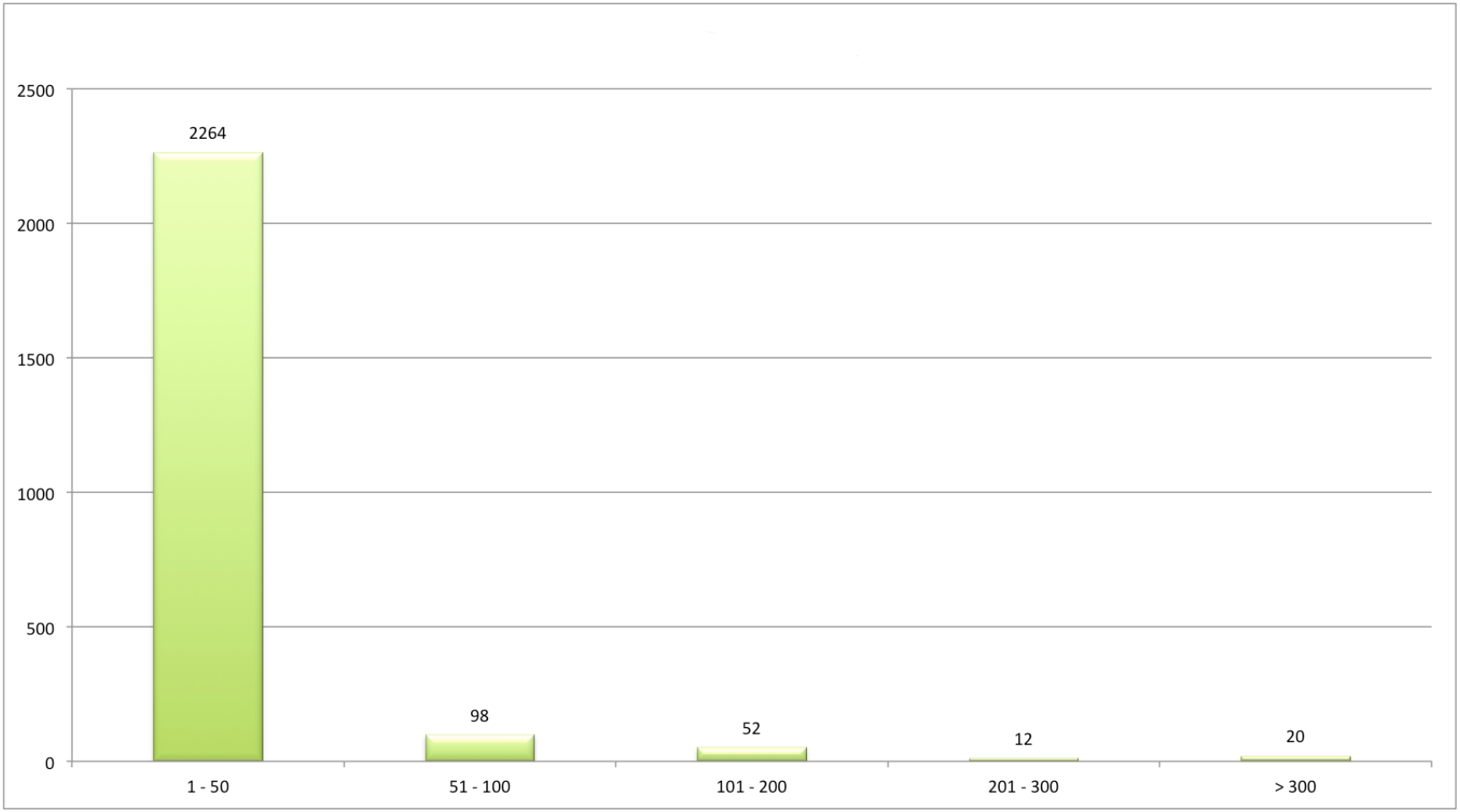
SSDP – Simple Service Discovery Protocol

Em ataque de amplificação, o SDDP é capaz de amplificar um ataque com taxas superiores a 30X.

