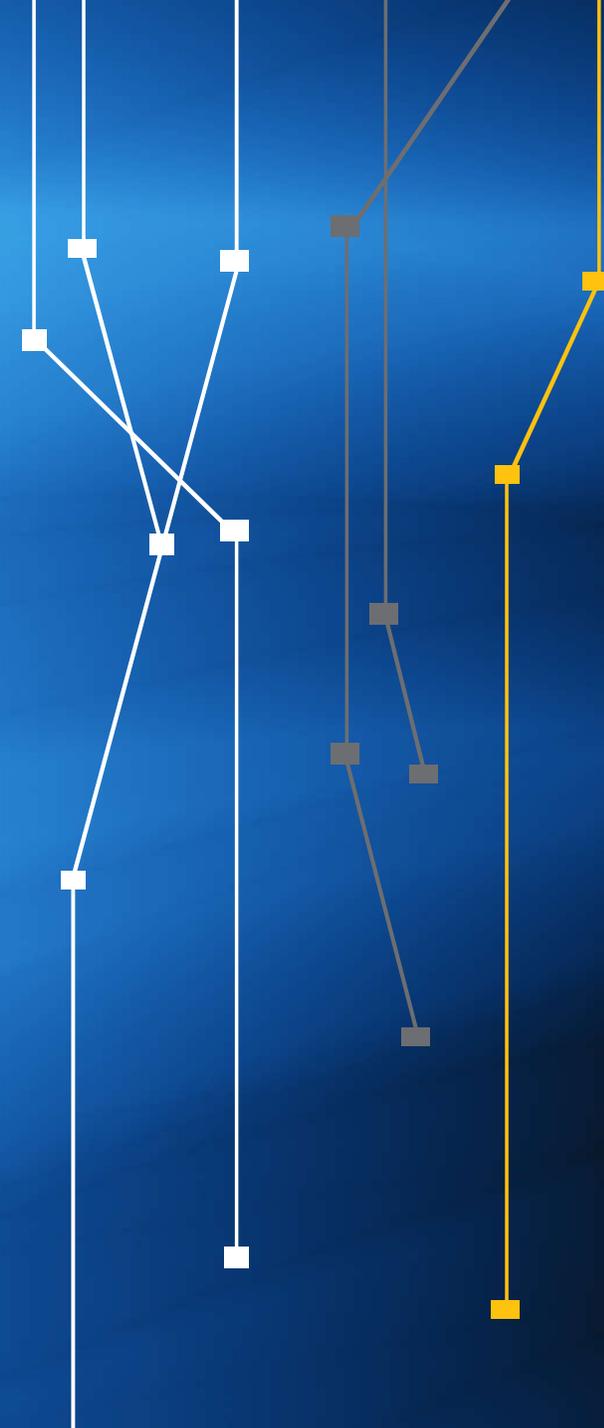


Panorama da segurança da informação

MG

André R. LANDIM
CAIS/RNP



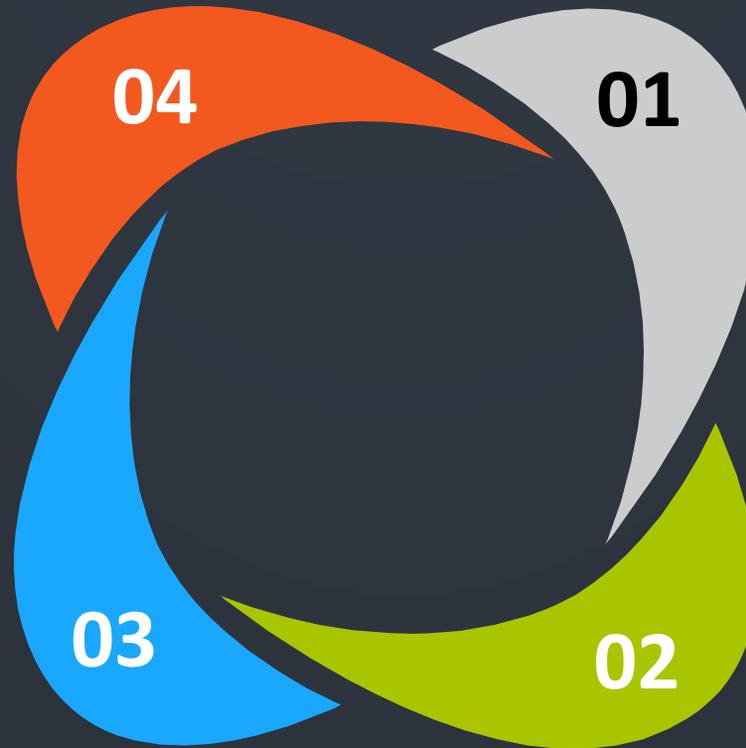
SEGURANÇA DA INFORMAÇÃO NA RNP

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.



CAIS

Centro de Atendimento a Incidentes de Segurança

20 anos de atuação na área de segurança da informação.

Detecção, resolução e prevenção.



SGIS – Sistema de Gestão de Incidentes de Segurança



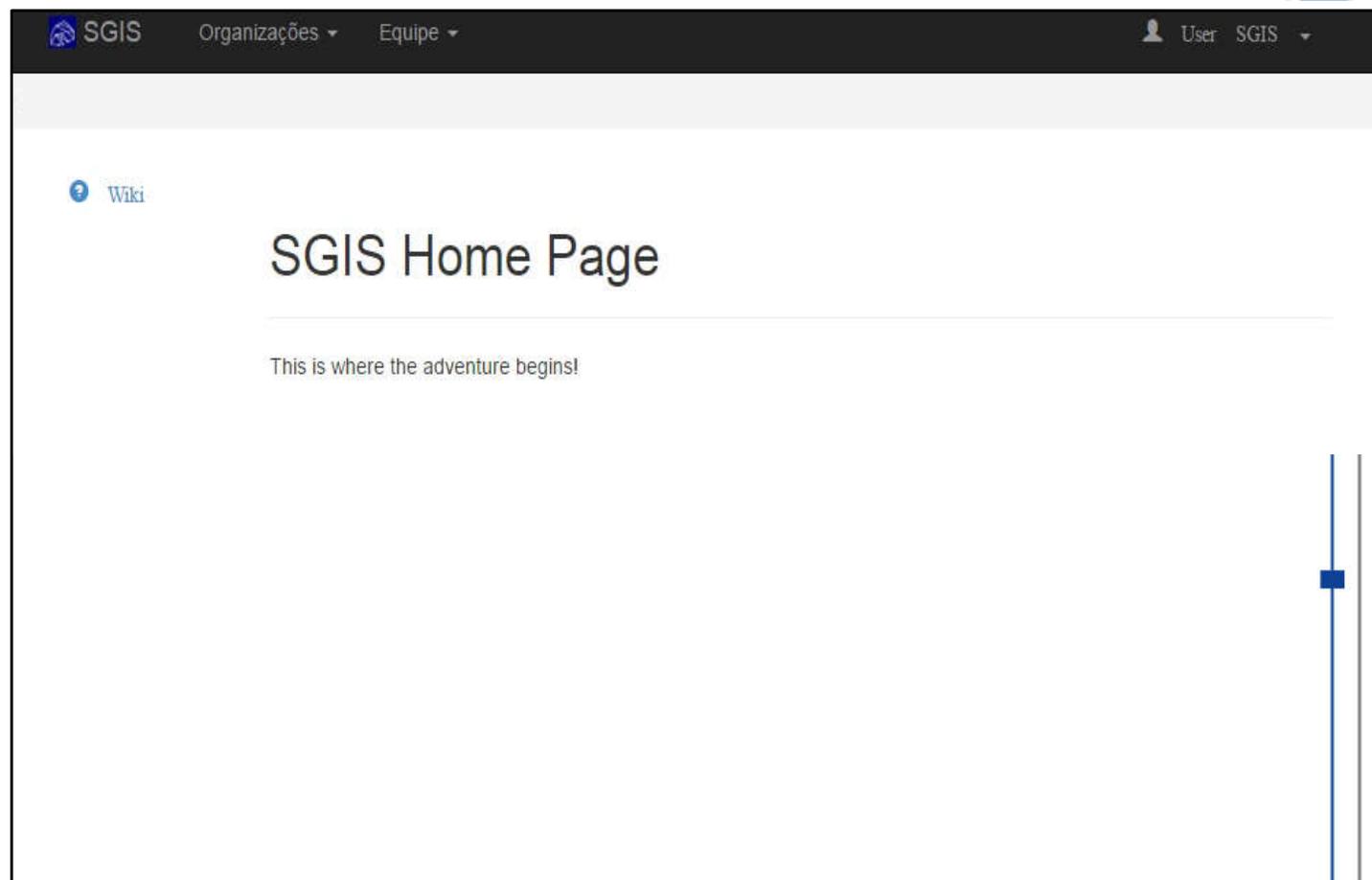
Sistema para gestão de incidentes e vulnerabilidades de segurança.

