

Panorama de Incidentes de DDoS na Rede IPê



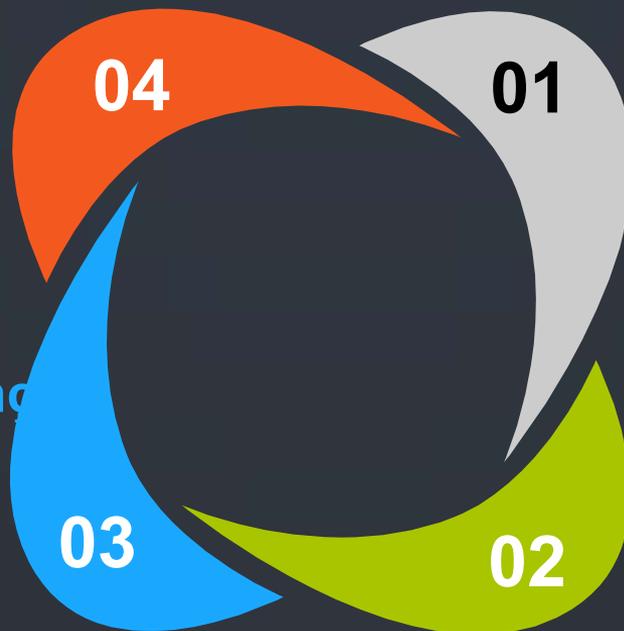
SEGURANÇA DA INFORMAÇÃO NA RNP

04 CAIS

CSIRT de coordenação da rede acadêmica brasileira. Foco na gestão da segurança do backbone e dos clientes da RNP.

03 Soluções em segurança

Atendimento a demandas por soluções de segurança dos clientes da RNP. Foco na consultoria de segurança em projetos especiais.



01 Segurança corporativa

Gestão da segurança corporativa. Foco na implantação da política de segurança e boas práticas na organização RNP.

02 Relações Institucionais

Gestão de relacionamento com clientes e parceiros estratégicos da RNP, com o foco em segurança da informação.

Centro de Atendimento a Incidentes de Segurança



20 anos de atuação na área de segurança da informação.

Detecção, resolução e prevenção.



Panorama de SegInfo na rede acadêmica

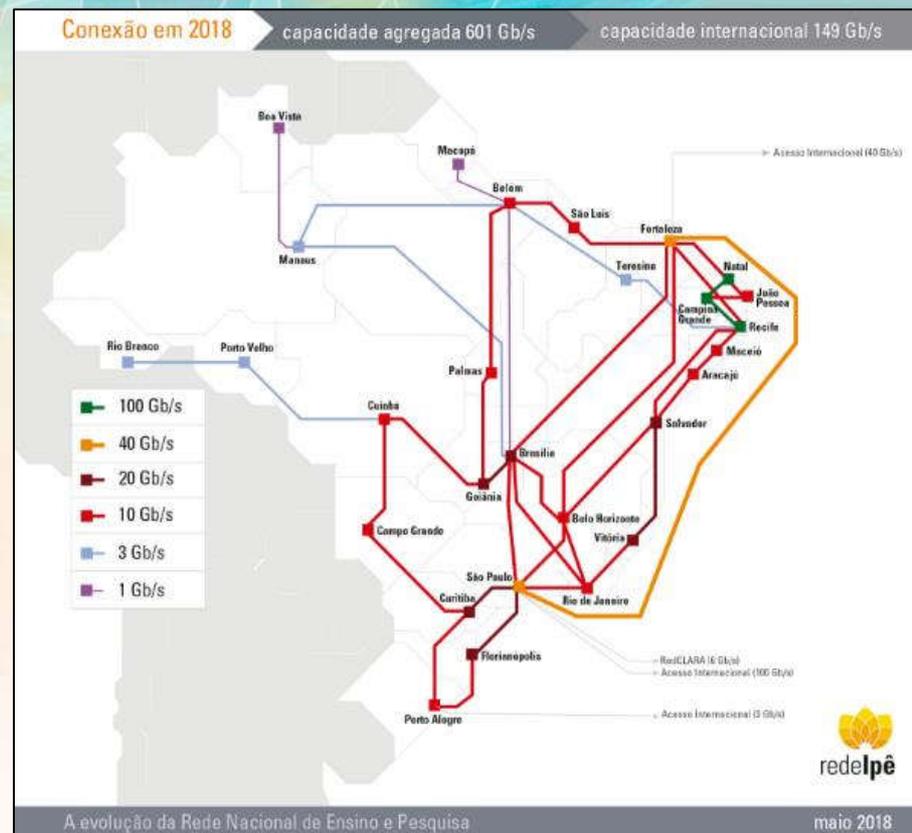
Rede Ipê, backbone da rede acadêmica.
Capacidade integrada > 600Gb/s.

CAIS coordena cerca de 1,393 clientes
(IFs, IFEs, Unidades de Pesquisa).
+100 clientes em RS

+10.000 mil notificações enviadas aos
administradores de redes e sistemas
nos últimos 12 meses*.