Protocolo: UDP

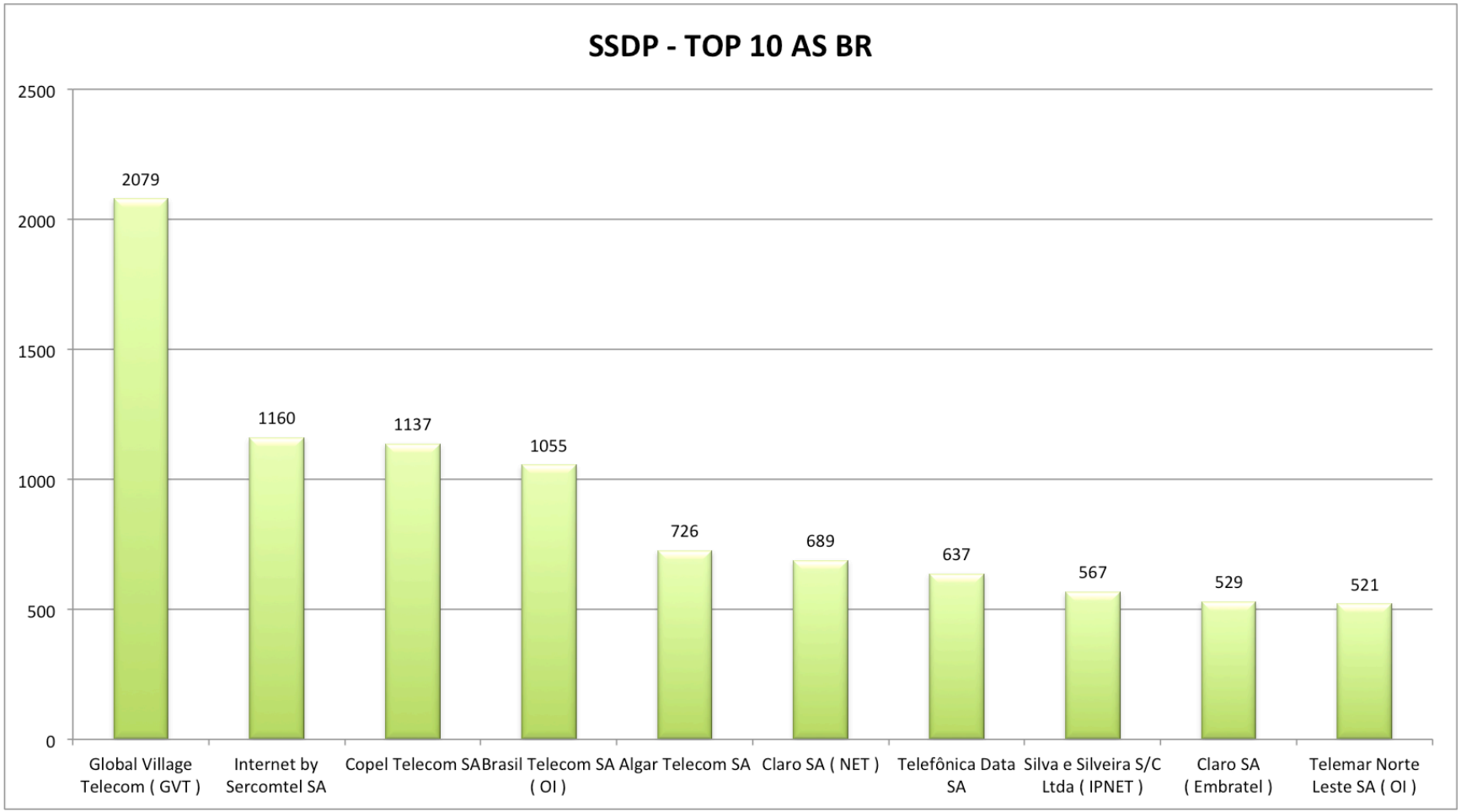
Porta: 1900

SSDP – Visão Geral ASN's BR



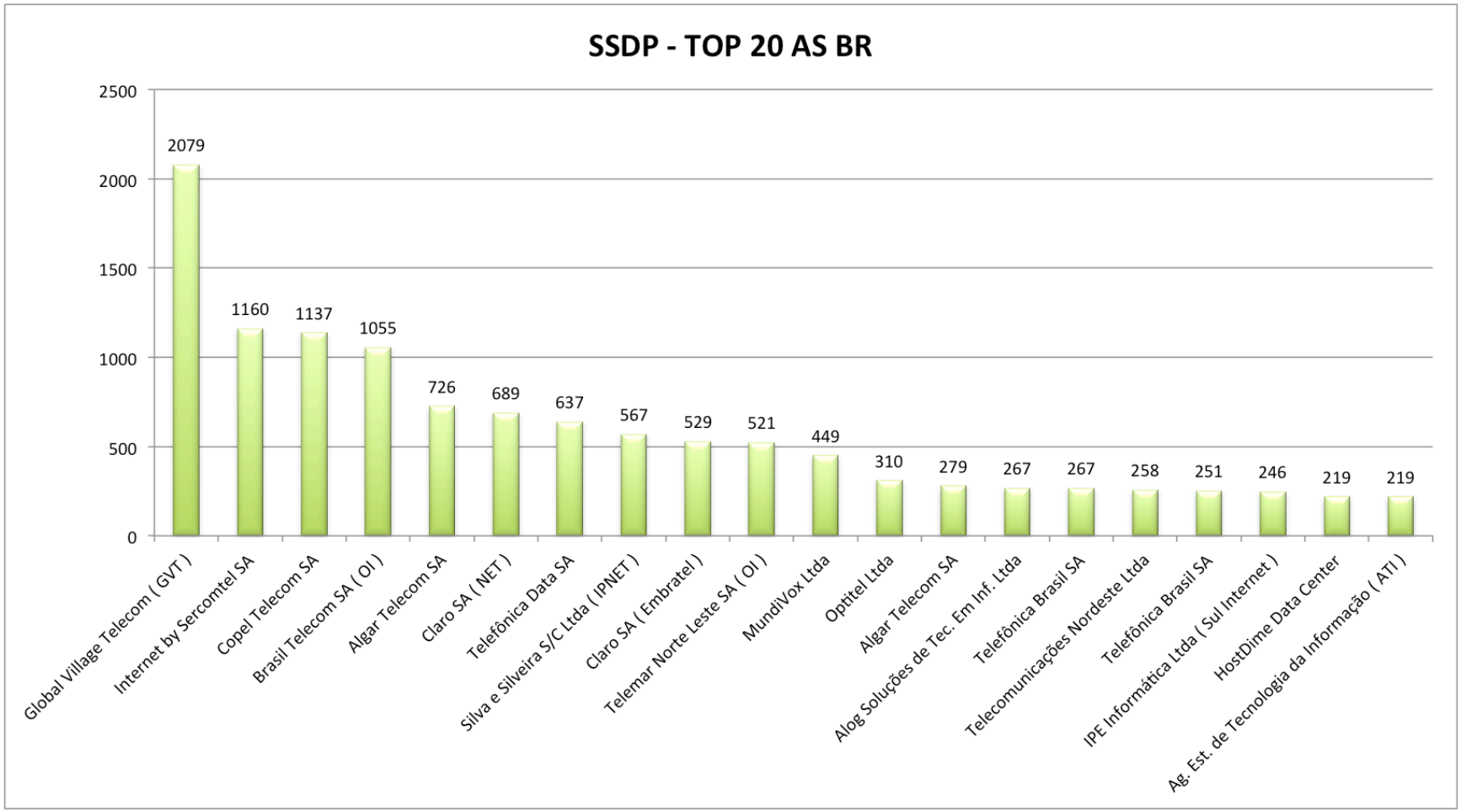
Network Education

SSDP – TOP 10 ASN's BR



Network Education

SSDP – TOP 20 ASN's BR



Network Education

SSDP – Prevenção

Evitar forward para clientes com destino a porta 1900 / UDP.

Evita o ataque?

NTP - Network Time Protocol

NTP é um protocolo de sincronização dos relógios de dispositivos e utiliza UDP para tal. O NTP permite manter o relógio de um dispositivo com a hora sempre certa e com grande exatidão.

