nic.br cgi.br | cert.br

**IX Fórum Regional**
**São Paulo, SP**
10 de junho de 2019

# Boas Práticas de Segurança para Sistemas Autônomos

**Cristine Hoepers, D.Sc.**
Gerente Geral
cristine@cert.br

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

cert.br nic.br cgi.br

# CERT.br:
# Estrutura e Serviços

## Serviços:

### 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
- Coleta e dissemina informações sobre ameaças e tendências de ataques
- Auxilia novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades

### Treinamento em Gestão de Incidentes

### Boas Práticas e Materiais de Conscientização

- Administradores de redes e sistemas
- Usuários finais, crianças e pais/educadores


FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

**SEI** Partner Network

The Honeynet PROJECT

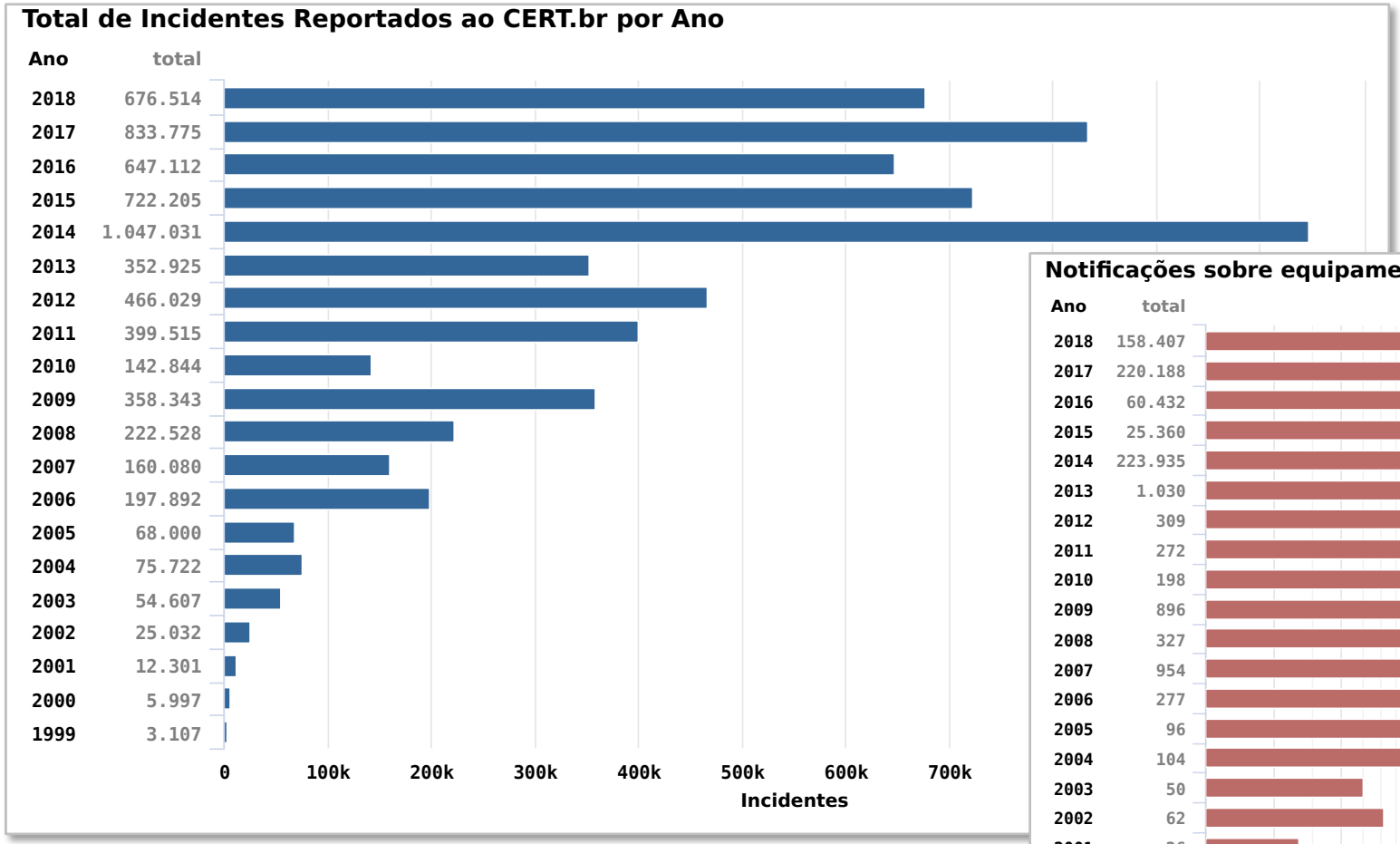
**Criação:**

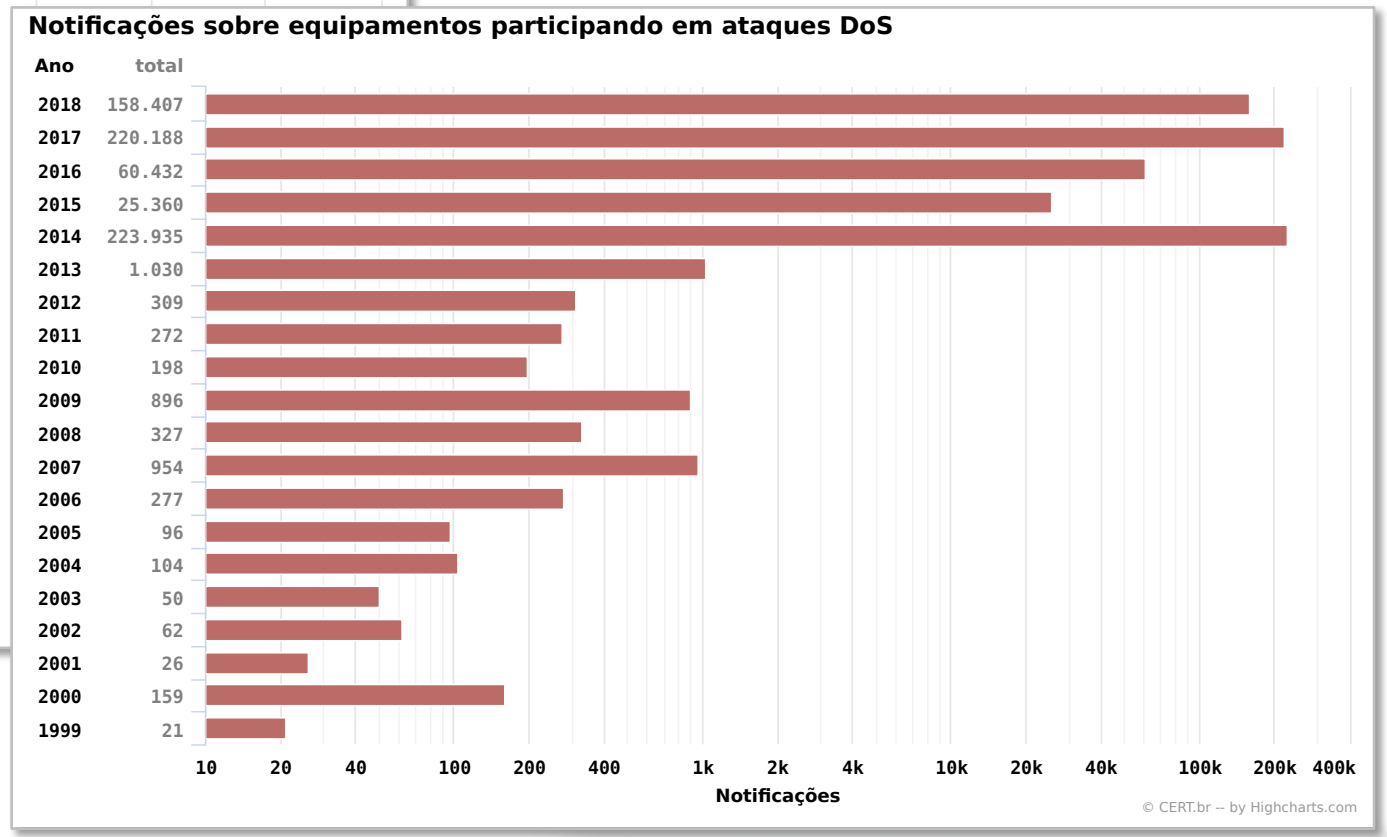
**Agosto/1996**: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br[1]

