Panorama da segurança da informação

MG

André R. LANDIM
CAIS/RNP

RNP
MINISTÉRIO DA DEFESA
MINISTÉRIO DA CULTURA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
BRASIL GOVERNO FEDERAL

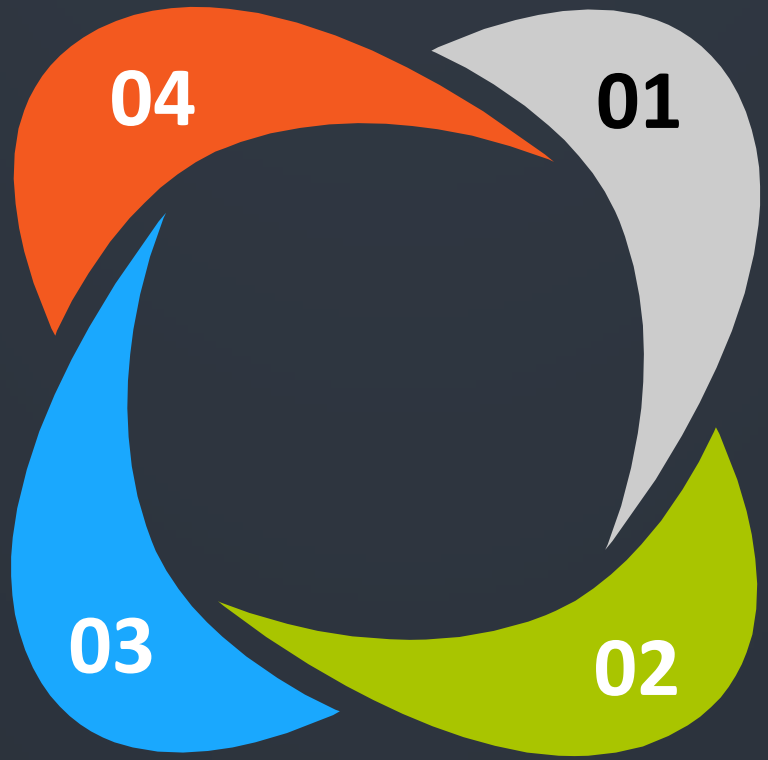
SEGURANÇA DA INFORMAÇÃO NA RNP

CAIS

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

Soluções em segurança

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



Segurança corporativa

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

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.

Serviços do CAIS

SGIS – Sistema de Gestão de Incidentes de Segurança

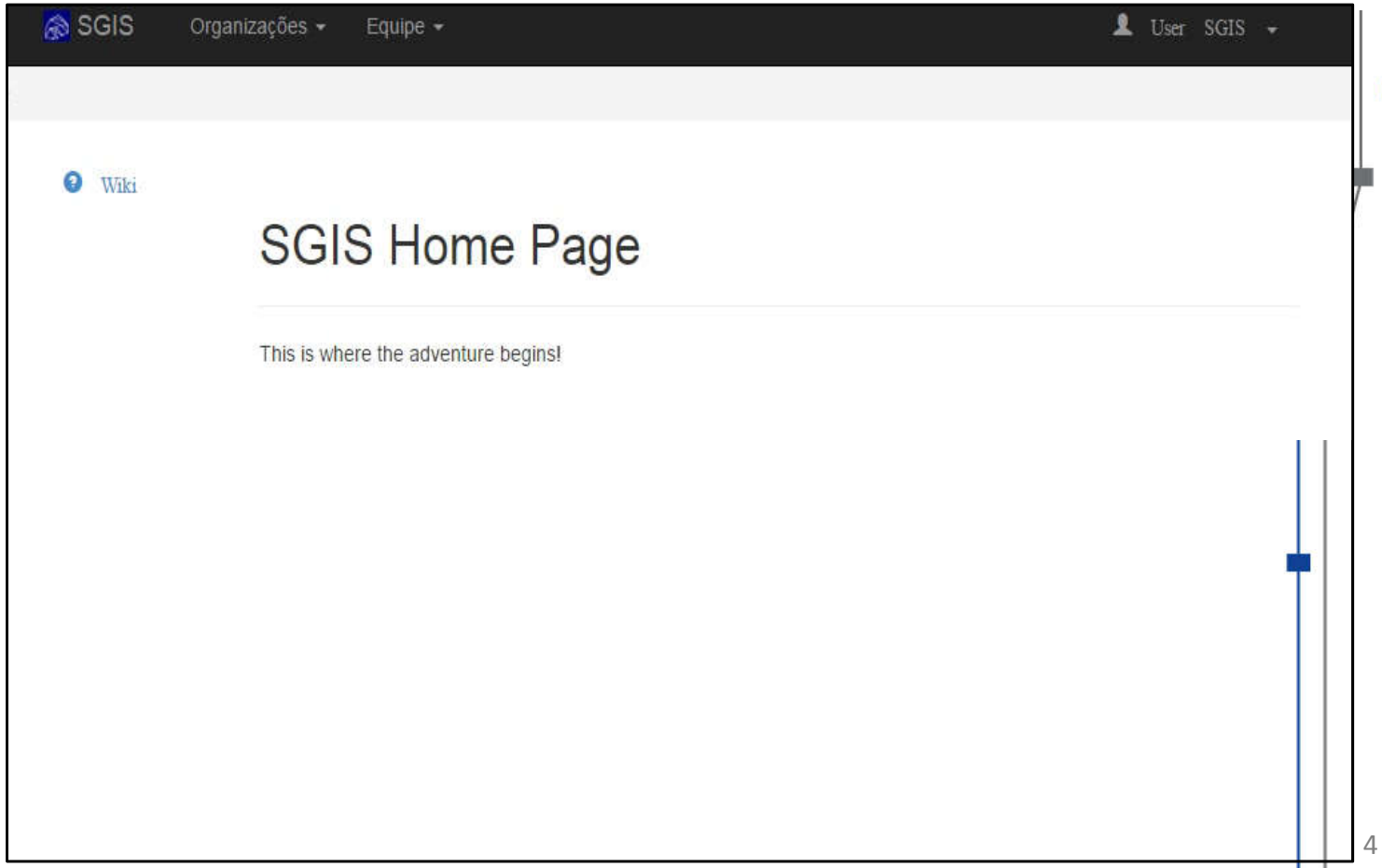
Sistema para gestão de incidentes e vulnerabilidades de segurança.

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

SGIS – Sistema de Gestão de Incidentes de Segurança

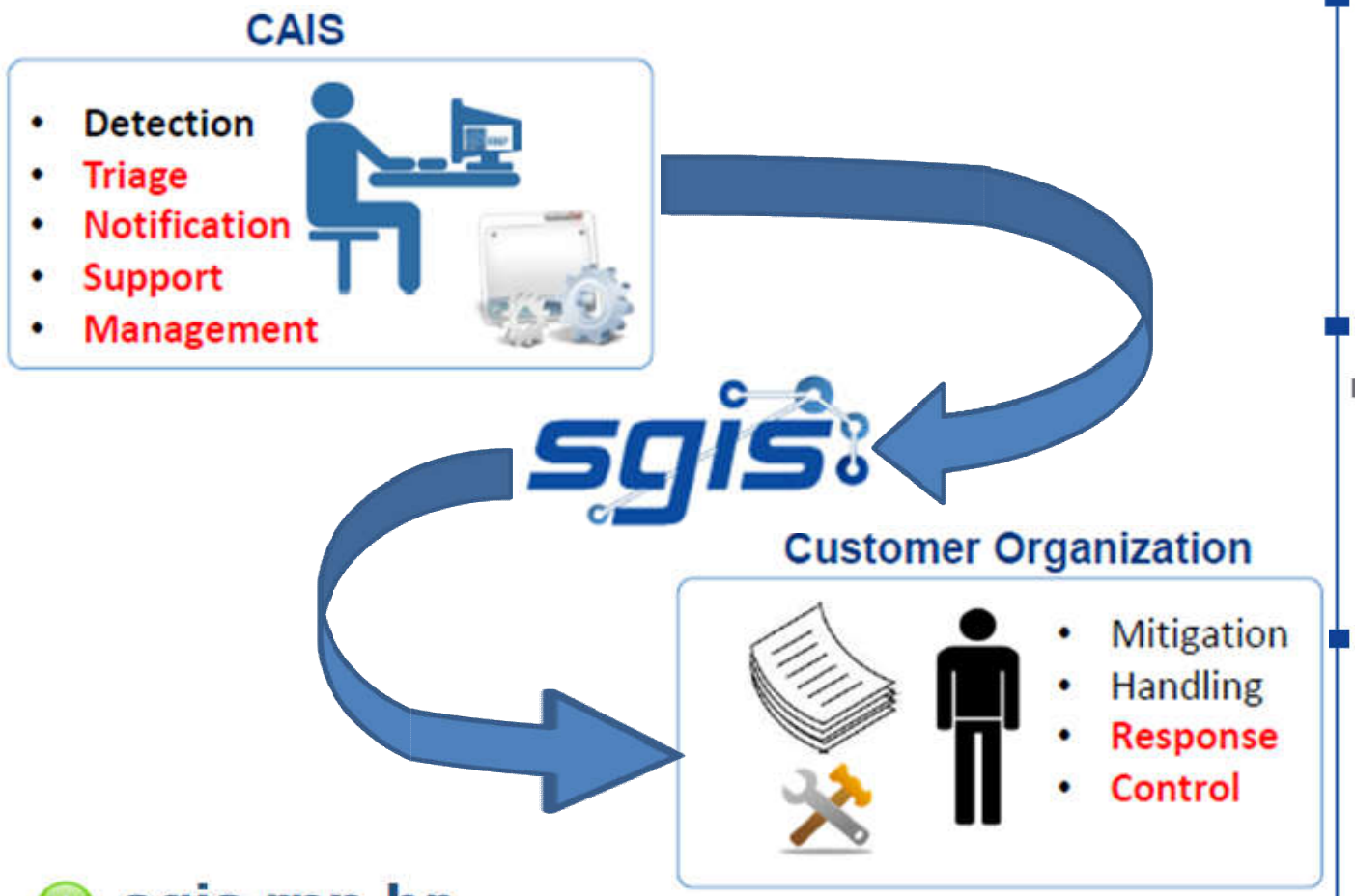
Sistema para gestão de incidentes e vulnerabilidades de segurança.

Muito mais informação sobre a segurança da rede.

Consolidador de todas as vulnerabilidades e incidentes.