Fonte: https://pt.wikipedia.org/wiki/Network_Time_Protocol

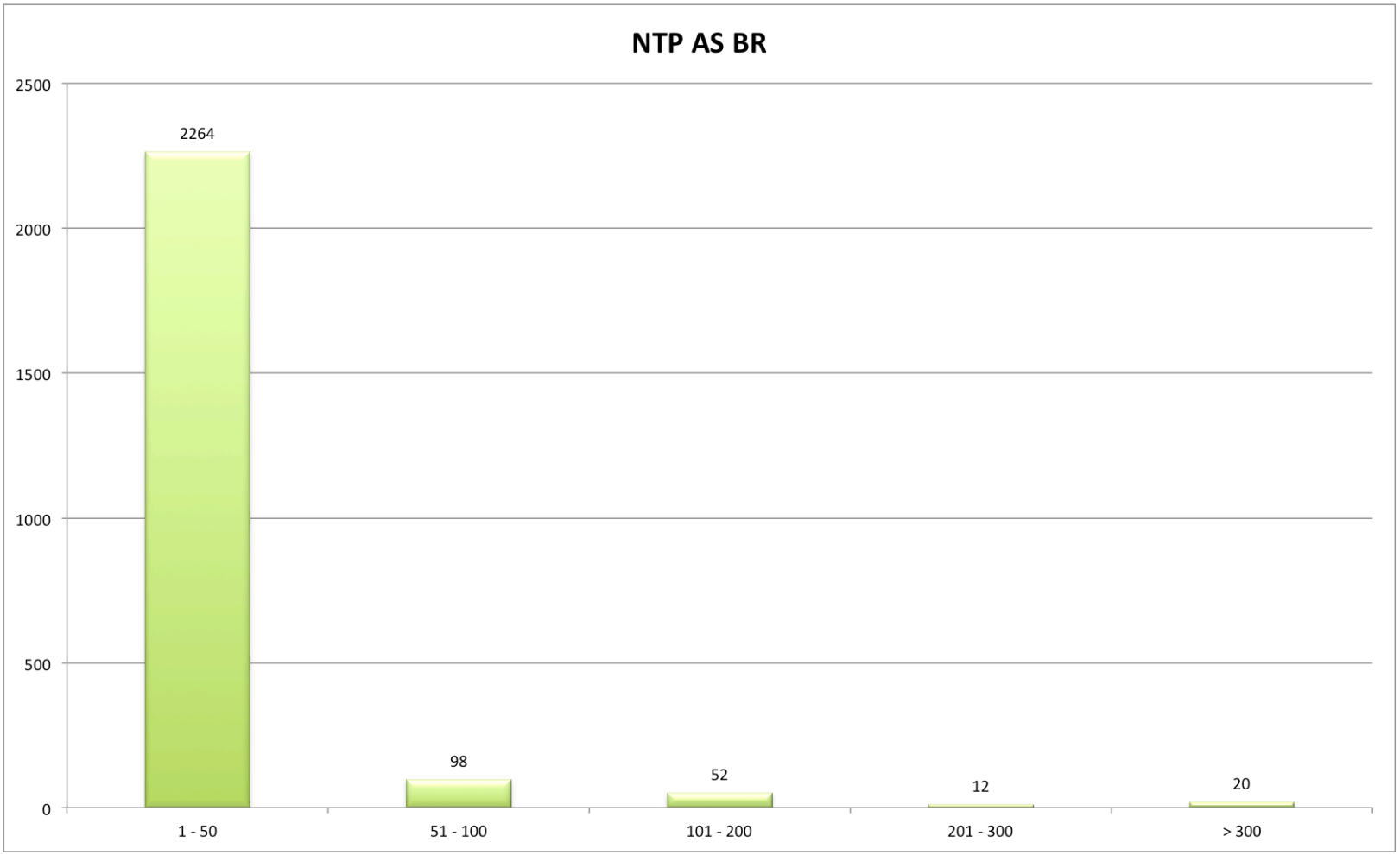
NTP – Network Time Protocol

Em ataque de amplificação, o NTP é capaz de amplificar um ataque com taxas superiores a 556.9 X.