**June/1997**: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]

[1] https://www.nic.br/grupo/historico-gts.htm
[2] https://www.nic.br/pagina/gts/157

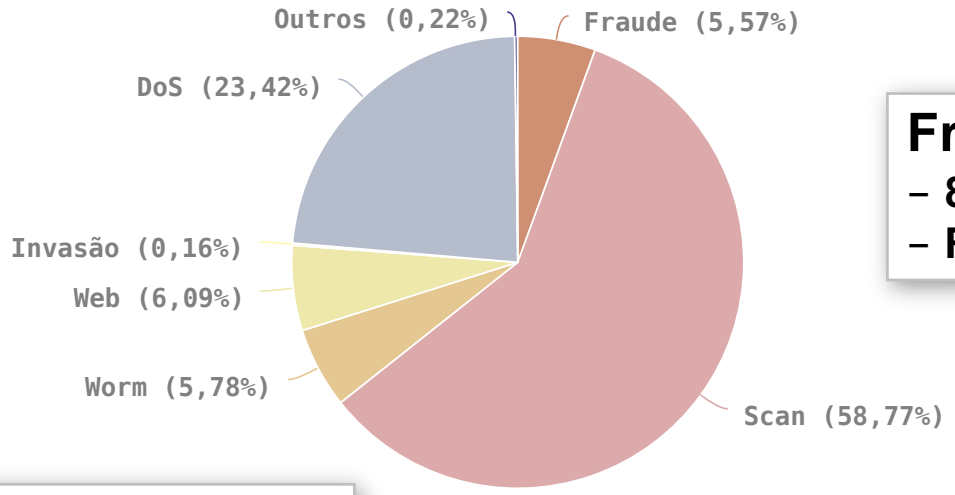
# Incidentes Reportados para o CERT.br:
# **Total e DDoS de 1999 a 2018**



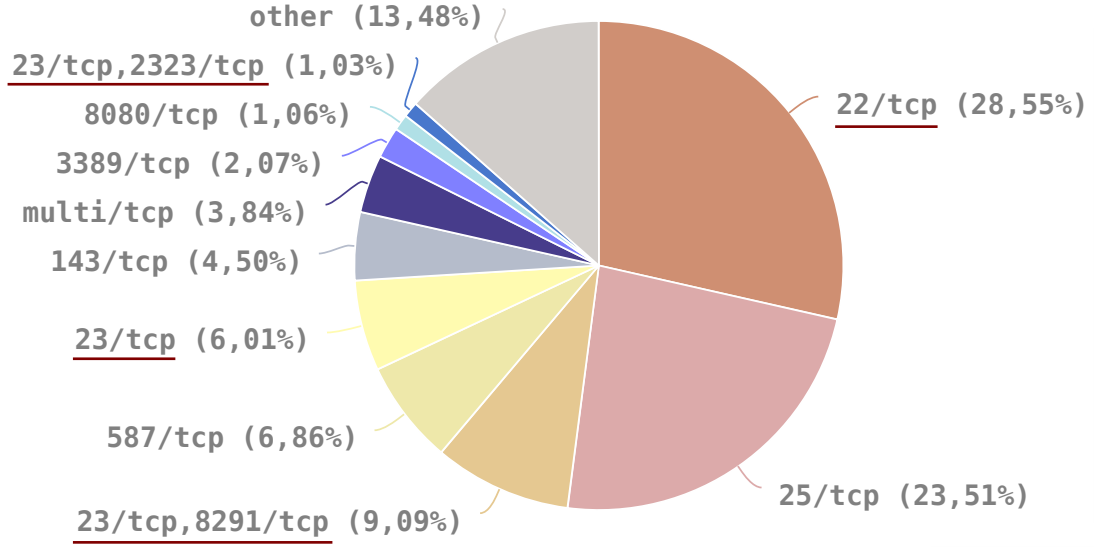

**Fonte:** https://www.cert.br/stats/incidentes/

# Incidentes Reportados para o CERT.br :
# **Detalhes sobre os tipos de incidentes vistos em 2018**




## Fraude
- 84% são páginas falsas (*phishing*)
- Relacionadas com ataques em CPEs

## DDoS
- Aumentou de patamar em 2014
- 300Gbps é o “normal”
- Até 1Tbps contra alguns alvos
- Tipos mais frequentes
  - *botnets* IoT
  - amplificação de tráfego