Mais de 1.400 usuários ativos (técnicos e gestores)

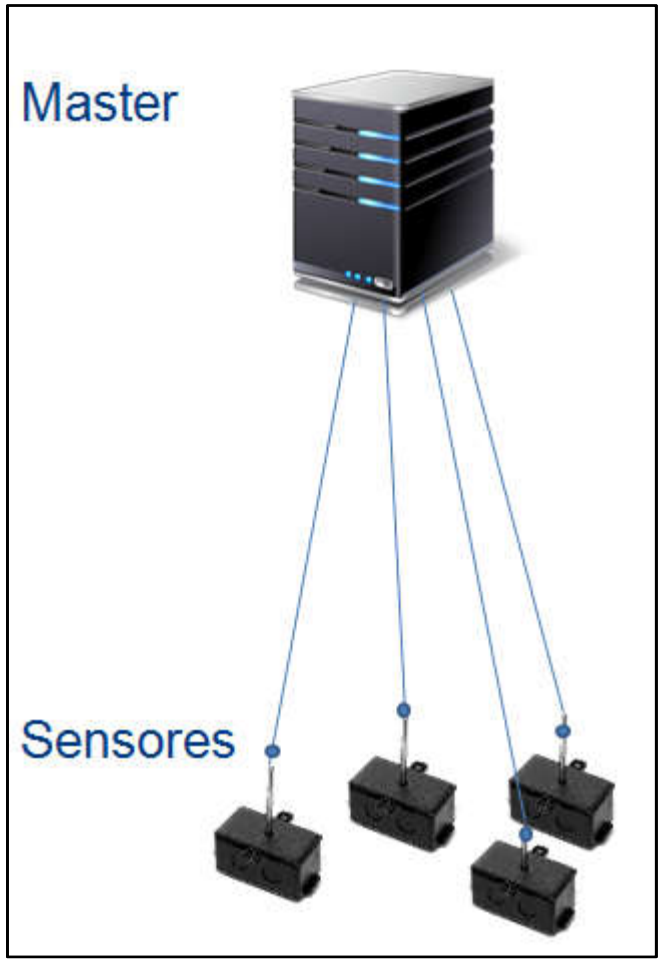
Sem custos para as OUs.

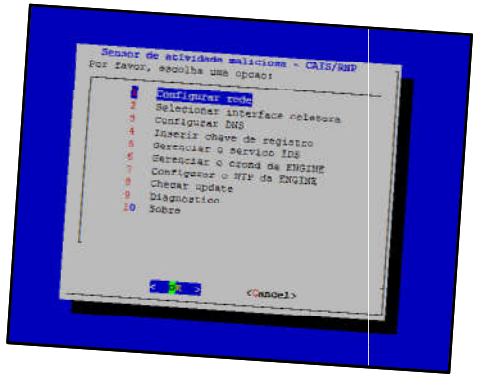


sgis.rnp.br

Serviços do CAIS

Rede de sensores distribuídos





46 sensores ativos (27 PoPs + 19 clientes)

~ 37mil detecções/dia

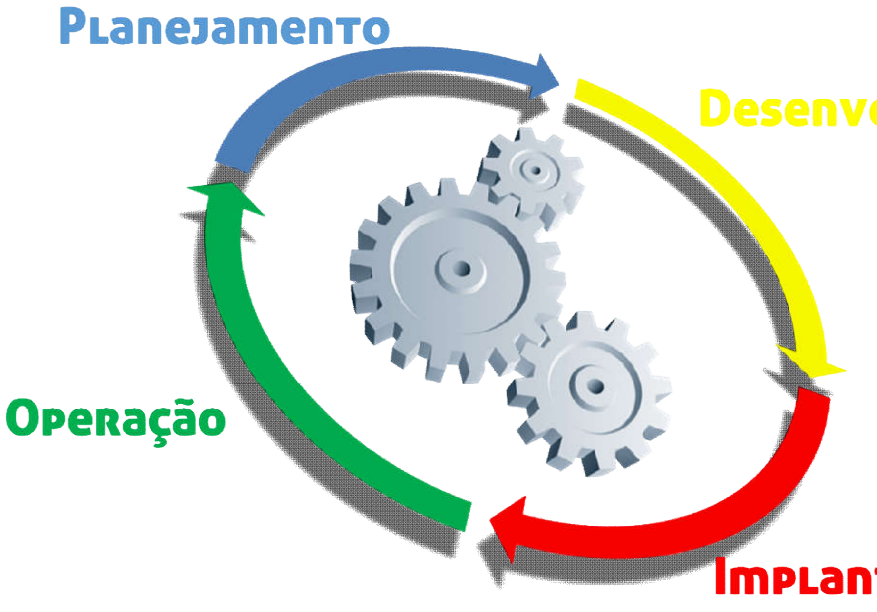
Integrado ao SGIS

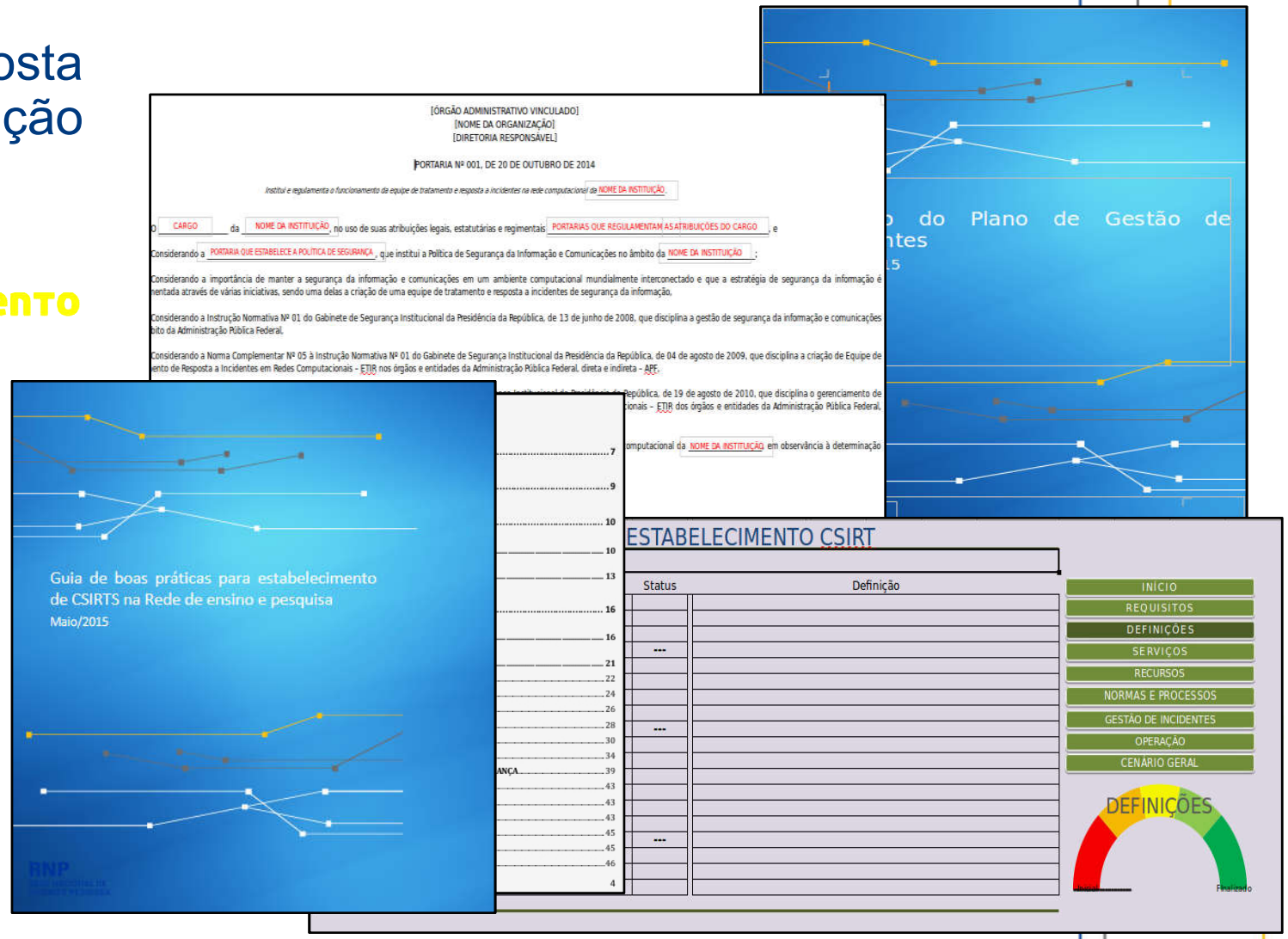
Escalabilidade e sustentabilidade

Serviços do CAIS

Gestão de segurança para Clientes

Estabelecimento de Equipes de Resposta a Incidentes de Segurança da Informação





Serviços do CAIS

Seminários on-line

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.

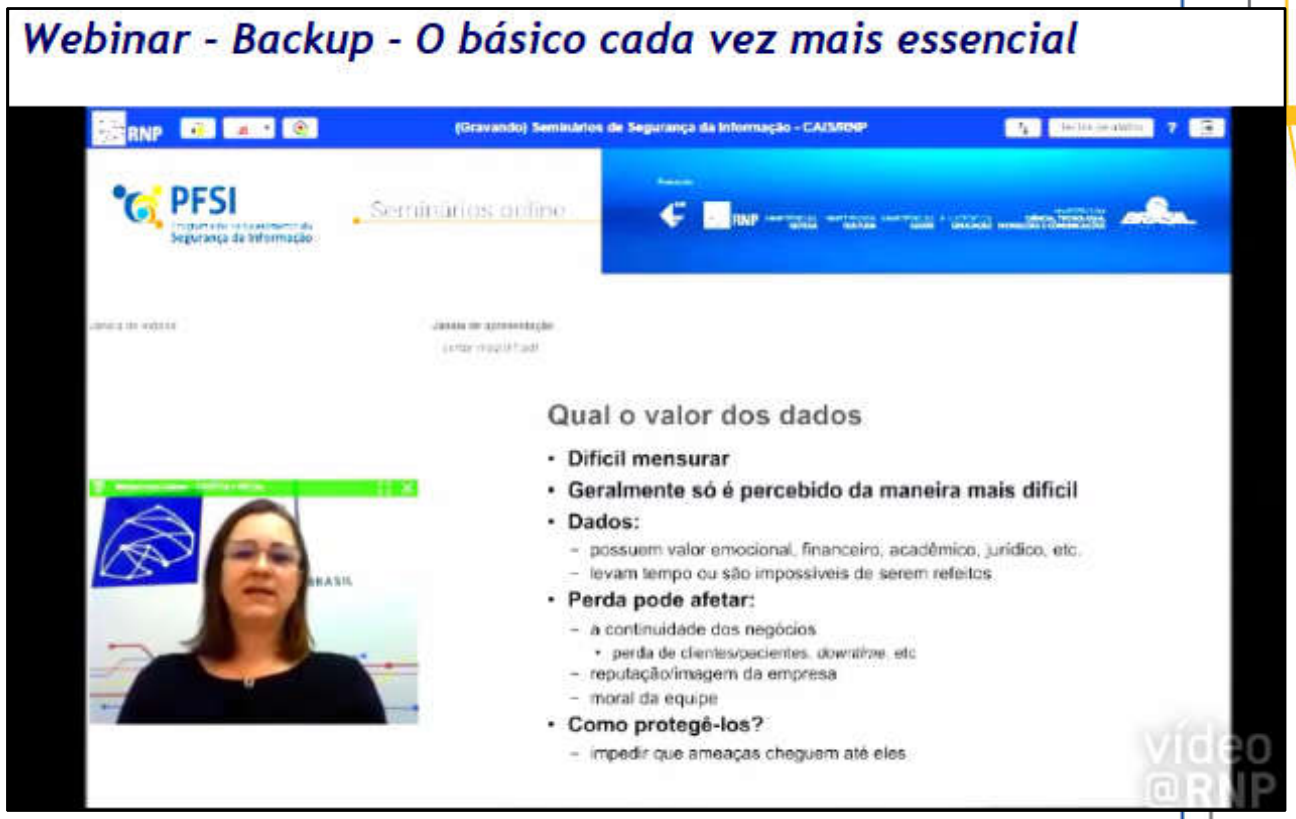
Serviços do CAIS

Seminários on-line

2018-1: Levando SegInfo para casa

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"