Protocolo: UDP

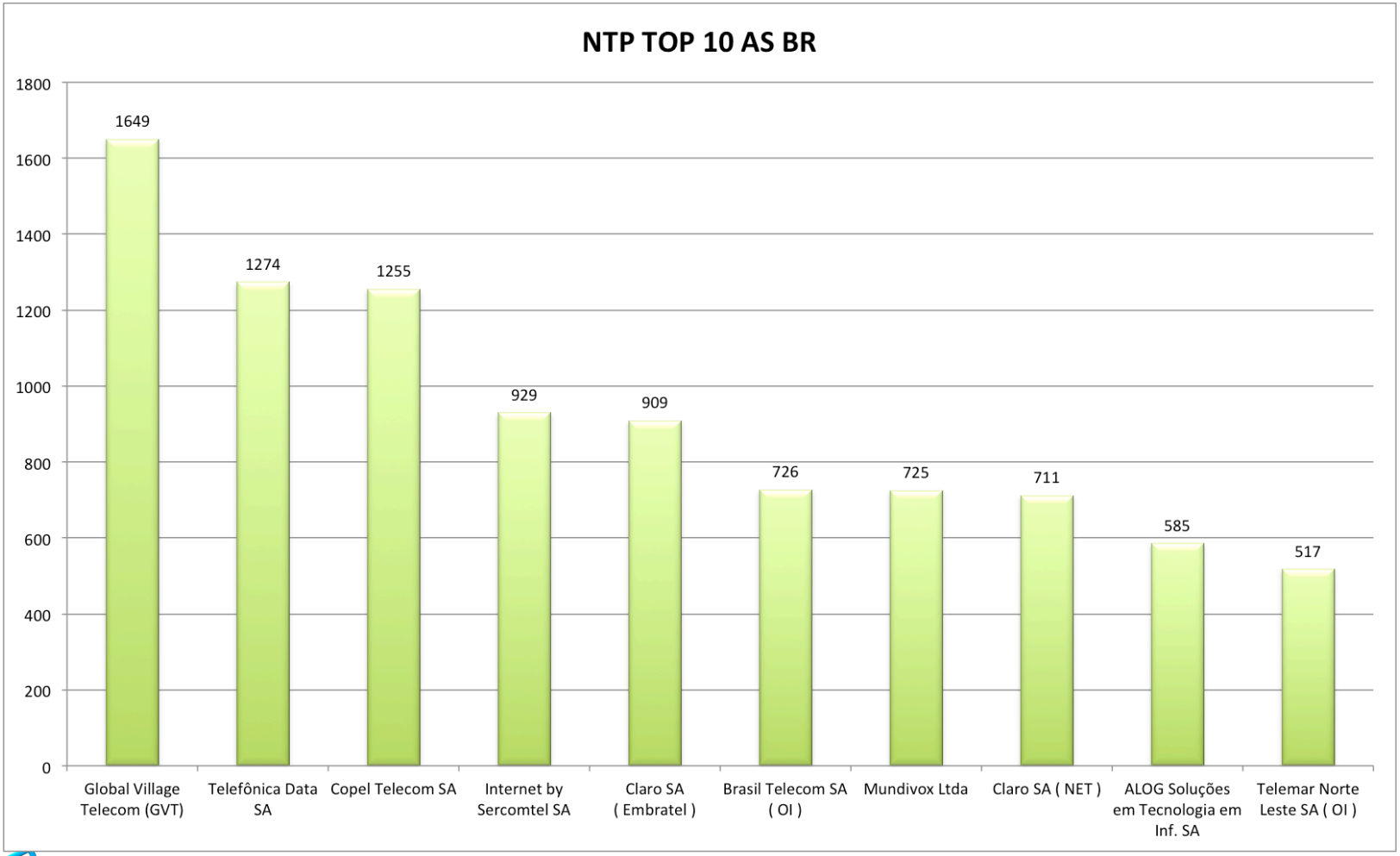
Porta: 123

NTP – Visão Geral ASN's BR



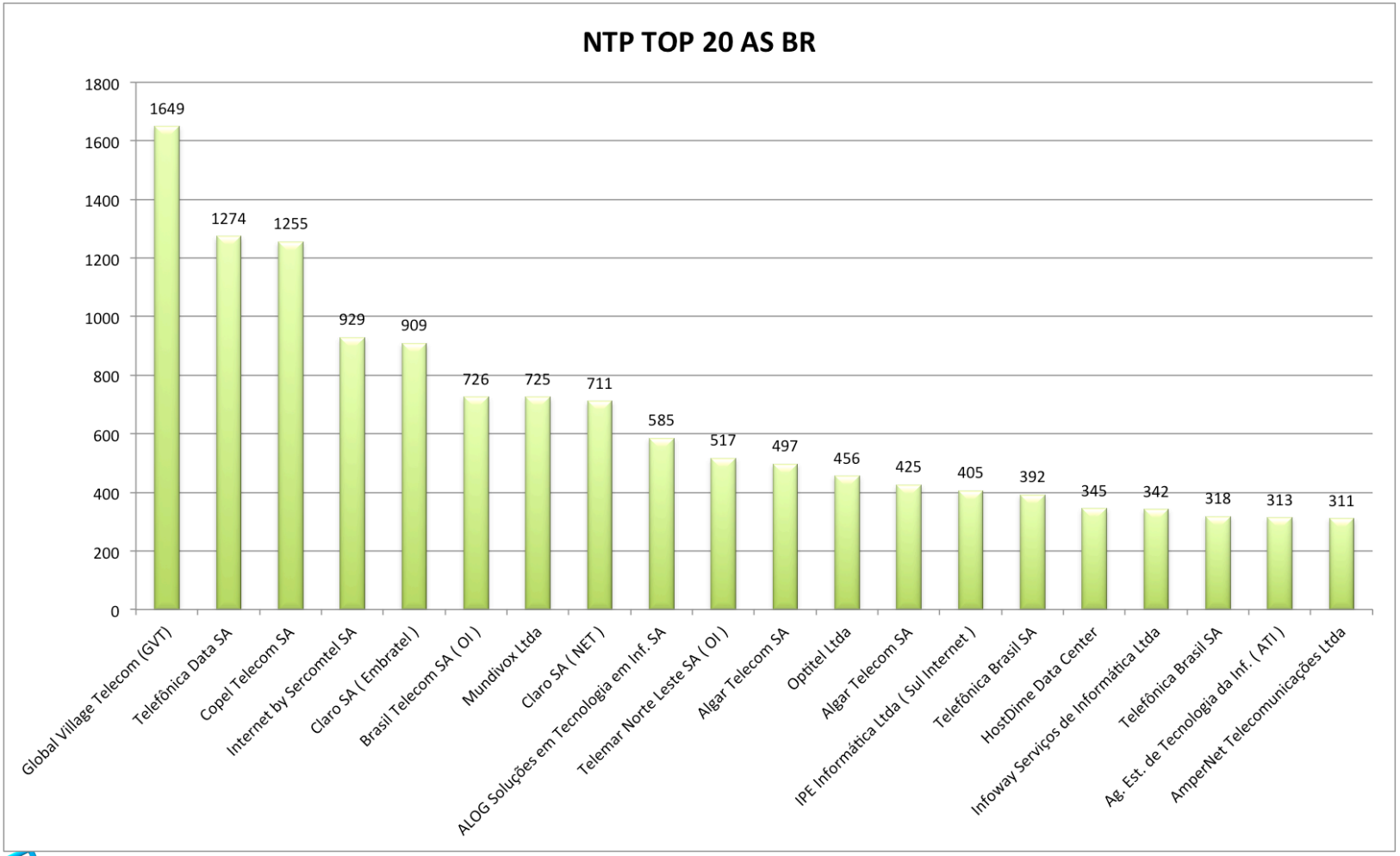
Network Education

NTP – Visão TOP 10 ASN's BR



Network Education

NTP – Visão TOP 20 ASN's BR



Network Education

NTP– Prevenção

Evitar input de redes indesejadas em seus servidores NTP e forward para clientes com destino a porta 123/ UDP.

Evita o ataque?

Maiores informações:

http://www.us-cert.gov/ncas/alerts/TA14-013A

http://ntp.br

DNS - Domain Name System

Domain Name System (**DNS**) é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. Ele baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu IP.