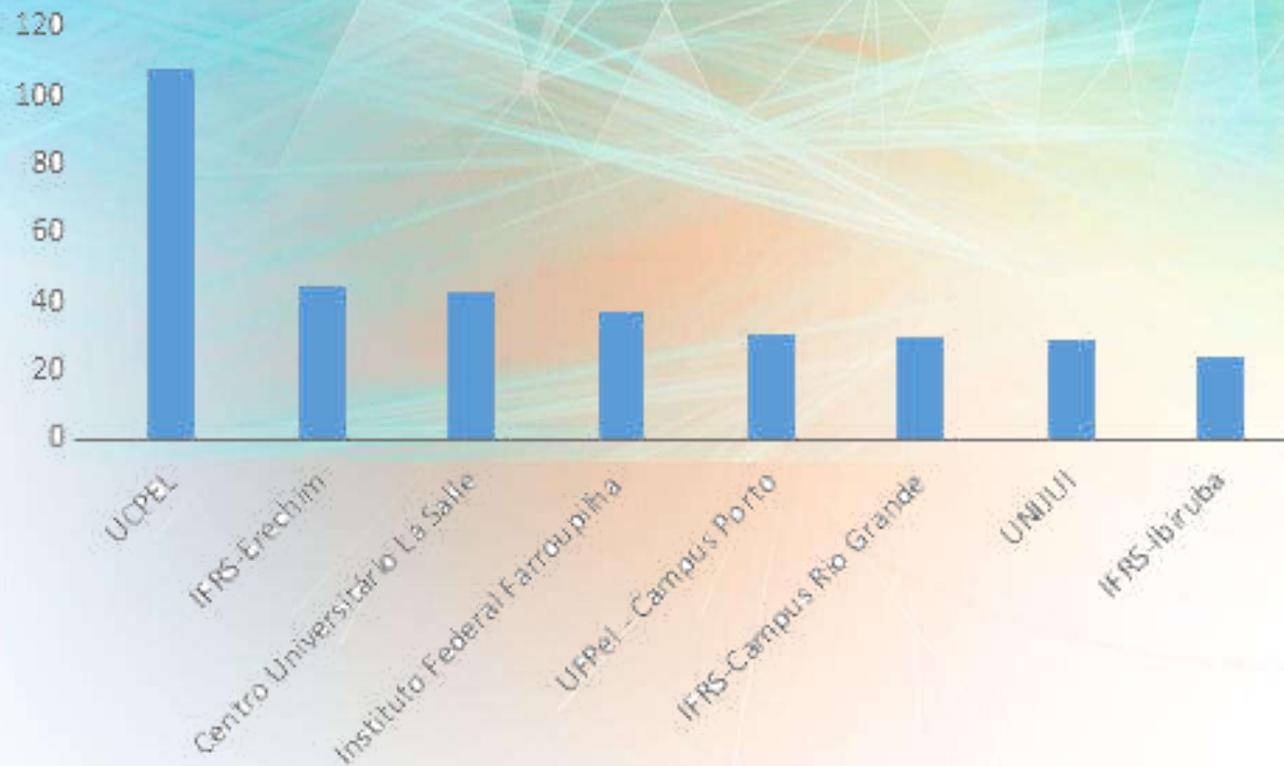
+8.000 (cerca de 75%) das notificações
são relativas a vulnerabilidades de
segurança.

*Nov 2017/Nov 2018



Segurança na Rede Acadêmica- RS

+3000 notificações de incidentes enviadas nos últimos 12 meses*

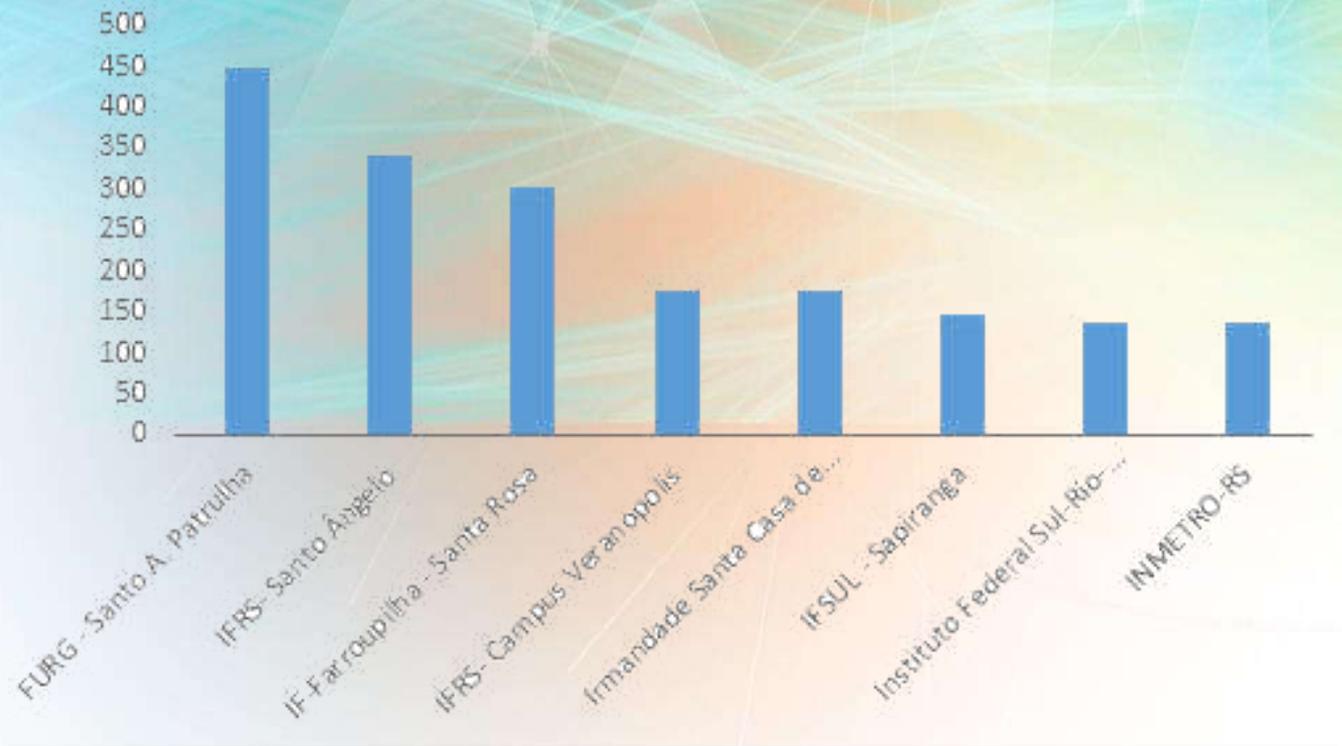


Deste total, cerca de **83%** foram resolvidos.

