nic.br cgi.br | 20 anos cert.br

IX Fórum Regional

17 de maio de 2018

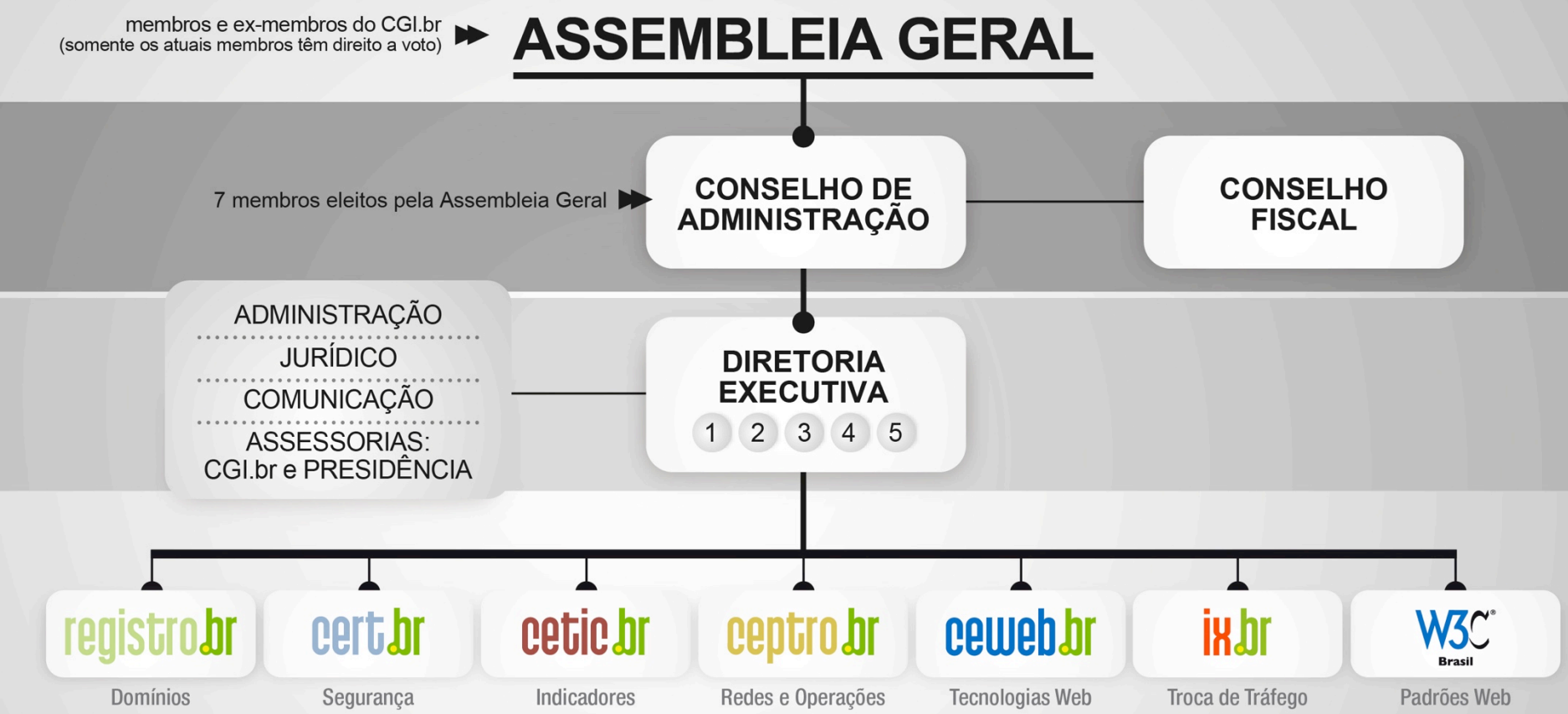
São Paulo, SP

Boas Práticas de Segurança para Sistemas Autônomos

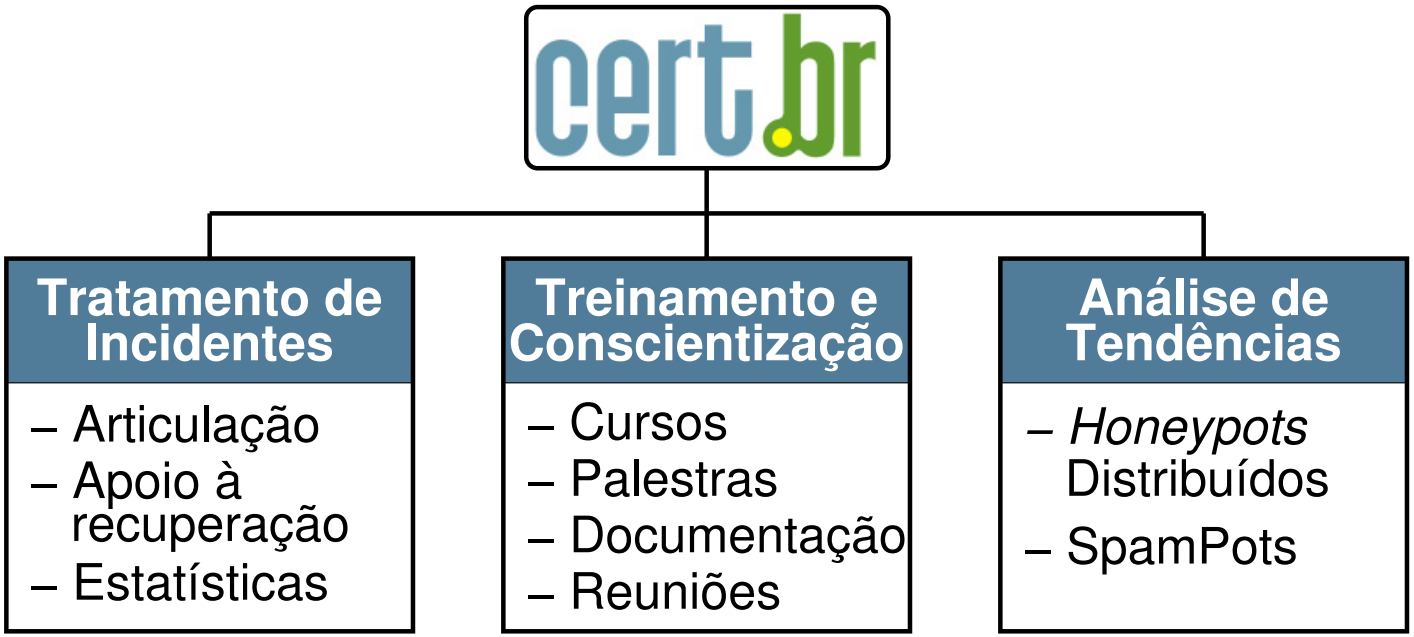
Klaus Steding-Jessen, D.Sc.
Gerente Técnico
jessen@cert.br