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 – Sistema de Gestão de Incidentes de Segurança

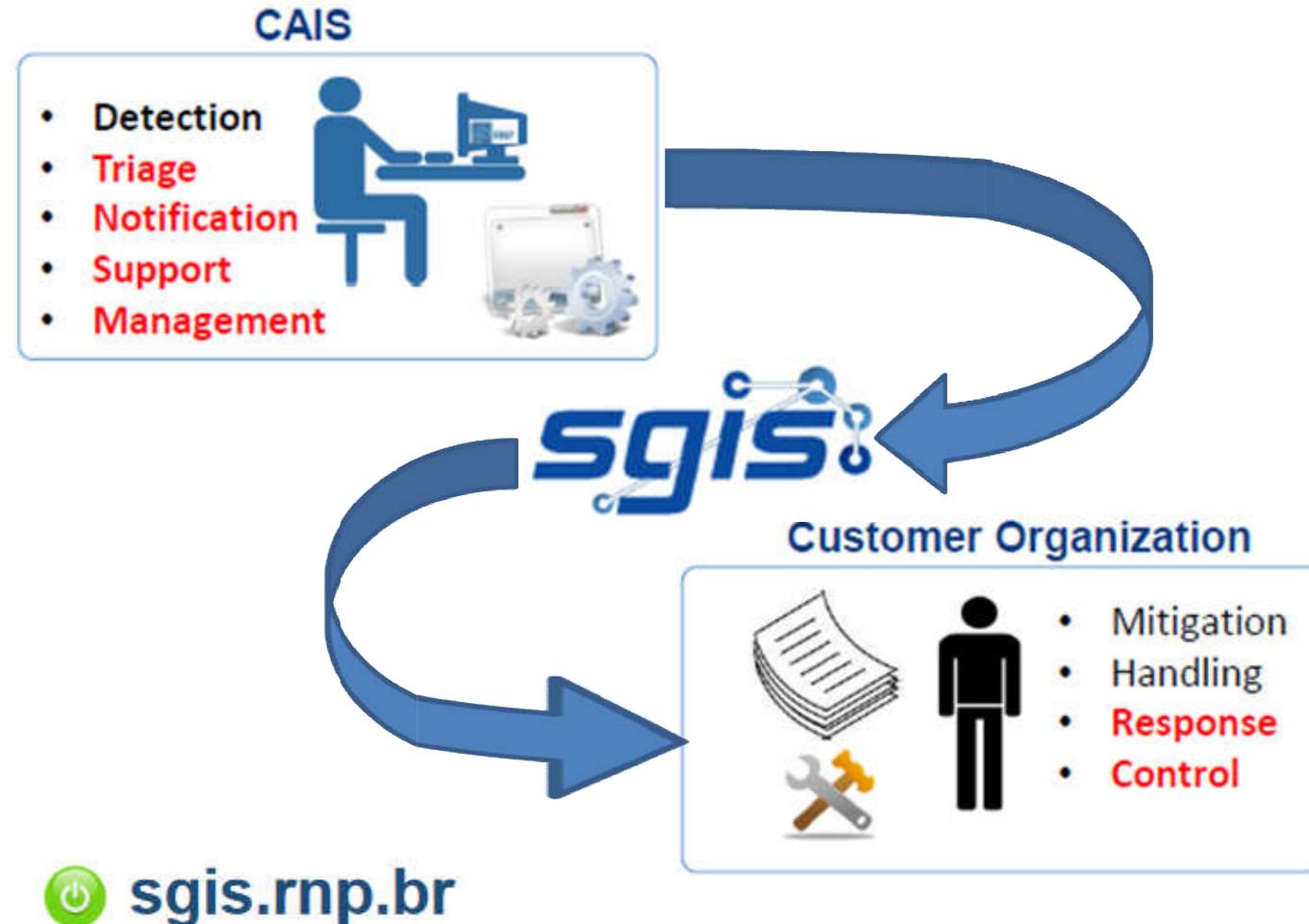
Sistema para gestão de incidentes e vulnerabilidades de segurança.

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.



Rede de sensores distribuídos

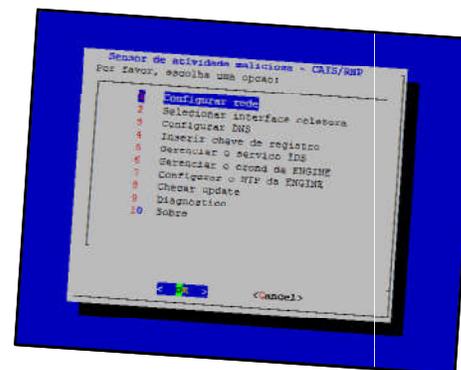


46 sensores ativos (27 PoPs + 19 clientes)

~ 37mil detecções/dia

Integrado ao SGIS

Escalabilidade e sustentabilidade



Seminários on-line

2018-1: Levando SegInfo para casa

2018-2: Usando wi-fi com segurança

2018-3: Configuração segura de DNS.