## *Scan*
- Portas 22 e 23, 2323: força bruta de senhas de servidores e de IoT
- Portas 23, 8291: força bruta e vulnerabilidade Winbox MikroTik
- Porta 25: força bruta de senhas de *e-mail*

# Ataques à Infraestrutura dos ASNs:
# **Comprometimento de Elementos de Rede**

## **Invasão de CPEs** (roteadores domésticos) **para trocar o DNS**

Invadidos

- 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

## **Invasão de Roteadores para Sequestro de Rota BGP**

- atacantes comprometem roteadores de borda de pequenos provedores
  - via força bruta de senhas (geralmente via telnet)
- anunciam prefixos de rede mais específicos da instituição vítima (em geral /24)
  - "*peers*" do provedor comprometido vão aprendendo a nova rota
  - clientes das redes que aprenderam a nova rota passam a ser roteados para o local errado
- início em março de 2017 e ainda está ocorrendo

# Ataques à Infraestrutura dos ASNs:
# **Roteadores e CPEs MikroTik Abusados de Vários Modos**

## Força Bruta de Senhas

Muito comum em ataques para

- sequestro de rotas BGP
- mudar DNS dos CPEs

Muito usado por

- *botnets* para envio de spam
- *cryptominers*

## Exploração de Vulnerabilidades

- em geral vulnerabilidade do Winbox
- muito usada por *botnets* e *cryptominers*

## *Botnets* MikroTik para envio de *spam*

Abuso de *Proxies* Abertos

- *proxies* SOCKS são habilitados por invasores ou por *malware*
- porta usual é a 4145/TCP

Envio de *e-mail* via *SSH Port Forwarding*

- obtém as credenciais via força bruta de senhas
- *port forwarding* funciona mesmo se explicitamente desligado
  - *bug* já foi reportado para a MikroTik e para o CERT.LV

IPs com MikroTik notificados pelo CERT.br:

- *Coinhive*: 161.848 IPs
- SOCKS 4145/TCP:

```
2019-03:  ASNs: 764  IPs: 4048
2019-04:  ASNs: 684  IPs: 4873
2019-05:  ASNs: 584  IPs: 3869
2019-06:  ASNs: 515  IPs: 3281
```

# Abuso de MikroTik:
# **Varreduras Contra os *Honeypots* e *Payload* do *Exploit***

Varreduras por Winbox (8291/TCP) nos *honeypots*

- praticamente inexistentes até o dia 23/mar/2018
- atingiram um pico no dia 29 de março
- tem se mantido constantes em valores significativos