*Nov 2017/Nov 2018

Segurança na Rede Acadêmica- RS

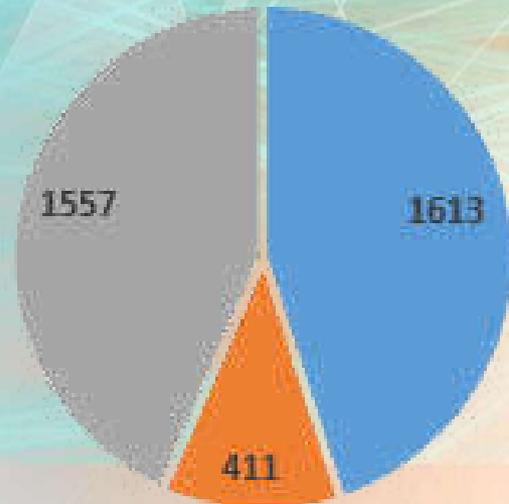
+8000 notificações enviadas nos últimos 12 meses*



60% das notificações de vulnerabilidades foram fechadas

*Nov 2017/Nov 2018

Segurança na Rede Acadêmica- RS

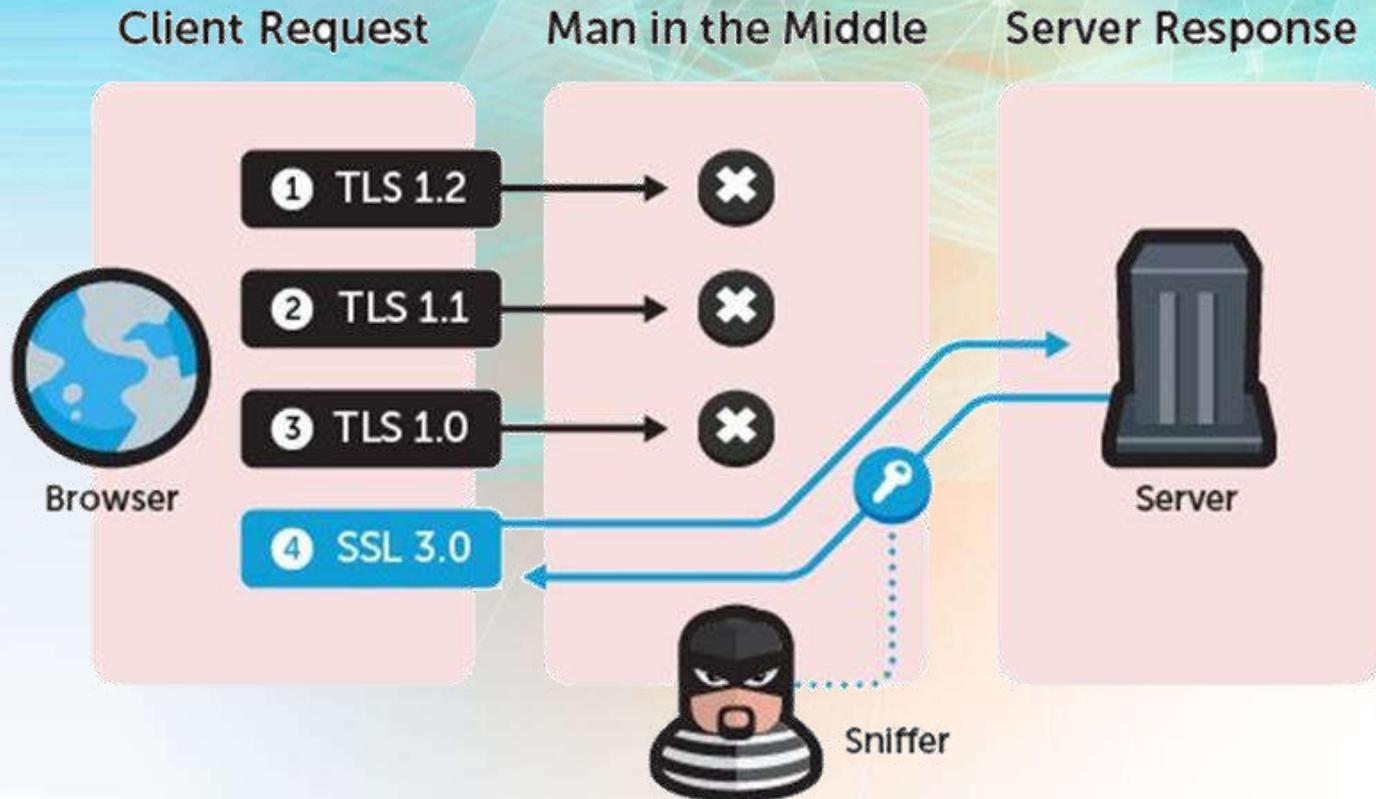


*TOP3 Notificações

- Vulnerabilidade Pooodle
- Host infectado com malware
- Hosts com vulnerabilidade em serviços que utilizam protocolo UDP