Webinar - Backup - O básico cada vez mais essencial



(Gravando) Seminários de Segurança da Informação - CAIS/RNP

PFSI
Instituto de Referência Nacional em Segurança da Informação

Seminários online

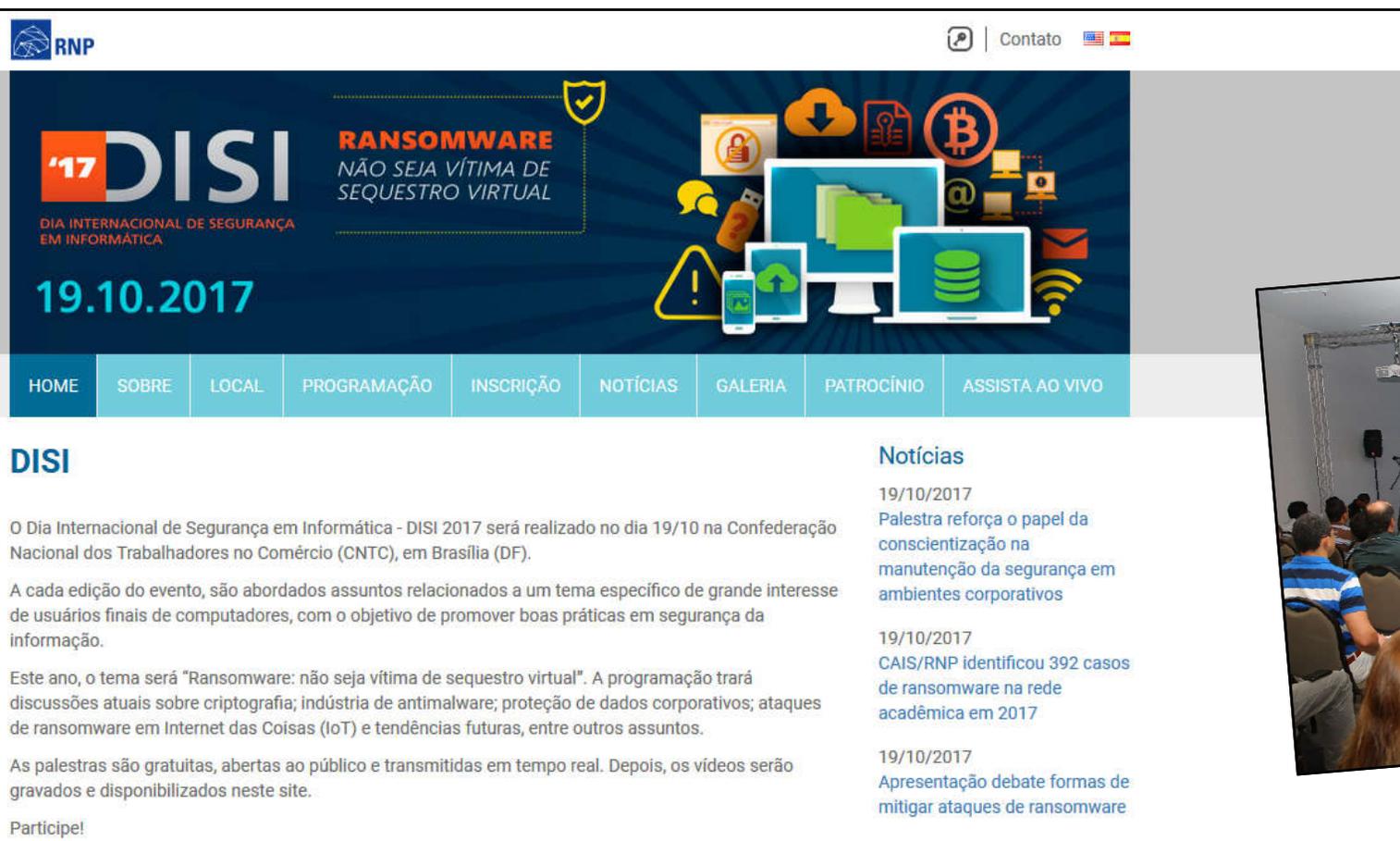
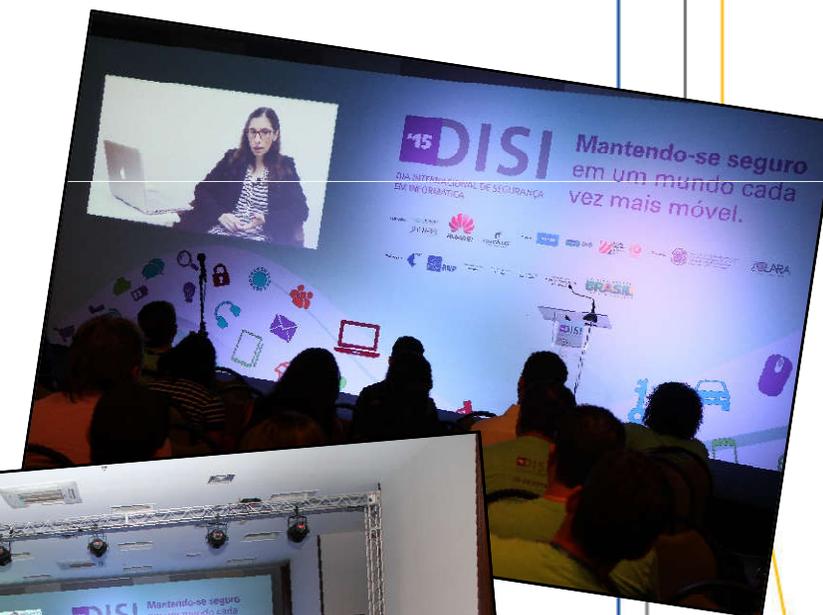
Qual o valor dos dados

- **Difícil mensurar**
- **Geralmente só é percebido da maneira mais difícil**
- **Dados:**
 - possuem valor emocional, financeiro, acadêmico, jurídico, etc.
 - levam tempo ou são impossíveis de serem refeitos.
- **Perda pode afetar:**
 - a continuidade dos negócios
 - + perda de clientes/pacientes, downtime, etc.
 - reputação/imagem da empresa
 - moral da equipe
- **Como protegê-los?**
 - impedir que ameaças cheguem até eles

vídeo @RNP

DISI – Dia Internacional de Segurança em Informática

DISI'18: 30 de agosto
Cibercrimes – “Fraudes virtuais, golpes reais”



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 trará 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