20 anos cert.br nic.br cgi.br

Estrutura do NIC.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Principais atividades:

- **Tratamento de Incidentes**
  - Ponto de contato nacional para notificação de incidentes
  - Atua facilitando o processo de resposta a incidentes das várias organizações
  - Trabalha em colaboração com outras entidades
  - Auxilia novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades
- **Formação de profissionais para atuar em Tratamento de Incidentes**
- **Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet para diversas audiências**

Agenda

Revisão de *NetFlows*

Ataques DDoS com *spoofing* e amplificação

- exemplos, análise de *logs* e testes
- boas práticas

Comprometimento de CPEs

- comprometidos para alteração de DNS
- infectados por *botnets* para DDoS
- exemplos e testes
- boas práticas

Comprometimento de roteadores de borda

- para sequestro de rotas BGP
- boas práticas

Conclusão e sumário das boas práticas

Revisão de *NetFlows*:
O que é um *NetFlow* (1/2)

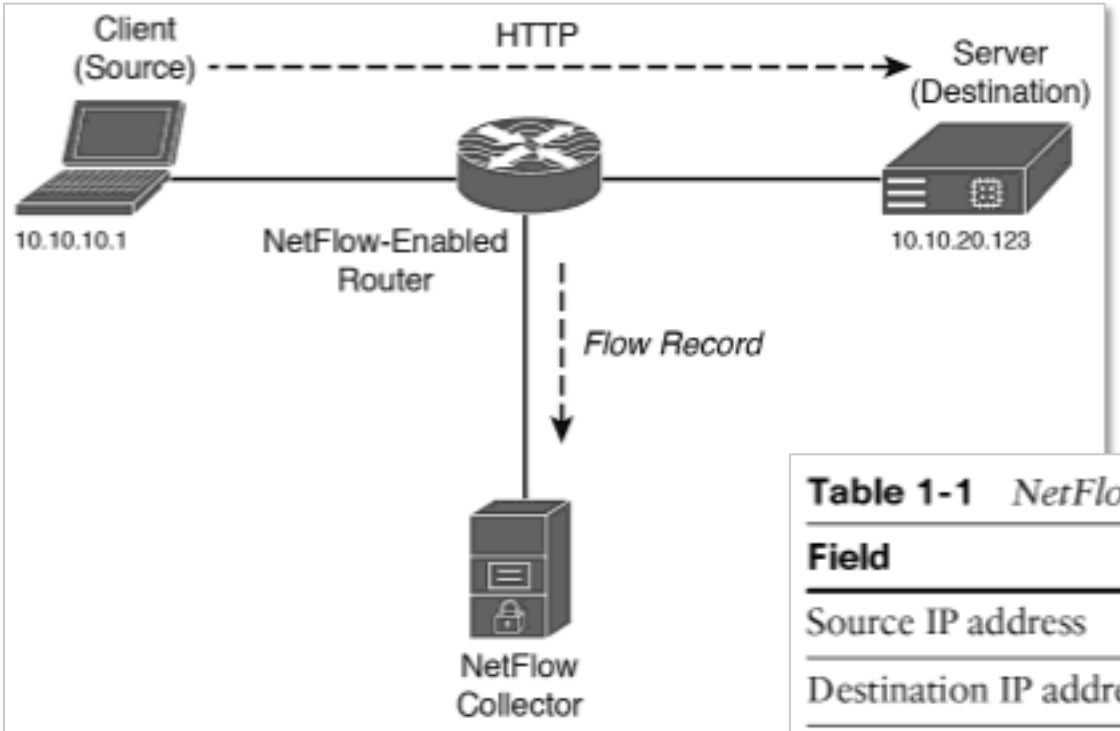


Figure 1-2 *Basic NetFlow Example*

Table 1-1 *NetFlow Five-Tuple*

Field	Value
Source IP address	10.10.10.1
Destination IP address	10.10.20.123
Source port	13578
Destination port	80
Protocol	TCP

Fonte: ***Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security***
http://www.ciscopress.com/store/network-security-with-netflow-and-ipfix-big-data-analytics-9781587144387

Revisão de *NetFlows*: **O que é um *NetFlow* (2/2)**

Campos de um registro *NetFlow*:

- ***Input interface***
- ***Output interface***
- ***Timestamps for the flow start and finish time***
- ***Number of bytes and packets observed in the flow***
- ***Layer 3 headers:***
  - *Source & destination IP addresses*
  - *ICMP Type and Code*
  - *IP protocol*
  - *Type of Service (ToS)*
- ***Source and destination port numbers for TCP, UDP***
- ***For TCP flows, the union of all TCP flags observed over the life of the flow***
- ***Layer 3 Routing information:***
  - *IP address of the immediate next-hop*
  - *Source & destination IP masks*