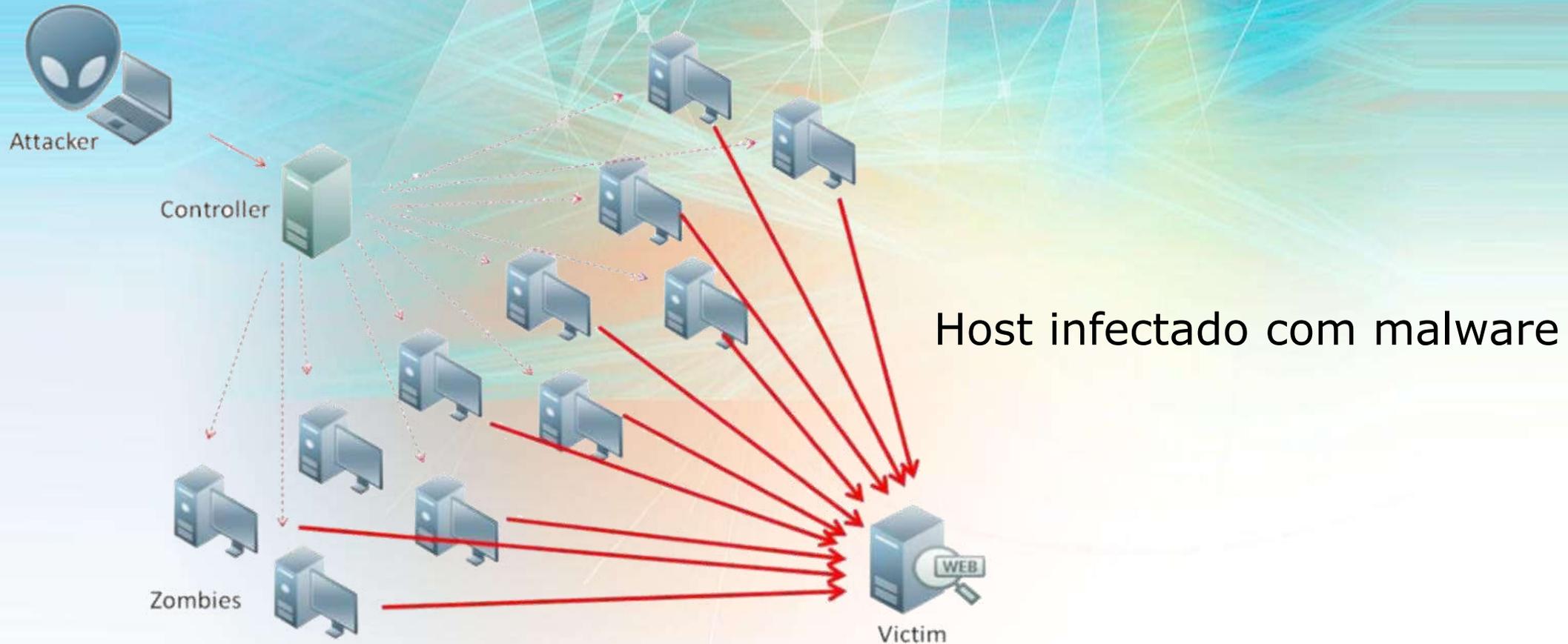
*Nov 2017/Nov 2018

Segurança na Rede Acadêmica- RS



Vulnerabilidade
Poodle

Segurança na Rede Acadêmica- RS



Segurança na Rede Acadêmica- RS

Hosts com vulnerabilidade em serviços que utilizam protocolo UDP

IP: 11.11.11.11



Sua instituição

IP: 22.22.22.22

DRDoS



Vítima

IP: 33.33.33.33