<http://disi.rnp.br>

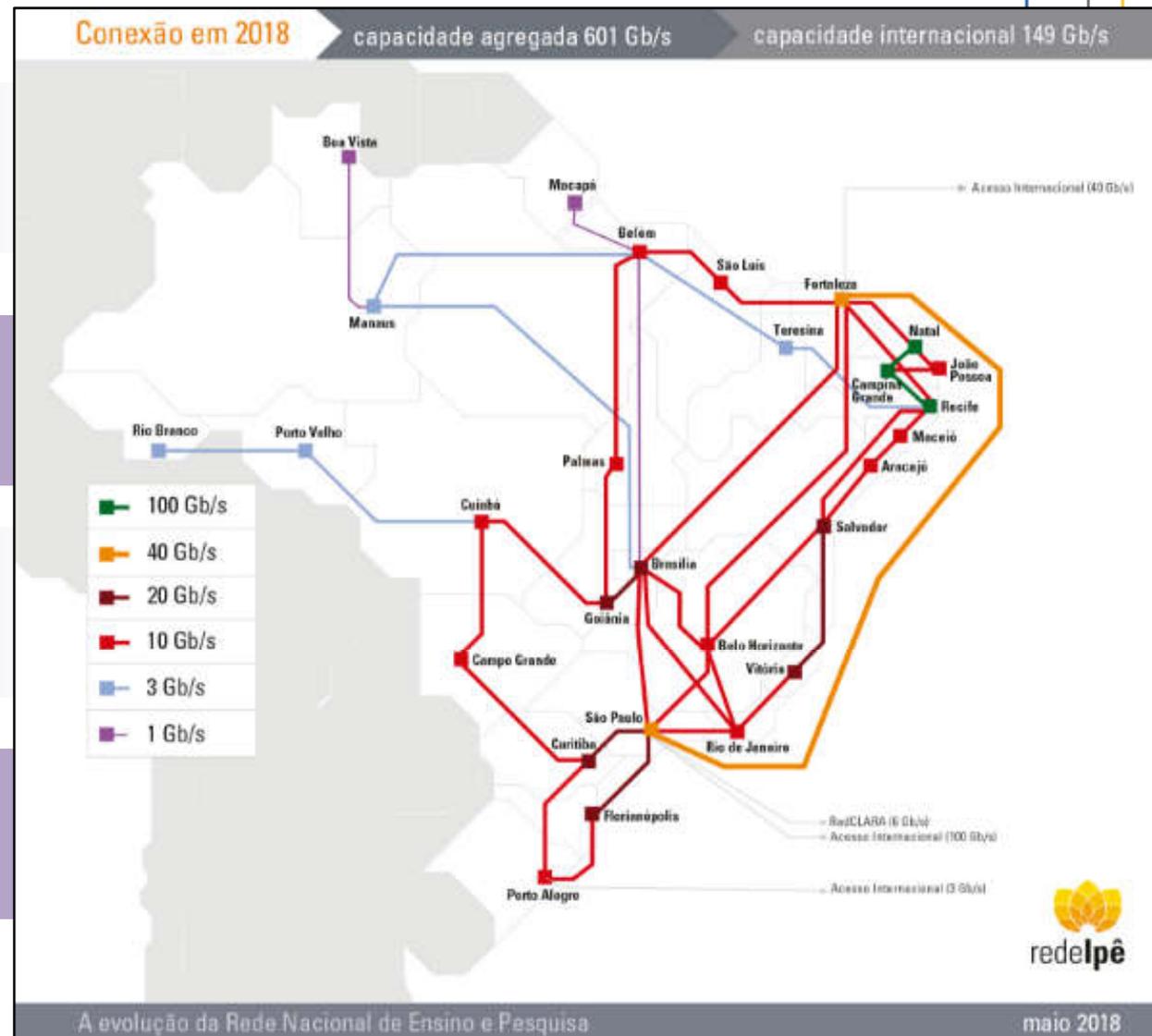
Panorama de SegInfo na rede acadêmica

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*.

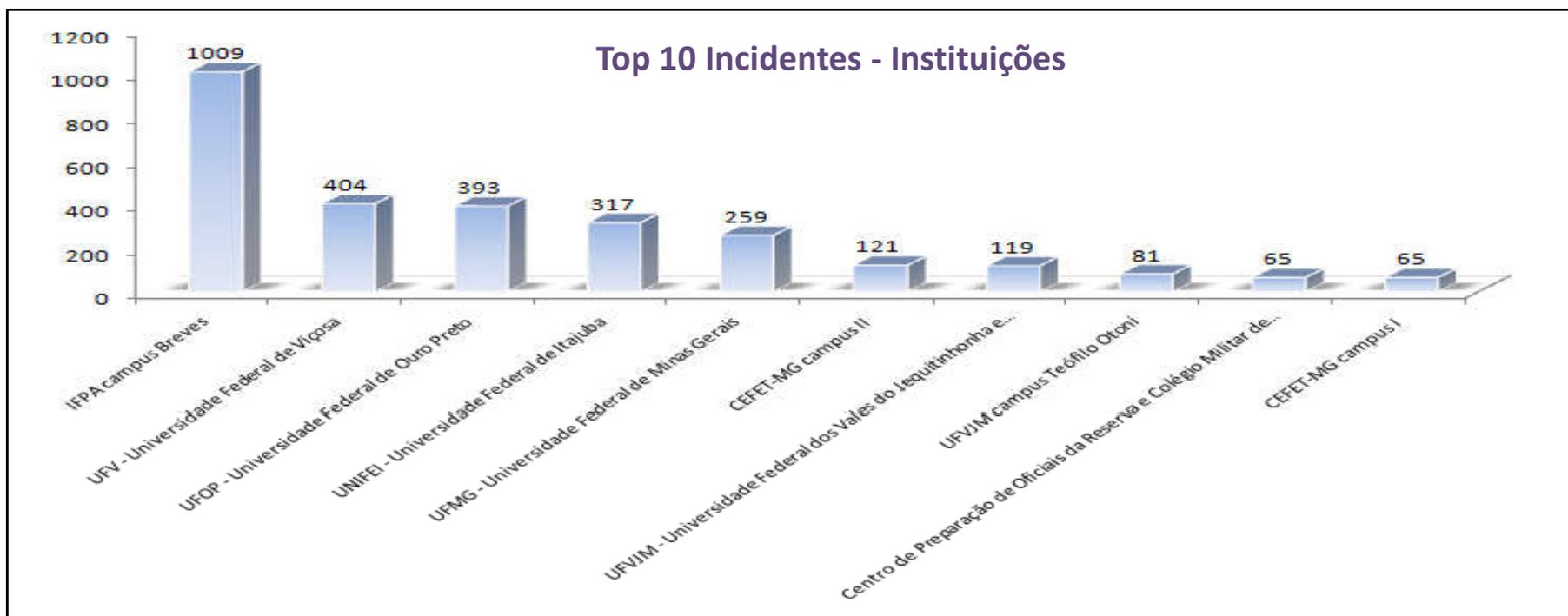
+37 mil (cerca de 6%) das notificações são relativas a incidentes de segurança.



*De maio/17 a maio/18

Panorama de SegInfo na rede acadêmica - MG

Mais de 21 mil notificações enviadas nos últimos 12 meses*



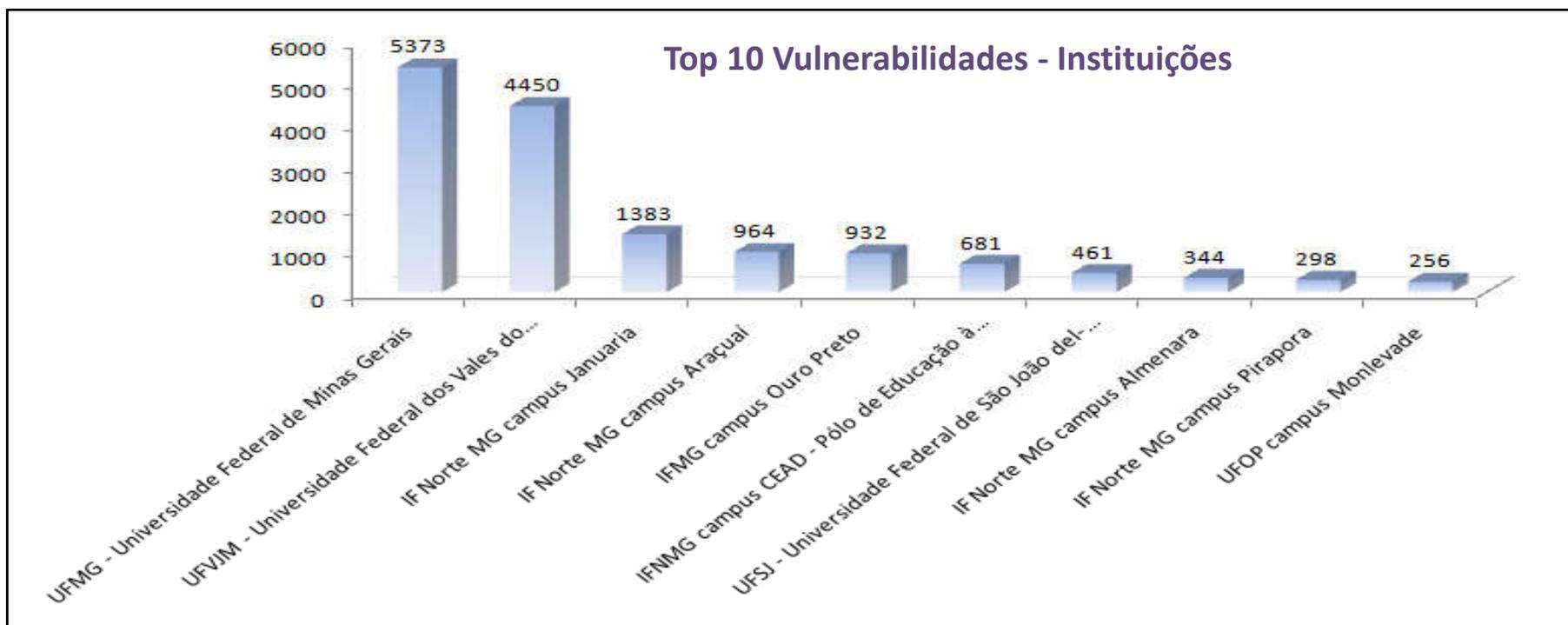
3.707 notificações de incidentes, apenas **573** foram fechadas.