Fonte: *NetFlow – Wikipedia*
https://en.wikipedia.org/wiki/NetFlow

Revisão de *NetFlows*: **Referências**

RFC 7011 / STD 77: *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*

- https://tools.ietf.org/html/rfc7011

NetFlow version 9

- https://www.cisco.com/c/en/us/products/ios-nx-os-software/netflow-version-9/

NFDUMP/ NfSen

- http://nfdump.sourceforge.net

Mikrotik Traffic Flow

- https://wiki.mikrotik.com/wiki/Manual:IP/Traffic_Flow

Juniper Flow Monitoring

- https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/services-interfaces/flow-monitoring.html

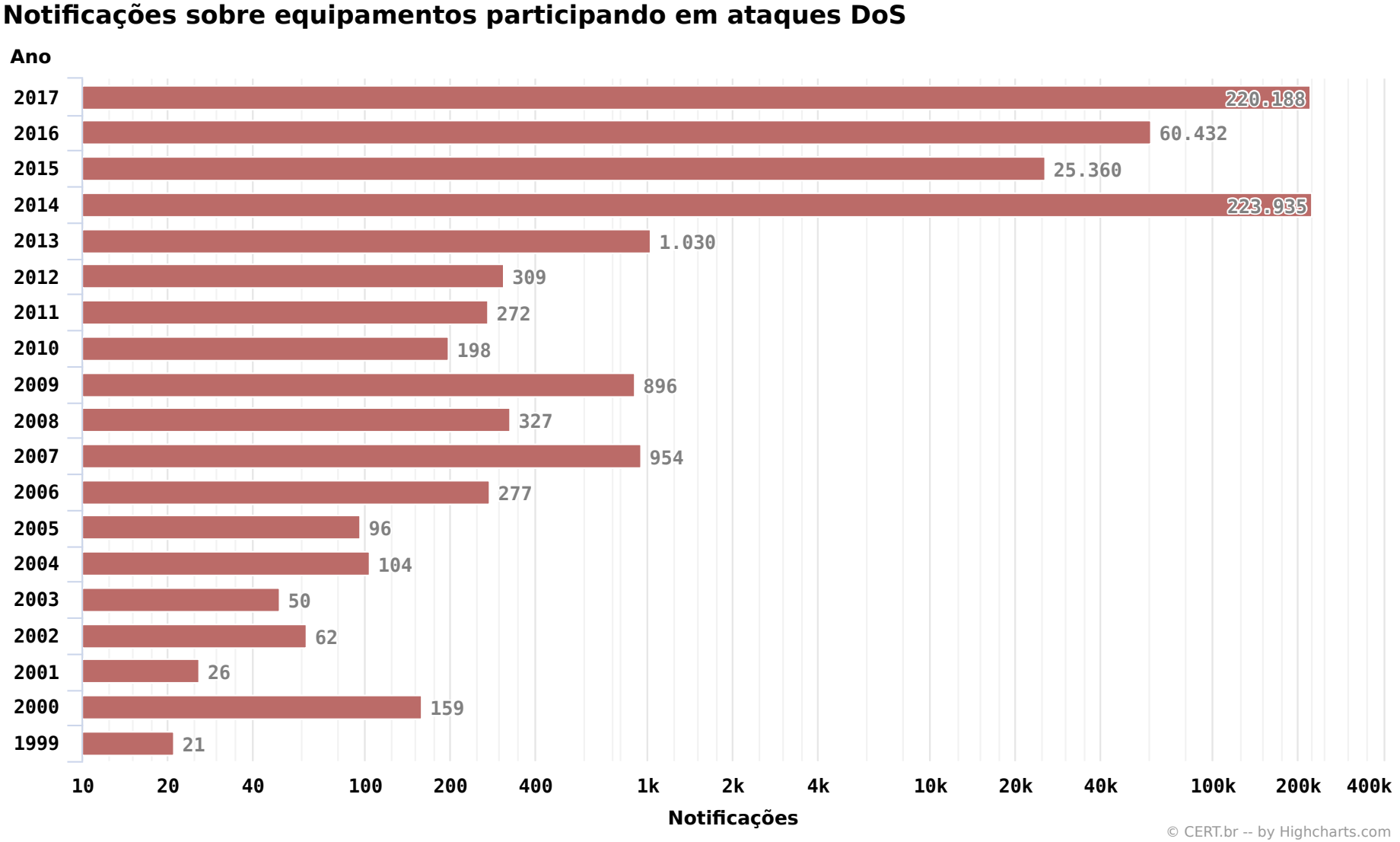
Uso de *Flows* no Tratamento de Incidentes da Unicamp

- ftp://ftp.registro.br/pub/gts/gts26/01-flows-unicamp.pdf
- https://youtu.be/ckEX7vUFOzk