http://disi.rnp.br

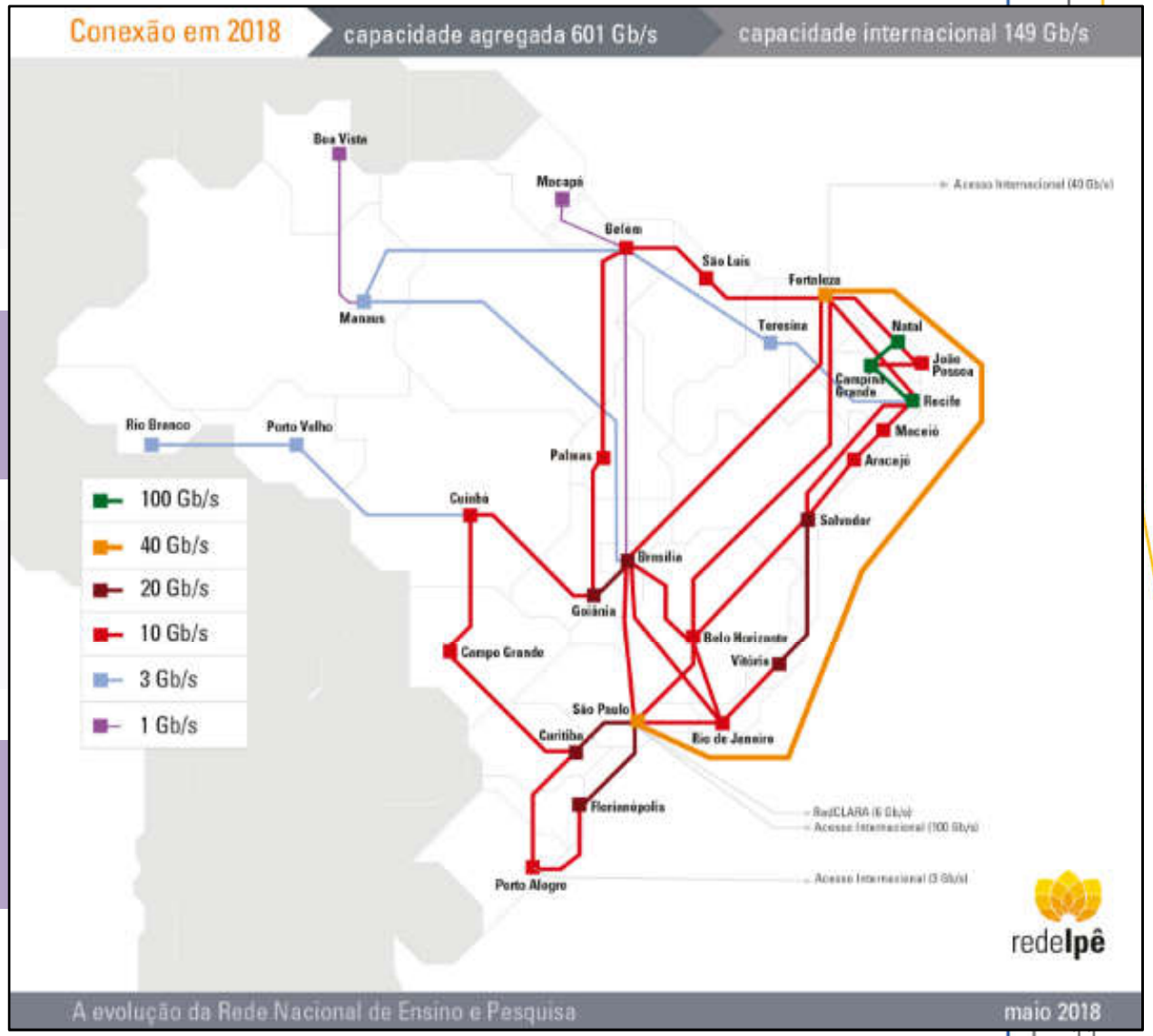
Panorama de SegInfo na rede acadêmica

Rede Ipê, backbone da rede acadêmica. Capacidade integrada de 601 Gb/s.

CAIS coordena cerca de 1,393 clientes (IFs, IFEs, Unidades de Pesquisa), 159 em MG

+620 mil notificações enviadas aos administradores de redes e sistemas nos últimos 12 meses*.

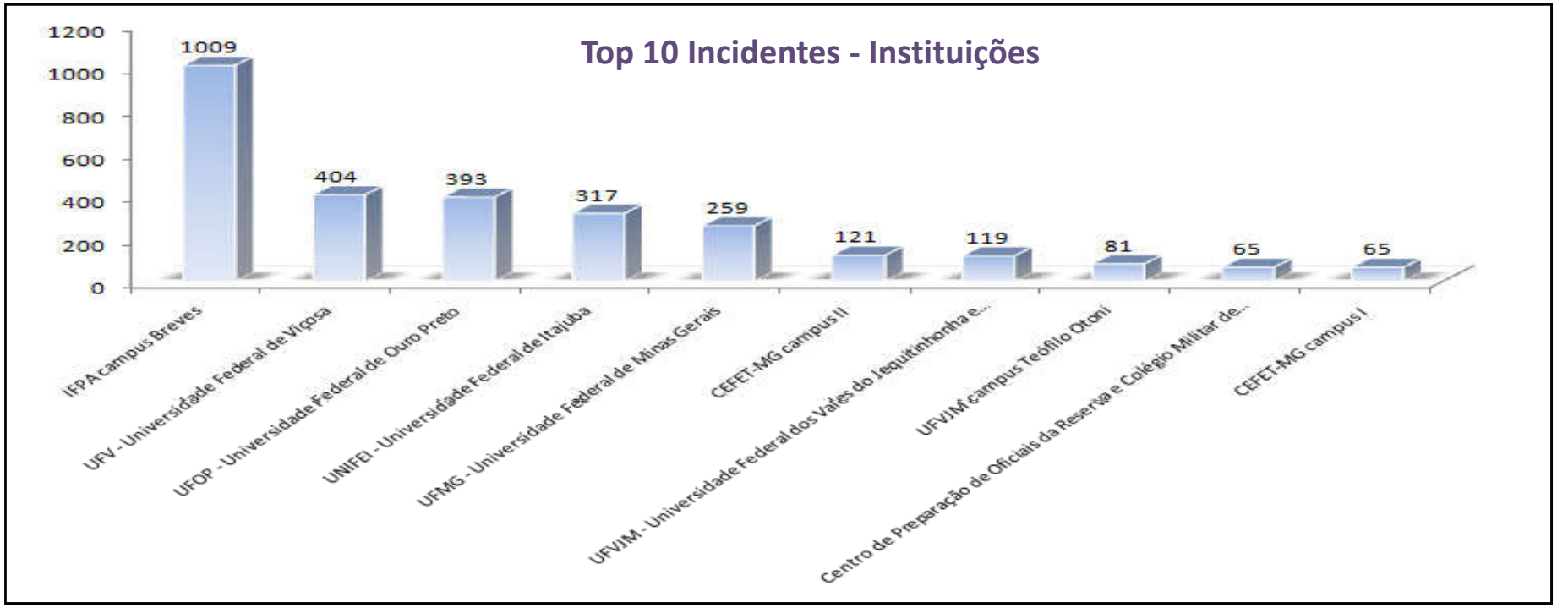
+37 mil (cerca de 6%) das notificações são relativas a incidentes de segurança.



*De maio/17 a maio/18

Panorama de SegInfo na rede acadêmica - MG

Mais de 21 mil notificações enviadas nos últimos 12 meses*

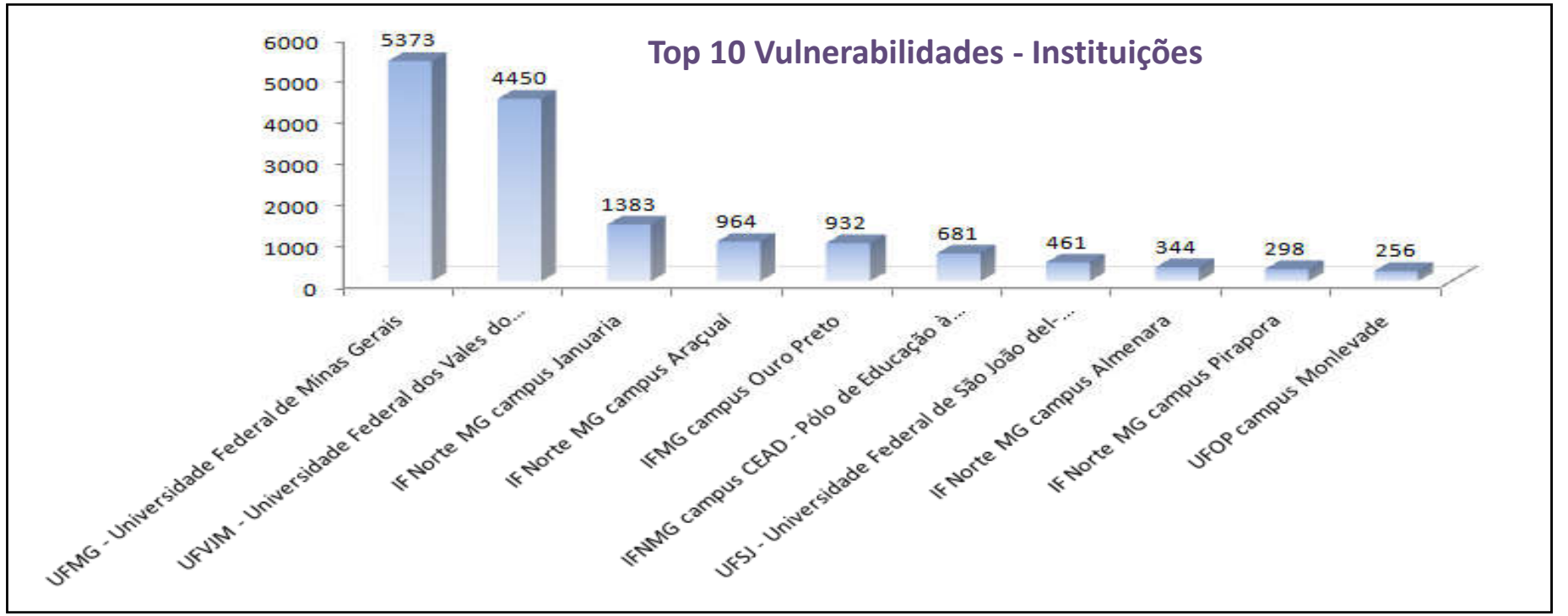


3.707 notificações de incidentes, apenas 573 foram fechadas.
Taxa de resposta a incidentes de 15.4%