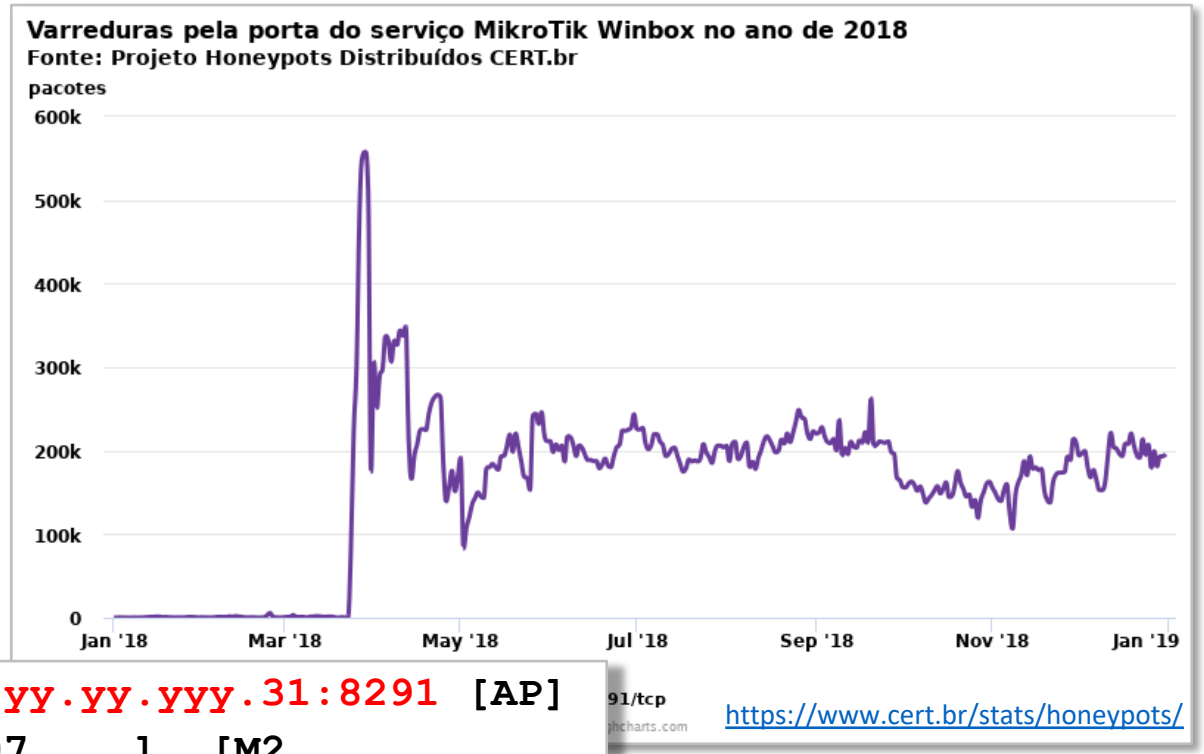
Recomendações:

- *hardening*
- manter RouterOS sempre na última versão Long-term

Referências:

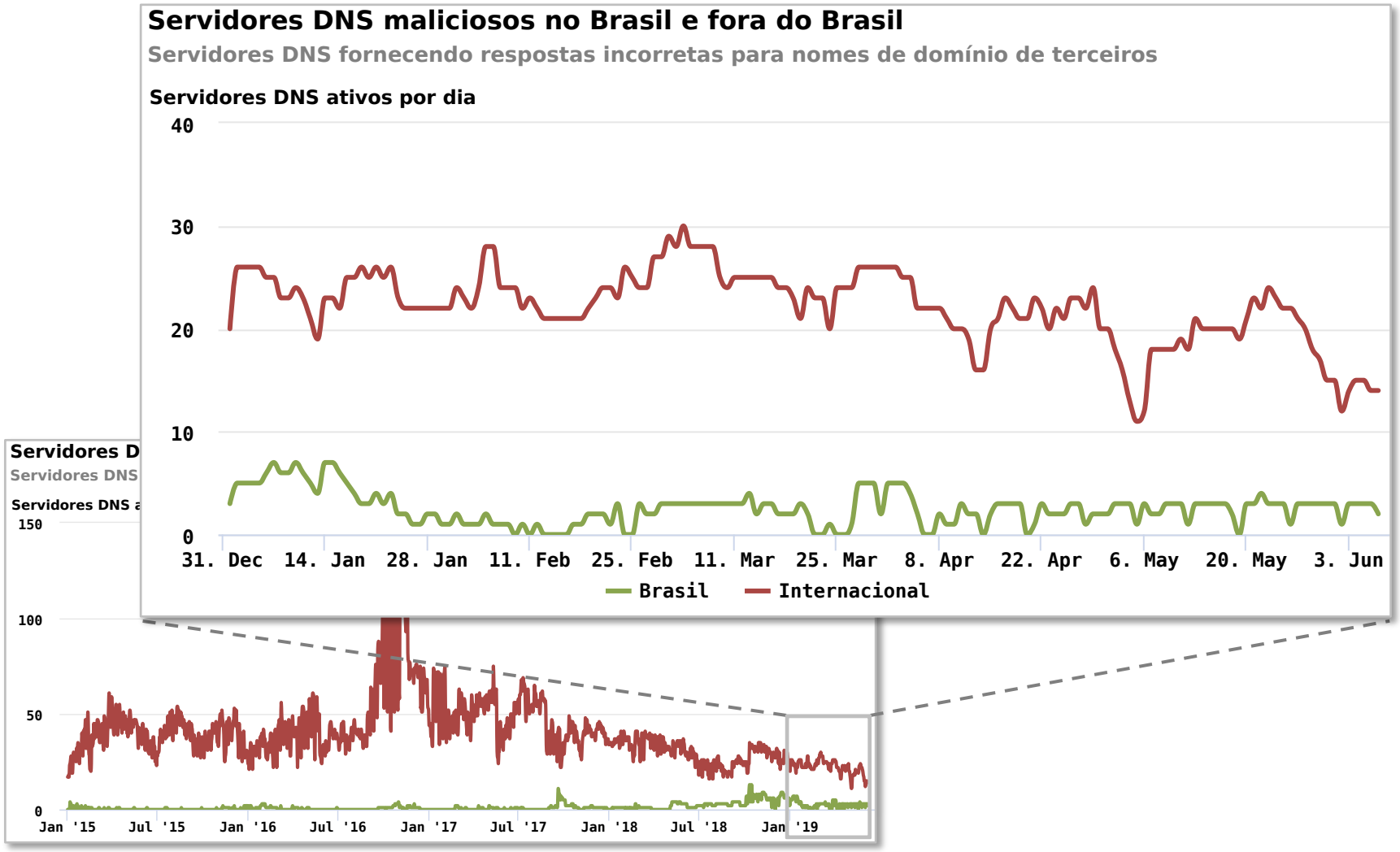
https://blog.mikrotik.com/security/winbox-vulnerability.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14847




```
T 2019/01/16 19:08:04.934837 xxx.xx.xx.86:51405 -> yy.yy.yyy.31:8291 [AP]
  5d 01 00 5b 4d 32 05 00    ff 01 06 00 ff 09 07 07    ]..[M2..........
  00 ff 09 07 01 00 00 21    2a 2e 2f 2e 2e 2f 2e 2f    .......!*./.././
  2e 2e 2f 2e 2f 2e 2e 2f    2e 2f 2e 2e 2f 2e 2f 2e    .././.././.././.
  2e 2f 72 77 2f 73 74 6f    72 65 2f 75 73 65 72 2e    ./rw/store/user.
  64 61 74 02 00 ff 88 02    00 00 00 00 00 08 00 00    dat.............
  00 01 00 ff 88 02 00 02    00 00 00 02 00 00 00       ...............
```