Ataques DDoS com *Spoofing* e Amplificação

cert.br nic.br cgi.br

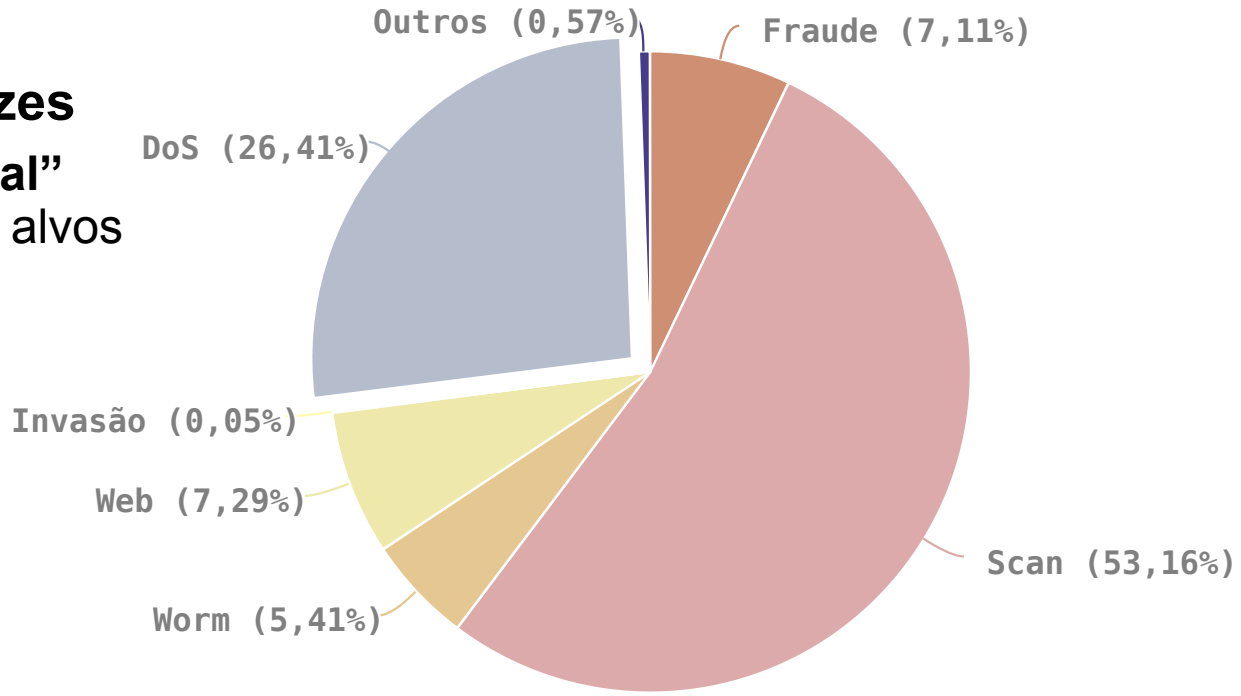
Incidentes Notificados ao CERT.br:
DDoS ao Longo do Tempo



Incidentes Notificados ao CERT.br em 2017: **Características dos Ataques DDoS**

DDoS – aumento de 4 vezes

- **300Gbps é o novo "normal"**
  - Até 1Tbps contra alguns alvos
- **Tipos mais frequentes**
  - amplificação
  - *botnets* IoT



Atividades nos *Honeypots* Distribuídos: **Serviços mais Visados**

Força bruta de senhas (usado por malwares de IoT e para invasão de servidores e roteadores):

- Telnet (23/TCP)
- SSH (22/TCP)
- Outras TCP (2323, 23231, 2222)

Protocolos explorados pela *botnet* Mirai, na variante para CPEs (roteadores de banda larga)

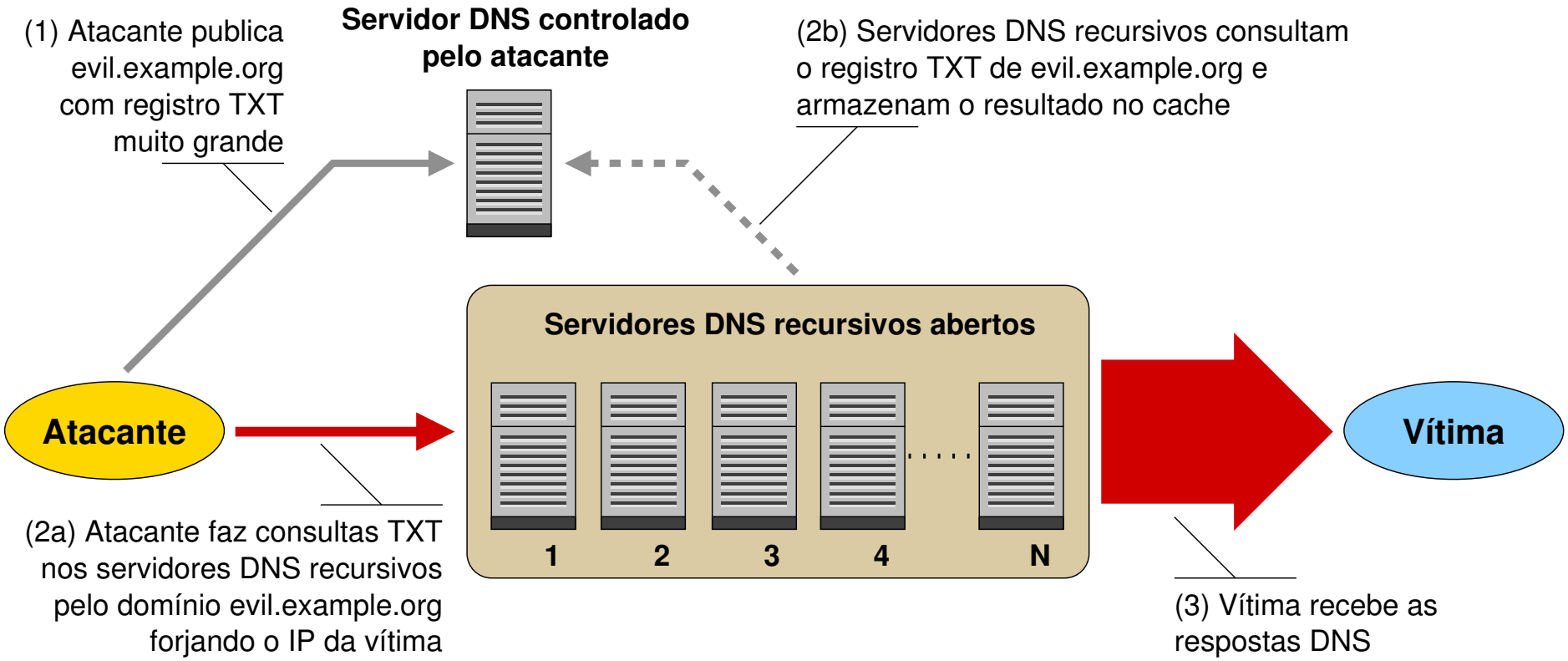
- TCP: 7547, 5555, 37777, 6789, 81, 37215, 52869