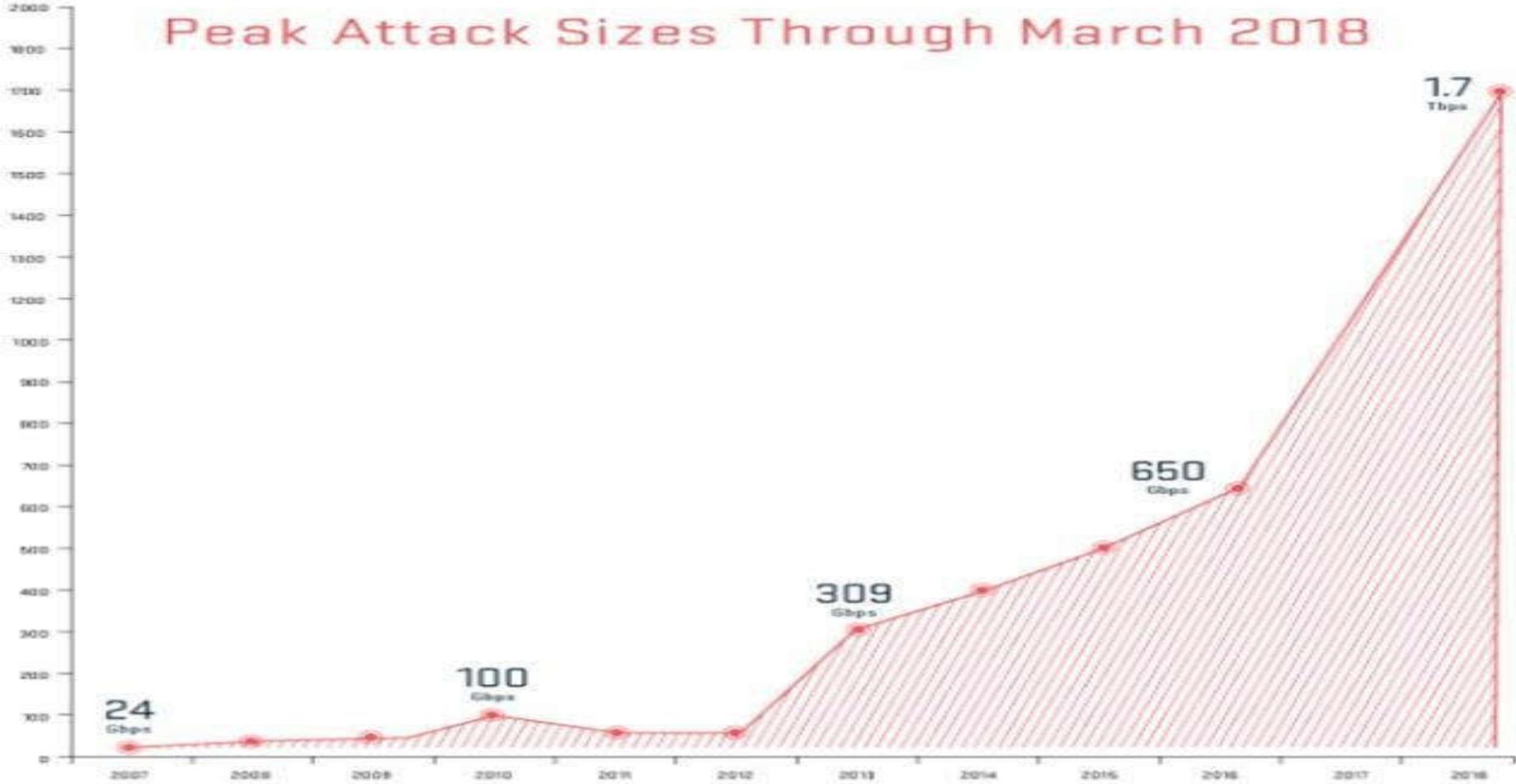
IP Destino: 22.22.22.22

IP Origem: 33.33.33.33



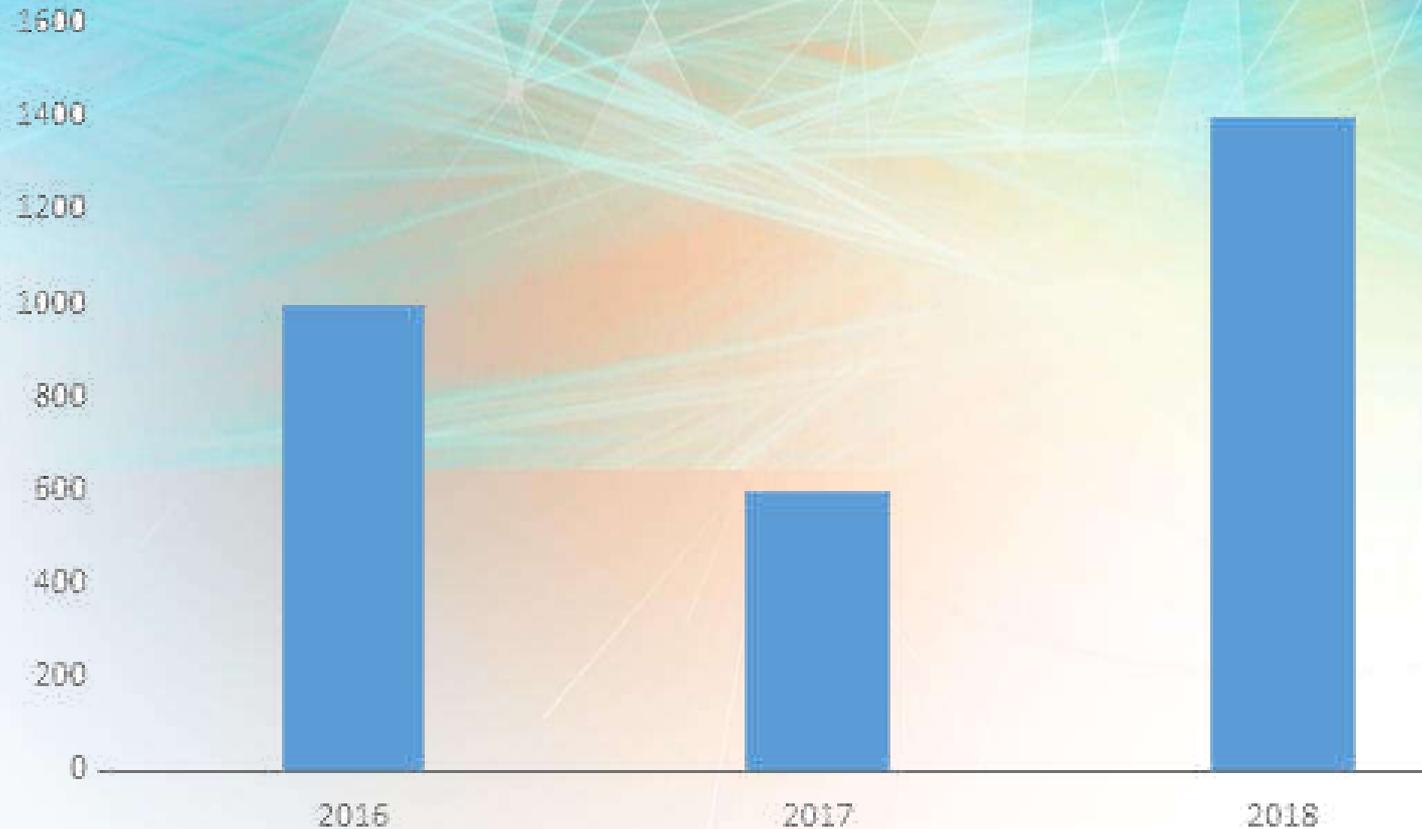
DDoS no Mundo

Peak Attack Sizes Through March 2018



DDoS: Clientes da RNP

Notificação de Hosts realizando DDoS



DDoS na RNP

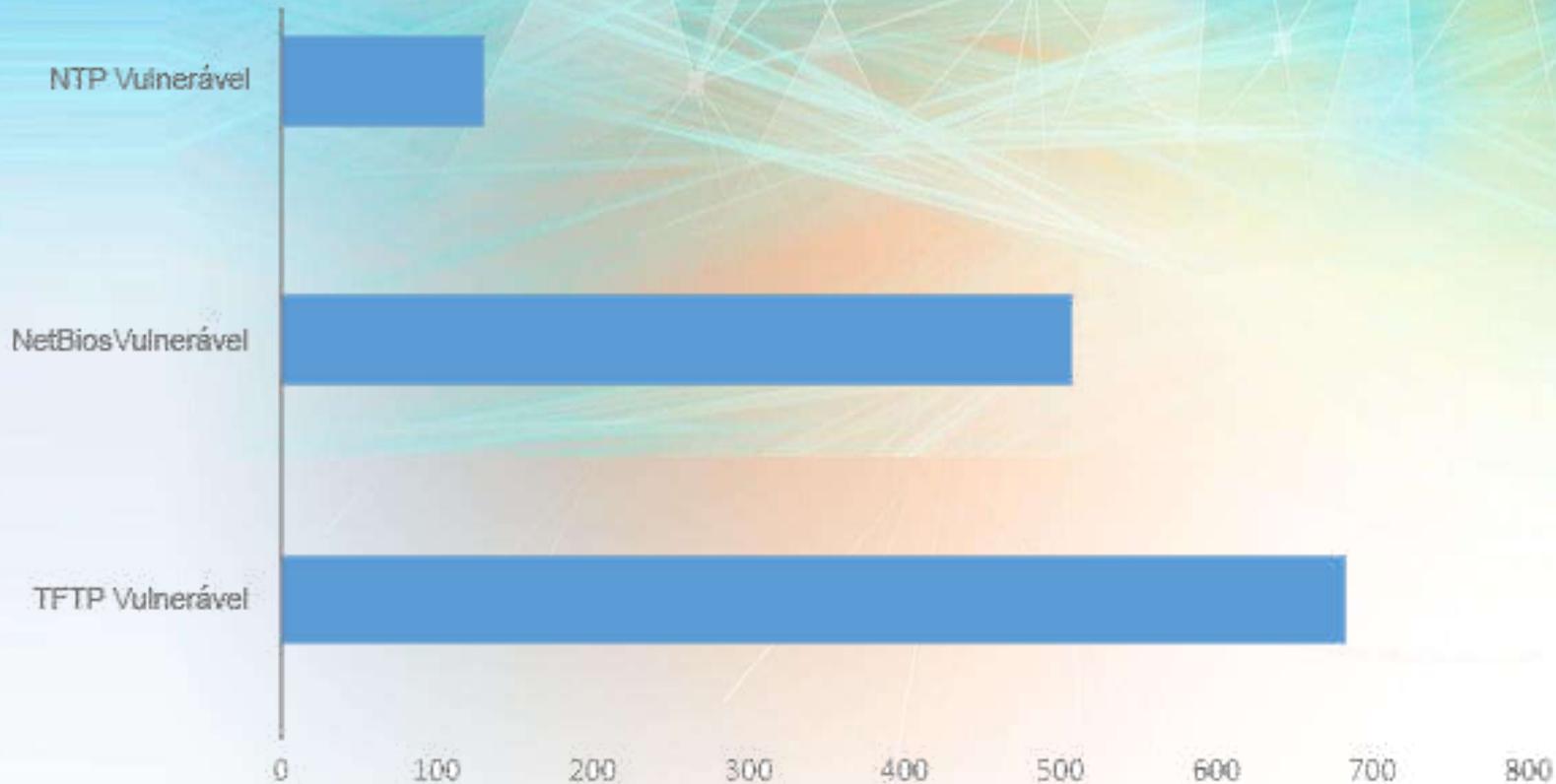
Ataques Amplificados:

- Amplificação é a forma como um determinado serviço se comporta quando recebe um tipo específico de conexão.

- Em outras palavras, uma consulta inicial a um servidor DNS pode ocasionar em uma resposta 50x maior, por exemplo.

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7][8]	56 to 70	—
TFTP [23][9]	60	—
Memcached [25]	10,000 to 51,000	—

DDoS na Rede Acadêmica - RS



Notificações
abertas

*Dez 2015/Nov 2018

Detectando Hosts Vulneráveis - NMAP

NTP Vulnerável

```
root@lab-ddos-atk00:~# nmap -sU -p U:123 -n -Pn 13.37.1.50 --script=ntp-monlist
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-26 04:19 -03
```

```
Nmap scan report for 13.37.1.50
```

```
Host is up (0.00029s latency).
```

```
PORT      STATE SERVICE
```

```
123/udp open  ntp
```

```
| ntp-monlist:
```

```
| Target is synchronised with 200.186.125.195
```

```
| Alternative Target Interfaces:
```

```
| 192.168.31.50
```

```
| Public Servers (9)
```

```
| 5.103.139.163 192.36.143.130 200.160.0.8 200.189.40.8
```

```
| 52.67.171.238 200.144.121.33 200.186.125.195 200.192.232.8
```

```
| 78.46.37.9
```

```
| Public Clients (1)
```

```
| 13.37.1.100
```

```
MAC Address: 08:00:27:46:05:65 (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

Detectando Hosts Vulneráveis - NMAP

NetBios Vulnerável

```
root@kali:~# nmap -sU --script nbstat.nse -p 137 192.168.225.13
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-27 10:25 BST
```

```
Nmap scan report for 192.168.225.13
```

```
Host is up (0.00032s latency).
```

```
PORT      STATE SERVICE
```

```
137/udp open  netbios-ns
```

```
MAC Address: 00:0C:29:FA:D0:00 (VMware)
```

```
Host script results:
```

```
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Detectando Hosts Vulneráveis - NMAP

TFTP Vulnerável



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU -p 69 --script tftp-enum.nse 192.168.56.101  
Starting Nmap 6.496ETA4 ( https://nmap.org ) at 2015-11-11 04:00 EST  
Nmap scan report for 192.168.56.101  
Host is up (0.00029s latency).  
PORT      STATE SERVICE  
69/udp    open  tftp  
| tftp-enum:  
|_  etc/passwd  
  