*De Jun/17 a Jun/18

Panorama de SegInfo na rede acadêmica - MG

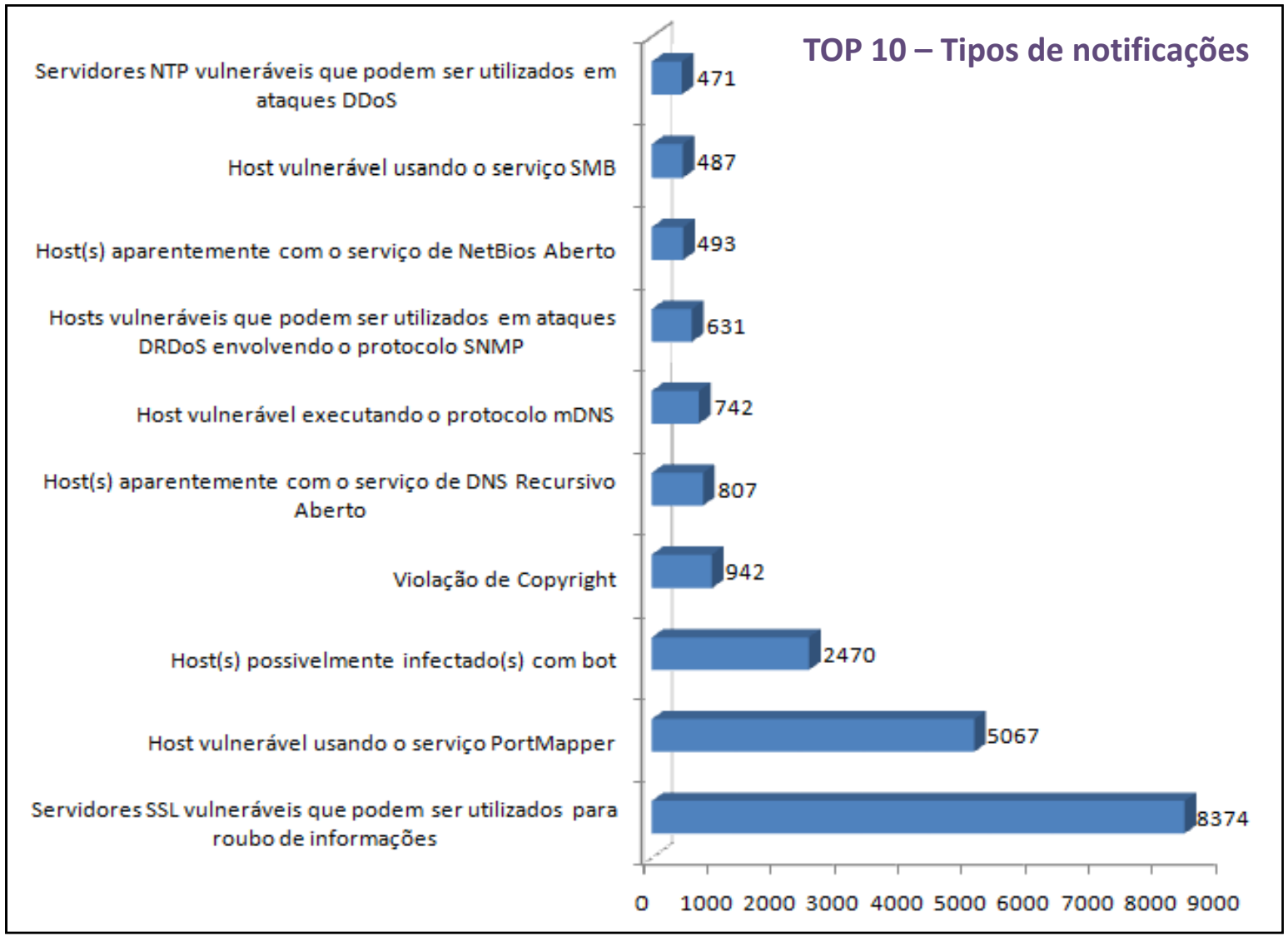
Mais de 21 mil notificações enviadas nos últimos 12 meses*



18.038 notificações de vulnerabilidades, 4.74% (855 notificações) foram fechadas

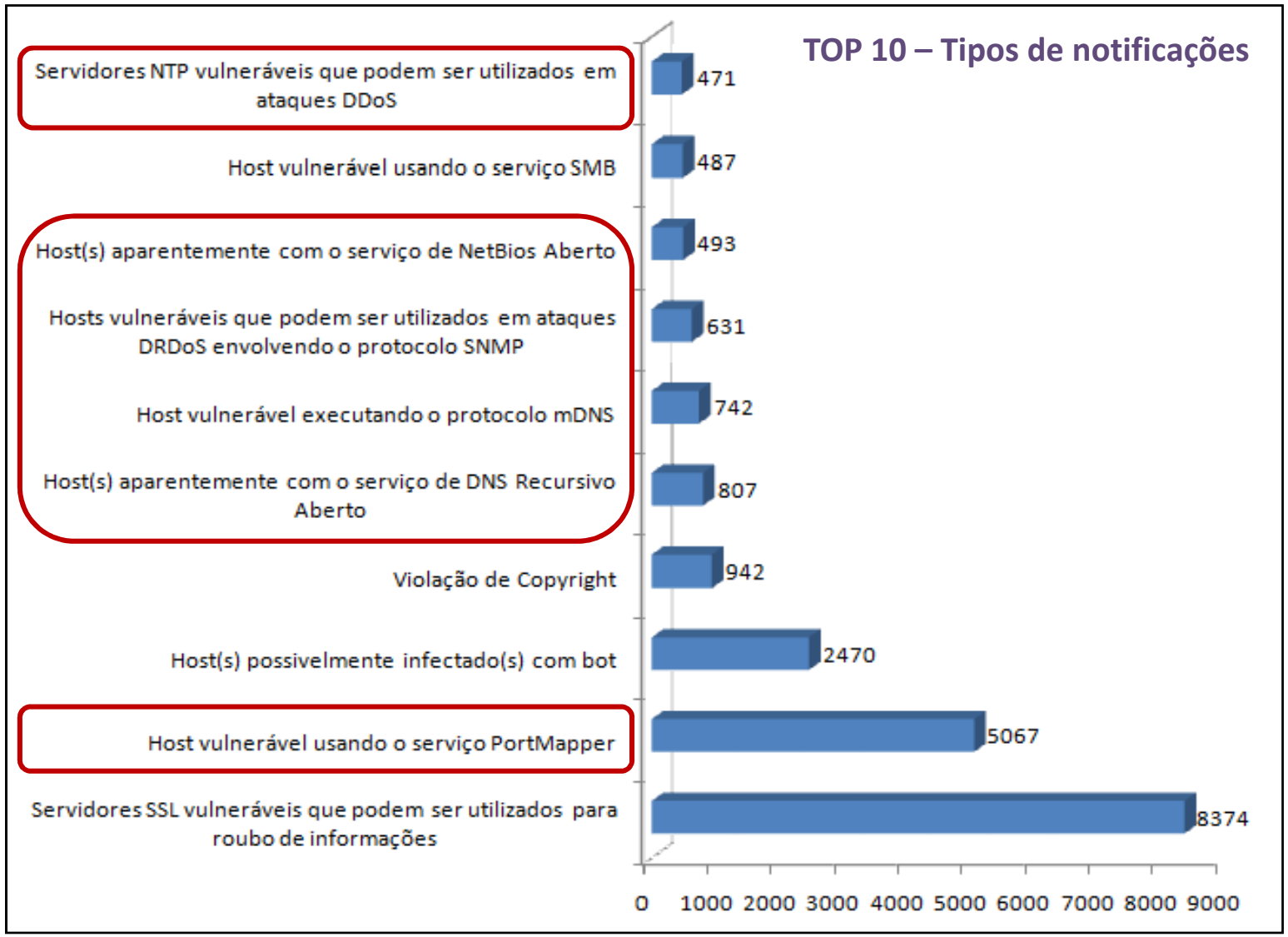
*De Jun/17 a Jun/18

Panorama de SegInfo na rede acadêmica - MG



*De Jun/17 a Jun/18

Panorama de SegInfo na rede acadêmica - MG



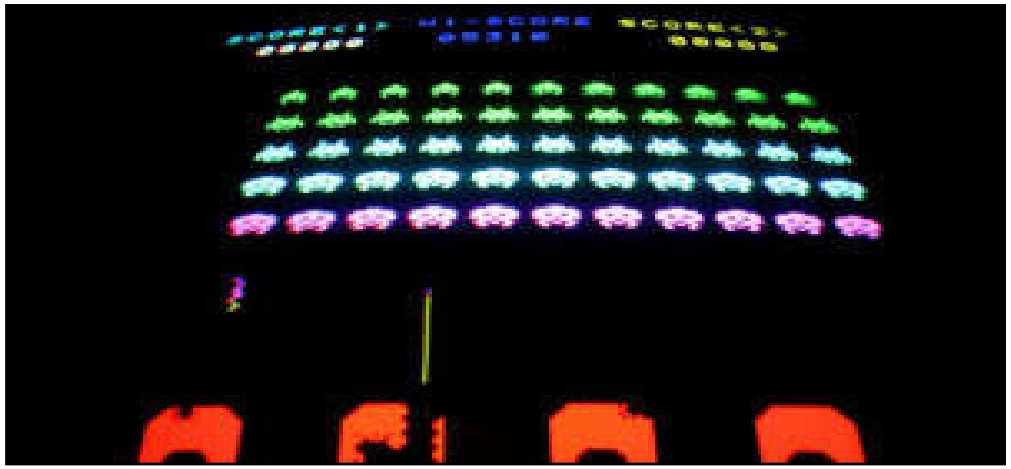
*De Jun/17 a Jun/18

Ataques de Negação de Serviço

- Um ataque de negação de serviço (Denial Of Service - DoS) tem o objetivo básico de consumir todos os recursos computacionais do "alvo" tornando-o indisponível;

- Denominamos "DoS" (Denial Of Service) quando apenas uma fonte origina o ataque contra um determinado alvo;

- Quando mais fontes estão envolvidas nos ataques é denominado "DDoS" (Distributed Denial Of Service).