Busca por protocolos que permitam amplificação

- UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

Projeto *Honeypots* Distribuídos
https://honeytarg.cert.br/honeypots/

Ataques DDoS com Amplificação: **Como Ocorrem**



Fonte:
Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
https://bcp.nic.br/dns-recursivo/

Ataques DDoS com 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

Fonte: https://www.us-cert.gov/ncas/alerts/TA14-017A

Dispositivos / Serviços que Permitem Amplificação: **Total no Brasil de ASNs e IPs Notificados**

	DNS		SNMP		NTP		SSDP	
2017	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.133	87.953	–	–	981	97.423	–	–
Fevereiro	2.066	67.159	1.681	573.373	–	–	805	37.459
Março	–	–	1.805	604.805	915	104.665	–	–
Abril	2.191	72.124	–	–	861	92.120	812	27.233
Maio	2.280	69.957	1.869	573.400	–	–	839	40.814
Junho	2.183	64.179	1.948	596.348	860	91.257	812	33.805
Julho	–	–	1.963	551.953	841	107.097	–	–
Agosto	2.347	72.677	2.018	554.457	872	108.168	891	27.209
Setembro	2.307	62.283	1.791	406.015	800	89.603	–	–
Outubro	2.328	67.066	1.886	343.674	845	108.605	902	32.056
Novembro	2.279	61.281	–	–	–	–	863	26.999
Dezembro	2.436	62.758	2.001	460.519	–	–	845	27.828
2018	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.412	61.875	2.130	479.247	823	97.075	888	25.982
Fevereiro	2.438	72.185	2.324	559.784	849	93.801	778	20.210
Março	2.476	63.811	2.278	515.345	844	84.483	544	11.431

Legenda: "–" significa que não foi realizada notificação desta categoria no referido mês

Ataques DDoS com Amplificação:
Volume de Tráfego LDAP – 1 dispositivo em 1 dia

Exemplo de consulta *NetFlow*

- origem com porta LDAP (389/UDP)
- *bytes*/pacote > 1000
- tráfego agregado por
  - protocolo, IP de origem, porta de origem

```
$ nfdump -R /var/log/flows/2017/12/06 -A proto,srcip,srcport -o line6 'src
net xx.xx.xx.xx/nn and not dst net xx.xx.xx.xx/nn and proto udp and bpp >
1000 and src port 389'

Aggregated flows 1

Date first seen          Duration Proto Src IP Addr:Port   Dst IP Addr:Port
Packets Bytes Flows

2017-12-06 00:00:04.368 86394.930 UDP   <ip-LDAP>:389 -> 0.0.0.0:0
4.7 M   7.1 G  9121

Summary: total flows: 9121, total bytes: 7107660800, total packets: 4669952,
avg bps: 658155, avg pps: 54, avg bpp: 1521

Time window: 2017-12-06 00:00:00 - 2017-12-06 23:59:59

Total flows processed: 77280421, Blocks skipped: 0, Bytes read: 4958493112

Sys: 29.131s flows/second: 2652796.7  Wall: 36.507s flows/second: 2116808.0
```

Ataques DDoS com Amplificação:
Detecção de grandes geradores de tráfego

```
$ nfdump -R /var/log/flows/2017/12/07 -s srcip/bytes -L 10G -n 10 'src net
xx.xx.xx.xx/nn and not dst net xx.xx.xx.xx/nn and not ip in [ @include
servers.txt ]'

Top 10 Src IP Addr ordered by bytes:
     Src IP Addr  Flows(%)     Packets(%)       Bytes(%)      pps       bps   bpp
    xxx.xxx.9.28  1.9 M(16.6) 983.8 M(16.6)   1.4 T(38.6) 17919  206.0 M  1436
   xxx.xxx.18.85 154428( 1.3)  79.1 M( 1.3) 100.8 G( 2.8)  1443   14.7 M  1275
   xxx.xxx.62.49 128903( 1.1)  66.0 M( 1.1)  94.6 G( 2.6)  2102   24.1 M  1432
   xxx.xxx.46.36 266474( 2.3) 136.4 M( 2.3)  93.3 G( 2.6)  2486   13.6 M   683
    xxx.x.106.10 109648( 0.9)  56.1 M( 0.9)  80.9 G( 2.2)  1126   13.0 M  1440
  xxx.xxx.75.167 108737( 0.9)  55.7 M( 0.9)  80.5 G( 2.2)  1296   15.0 M  1446
    xxx.xxx.2.21 134183( 1.2)  68.7 M( 1.2)  80.0 G( 2.2)  1251   11.7 M  1164
 xxx.xxx.236.103 103314( 0.9)  52.9 M( 0.9)  75.2 G( 2.1)   965   11.0 M  1421
  xxx.xxx.10.215  73854( 0.6)  37.8 M( 0.6)  54.9 G( 1.5)   688    8.0 M  1451
   xxx.xxx.125.2  83531( 0.7)  42.8 M( 0.7)  46.2 G( 1.3)   779    6.7 M  1080

Summary: total flows: 11587182, total bytes: 3657941800960, total packets:
5932637184, avg bps: 533034287, avg pps: 108062, avg bpp: 616
Time window: 2017-12-07 00:00:00 - 2017-12-07 15:14:59
Total flows processed: 41883344, Blocks skipped: 0, Bytes read: 2687644604
Sys: 16.990s flows/second: 2465146.9  Wall: 16.975s flows/second: 2467332.3
```

Testes por Amplificação: **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`