Taxa de resposta a incidentes de **15.4%**

*De Jun/17 a Jun/18

Panorama de SegInfo na rede acadêmica - MG

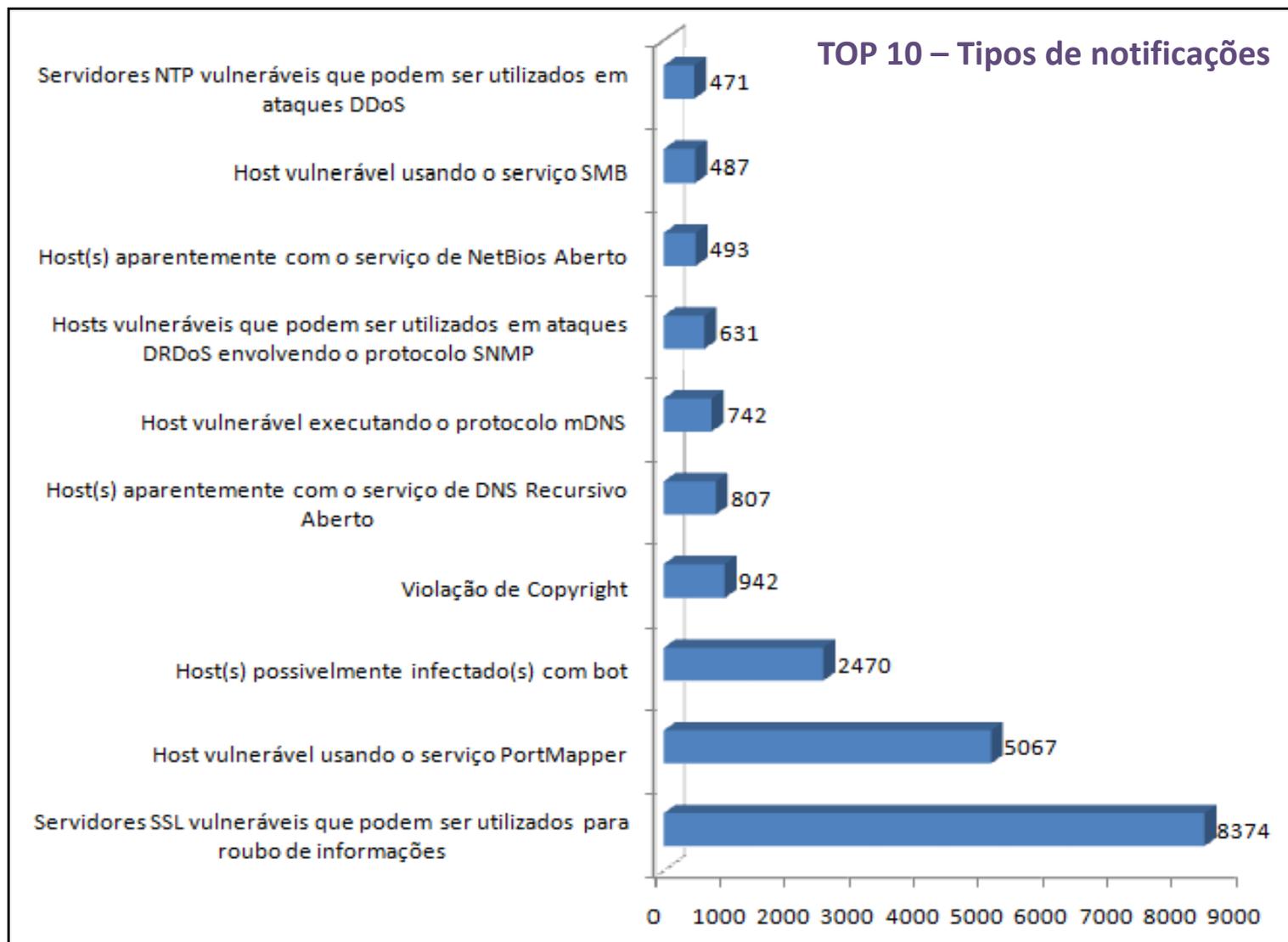
Mais de 21 mil notificações enviadas nos últimos 12 meses*



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

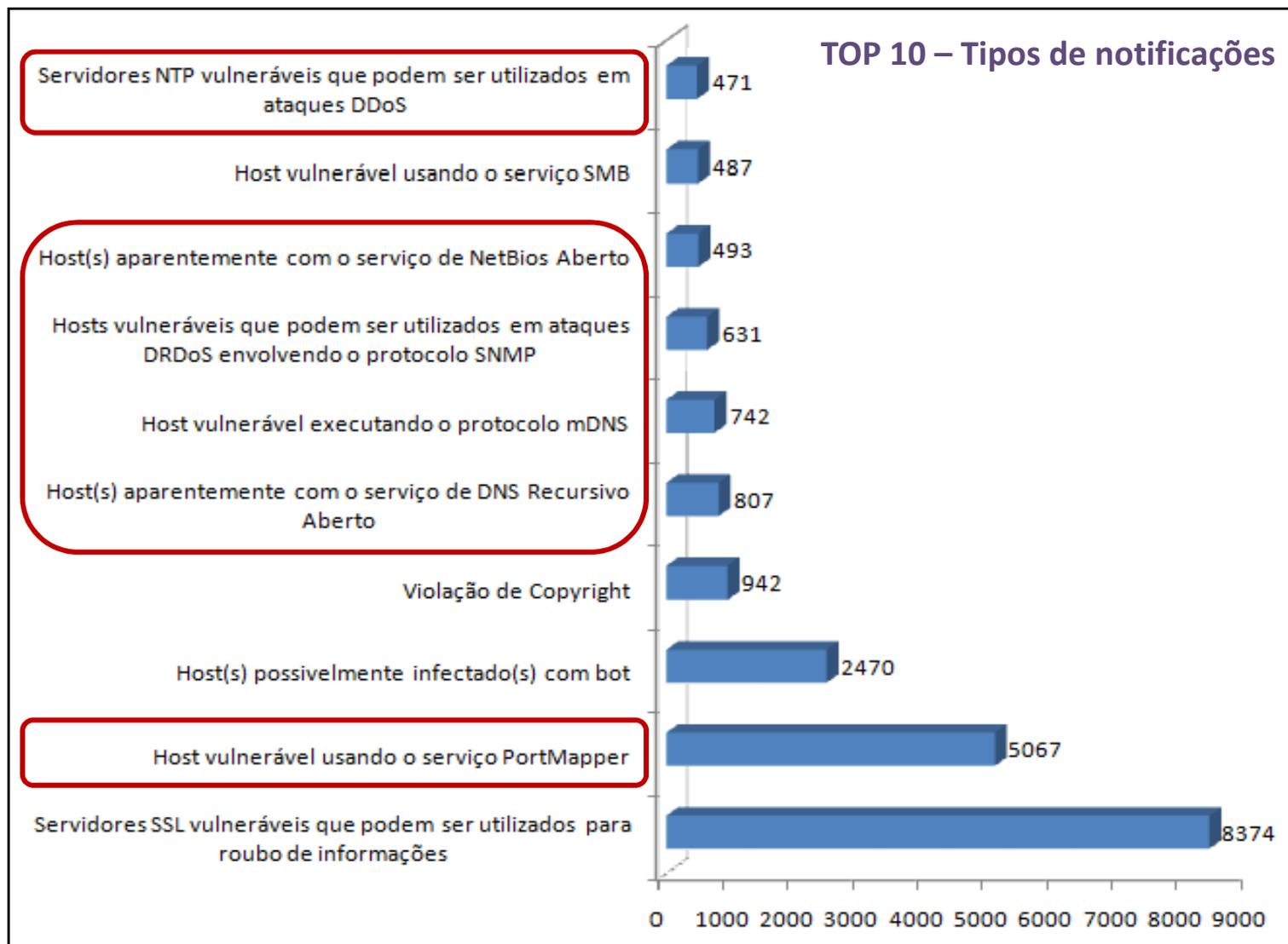
*De Jun/17 a Jun/18

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

- 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).