Endereço -> IP

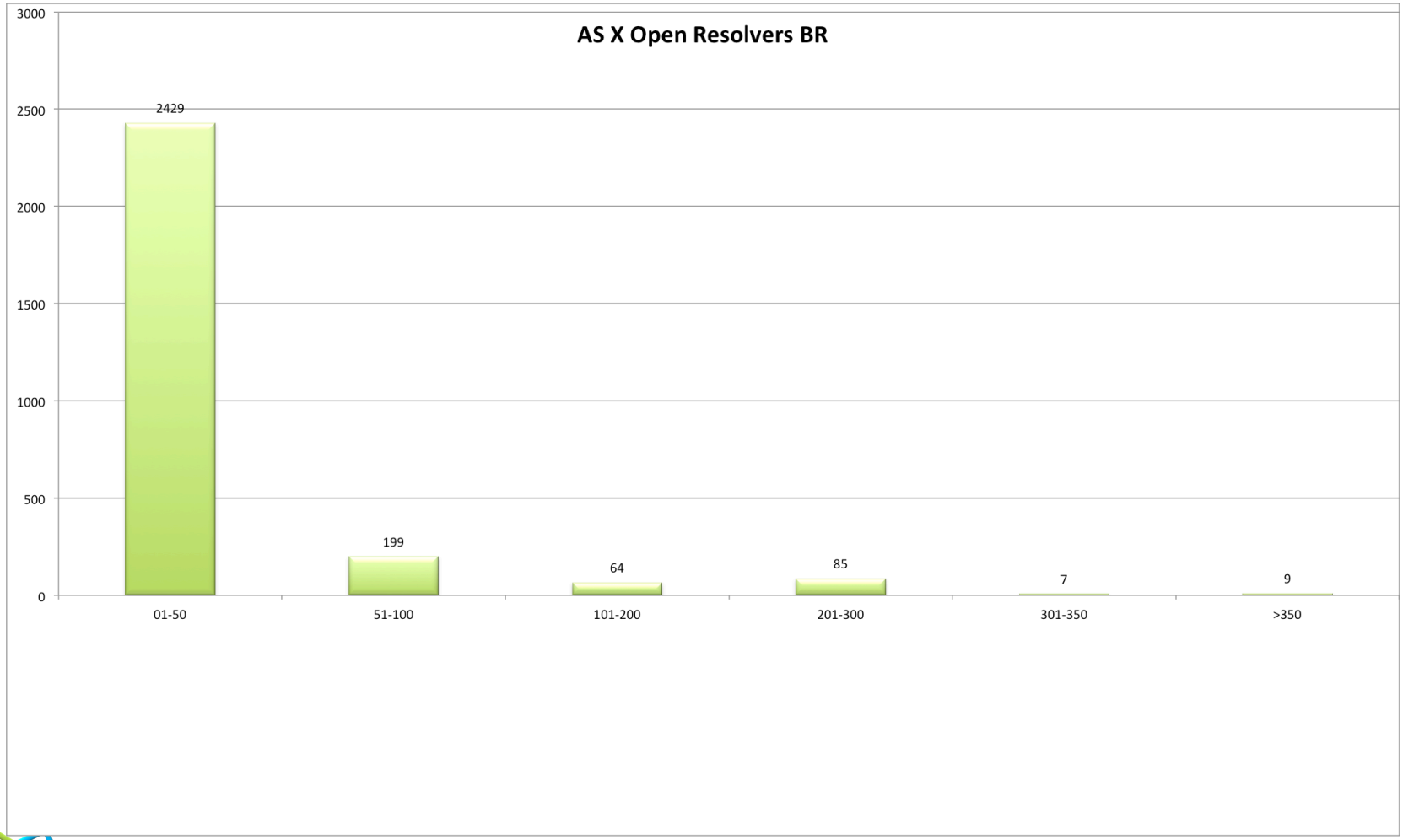
DNS – Domain Name System

Em ataque de amplificação, o DNS é capaz de amplificar um ataque com taxas de 28 a 54 X*.