Exemplo de *log* de notificação de incidente: **DRDoS com Amplificação DNS**

```
14:35:45.162708 IP (tos 0x0, ttl 49, id 46286, offset 0, flags [+], proto
UDP (17), length 1500) <recursivo-aberto>.53 > <vitima>.17824: 57346 243/2/0
saveroads.ru. A 204.46.43.71, saveroads.ru.[|domain]
        0x0000:  4500 05dc b4ce 2000 3111 c6fa xxxx xxxx  E.....1...._P.
        0x0010:  xxxx xxxx 0035 45a0 0f99 9769 e002 8180  ...0.5E....i....
        0x0020:  0001 00f3 0002 0000 0973 6176 6572 6f61  .........saveroa
        0x0030:  6473 0272 7500 00ff 0001 c00c 0001 0001  ds.ru...........
        0x0040:  0000 707b 0004 cc2e 2b47 c00c            ..p{....+G..
14:35:45.163029 IP (tos 0x0, ttl 49, id 46287, offset 0, flags [+], proto
UDP (17), length 1500) <recursivo-aberto>.53 > <vitima>.17824: 57346 243/2/0
saveroads.ru. A 204.46.43.72, saveroads.ru.[|domain]
        0x0000:  4500 05dc b4cf 2000 3111 c6f9 xxxx xxxx  E.....1...._P.
        0x0010:  xxxx xxxx 0035 45a0 0f99 1946 e002 8180  ...0.5E....F....
        0x0020:  0001 00f3 0002 0000 0973 6176 6572 6f61  .........saveroa
        0x0030:  6473 0272 7500 00ff 0001 c00c 0001 0001  ds.ru...........
        0x0040:  0000 707b 0004 cc2e 2b48 c00c            ..p{....+H..
14:35:45.164011 IP (tos 0x0, ttl 49, id 46288, offset 0, flags [+], proto
UDP (17), length 1500) <recursivo-aberto>.53 > <vitima>.17824: 57346 243/2/0
saveroads.ru. A 204.46.43.73, saveroads.ru.[|domain]
        0x0000:  4500 05dc b4d0 2000 3111 c6f8 xxxx xxxx  E.....1...._P.
        0x0010:  xxxx xxxx 0035 45a0 0f99 5e23 e002 8180  ...0.5E...^#....
        0x0020:  0001 00f3 0002 0000 0973 6176 6572 6f61  .........saveroa
        0x0030:  6473 0272 7500 00ff 0001 c00c 0001 0001  ds.ru...........
        0x0040:  0000 707b 0004 cc2e 2b49 c00c            ..p{....+I..
```

DRDoS - ***Distributed Reflective Denial of Service***

Exemplo de *log* de notificação de incidente: **DRDoS com Amplificação NTP**

```
19:08:57.264596 IP <ntp-aberto>.123 > <vitima>.25565: NTPv2, Reserved,
length 440
        0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
        0x0010:  xxxx xxxx 007b 63dd 01c0 cca8 d704 032a  .....{c........*
        0x0020:  0006 0048 0000 0021 0000 0080 0000 0000  ...H...!........
        0x0030:  0000 0005 c6fb 5119 bd2a 78e1 0000 0001  ......Q..*x.....
        0x0040:  1b5c 0702 0000 0000 0000 0000            .\..........
19:08:57.276585 IP <ntp-aberto>.123 > <vitima>.25565: NTPv2, Reserved,
length 440
        0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
        0x0010:  xxxx xxxx 007b 63dd 01c0 03a7 d707 032a  .....{c........*
        0x0020:  0006 0048 0000 000c 0000 022d 0000 0000  ...H.......-....
        0x0030:  0000 001c 32a8 19e0 bd2a 78e1 0000 0001  ....2....*x.....
        0x0040:  0c02 0702 0000 0000 0000 0000            ............
19:08:57.288489 IP <ntp-aberto>.123 > <vitima>.25565: NTPv2, Reserved,
length 440
        0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
        0x0010:  xxxx xxxx 007b 63dd 01c0 e8af d735 032a  .....{c......5.*
        0x0020:  0006 0048 0000 00bf 0000 782a 0000 0000  ...H......x*....
        0x0030:  0000 0056 ae7f 7038 bd2a 78e1 0000 0001  ...V..p8.*x.....
        0x0040:  0050 0702 0000 0000 0000 0000            .P..........
19:08:57.296481 IP <ntp-aberto>.123 > <vitima>.25565: NTPv2, Reserved,
length 440
        0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
        0x0010:  xxxx xxxx 007b 63dd 01c0 03ae d75e 032a  .....{c......^.*
        0x0020:  0006 0048 0000 004d 0000 bb31 0000 0000  ...H...M...1....
        0x0030:  0000 0014 4814 25da bd2a 78e1 0000 0001  ....H.%..*x.....
        0x0040:  0050 0702 0000 0000 0000 0000            .P..........
```

Exemplo de *log* de notificação de incidente: **DRDoS com Amplificação Chargen**

```
20:04:33.857139 IP <ip-chargen>.19 > <vitima>.3074: UDP, length 3665
        0x0000:  4500 05c4 2f7f 2000 7611 8ba4 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0e59 e56d 2021 2223  H........Y.m.!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
20:04:33.894696 IP <ip-chargen>.19 > <vitima>.3074: UDP, length 3676
        0x0000:  4500 05c4 2f80 2000 7611 8ba3 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0e64 2e82 2021 2223  H........d...!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
20:04:33.932308 IP <ip-chargen>.19 > <vitima>.3074: UDP, length 3687
        0x0000:  4500 05c4 2f81 2000 7611 8ba2 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0e6f 3199 2021 2223  H........o1..!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
20:04:33.970323 IP <ip-chargen>.19 > <vitima>.3074: UDP, length 3797
        0x0000:  4500 05c4 2f82 2000 7611 8ba1 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0edd 44dc 2021 2223  H.........D..!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
20:04:34.008938 IP <ip-chargen>.19 > <vitima>.3074: UDP, length 3797
        0x0000:  4500 05c4 2f83 2000 7611 8ba0 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0edd 44dc 2021 2223  H.........D..!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
```