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	—

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.

Veja como o ataque funciona:

O atacante forja o endereço IP da vítima e envia pacotes a inúmeras máquinas comprometidas (conhecidas como "máquinas zumbi")

①



②

Como o protocolo UDP não valida os endereços IP de origem, é muito fácil forjar um endereço IP arbitrário. Quando muitos pacotes UDP têm o seu endereço IP de origem forjado para um único endereço, os serviços UDP respondem a essa vítima (máquina "zumbi"), criando um ataque de Negação de Serviço Distribuído (DDoS).

③

A vítima é inundada por todos os dados enviados a partir dos serviços UDP. Adicionalmente, onde antes os atacantes eram limitados pelo número de pacotes enviados diretamente para o alvo, para realizar um ataque de Negação de Serviço, agora um único pacote pode gerar dezenas ou centenas de vezes a largura de banda em sua resposta. Isto é chamado de ataque de amplificação e, quando combinado com um ataque Reflexivo de Negação de Serviço em grande escala, faz com que seja relativamente fácil realizar ataques DDoS.



Atacante



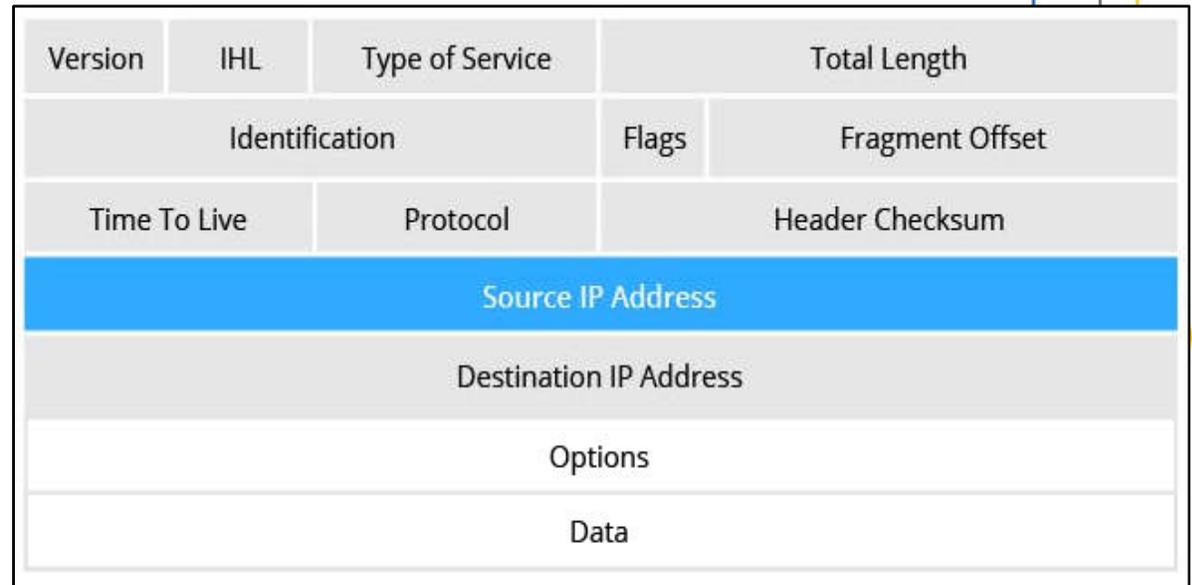
Alvo

Ataques de Negação de Serviço



IP Spoofing

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

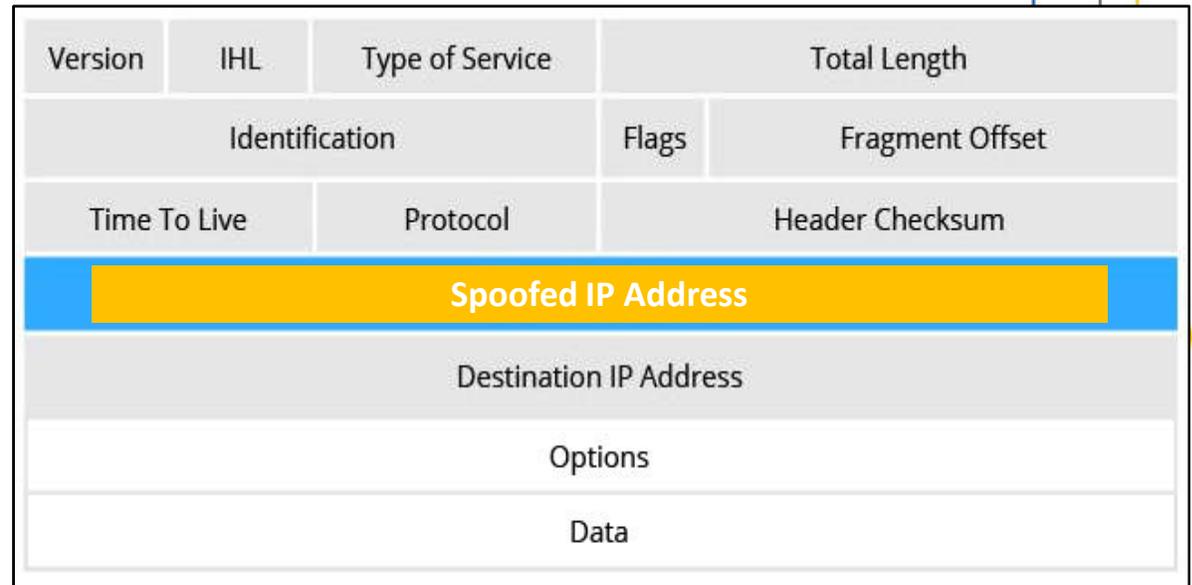


Ataques de Negação de Serviço



IP Spoofing

- Obter acesso concedido a um IP específico
- Mascaram 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

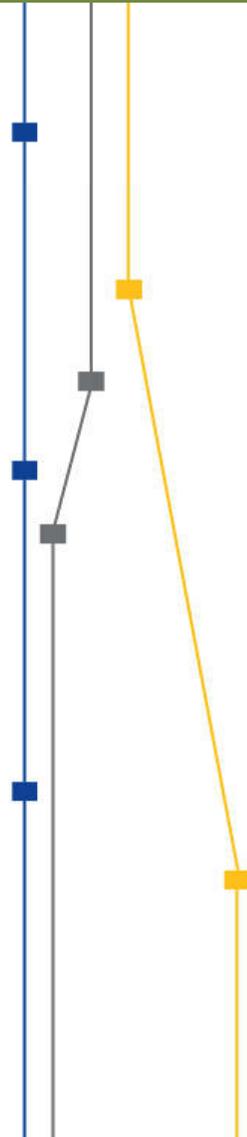


Detectando hosts vulneráveis - NMAP

```
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

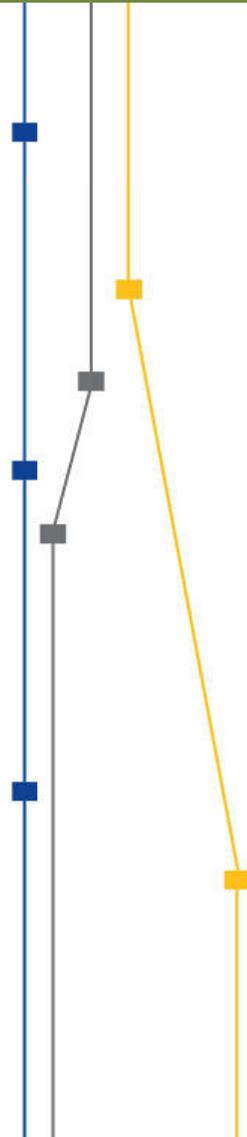


Detectando hosts vulneráveis - NMAP