Nmap done: 1 IP address (1 host up) scanned in 31.85 seconds  
root@kali:~#
```

Lista de Hosts Vulneráveis - Pastebin

PASTEBIN + new paste API tools faq search...

4500 IPS / x440 AMP NTP
GOLDENDAGGER MAY 18TH, 2018 112 NEVER

Pay What You Want: The Ultimate White Hat Hacker 2018 Bundle
Master the Essential Ethical Hacking Tools & Tricks (68+ Hours!) to Launch an Et in 2018
Normally: \$4528 Now: \$1

Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

text 85.91 KB

1.	99.25	217 440
2.	98.5.	1 440
3.	98.25	6 440
4.	98.22	189 440
5.	98.21	192 440
6.	98.15	72 440
7.	98.11	143 440
8.	98.10	42 440
9.	98.10	40 440
10.	98.10	133 440

PASTEBIN + new paste API tools faq search...

24000 IPS list of LDAP AMP.
GOLDENDAGGER [GIFT PRO] MAY 19TH, 2018 160 NEVER

Pay What You Want: The Ultimate White Hat Hacker 2018 Bundle
Master the Essential Ethical Hacking Tools & Tricks (68+ Hours!) to La in 2018
Normally: \$4528 Now: \$1

Pastebin PRO Accounts **SPRING SPECIAL!** For a limited time get 40% discount on a

text 479.08 KB

1.	99.E	.253 2909
2.	99.E	151 2996
3.	99.E	.190 2989
4.	99.E	.154 2913
5.	99.E	.197 2866
6.	99.2	83 2843
7.	99.2	.14 2710
8.	99.2	.160 2990
9.	99.2	.166 2648
10.	99.2	.179 2885

Segurança na Rede Acadêmica - RS

Como se proteger?



Segurança na Rede Acadêmica - RS

Como se proteger?

Gestão de Incidentes

Gestão de vulnerabilidades

Monitoramento efetivo de recursos

Hardening de serviços

- NTP
- NetBios
- TFTP
- TLS (SSL)



Segurança na Rede Acadêmica - RS

Como se proteger?

Estabelecer um processo de Tratamento de Incidentes de Segurança

3. contenção

2. detecção

1. preparação

resposta a
incidentes



4. erradicação

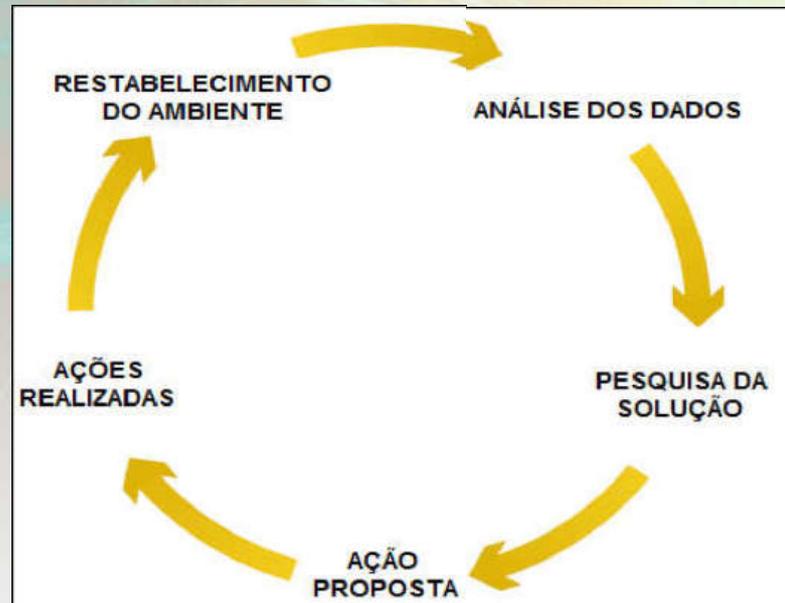
5. recuperação

6. avaliação

Segurança na Rede Acadêmica - RS

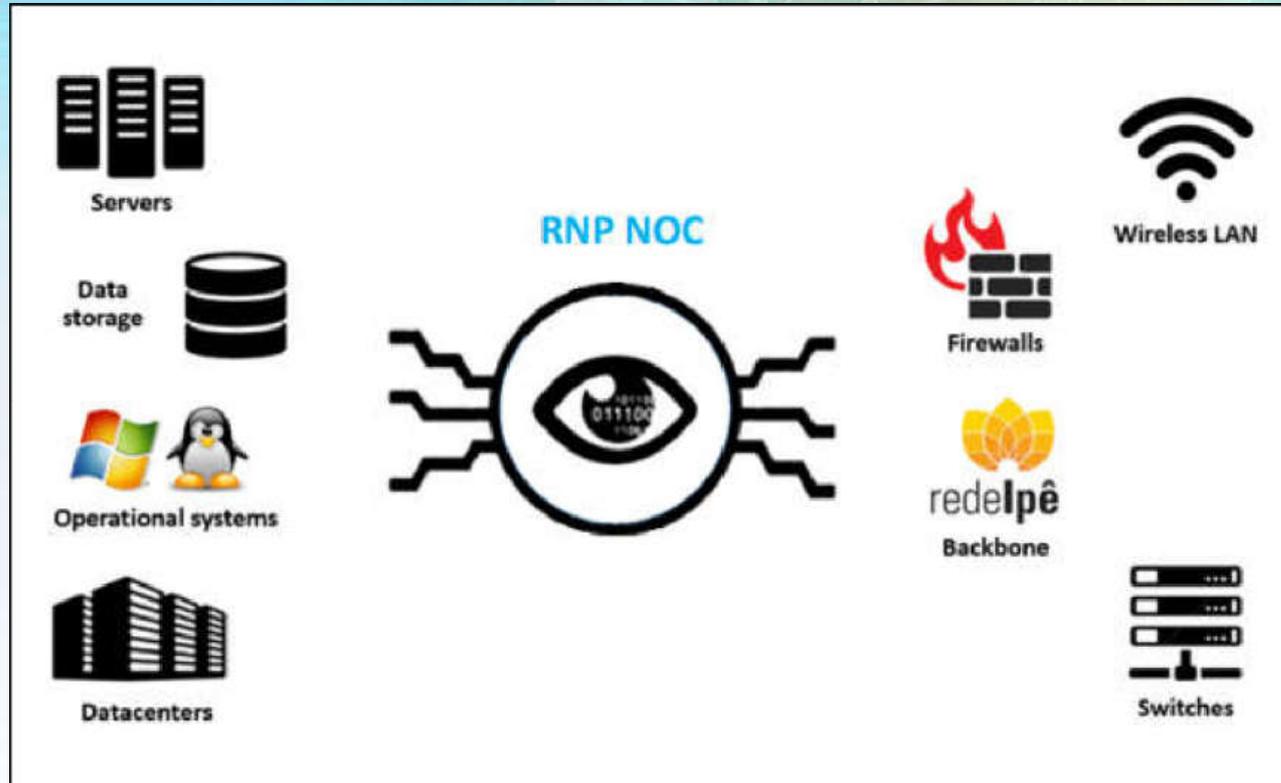
Como se proteger?

Estabelecer um processo de Gestão de Vulnerabilidades de Segurança



Segurança na Rede Acadêmica - RS

Como se proteger?



Monitoramento Efetivo
e Pró-Ativo

Segurança na Rede Acadêmica - RS

Como se proteger ?

Vulnerabilidade NTP

- ACL's
- "restrict default kod notrap nomodify nopeer noquery"
- "disable monitor"
- Utilizar "OpenNTPd"
 - <http://www.openntpd.org/>



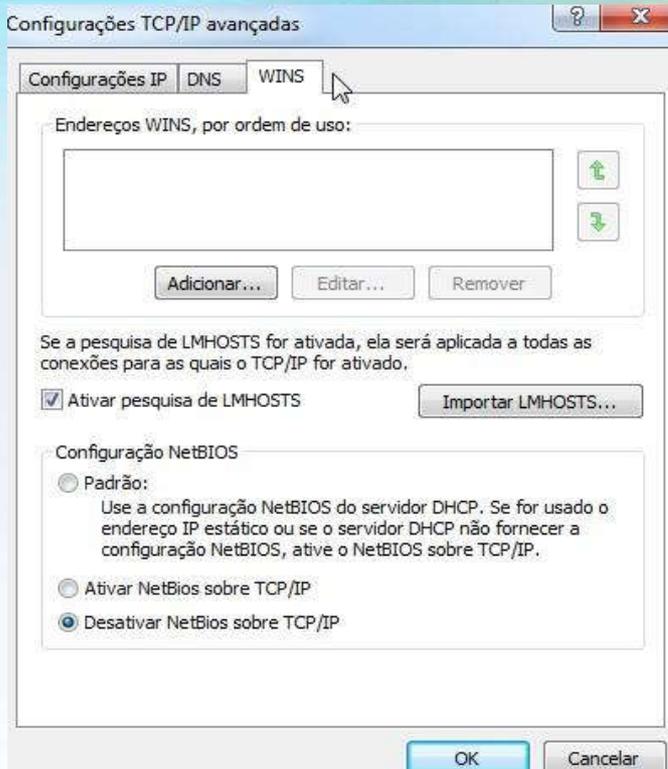
Segurança na Rede Acadêmica - RS

Como se proteger?

Vulnerabilidade NetBios:

*Desativar o NetBios

Limitar consultas externas



Segurança na Rede Acadêmica - RS

Como se proteger?