Ataques DDoS com *Spoofing* e Amplificação: **Boas Práticas**

Reduzir ataques DDoS saindo de sua rede

- implementar *antispoofing* (BCP 38) - https://bcp.nic.br/antispoofing
- fechar servidores DNS recursivos abertos - https://bcp.nic.br/dns-recursivo
- configurar os CPEs, servidores, roteadores e elementos de rede para
  - não ter serviços abertos de frente para a Internet
    - como SNMP, NTP, DNS, Chargen, SSDP

Ativar *NetFlows* para detectar abuso de sua rede

- ótimas opções de *software* livre (`nfdump`/`nfsen`)

Receber e tratar notificações, que são enviadas para:

- *e-mail* do contato `abuse-c` do ASN no serviço whois
- *e-mail* de abuse ou do grupo de tratamento de incidentes

Estas e outras recomendações em:

- Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS), Seção 5
  https://bcp.nic.br/ddos#5

Comprometimento de CPEs (*modems* e roteadores de banda larga)

cert.br nic.br cgi.br

Atividades nos *Honeypots* Distribuídos: **Serviços mais Visados**

Força bruta de senhas (usado por *malwares* de IoT e para invasão de servidores e roteadores):

- Telnet (23/TCP)
- SSH (22/TCP)
- Outras TCP (2323, 23231, 2222)

Protocolos explorados pela *botnet* Mirai, nas variantes para CPEs (roteadores de banda larga)

- TCP: 7547, 5555, 37777, 6789, 81, 37215, 52869

Ataques a *Modems* / Roteadores de Banda Larga **para Alteração de DNS para fraudes**

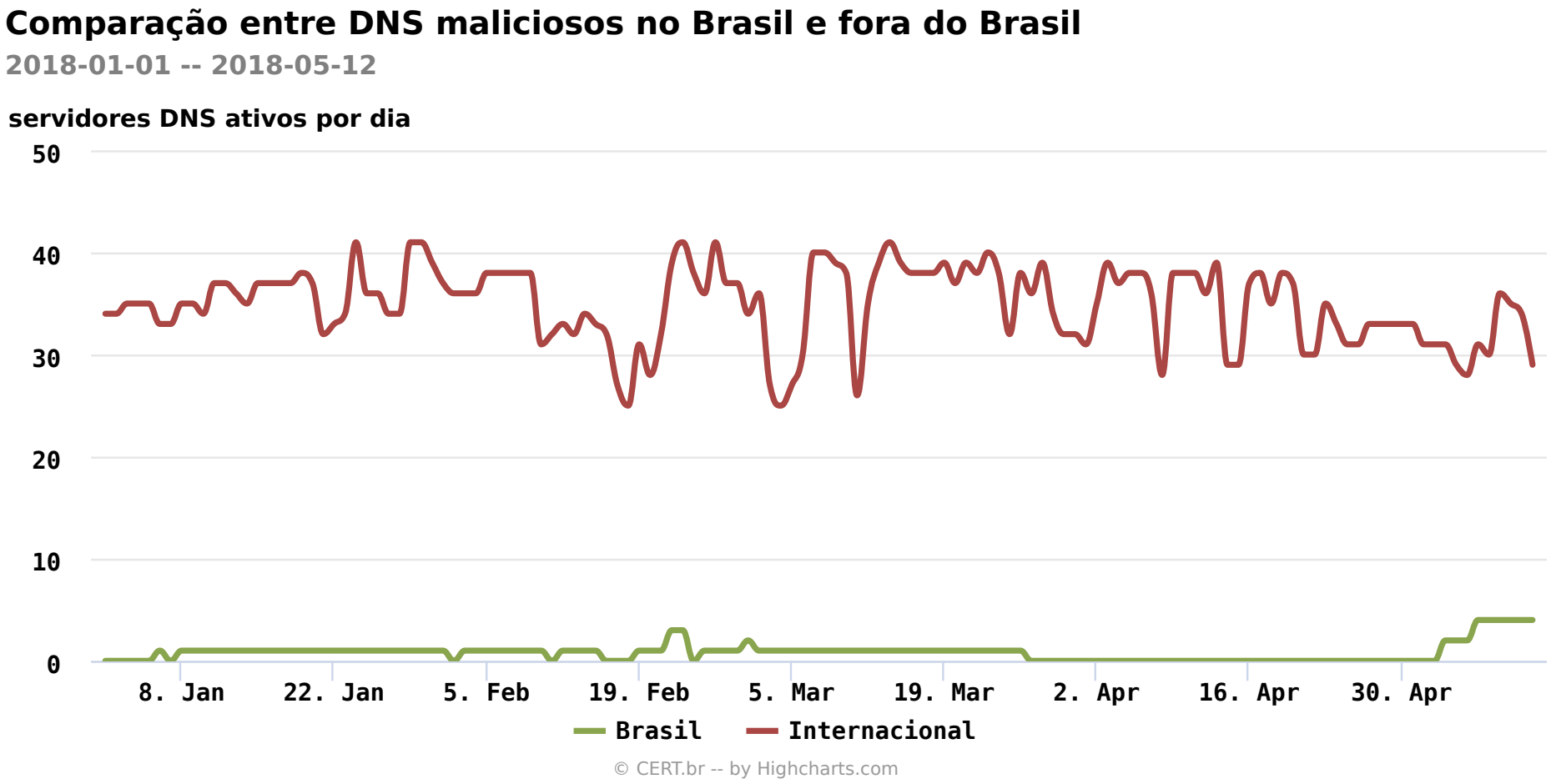
Comprometidos

- via força bruta de senhas (geralmente via telnet)
- explorando vulnerabilidades
- via ataques CSRF, através de *iFrames* com *JavaScripts* maliciosos
  - Colocados em *sites* legítimos comprometidos pelos fraudadores

Objetivos dos ataques

- **alterar a configuração de DNS para que consultem servidores sob controle dos atacantes**
- servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud*
  - casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

Servidores DNS Maliciosos *Online*/Dia: **Volume Constante Indica que é Efetivo**