Protocolo: UDP/TCP

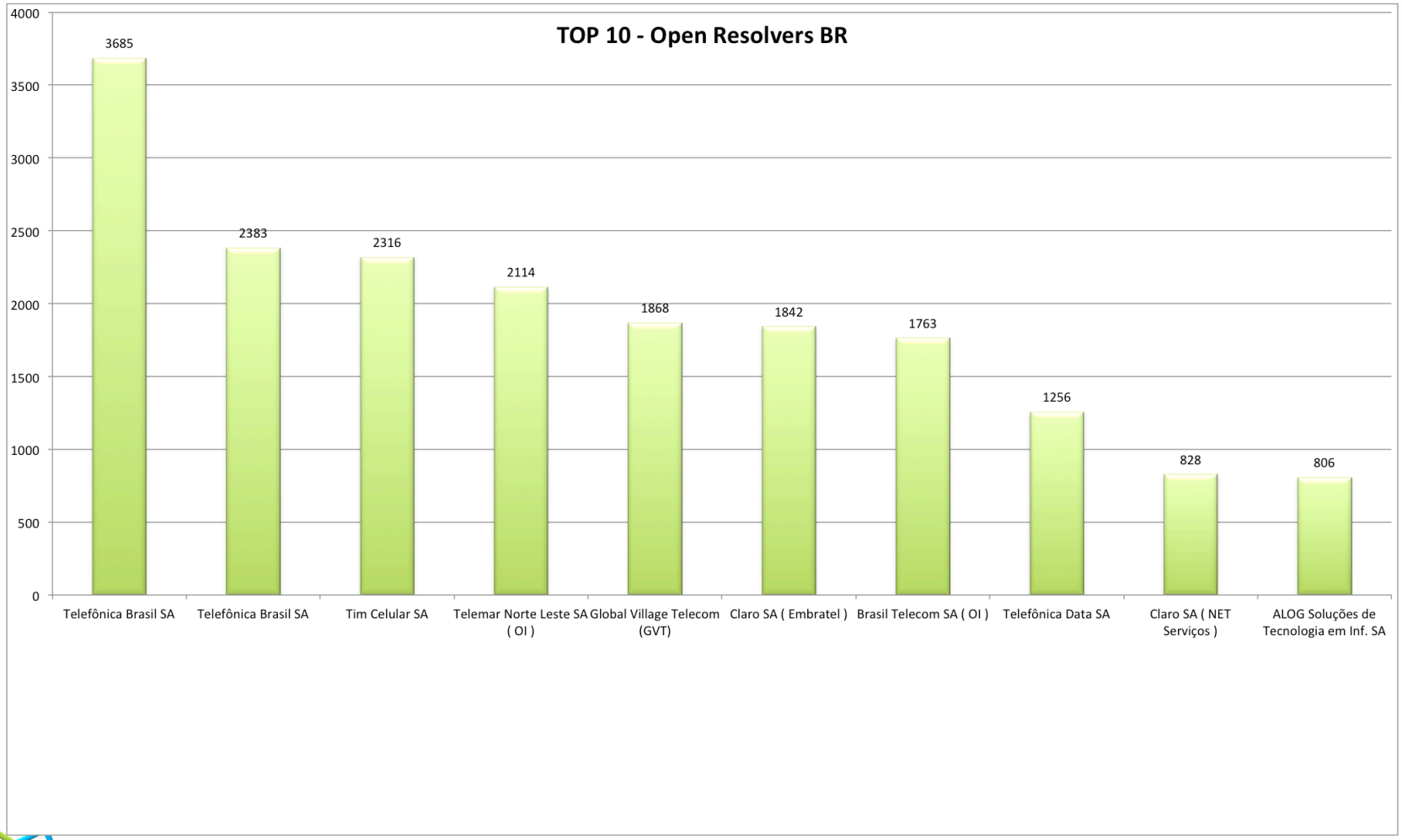
Porta: 53

DNS – Visão Geral ASN's BR



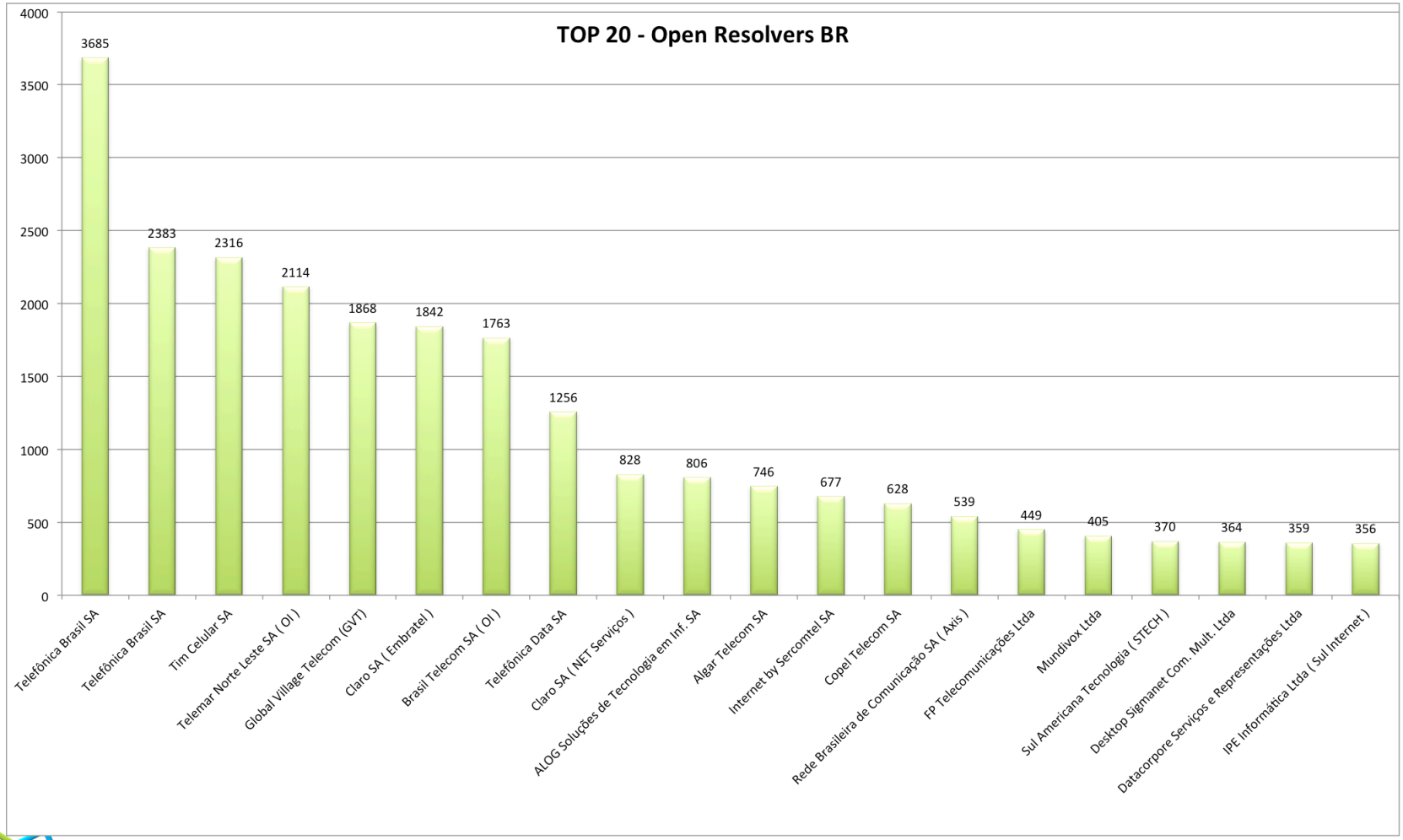
Network Education

DNS – TOP 10 ASN's BR



Network Education

DNS – TOP 20 ASN's BR



Network Education

DNS – Prevenção

Evitar input de redes indesejadas em seus servidores DNS e forward para clientes com destino a porta 53/ UDP/TCP.

Evita o ataque?

http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Considerações

- Posso bloquear o tráfego para meu cliente? Não fere o Marco Civil?

Considerações

- Posso bloquear o tráfego para meu cliente? Não fere o Marco Civil?