```
[root@centos52-mysql /]# cat /etc/xinetd.d/tftp
% default: off
% description: The tftp server serves files using the trivial file transfer \
%   protocol.  The tftp protocol is often used to boot diskless \
%   workstations, download configuration files to network-aware printers, \
%   and to start the installation process for some operating systems.
service tftp
{
    disable = no
    socket_type      = dgram
    protocol         = udp
    wait            = yes
    user            = root
    server          = /usr/sbin/in.tftpd
    server_args     = -s /tftpboot
    disable         = no
    per_source      = 11
    cps             = 100 2
    flags           = IPv4
}
[root@centos52-mysql /]#
```

<http://wiki.r1soft.com/display/CDP3/Configuring+TFTP+Server+on+Linux>

Vulnerabilidade TFTP:

Utilizar SSH

*Utilizar SFTP

Limitar consultas externas

Segurança na Rede Acadêmica - RS

A RNP pode ajudar ?

Serviços do CAIS

SGIS – Sistema de Gestão de Incidentes de Segurança

Sistema para gestão de incidentes e vulnerabilidades de segurança.

Muito mais informação sobre a segurança da rede.

Consolidador de todas as vulnerabilidades e incidentes.

Mais de 1.400 usuários ativos (técnicos e gestores)

Sem custos para as OUs.



Serviços do CAIS

Rede de Sensores Distribuídos



46 sensores ativos (27 PoPs + 19 clientes)
~ 3 mil detecções/dia

Integrado ao SGIS
Escalabilidade e sustentabilidade

Serviços do CAIS

Seminários Online

2017-1: Ataques de Negação de Serviço

2017-2: Importância do Backup

2017-3: Preservação de evidências de incidentes de segurança e comunicação às autoridades.

Webinar - A evolução dos ataques de DoS



Comissão de Inquérito
Poder Judiciário - EMBRAER
Instituto de Defesa do Consumidor
Instituto de Defesa do Consumidor - Procon
Instituto de Defesa do Consumidor - Procon

A evolução dos ataques
de negação de serviço (DoS)
Por: Rildo Antonio de Souza - CAIS/RNP

27 de abril de 2017

Rildo @RNP

Serviços do CAIS

Seminários Online

2018-1: Lei Geral de Proteção de Dados

2018-2: Usando wi-fi com segurança

2018-3: Configuração segura de DNS.

Serviços do CAIS

DISI – Dia Internacional de Segurança em Informática

DISI'18: 30 de agosto

Cibercrimes – “Fraudes virtuais, golpes reais”



RNP | Contato

'17 DISI

DIA INTERNACIONAL DE SEGURANÇA EM INFORMÁTICA

19.10.2017

RANSOMWARE
NÃO SEJA VÍTIMA DE SEQUESTRO VIRTUAL

HOME | SOBRE | LOCAL | PROGRAMAÇÃO | INSCRIÇÃO | NOTÍCIAS | GALERIA | PATROCÍNIO | ASSISTA AO VIVO

DISI

O Dia Internacional de Segurança em Informática - DISI 2017 será realizado no dia 19/10 na Confederação Nacional dos Trabalhadores no Comércio (CNTC), em Brasília (DF).

A cada edição do evento, são abordados assuntos relacionados a um tema específico de grande interesse de usuários finais de computadores, com o objetivo de promover boas práticas em segurança da informação.

Este ano, o tema será "Ransomware: não seja vítima de sequestro virtual". A programação terá discussões atuais sobre criptografia; indústria de antimalware; proteção de dados corporativos; ataques de ransomware em Internet das Coisas (IoT) e tendências futuras, entre outros assuntos.

As palestras são gratuitas, abertas ao público e transmitidas em tempo real. Depois, os vídeos serão gravados e disponibilizados neste site.

Participe!

Notícias

19/10/2017
Palestra reforça o papel da conscientização na manutenção da segurança em ambientes corporativos.

19/10/2017
CAIS/RNP identificou 392 casos de ransomware na rede acadêmica em 2017

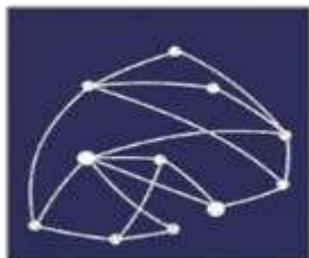
19/10/2017
Apresentação debate formas de mitigar ataques de ransomware

Considerações finais...



<https://www.google.com.br/imghp?hl=pt-BR&tab=wi>

Considerações finais...



RNP

Service Desk
Integrado

A qualquer hora você pode contar com a gente!



atendimento@rnp.br



Atendimento online



0800 722 0216



INOC-DBA
1916*800



cais@cais.rnp.br

Considerações finais...

OBRIGADO!!!

Rildo Souza

rildo.souza@rnp.br