Teste de Servidores DNS Maliciosos: **Para Verificar se a Resposta é Maliciosa**

```
$ dig @<ip-rogue-dns> <domínio-vítima> A
```

```
$ dig @<ROGUE_DNS> paypal.com.br A
; <<>> DiG 9.9.7-P3 <<>> @<ROGUE_DNS> paypal.com.br A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22468
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;paypal.com.br. IN A

;; ANSWER SECTION:
paypal.com.br. 10800 IN A <PHISHING_IP>

;; Query time: 185 msec
;; SERVER: <ROGUE_DNS>#53(<ROGUE_DNS>)
;; WHEN: Thu Dec 07 17:05:09 -02 2017
;; MSG SIZE  rcvd: 58
```

Detecção de CPEs Comprometidos: **Via Acessos a Servidores DNS Maliciosos**

Sugestão de consulta *NetFlow*

- protocolo UDP porta destino 53 (DNS)
- origem no bloco de clientes
- cujo destino **não** seja
  - o seu recursivo
  - os servidores do Google

```
$ nfdump -R /var/log/flows/2017/12/06 'proto udp and dst port
53 and src net xx.xx.xx.xx/nn and not (dst host 8.8.4.4 or dst
host 8.8.8.8 or dst host <seu-recursivo>)'
```

Detecção de CPEs Comprometidos:
Via Acessos a Comando e Controle de *Botnets*

Sugestão de consulta *NetFlow*

- destino a IPs publicamente listados como comando e controle de *botnets* IoT (que incluem *botnets* de CPEs)

  https://www.abuseat.org/iotcc.txt

```
$ nfdump -R /var/log/flows/2017/12/06 'proto tcp and dst ip in
[ @include iotcc.txt ]'
```

Segurança de CPEs (*modems*/roteadores): **Boas Práticas de Especificação e Compra**

Ser criterioso ao escolher o fornecedor

- verificar se possui política de atualização de *firmware*
- verificar histórico de tratamento de vulnerabilidades
- identificar qual o *chipset*
  - verificar histórico de tratamento de vulnerabilidades do fabricante do *chipset*
- fazer testes antes de comprar
- checar se é possível desabilitar serviços desnecessários e trocar senhas

Antes de fazer a implantação, planejar

- algum esquema de gerência remota
- como atualizar remotamente

Segurança de CPEs (*modems*/roteadores): **Boas Práticas de Implantação e *Hardening***

Desabilitar serviços que não devem estar de frente para a Internet

- Telnet, SSH, Web, Recursivo aberto (“relay” DNS), SNMP, NTP, Chargen, SSDP, etc

Mudar senhas padrão

Manter os equipamentos atualizados

Utilizar sempre que possível uma rede de gerência

Mesmo escolhendo criteriosamente o fornecedor, assumir que os dispositivos virão com sérios problemas

- testar em ambiente controlado
- assumir que terá um “*backdoor”* do fabricante

Comprometimento de Roteadores de Borda

cert.br nic.br cgi.br

Ataques de Sequestro de Rotas BGP: **Objetivo de Perpetrar Fraudes Financeiras**

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

Equipamentos:

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

Prefixos sequestrados:

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

Levantados túneis GRE:

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

Comprometimento de Roteadores / Servidores: **Monitoração**

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

Aumentar *accounting* do roteador

- Habilitar *log* remoto dos comandos executados
- Gerar *logs* e alertas para modificações de configurações

Comprometimento de Roteadores / Servidores: **Boas Práticas para Acesso Remoto**

Para todos os serviços que necessitam de autenticação

- Jamais utilizar contas e senhas padrão ou de teste
- Utilizar senhas fortes
- Considerar autenticação de dois fatores
- Aumentar monitoração

SSH

- Permitir acesso somente via par de chaves
- Reduzir os equipamentos com o serviço aberto para a Internet
- Filtragem de origem
- Mover o serviço para uma porta não padrão
- Considerar o uso de um *gateway* de autenticação
- Acesso a elementos de rede somente via rede de gerência

Estas e outras recomendações em:

- Sugestões para defesa contra ataques de força bruta para SSH
  https://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/

Comprometimento de Roteadores / Servidores: **Boas Práticas Adicionais**

Telnet

- Certificar-se que o serviço está desabilitado quando não necessário
- Utilizar esse serviço apenas se não tiver opção de utilizar outro com suporte à criptografia
- Utilizar rede de gerência

Referências para Mikrotik

- *Hardening MikroTik RouterOS*
  https://mum.mikrotik.com/presentations/KH17/presentation_4162_1493374113.pdf
- *Manual:Securing Your Router*
  https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router
- *MikroTik Router Hardening*
  https://www.manitonetworks.com/networking/2017/7/25/mikrotik-router-hardening
- *Slides* variados de cursos e treinamentos
  http://mdbrasil.com.br/cursosetreinamentos/downloads/

Resumo das Boas Práticas

cert.br nic.br cgi.br

Recomendações

Fazer *hardening* de roteadores e elementos de rede

- senhas fortes e acesso via chaves SSH
  - desabilitar `telnet`, `ftp` e outros acessos sem criptografia ou autenticação
- rede de gerência
- desativar serviços desnecessários/não utilizados

Reduzir ataques DDoS saindo de sua rede

- implementar *antispoofing* (BCP 38)
- detectar ataques saindo de sua rede
- CPEs com gerência remota e configurados para
  - não ter serviços abertos, não ter senha padrão, etc

Ativar *NetFlows*

- ótimas opções de *software* livre (`nfdump`/`nfsen`)
- usos reativos e pró-ativos
  - como consultas DNS para servidores maliciosos

Receber e tratar notificações, que são enviadas para:

- *e-mail* do contato `abuse-c` do ASN no serviço whois
- *e-mail* de abuse ou do grupo de tratamento de incidentes

Obrigado

www.cert.br

jessen@cert.br

@certbr

17 de maio de 2018

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br