```
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

PASTE BIN + 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
Master the Essential Ethical Hacking Tools & Tricks (68+ Hours!) to Learn in 2018
Normally: \$1528 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	8 440
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

PASTE BIN + 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 Learn in 2018
Normally: \$1528 Now: \$1

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

text 479.88 KB

1.	99.8	.253 2909
2.	99.6	151 2996
3.	99.5	..190 2989
4.	99.3	.154 2913
5.	99.3	..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	9.179 2885

Ataques de Negação de Serviço



Casos interessantes...

Chargen Amplification (UDP/111)

DETAILS Period: Units: View:

Severity Level:	Max Severity Percent: <input type="button" value="i"/>	Max Impact of Alert Traffic: <input type="button" value="i"/>	Direction:	Misuse Types:	Managed Object:	Target:	View Raw Flows »
High	270.0% of 10 Kpps	252.4 Mbps/27.0 Kpps	Incoming	IP Fragmentation, chargen Amplification	PoP-MG	200.238.249.82	
Top Misuse Type: IP Fragmentation		at jmx_mia2					

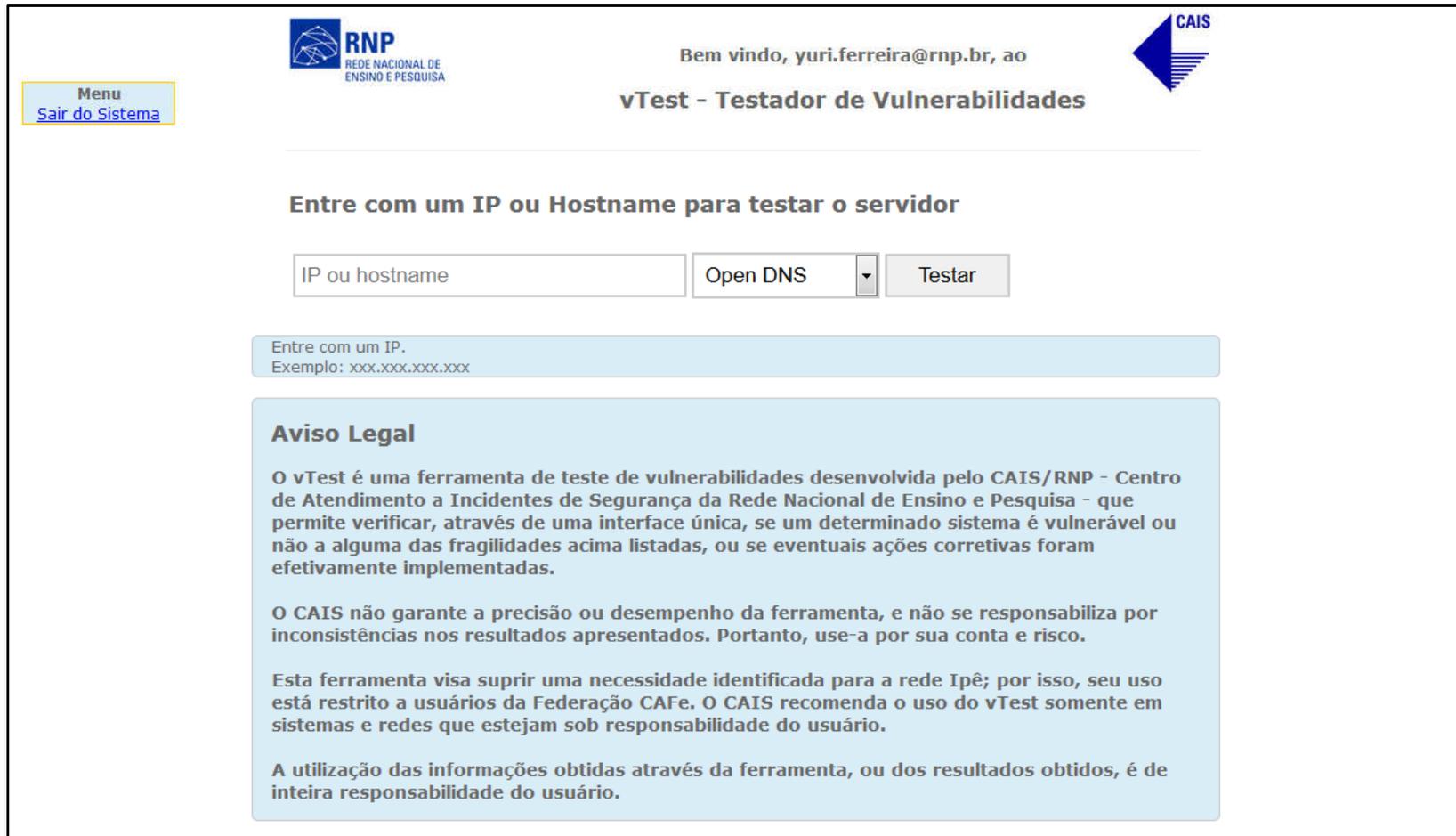
CLDAP Amplification (UDP/389)

DETAILS Period: Units: View:

Router (Severity):

Severity Level:	Max Severity Percent: <input type="button" value="i"/>	Max Impact of Alert Traffic: <input type="button" value="i"/>	Direction:	Misuse Types:	Managed Object:	Target:	View Raw Flows »
Medium	321.0% of 10 Kpps	239.6 Mbps/32.1 Kpps	Incoming	IP Fragmentation, CLDAP Amplification	UFMG	150.164.129.18	
Top Misuse Type: IP Fragmentation		at jmx_mia2					

Testador de vulnerabilidades



The screenshot shows the vTest web interface. At the top left, there is a 'Menu' button with a sub-link 'Sair do Sistema'. The RNP logo is in the top left, and the CAIS logo is in the top right. The user is logged in as 'yuri.ferreira@rnp.br'. The main heading is 'vTest - Testador de Vulnerabilidades'. Below this, there is a form with a text input for 'IP ou hostname', a dropdown menu for 'Open DNS', and a 'Testar' button. A light blue box provides an example: 'Entre com um IP. Exemplo: xxx.xxx.xxx.xxx'. A larger light blue box contains the 'Aviso Legal' (Legal Notice), which states that the tool is developed by CAIS/RNP and is used to verify system vulnerabilities. It also includes a disclaimer that CAIS does not guarantee accuracy and that the user is responsible for their actions. The notice concludes by stating that the tool's use is restricted to users of the CAFE Federation and that the user is responsible for any information obtained.

Ataques de Negação de Serviço

Como se proteger?



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)



Como se proteger?