"III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede;"

LEI Nº 12.965, DE 23 DE ABRIL DE 2014

Informações: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

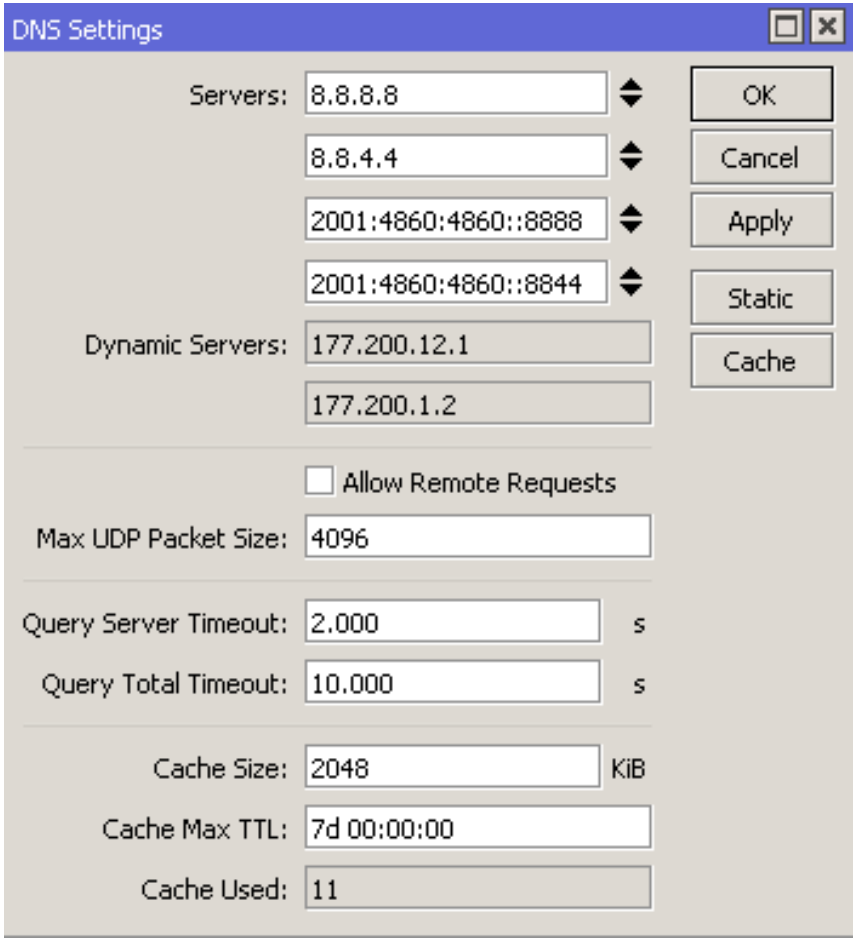
Considerações – Usuários Mikrotik

Em 93% (média) dos ASN's "menores", os dispositivos com dns "aberto" são dispositivos que rodam **RouterOS (Mikrotik)**.

FONTE: Scan com NMAP em mais de 30 asns.

Considerações – Usuários Mikrotik

É culpa da Mikrotik?



Network Education

Considerações – Usuários Mikrotik

A Wiki Oficial deixa bem claro:

DNS Cache Setup

- Submenu level: **/ip dns**

Description

DNS facility is used to provide domain name resolution for router itself as well as for the clients connected to it.

Property Description

Property	Desciption
allow-remote-requests (*yes / no; default: no*)	specifies whether to allow network requests
cache-max-ttl (*time; default: 1w*)	specifies maximum time-to-live for cache records. In other words, cache records will expire unconditionally after cache-max-ttl time. Shorter TTL received from DNS servers are respected
cache-size (*integer: 512..10240; default: 2048KiB*)	specifies the size of DNS cache in KiB
cache-used (*read-only: integer*)	displays the current cache size in KiB
servers (*IPv4/IPv6 address list; default: 0.0.0.0*)	comma seperated list of DNS server IP addresses

Considerações – Usuários Mikrotik

- Então, como utilizar?

1 – Diferentemente de outros serviços, o servidor de dns do mikrotik não permite especificar a range ou networks que poderão “usufruir” do serviço.

Considerações – Usuários Mikrotik

- Então, como utilizar?

2 – Habilitar a função para permitir requests remotos, mas se certificar que o firewall estará “vigiando” e impedindo que nenhuma requisição de fora da sua rede seja respondida.

Considerações – Usuários Mikrotik

- Então, como utilizar?

3 (~~A Melhor~~) – Não utilizar o DNS do Mikrotik.

Tenha seu próprio DNS dentro da sua rede.

NÃO EM ROUTEROS (MIKROTIK) !