Ataques de Negação de Serviço

Classificação

Ataques volumétricos

- Ocorrem quando uma grande quantidade de banda é utilizada para interromper ou degradar a operação de um servidor e/ou rede

Ataques no nível de aplicação

- Exploram comportamentos dos serviços e/ou protocolos em execução e por diversas vezes não necessita de uma grande quantidade de banda para sua realização

Ataques em nível de protocolos

- Exploram comportamento específicos dos protocolos dando uma aparência normal em uma comunicação

Ataques de Negação de Serviço

Amplificação

- 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.

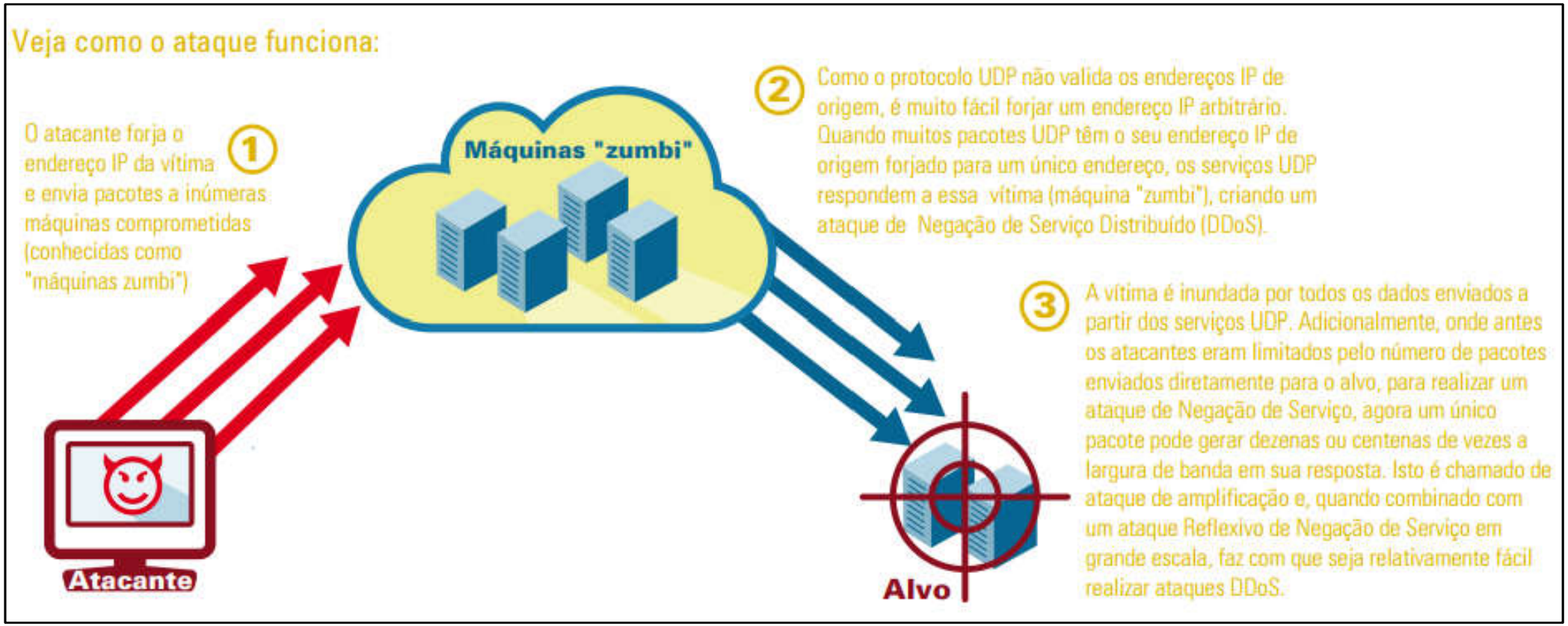
Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	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]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—

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

Ataques de Negação de Serviço

DRDoS

Ataque DRDoS ocorre quando um atacante forja o IP origem de uma conexão e realiza requisições para serviços específicos, as respostas dessas requisições são direcionadas para a vítima de forma que ela se torna incapaz de processar todo o volume de informação podendo ficar indisponível.

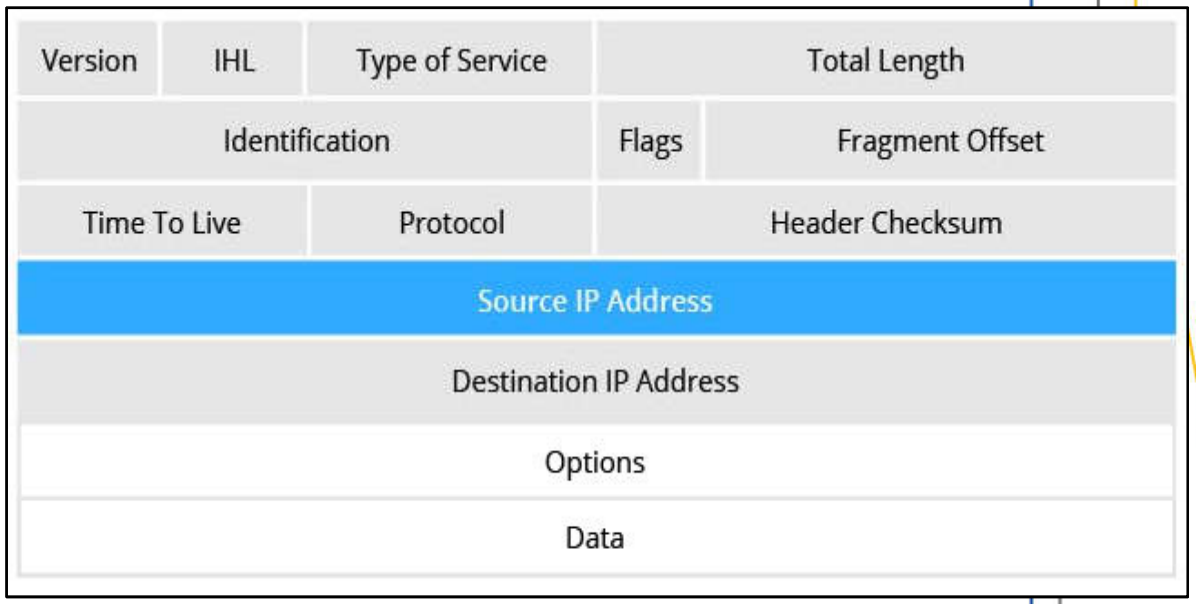


https://www.rnp.br/sites/default/files/cais_em_resumo_2014_2.pdf

Ataques de Negação de Serviço

IP Spoofing

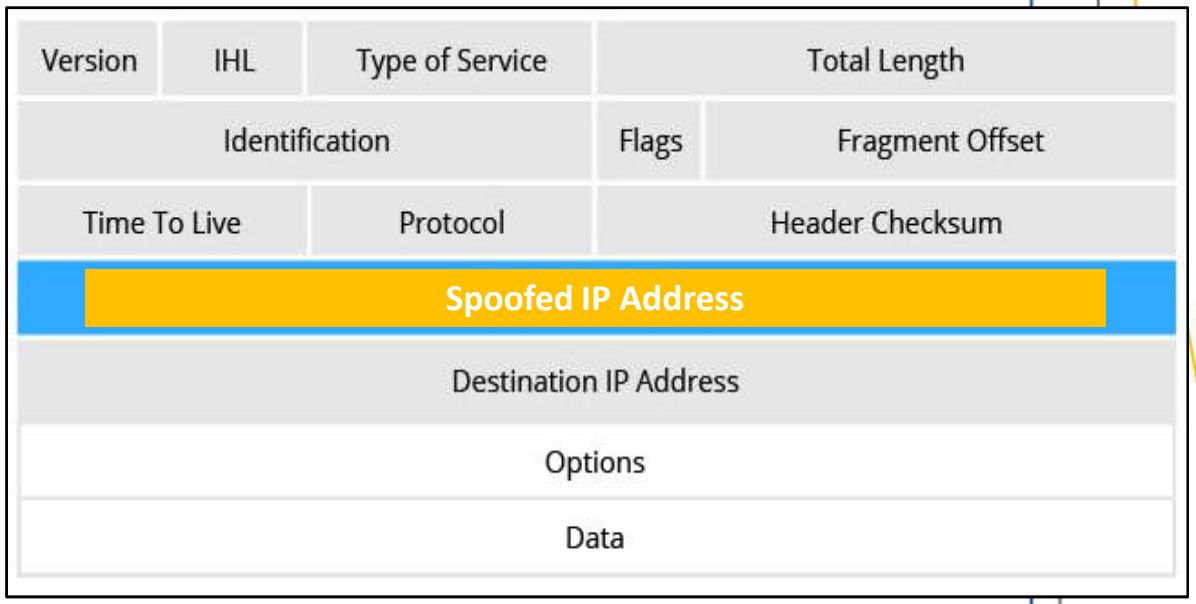
- Obter acesso concedido a um IP específico
- Mascarar um ataque realizado, dificultando a rastreabilidade
- Realizar ataques de flood
- Coordenar ataques de negação de serviço distribuídos e reflexivos