NTP Hardening

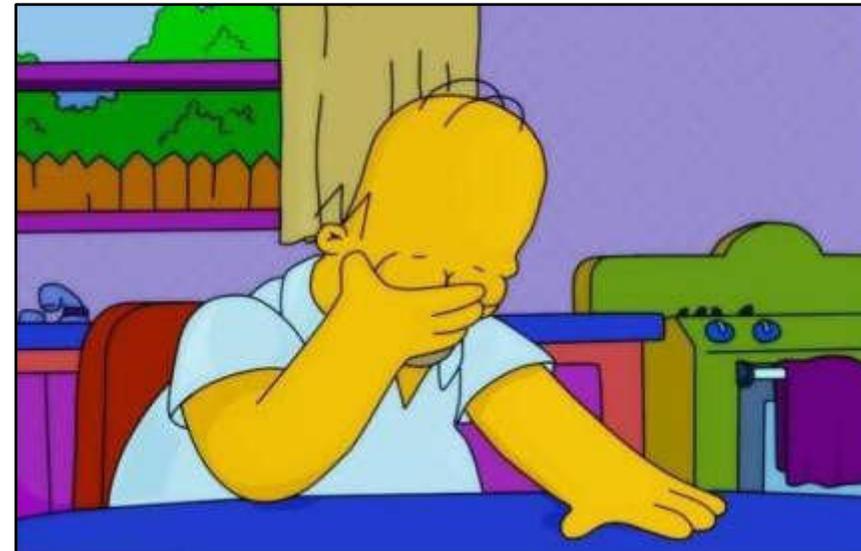
- ACL's
- "restrict default kod notrap nomodify nopeer noquery"
- "disable monitor"
- Utilizar "OpenNTPd"



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...



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)

Você sabe o que é IP Spoofing?

Veja como a técnica pode ser explorada em ataques cibernéticos e descubra como se proteger

1 Comunicação padrão
A comunicação pela internet é realizada pela troca de pacotes de dados, com base nas informações do endereço IP de origem e de destino. Cada pacote enviado precisa ter em sua cabeçalho, entre outras informações, o endereço do seu destino e também o endereço de origem, para que a outra parte possa respondê-lo.

2 Técnica do spoofing
Quando um atacante quer se passar por outro host, ele manipula o campo de endereço de origem do pacote. Isso é possível porque os roteadores de rede geralmente não estão configurados para validar se o endereço de origem do pacote está correto. A técnica que explora esse tipo de comportamento é chamada de IP Spoofing.

3 Exemplos de ataques
Um exemplo é o Ataque de Negação de Serviço Distribuído (DDoS, em inglês), em que o atacante forja o endereço IP de origem e envia pequenas requisições a servidores vulneráveis na internet, que respondem com um volume de dados amplificado e direcionado à vítima, provocando sobrecarga e até queda do serviço.

4 Recomendações
Por conta disso, tornou-se fundamental implementar controles para evitar o IP Spoofing. Diversas normas têm sido divulgadas para realizar a filtragem e a validação dos pacotes que chegam às redes, tais como o BCP38 e o DCP84.

AQUI TEM PROTEÇÃO
RNP

RNP
REDES COMEPES
PoPs
ISP
CLIENTES DE IX

AntiSpoofing

Campanha Técnica 2018 Antispoofing



Introdução	pág 2
Recomendações	pág 6
Guias técnicos	pág 7

Especificamente no caso do IP Spoofing, um atacante manipula intencionalmente as informações do campo "origem" no cabeçalho do protocolo IP. Dessa forma, o pacote chega ao destino com a informação do endereço IP de origem forjado, o que permite que o spoofing ocorra.

Cabeçalho do protocolo IPv4.

D finge ser A

Pacote falso aceito

3

AntiSpoofing

Campanha Técnica 2018 Antispoofing



APOIO RNP



<http://url.rnp.br?campanhaantispoofing>

Campanha Técnica 2018



AntiSpoofing

Campanha Técnica 2018 Antispoofing



Campanha Técnica 2018 Antispoofing



https://www.rnp.br/servicos/seguranca/educacao-e-conscientizacao-seguranca

RNP REDE NACIONAL DE ENSINO E PESQUISA

HOME INSTITUCIONAL SERVIÇOS SOLUÇÕES PESQUISA E DESENVOLVIMENTO

Início > Serviços > Segurança > Educação e Conscientização em Segurança

Educação e Conscientização em Segurança

A RNP promove, através do CAIS, ações de disseminação da cultura de segurança no ambiente acadêmico, como eventos, materiais educativos e cursos na área de segurança da informação.

Eventos

- Mês de Segurança
- Dia Internacional de Segurança em Informática (DISI)
- EnCSIRTs

Alertas

O CAIS notifica sobre as vulnerabilidades e falhas de maior relevância. Também apresenta um resumo das estatísticas do tratamento de incidentes, alertas e notícias sobre segurança quadrimestrais.

Assine a [lista de alertas](#) e receba antecipadamente, por e-mail, as mais recentes notificações sobre segurança.

- 2018
- 2017
- 2016
- 2015
- 2014

Materiais educativos

- Proteção contra o IP Spoofing

Cartilha

Cartaz

Anexo A - Tutorial Juniper - Clientes - Provedores

Anexo B - Tutorial Cisco - Clientes - Provedores

- Compras seguras na internet
- Segurança em redes sociais
- Privacidade de dados

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...



Considerações finais





RNP

Atendimento Integrado de Serviços



sd@rnp.br



0800 722 0216



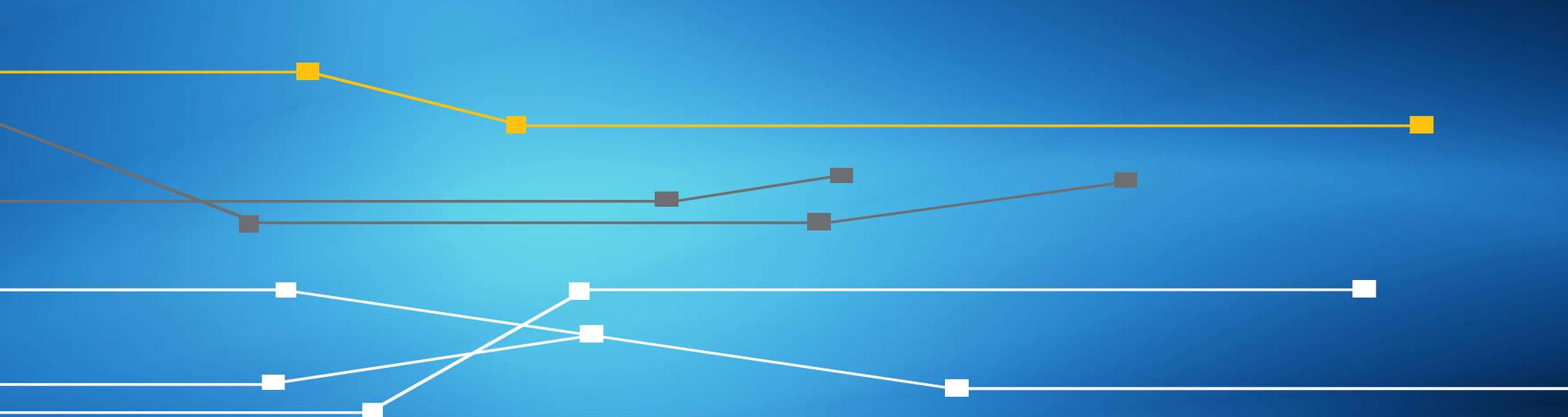
(61) 9 9960 5971



1916*800



cais@cais.rnp.br



Obrigado!

André R. LANDIM
CAIS/RNP
andre.landim@rnp.br



MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
**CIÊNCIA, TECNOLOGIA,
INovações E COMUNICAÇÕES**