Network Education

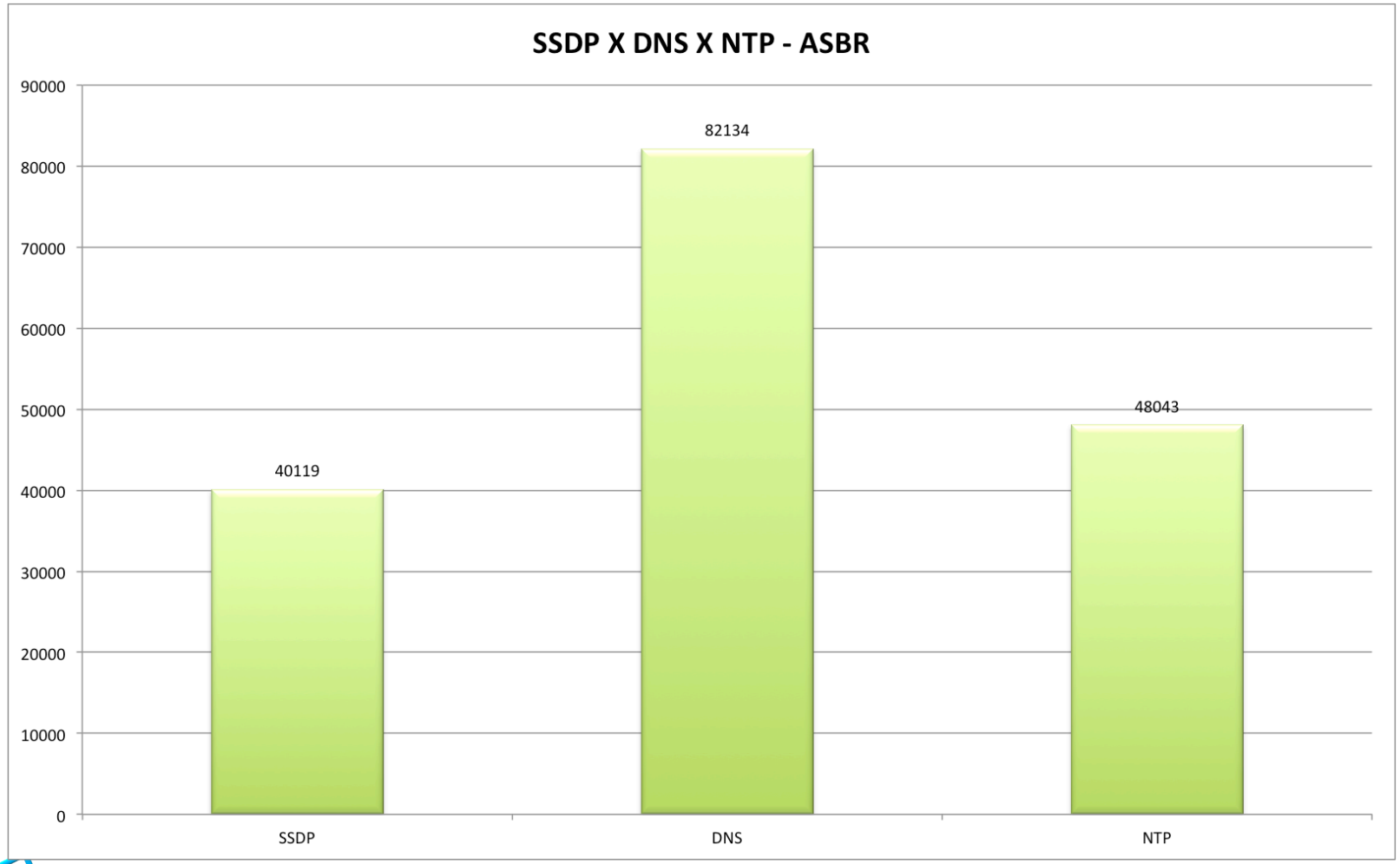
Considerações – Usuários Mikrotik

- E o firewall?

Lembre-se, que neste natal o presente pode vir em IPv6!

Network Education

Visão Geral ASN's BR



Network Education

TOP 20 – Poder de Fogo (SSDP)

ASN	Disp. Vul	Proprietário ASN	Gbps
18881	2079	Global Village Telecom (GVT)	60,91
22689	1160	Internet by Sercomtel SA	33,98
14868	1137	Copel Telecom SA	33,31
8167	1055	Brasil Telecom SA (OI)	30,91
53006	726	Algar Telecom SA	21,27
28573	689	Claro SA (NET)	20,19
10429	637	Telefônica Data SA	18,66
28668	567	Silva e Silveira S/C Ltda (IPNET)	16,61
4230	529	Claro SA (Embratel)	15,50
7738	521	Telemar Norte Leste SA (OI)	15,26
17222	449	MundiVox Ltda	13,15
28303	310	Optitel Ltda	9,08
16735	279	Algar Telecom SA	8,17
16397	267	Alog Soluções de Tec. Em Inf. Ltda	7,82
26599	267	Telefônica Brasil SA	7,82
28652	258	Telecomunicações Nordeste Ltda	7,56
27699	251	Telefônica Brasil SA	7,35
11835	246	IPE Informática Ltda (Sul Internet)	7,21
53055	219	HostDime Data Center	6,42
10938	219	Ag. Est. de Tecnologia da Informação (ATI)	6,42

TOP 20 – Poder de Fogo (DNS)

ASN	Disp. Vuln.	Proprietário ASN	Gbps
26599	3685	Telefônica Brasil SA	194,33
27699	2383	Telefônica Brasil SA	125,67
26615	2316	Tim Celular SA	122,13
7738	2114	Telemar Norte Leste SA (OI)	111,48
18881	1868	Global Village Telecom (GVT)	98,51
4230	1842	Claro SA (Embratel)	97,14
8167	1763	Brasil Telecom SA (OI)	92,97
10429	1256	Telefônica Data SA	66,23
28573	828	Claro SA (NET Serviços)	43,66
16397	806	ALOG Soluções de Tecnologia em Inf. SA	42,50
16735	746	Algar Telecom SA	39,34
22689	677	Internet by Sercomtel SA	35,70
14868	628	Copel Telecom SA	33,12
28202	539	Rede Brasileira de Comunicação SA (Axis)	28,42
262346	449	FP Telecomunicações Ltda	23,68
17222	405	Mundivox Ltda	21,36
25933	370	Sul Americana Tecnologia (STECH)	19,51
28649	364	Desktop Sigmanet Com. Mult. Ltda	19,20
28271	359	Datacorpore Serviços e Representações Ltda	18,93
11835	356	IPE Informática Ltda (Sul Internet)	18,77

Network Education

TOP 20 – Poder de Fogo (NTP)

ASN	Disp. Vul.	Proprietário ASN	Gbps
18881	1649	Global Village Telecom (GVT)	895,36
10429	1274	Telefônica Data SA	691,74
14868	1255	Copel Telecom SA	681,43
22689	929	Internet by Sercomtel SA	504,42
4230	909	Claro SA (Embratel)	493,56
8167	726	Brasil Telecom SA (OI)	394,20
17222	725	Mundivox Ltda	393,65
28573	711	Claro SA (NET)	386,05
16397	585	ALOG Soluções em Tecnologia em Inf. SA	317,64
7738	517	Telemar Norte Leste SA (OI)	280,71
16735	497	Algar Telecom SA	269,86
28303	456	Optitel Ltda	247,59
53006	425	Algar Telecom SA	230,76
11835	405	IPE Informática Ltda (Sul Internet)	219,90
27699	392	Telefônica Brasil SA	212,84
53055	345	HostDime Data Center	187,32
28368	342	Infoway Serviços de Informática Ltda	185,70
26599	318	Telefônica Brasil SA	172,66
10938	313	Ag. Est. de Tecnologia da Inf. (ATI)	169,95
28158	311	AmperNet Telecomunicações Ltda	168,86

Visão Geral – Poder de Amplificação

Dispositivo vulnerável com 1 Mb de upload.

DNS (54x) = 1Mb X 54 X 48043 = **2,47 Tb**

SSDP (30x) = 1Mb X 30 X 40119 = **1,14 Tb**

NTP (556x) = 1Mb X 556 X 82134 = **43,55 Tb**

2,47 + 1,14 + 43,55 = 47,16 Tb

Network Education

Agradecimentos

Rubens Kuhl

Uesley Corrêa

nic.br

Network Education

Obrigado!!!

Elizandro Pacheco

(Network Education)

elizandro@network.education

Skype: elizandropacheco

Fone: +55 (48) 99144771

Uesley Corrêa

(Network Education)

uesley@network.education

Skype: uesleycorrea

Network Education

UBIQUITI NETWORKS

AUTHORIZED TRAINING PARTNER