Ataques de Negação de Serviço

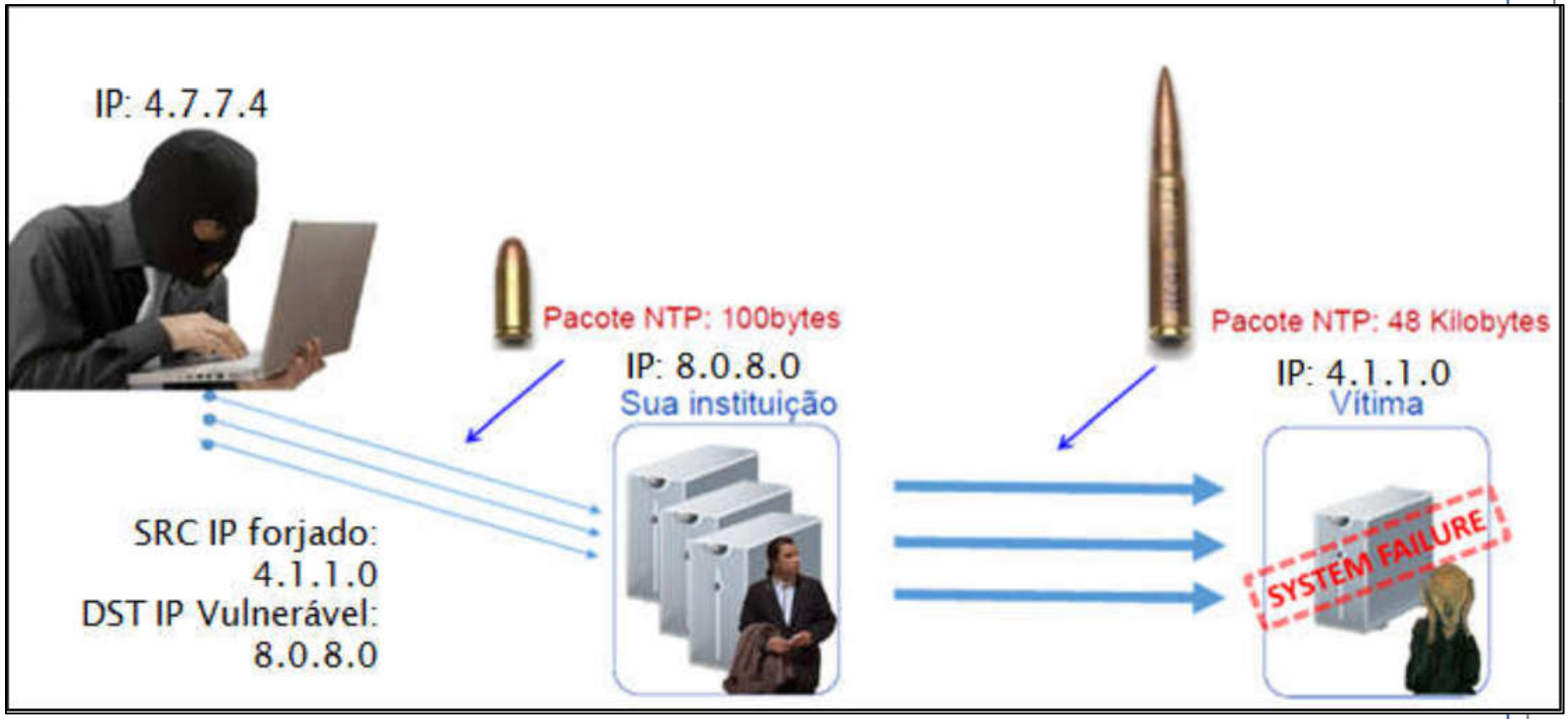
IP Spoofing

- Obter acesso concedido a um IP específico
- Mascarar um ataque realizado, dificultando a rastreabilidade
- Realizar ataques de flood
- Coordenar ataques de negação de serviço distribuídos e reflexivos



Ataques de Negação de Serviço

DRDoS



Ataques de Negação de Serviço

Detectando hosts vulneráveis - NMAP

```
root@lab-ddos-atk00:~# nmap -sU -p U:53 -n -Pn 13.37.1.50 --script=dns-recursion

Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-26 04:17 -03
Nmap scan report for 13.37.1.50
Host is up (0.00028s latency).
PORT   STATE SERVICE
53/udp open  domain
|_dns-recursion: Recursion appears to be enabled
MAC Address: 08:00:27:46:05:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
root@lab-ddos-atk00:~#
```

Ataques de Negação de Serviço

Detectando hosts vulneráveis - NMAP

```
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
```

Ataques de Negação de Serviço

Detectando hosts vulneráveis - NMAP

```
root@lab-ddos-atk00:~# nmap -sU -p U:161 -n -Pn 13.37.1.50 --script=snmp-info,snmp-sysdescr

Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-26 04:23 -03
Nmap scan report for 13.37.1.50
Host is up (0.00024s latency).
PORT    STATE SERVICE
161/udp open  snmp
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 96c94322cf2e2c5b00000000
|   snmpEngineBoots: 13
|_  snmpEngineTime: 9m55s
| snmp-sysdescr: Linux lab-ddos-amp00 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64
|_  System uptime: 9m56.18s (59618 timeticks)
MAC Address: 08:00:27:46:05:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

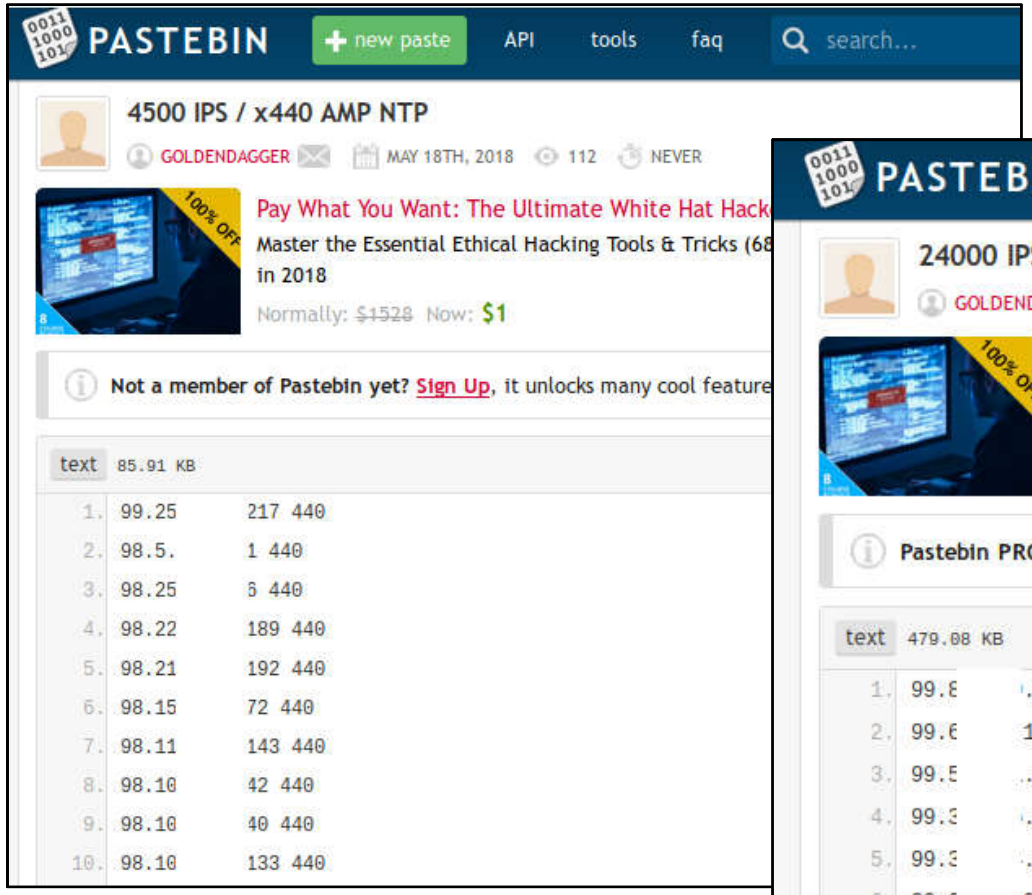
Ataques de Negação de Serviço

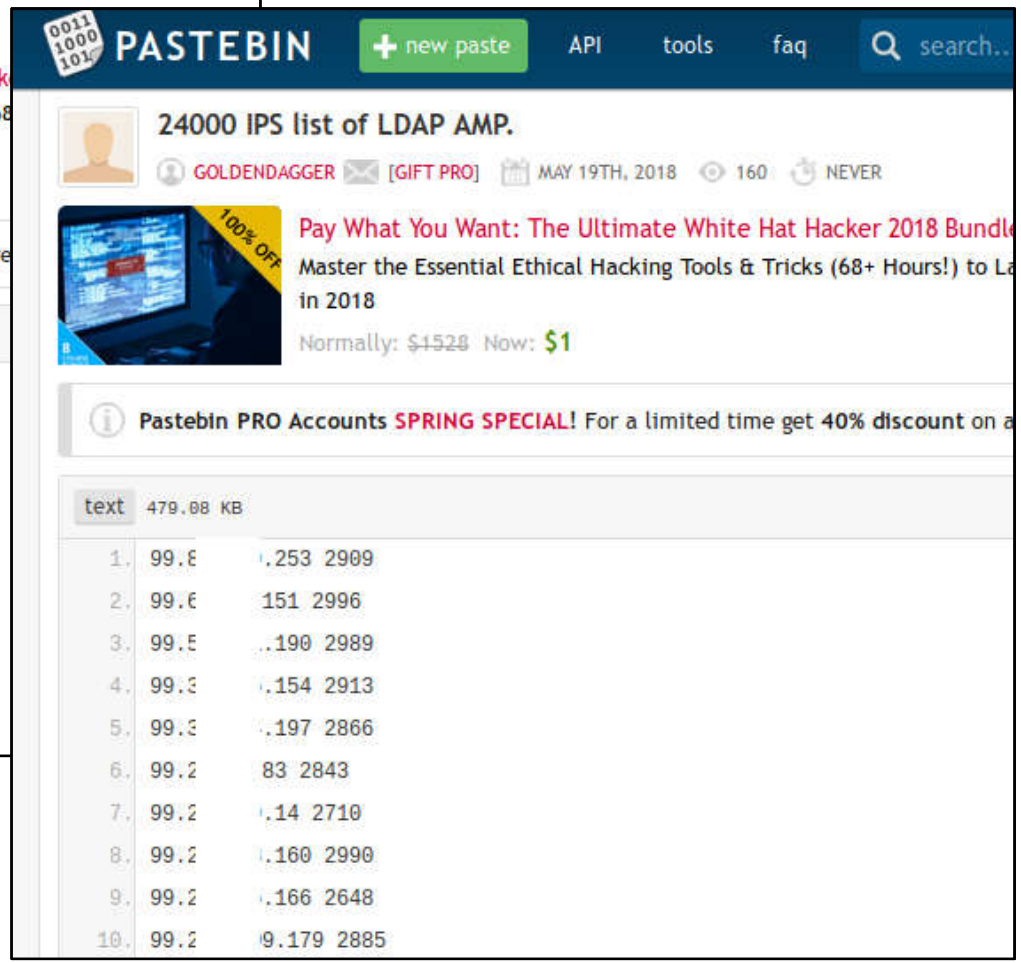
Detectando hosts vulneráveis - NMAP

```
root@lab-ddos-atk00:~# nmap -sU -p U:111 -n -Pn 13.37.1.50 --script=rpcinfo

Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-28 02:53 -03
Nmap scan report for 13.37.1.50
Host is up (0.00027s latency).
PORT    STATE SERVICE
111/udp open  rpcbind
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|_  100000  2,3,4        111/udp  rpcbind
MAC Address: 08:00:27:46:05:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

Ataques de Negação de Serviço

Lista de hosts vulneráveis - Pastebin

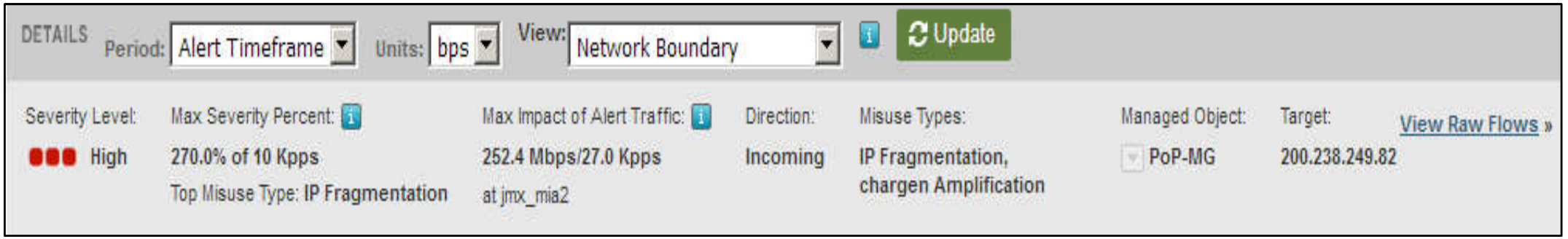




Ataques de Negação de Serviço

Casos interessantes...