# Servidores DNS Maliciosos Usados nos CPEs Invadidos: **Fornecem Respostas Autoritativas Erradas**




**Fonte:** https://www.cert.br/stats/dns-malicioso/

**Semântica é importante ao reportar incidentes ou pedir takedown!**

- Isto **não é** um DNS invadido
- Isto **não é** envenenamento (*cache poisoning*)
- Isto **não é** sequestro de domínio (*domain hijacking*)

Isto é um **servidor DNS malicioso** (*rogue*) sendo usado para **sequestro de DNS** (*DNS hijacking*)

- autoritativo para os domínios das vítimas
- recursivo aberto respondendo ao restante das consultas

# *Payload* em um *Honeypot*:
# Exploração de Vulnerabilidade p/ Alteração de DNS

```
T 2018/12/01 00:13:02.742932 35.205.103.100:43542 -> xxx.xxx.xxx.58:80 [AP] GET
  /dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
  HTTP/1.1..Host: xxx.xxx.xxx.58..User-Agent: curl/7.52.1..Accept: */*....
T 2018/12/01 03:52:37.438432 35.236.45.29:36632 -> xxx.xxx.xxx.60:80 [AP] GET
  /dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
  HTTP/1.1..Host: xxx.xxx.xxx.60..User-Agent: curl/7.52.1..Accept: */*....
T 2018/12/01 06:48:30.245365 35.203.18.219:35968 -> xxx.xxx.xxx.61:80 [AP] GET
  /dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
  HTTP/1.1..Host: xxx.xxx.xxx.61..User-Agent: curl/7.52.1..Accept: */*....
T 2018/12/01 06:56:54.171910 35.203.18.219:57706 -> xxx.xxx.xxx.56:80 [AP] GET
  /dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
  HTTP/1.1..Host: xxx.xxx.xxx.56..User-Agent: curl/7.52.1..Accept: */*....
T 2018/12/01 06:57:48.285789 35.203.18.219:35304 -> xxx.xxx.xxx.62:80 [AP] GET
  /dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
  HTTP/1.1..Host: xxx.xxx.xxx.62..User-Agent: curl/7.52.1..Accept: */*....
T 2018/12/01 08:17:57.210273 35.242.154.70:48598 -> xxx.xxx.xxx.57:80 [AP] GET
  /dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
  HTTP/1.1..Host: xxx.xxx.xxx.57..User-Agent: curl/7.52.1..Accept: */*....
T 2018/12/01 09:49:52.610024 35.242.154.70:40022 -> xxx.xxx.xxx.60:80 [AP] GET
  /dnscfg.cgi?dnsPrimary=195.128.126.170&dnsSecondary=139.60.162.180&dnsDynamic=0&dnsRefresh=1
  HTTP/1.1..Host: xxx.xxx.xxx.60..User-Agent: curl/7.52.1..Accept: */*....
```

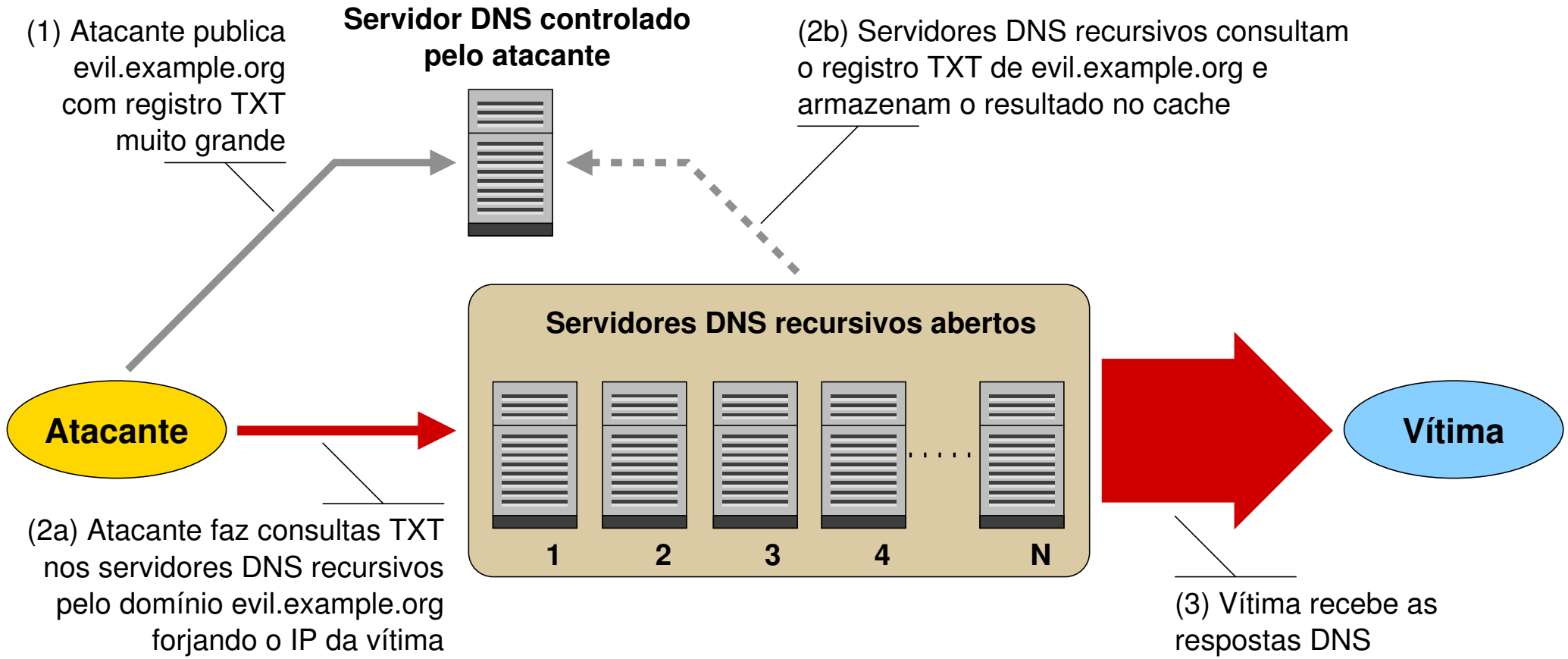
# Detecção via *NetFlow*:
# **Acessos a Servidores DNS Maliciosos**