Chargen Amplification (UDP/111)



CLDAP Amplification (UDP/389)

Ataques de Negação de Serviço

Testador de vulnerabilidades

http://vtest.rnp.br

Ataques de Negação de Serviço

Como se proteger?

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

Ataques de Negação de Serviço

Como se proteger?

DNS (BIND) Hardening

- ACL's
- Views
- "recursion no"
- Monitoramento de consultas
  - "rate-limit" (RRL)
- Descartar consultas com SRC IP inválidos
  - RFC 1918 (observar em qual "view/acl" deve-se aplicar o descarte)

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

Ataques de Negação de Serviço

Como se proteger?

NTP Hardening

- ACL's
- "restrict default kod notrap nomodify nopeer noquery"
- "disable monitor"
- Utilizar "OpenNTPd"

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

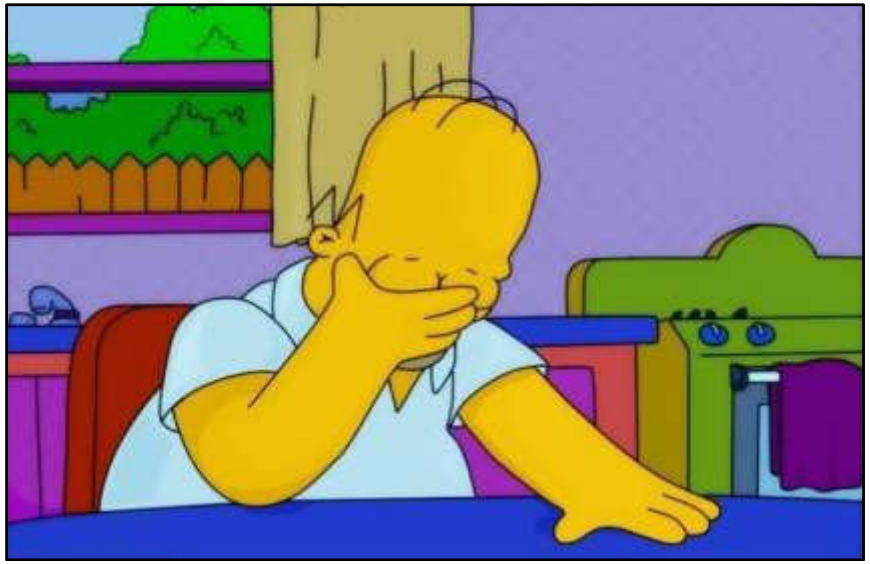
Ataques de Negação de Serviço

Como se proteger?

SNMP Hardening

- ACLs
- "rocommunity DIFERENTE_DE_PUBLIC"
- "rwcommunity DIFERENTE_DE_SECRET"
- Preferencialmente usar SNMPv3

- Desativar serviços desnecessários
  - Portmapper?
    - update-rc.d rpcbind disable
  - Outros...



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

AntiSpoofing

Campanha Técnica 2018
Antispoofing

- Incentivo à aplicação do BCP 38 e BCP 84.
- Guias técnicos de como configurar roteadores (Cisco e Juniper)
- De uso para todos os clientes da RNP, Redes COMEPEs, PoPs, ISP e clientes de IX (troca de tráfego)