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>)'
```

# Ataques DDoS com Amplificação:
# **Relembrando como Funcionam**




**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 de ASNs e IPs Brasileiros Notificados pelo CERT.br**

| | DNS | | SNMP | | NTP | | SSDP | | Ubiquiti | |
|---|---|---|---|---|---|---|---|---|---|---|
| month | ASNs | IPs | ASNs | IPs | ASNs | IPs | ASNs | IPs | ASNs | IPs |
| 2018-06 | 2.629 | 70.188 | 2.284 | 447.411 | 805 | 87.408 | 817 | 23.340 | - | - |
| 2018-07 | 2.721 | 68.415 | 2.436 | 431.907 | 881 | 89.484 | 787 | 17.255 | - | - |
| 2018-08 | 2.459 | 56.555 | 2.411 | 397.622 | 895 | 89.353 | 613 | 11.855 | - | - |
| 2018-09 | 2.767 | 62.942 | 2.366 | 193.432 | 772 | 87.378 | 836 | 21.836 | - | - |
| 2018-10 | 2.806 | 64.912 | 2.383 | 163.987 | 856 | 85.911 | 789 | 20.233 | - | - |
| 2018-11 | 2.604 | 60.937 | 2.376 | 137.331 | 851 | 87.155 | 814 | 20.124 | - | - |
| 2018-12 | 2.849 | 64.649 | 2.361 | 137.463 | 719 | 82.610 | 832 | 21.704 | - | - |
| 2019-01 | 2.960 | 74.257 | 2.583 | 137.253 | 923 | 89.567 | 840 | 17.348 | - | - |
| 2019-02 | 2.905 | 69.093 | 2.556 | 136.401 | 944 | 80.838 | 868 | 20.689 | 2.690 | 180.756 |
| 2019-03 | 2.933 | 63.895 | 2.661 | 111.561 | 914 | 72.873 | 847 | 18.837 | 2.042 | 95.974 |
| 2019-04 | 2.898 | 59.865 | 2.662 | 123.241 | 997 | 79.698 | 886 | 18.919 | 1.909 | 76.666 |
| 2019-05 | 3.045 | 68.764 | 2.633 | 103.204 | 1.019 | 77.979 | 953 | 18.564 | 1.797 | 64.729 |

Obs.: Notificações realizadas após confirmar dados do ShadowServer sobre amplificadores no Brasil
http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/

**Dados disponíveis em:** https://www.cert.br/stats/amplificadores/

# Detecção via *NetFlow:*
# Ataques DDoS com Amplificação Saindo da sua Rede

## Consulta para detecção de grandes geradores de tráfego ("*top-talkers*")

```
$ 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
```

# Detecção via *NetFlow:*
# **Ataques DDoS com Amplificação Saindo da sua Rede**

## Consulta *NetFlow* para detectar tráfego LDAP amplificado

- 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 '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
```

# Recomendações

cert.br nic.br cgi.br

# Recomendações

PROGRAMA INTERNET +SEGURA
https://bcp.nic.br/i+seg/

**Fazer *hardening* de roteadores e elementos de rede**

- atualização de firmware
- 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
- configurar os CPEs para
  - não ter serviços abertos, não ter senha padrão, etc

**Para *hardening* e aquisição de CPEs consultar a BCOP Conjunta LACNOG e M³AAWG:**
**www.lacnog.net/docs/lac-bcop-1 -- www.m3aawg.org/CPESecurityBP**

**Ativar *netflows***

- ótimas opções de *software* livre
  - `nfdump` https://github.com/phaag/nfdump
  - SiLK https://tools.netsa.cert.org/silk/
- 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

# *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

- https://github.com/phaag/nfdump

*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

# Obrigado

www.cert.br

cristine@cert.br jessen@cert.br @certbr

10 de junho de 2019

nic.br cgi.br

www.nic.br | www.cgi.br