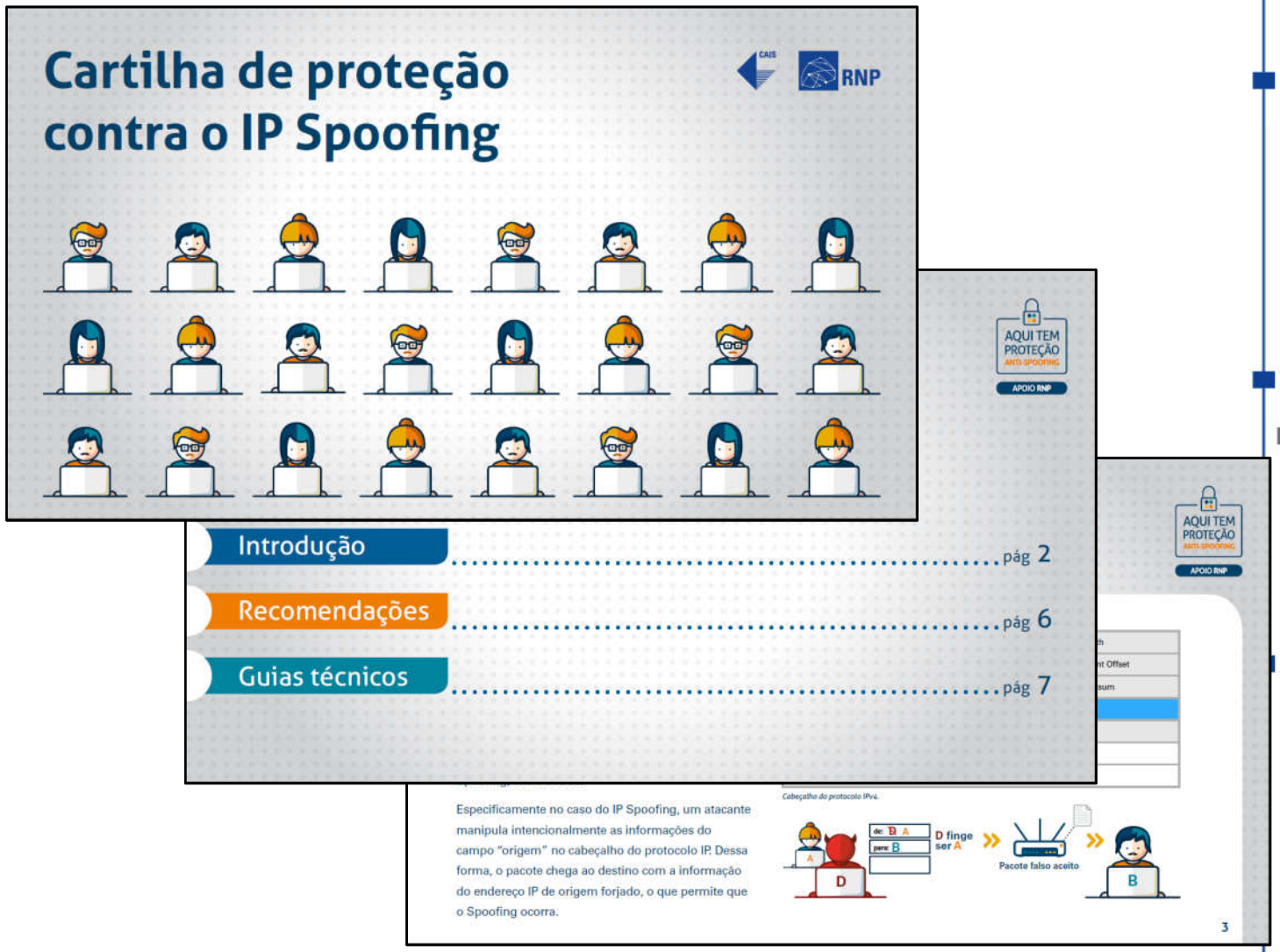
Campanha Técnica 2018

AntiSpoofing

Campanha Técnica 20
Antispoofing

AQUI TEM PROTEÇÃO
ANTI-SPOOFING

APOIO RNP

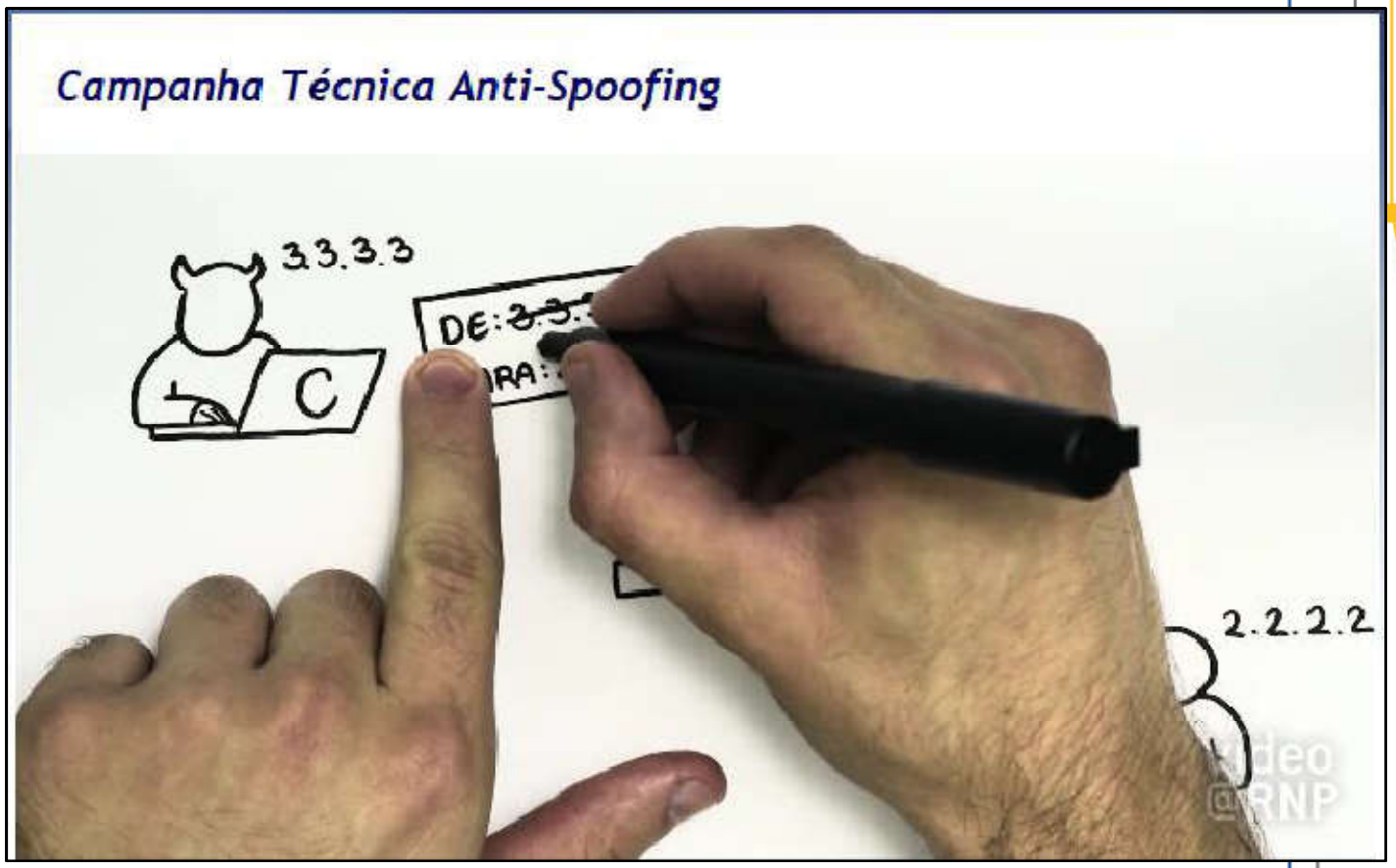


AntiSpoofing

Campanha Técnica 2018
Antispoofing

AQUI TEM PROTEÇÃO
ANTI-SPOOFING

APOIO RNP



http://url.rnp.br?campanhaantispoofing

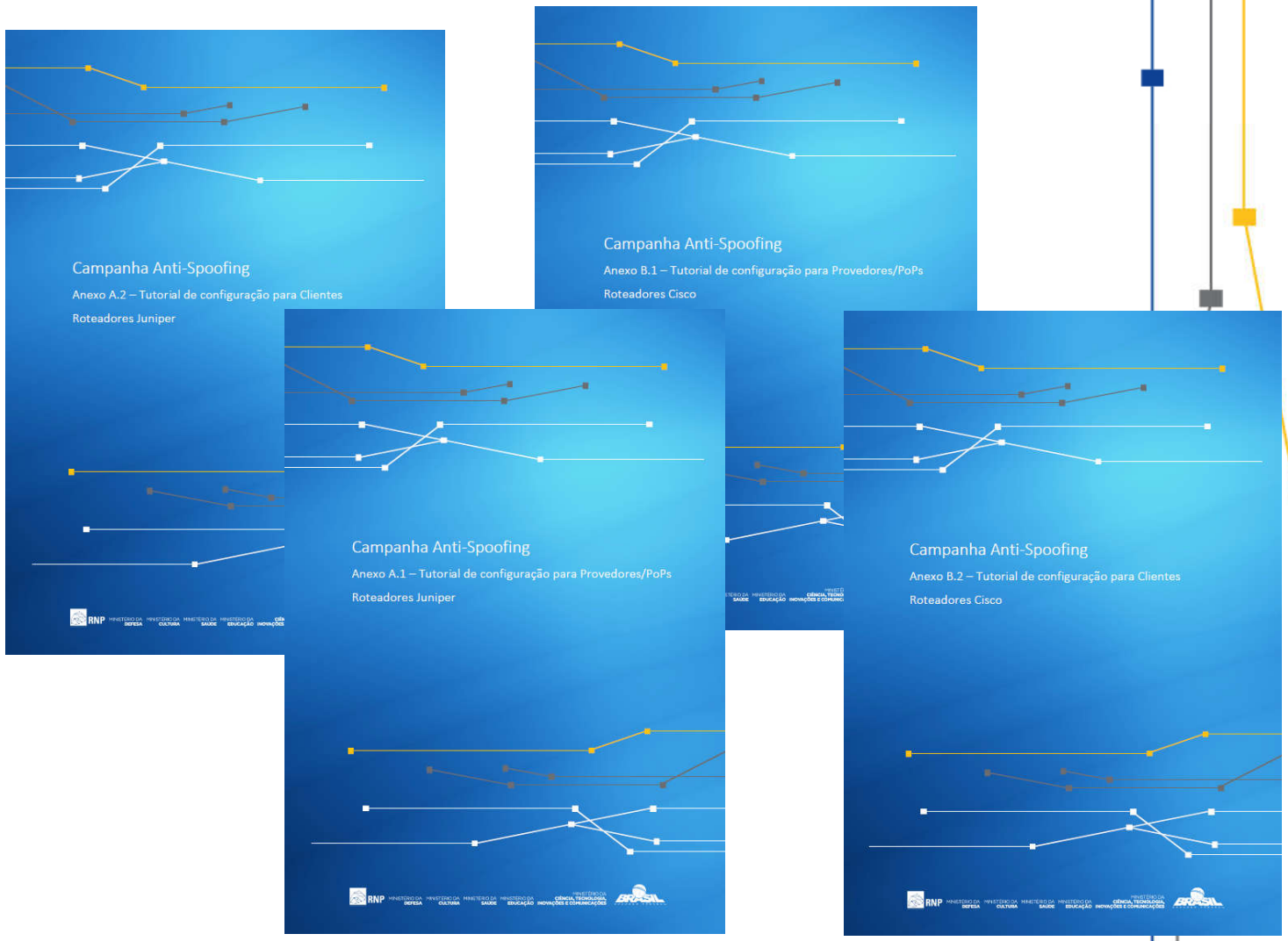
Campanha Técnica 2018

AntiSpoofing

Campanha Técnica 2018
Antispoofing

AQUI TEM PROTEÇÃO
ANTI-SPOOFING

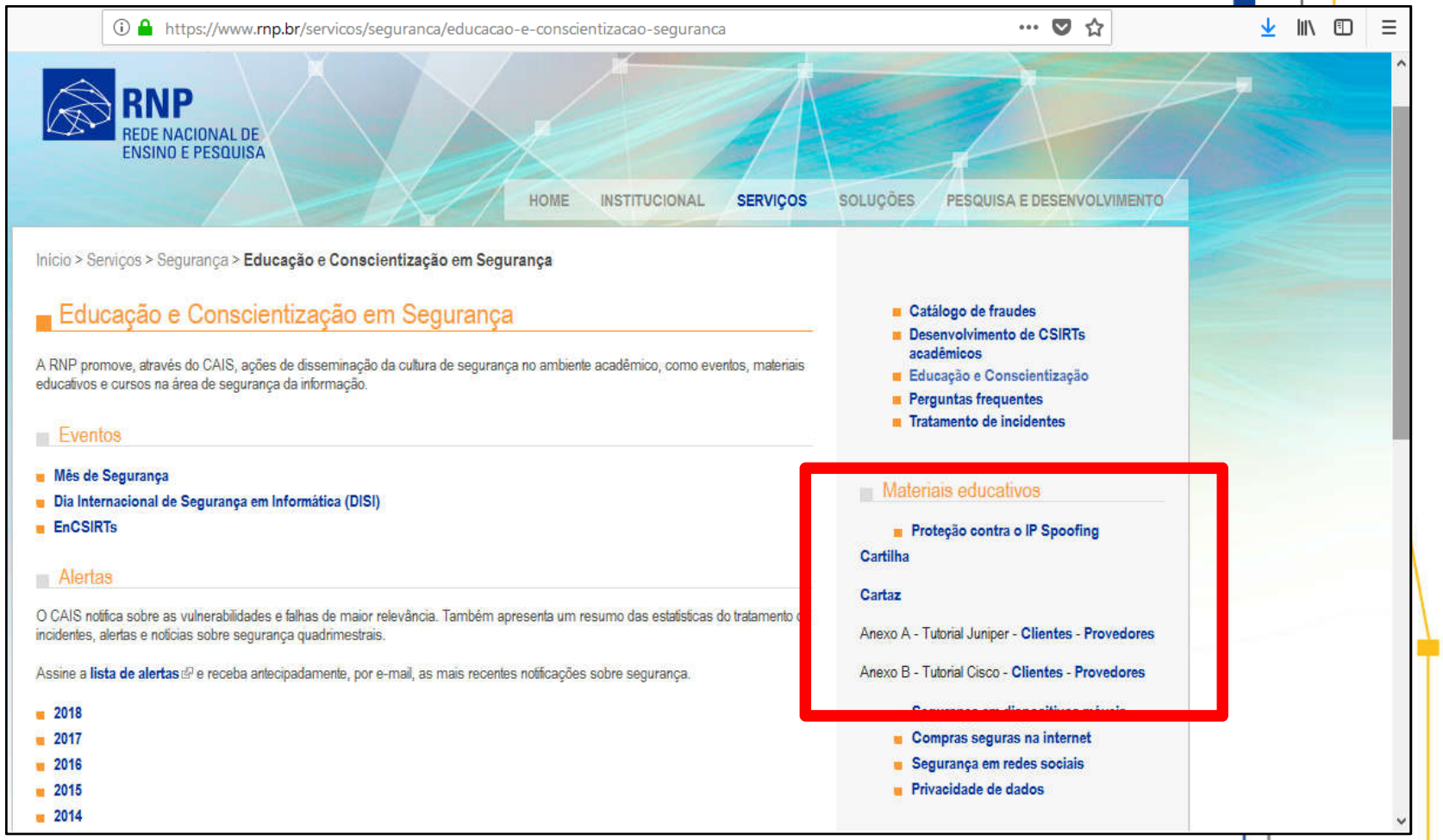
APOIO RNP



Campanha Técnica 2018

AntiSpoofing

Campanha Técnica 2018
Antispoofing



Ataques de Negação de Serviço

Considerações finais

- Considerações finais
- Manter uma boa relação com seu ISP
  - PoP-MG
- Implementar BCP38/BCP84 (Tratamento antispoofing)
- Hardening de serviços considerados mais explorados
- Monitoramento efetivo e pró-ativo
- E por fim...

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

Ataques de Negação de Serviço

Considerações finais

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

Contatos

RNP Atendimento Integrado de Serviços

sd@rnp.br

0800 722 0216

(61) 9 9960 5971

1916*800

cais@cais.rnp.br

Obrigado!

André R. LANDIM

CAIS/RNP

andre.landim@rnp.br

RNP

MINISTÉRIO DA DEFESA

MINISTÉRIO DA CULTURA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL