

Retrospectiva na área de segurança

Rede Nacional de Ensino e Pesquisa - RNP
Centro de Atendimento a Incidentes de Segurança - CAIS
Novembro de 2003



RNP/PAL/0198
© 2003 – RNP



Retrospectiva na área de segurança



Sumário

- Apresentação
- Retrospectiva 2003
- Tipos de ataques mais comuns no ano 2003
- Panorama atual na área de segurança
- Expectativas para o ano 2004

Retrospectiva na área de segurança



Janeiro de 2003

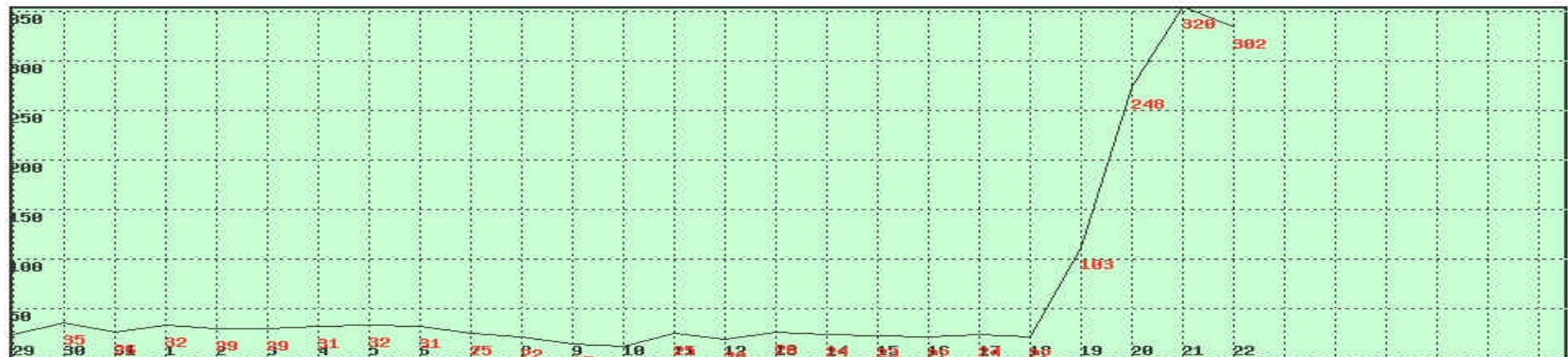
- Spam se consolida como praga

<http://www.terra.com.br/informatica/2002/12/31/008.htm>

- Propagação do W32/SQLSlammer

<http://www.rnp.br/cais/alertas/2003/CA200304.html>

- 376 bytes x 1.000.00 de máquinas



Retrospectiva na área de segurança



Fevereiro de 2003

- ☞ Museu do Spam encerra atividades!
- ☞ Vítima de spam é suspeita de matar embaixador da Nigéria
<http://www.terra.com.br/informatica/2003/02/20/015.htm>
- ☞ Preso hacker que clonava sites de bancos
<http://www1.folha.uol.com.br/folha/informatica/ult124u12342.shtml>
- ☞ Preso no RJ hacker que clonou cartões
<http://infoexame.abril.uol.com.br/aberto/infonews/022003/21022003-10.shl>
- ☞ Marcha Virtual contra a guerra agita os EUA
<http://www.terra.com.br/informatica/2003/02/27/004.htm>

Retrospectiva na área de segurança



Março de 2003

- UOL barra 7 milhões de spams por dia

<http://noticias.uol.com.br/mundodigital/ultimas/2003/03/11/ult8u613.jhtm>

- E-mail pede atualização de dados em site falso do Banco do Brasil

<http://www.terra.com.br/informatica/2003/03/03/000.htm>

- Hackers tentam enganar correntistas do Itaú

http://www.infoworld.com/article/03/03/19/HNwinpatch_1.html

- Boato na internet promete cesta de produtos da Nestlé

<http://www1.folha.uol.com.br/folha/informatica/ult124u12577.shtml>

Retrospectiva na área de segurança



Março de 2003

- ⌘ Remote Buffer Overflow in Sendmail

<http://www.rnp.br/cais/alertas/2003/CA200307.html>

- ⌘ Nova versão do worm CodeRed **F**

<http://www.rnp.br/cais/alertas/2003/CAIS-ALR-11032003.html>

- ⌘ Remote Buffer Overflow in Sendmail - Nova vulnerabilidade

<http://www.rnp.br/cais/alertas/2003/ca200312.html>

- ⌘ CAIS Resumo RES-012003

<http://www.rnp.br/cais/alertas/2003/RES-012003.html>

Retrospectiva na área de segurança



Março de 2003

Exemplo prático de 2003, CodeRed.F

Date: Tue, 11 Mar 2003 00:00:21 -0300 (BRT)

From: [Redacted]

To: [Redacted]

Subject: ios-portas diaria Tue Mar 11 00:00:00 BRT 2003

445 792

80 534

524 162

139 24

1080 20

3128 12



Retrospectiva na área de segurança



Março de 2003

Exemplo prático de 2003, CodeRed.F

Date: Wed, 12 Mar 2003 00:02:34 -0300 (BRT)

From: [Redacted]

To: [Redacted]

Subject: ins-portas diaria Wed Mar 12 00:00:00 BRT 2003

80 4683

445 244

524 150

1080 82

139 79

3128 41

8080 37



Retrospectiva na área de segurança



Março de 2003

Exemplo prático de 2003, CodeRed.F

Date: Thu, 13 Mar 2003 00:03:09 -0300 (BRT)

From: [redacted]

To: [redacted]

Subject: [top-10] ins-portas diaria Thu Mar 13 00:00:00 BRT 2003

80 7007

139 90

1080 16

25 14

21 12

22 6

Retrospectiva na área de segurança



Abril de 2003

☞ Alerta do CAIS ALR-02042003

Fraudes em Internet Banking

[CAIS, 02.04.2003]

<http://www.rnp.br/cais/alertas/2003/cais-alr-02042003.html>

Retrospectiva na área de segurança



Maio de 2003

Volume de spam ameaça futuro do e-mail

<http://www1.folha.uol.com.br/folha/informatica/ult124u12845.shtml>

É quinta-feira? Então, é dia de spam!

<http://infoexame.abril.uol.com.br/aberto/infonews/052003/07052003-6.shl>

Programas roubam senhas de teclados virtuais

<http://informatica.terra.com.br/interna/0,5862,OI106970-EI559,00.html>

Falso site da Embratel tem arquivo suspeito

<http://infoexame.abril.uol.com.br/aberto/infonews/052003/15052003-10.shl>

E-mail sobre Big Brother Brasil 4 é falso

<http://informatica.terra.com.br/interna/0,5862,OI109403-EI553,00.html>

Retrospectiva na área de segurança



Maio de 2003

That's right: Trinity uses a 'sploit.

```
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned
# sshnuke 10.2.2.2 -rootpu-"210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "210N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:

RRF-CONTROL> disable grid nodes 21 - 48
Warning: Disabling nodes 21-48 will disconnect sector 1
```



Retrospectiva na área de segurança



Junho de 2003

- ☞ Servidores Linux viram alvo de hackers

<http://informatica.terra.com.br/interna/0,5862,OI110958-EI559,00.html>

- ☞ Invasões a sistemas Linux batem recorde em maio

<http://www1.folha.uol.com.br/folha/informatica/ult124u13123.shtml>

- ☞ Spam custará US\$ 20,5 bilhões às empresas este ano, prevê estudo

<http://www1.folha.uol.com.br/folha/informatica/ult124u13138.shtml>

- ☞ Site do Banco do Brasil é clonado

<http://infoexame.abril.uol.com.br/aberto/infonews/062003/13062003-13.shl>

Retrospectiva na área de segurança



Junho de 2003

CAIS Resumo RES-022003

Alertas, vulnerabilidades e incidentes de segurança

[CAIS, 11.06.2003]

<http://www.rnp.br/cais/alertas/2003/RES-022003.html>

Alerta do CAIS ALR-27062003b

Proliferação de golpes por e-mail

[CAIS, 27.06.2003]

<http://www.rnp.br/cais/alertas/2003/cais-alr-27062003b.html>

Retrospectiva na área de segurança



Julho de 2003

- Ataques programados para 06/07/2003

<http://www.rnp.br/cais/alertas/2003/cais-alr-03072003.html>

- Vulnerabilidade no RPC da Microsoft (823980)

<http://www.rnp.br/cais/alertas/2003/MS03-026.html>



Retrospectiva na área de segurança



Julho de 2003

- ⌘ Até setembro, pelo menos 50% do tráfego de e-mail será spam

<http://www1.folha.uol.com.br/folha/informatica/ult124u13310.shtml>

- ⌘ Coca-Cola usa site para rebater boato de veneno no Kwat

<http://www1.folha.uol.com.br/folha/dinheiro/ult91u69709.shtml>

- ⌘ Número de vírus cresceu 17,5%, diz Sophos

<http://infoexame.abril.uol.com.br/aberto/infonews/072003/08072003-10.shl>

- ⌘ Estudo indica as dez linhas de assunto mais usadas em spam

<http://www1.folha.uol.com.br/folha/informatica/ult124u13377.shtml>

- ⌘ Concurso de hackers tem vitórias modestas

<http://informatica.terra.com.br/interna/0,5862,0I118873-EI559,00.html>

Retrospectiva na área de segurança



Julho de 2003

- ✦ Spammers criam temporada de e-mails falsos

<http://infoexame.abril.uol.com.br/aberto/infonews/072003/16072003-4.shl>

- ✦ Big Brother Brasil 4

- ✦ Conta Fácil 21

- ✦ Americanas.com

- ✦ Banco do Brasil, Itaú, Editora Abril e jornal O Estado de S. Paulo

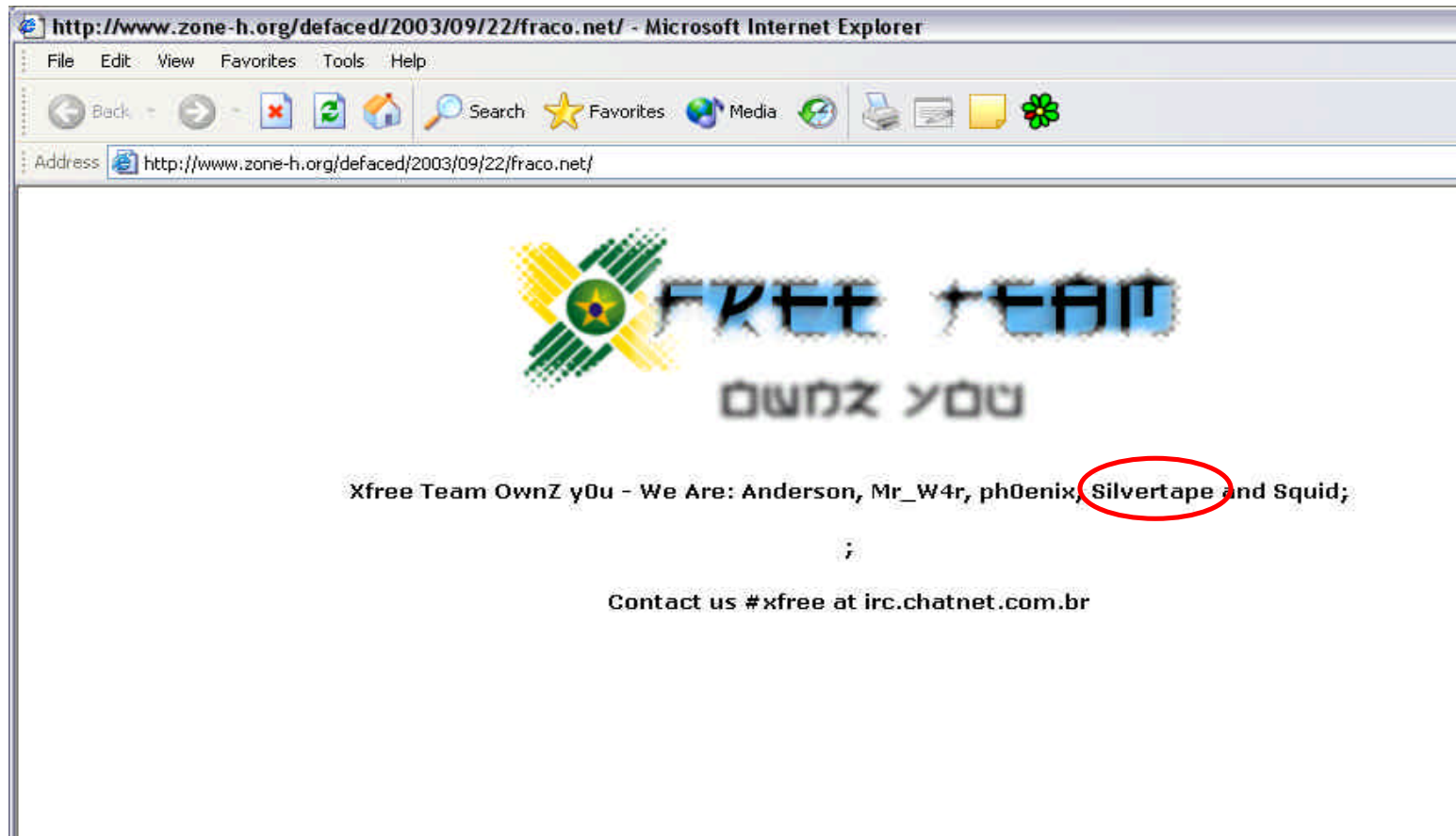
- ✦ Submarino.com

- ✦ Criança Esperança, Show do Milhão

Retrospectiva na área de segurança



Agosto de 2003



Retrospectiva na área de segurança



Agosto de 2003

'Xfree Team'

Integrantes: Anderson, Bobx, boy, ph0enix, **Silvertape**, Squid

<http://www.audioslave.com.br/xfree.gif>

person: Tiago S. Severo

e-mail: **silvertape**@USA.COM

address: Rua **Silvertape**, 214,

address: 99700-000 - Erechim - RS

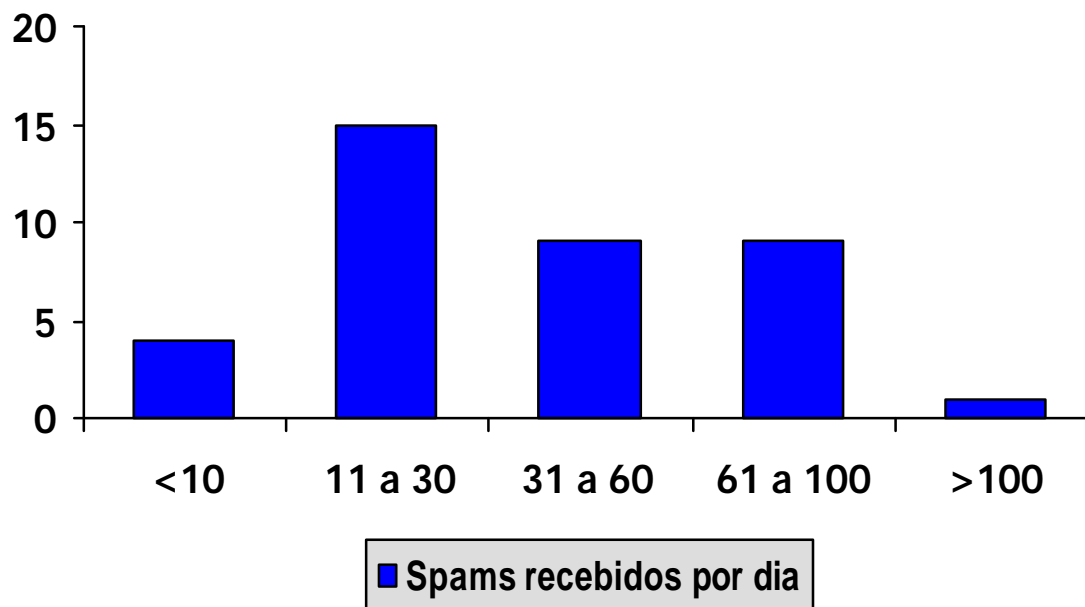
phone: (54) 99823759 []

Retrospectiva na área de segurança



Agosto de 2003

Resultados da Segunda Pesquisa de Spam na RNP



Retrospectiva na área de segurança



Agosto de 2003

Alerta do CAIS ALR-11082003

Propagação do Worm Blaster (DCOM RPC)

[CAIS, 11.08.2003]

<http://www.rnp.br/cais/alertas/2003/cais-alr-11082003.html>

Comprometimento de FTP.GNU.ORG

<http://www.rnp.br/cais/alertas/2003/FSF130803.html>

Retrospectiva na área de segurança



Agosto de 2003

- ⌘ Ataques hackers em 2003 devem crescer 85% em relação a 2002

<http://www1.folha.uol.com.br/folha/informatica/ult124u13561.shtml>

- ⌘ Bancos costumam ser vítimas de sites clonados

<http://noticias.uol.com.br/mundodigital/proteja/ult262u83.jhtm>

- ⌘ Vírus Blaster explora falha recente do Windows

<http://informatica.terra.com.br/interna/0,5862,OI131137-EI559,00.html>

- ⌘ Spread of 'Sobig.F' Virus Is Fastest Ever

<http://www.siliconvalley.com/mld/siliconvalley/news/6580139.htm?template=contentModules/printstory.jsp>

Retrospectiva na área de segurança



Agosto de 2003

Alerta do CAIS ALR-19082003

Propagação do vírus W32.Sobig.F@mm

<http://www.rnp.br/cais/alertas/2003/cais-alr-19082003.html>

Vulnerabilidade remota no Sendmail

<http://www.rnp.br/cais/alertas/2003/FreeBSD260803.html>

Retrospectiva na área de segurança



Setembro de 2003

MSBlaster

Jeffrey Lee Parson, aka, teekid

```
C:\>rename msbaster.exe teekid.exe
```

```
C:\>teekid
```

```
C:\>
```

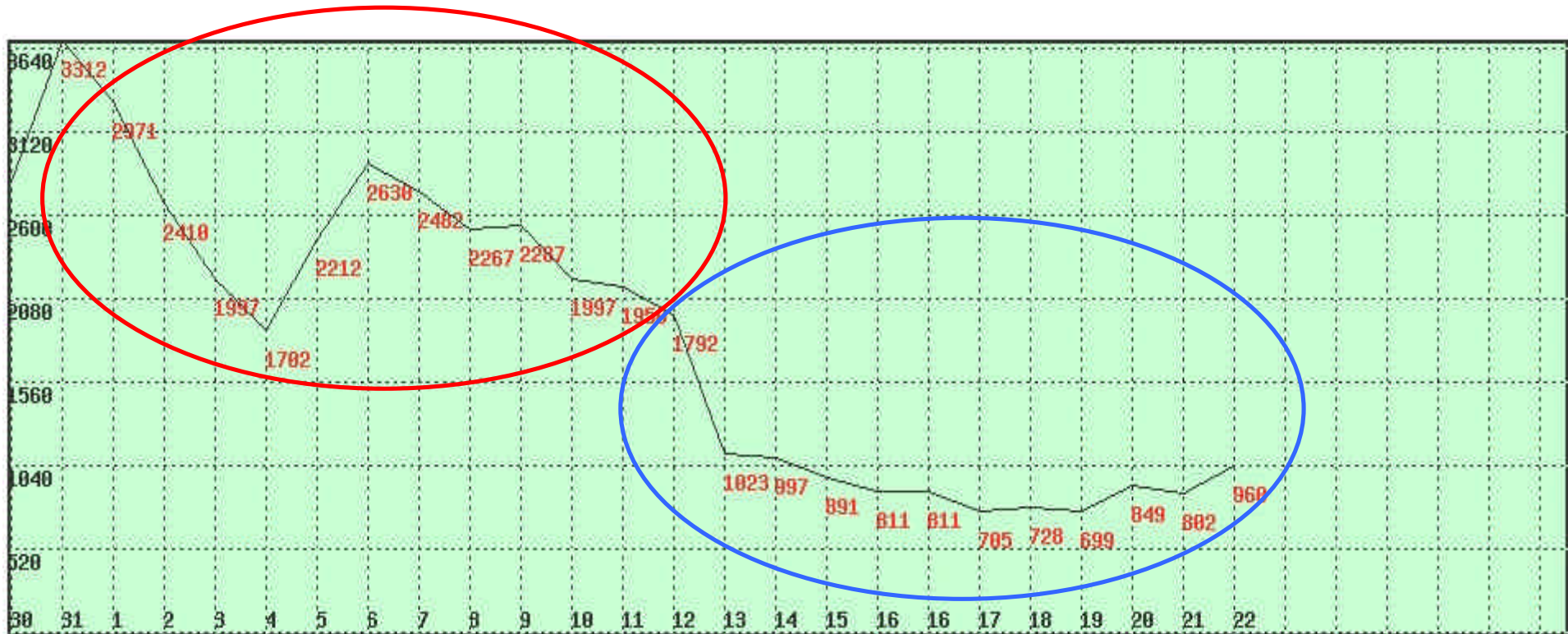


Retrospectiva na área de segurança



Setembro de 2003

Dois anos depois, vírus Nimda ainda ataca.



Retrospectiva na área de segurança



Setembro de 2003

- ✦ Vulnerabilidade remota no OpenSSH
- ✦ Novidades sobre a vulnerabilidade do OpenSSH
- ✦ Falso exploit para a vulnerabilidade do OpenSSH



- ✦ Buffer Overflow in Sendmail

Retrospectiva na área de segurança



Setembro de 2003

- ⌘ Vulnerabilidade no Microsoft NetBIOS (824105)
- ⌘ Vulnerabilidade no Microsoft Word (827653)
- ⌘ Vulnerabilidade no Microsoft WordPerfect Converter (827103)
- ⌘ Vulnerabilidade no Microsoft Visual Basic for Applications (822715)
- ⌘ Vulnerabilidade no Microsoft Access (827104)



Retrospectiva na área de segurança



Outubro de 2003

✍ Estudo analisa ataques via Internet em 180 países

<http://informatica.terra.com.br/interna/0,,OI151666-EI559,00.html>

15º lugar no ranking

✍ Microsoft IIS é o software mais vulnerável, segundo lista do Sans

<http://www1.folha.uol.com.br/folha/informatica/ult124u14092.shtml>

✍ Romania Emerges As Nexus of Cybercrime

<http://www.bayarea.com/mld/mercurynews/business/technology/7053236.htm>

Retrospectiva na área de segurança



Outubro de 2003

🔗 **Microsoft lança 7 boletins de segurança de uma vez**

[http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1066341186,75760,](http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1066341186,75760)

MS03-041: (823182)

MS03-042: (826232)

MS03-043: (828035)

MS03-044: (825119)

MS03-045: (824141)

MS03-046: (829436)

MS03-047: (828489)

Retrospectiva na área de segurança



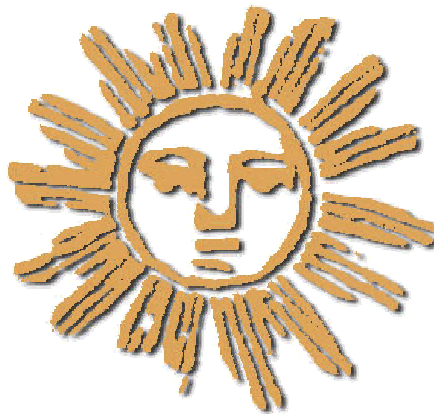
Outubro de 2003

✍ Início do Horário de Verão 2003/2004

<http://www.rnp.br/cais/alertas/2003/cais-alr-17102003.html>

<http://www.rnp.br/cais/alertas/2003/cais-alr-06102003a.html>

<http://www.rnp.br/cais/alertas/2003/cais-alr-06102003.html>



Retrospectiva na área de segurança



Novembro de 2003

✍ s3r14l k1ll3r preso no Japão

<http://informatica.terra.com.br/interna/0,,OI203214-EI559,00.html>

Retrospectiva na área de segurança



Premio



Date: [REDACTED]
From: [REDACTED]
To: Cais <cais@rnp.br>
Subject: Notificação de Incidentes de Segurança: [REDACTED]
Notificação de Incidentes de Segurança através de formulário Web
Enviado a partir do endereço [REDACTED]

Nome [REDACTED]
Email [REDACTED].br
Telefone [REDACTED]

Retrospectiva na área de segurança



Premio

Empresa



Contato técnico

sim

Vitima



Atacante

127.0.0.1

Tipo de ataque

Outros

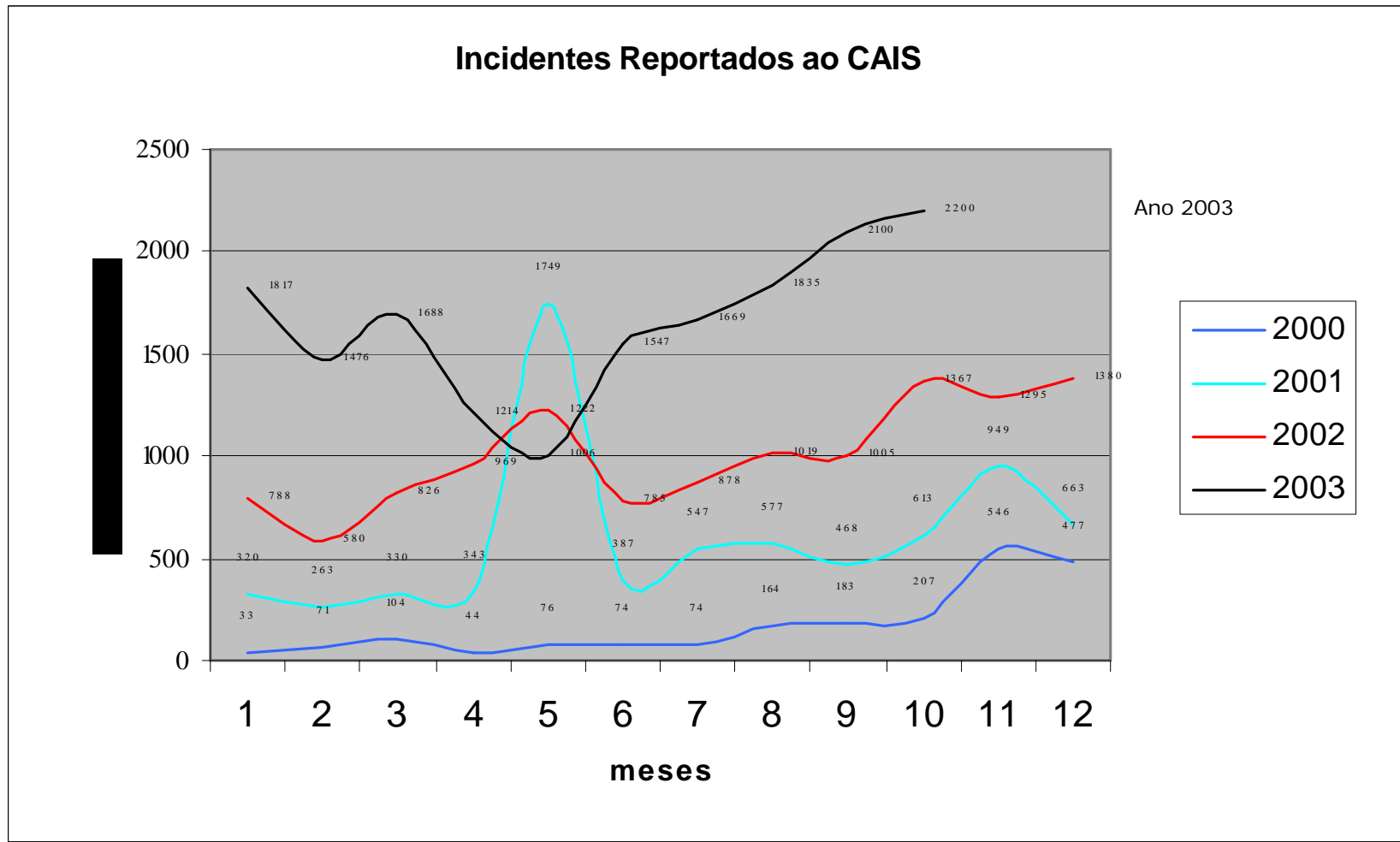
Outras informações



Retrospectiva na área de segurança



Estatísticas 2003



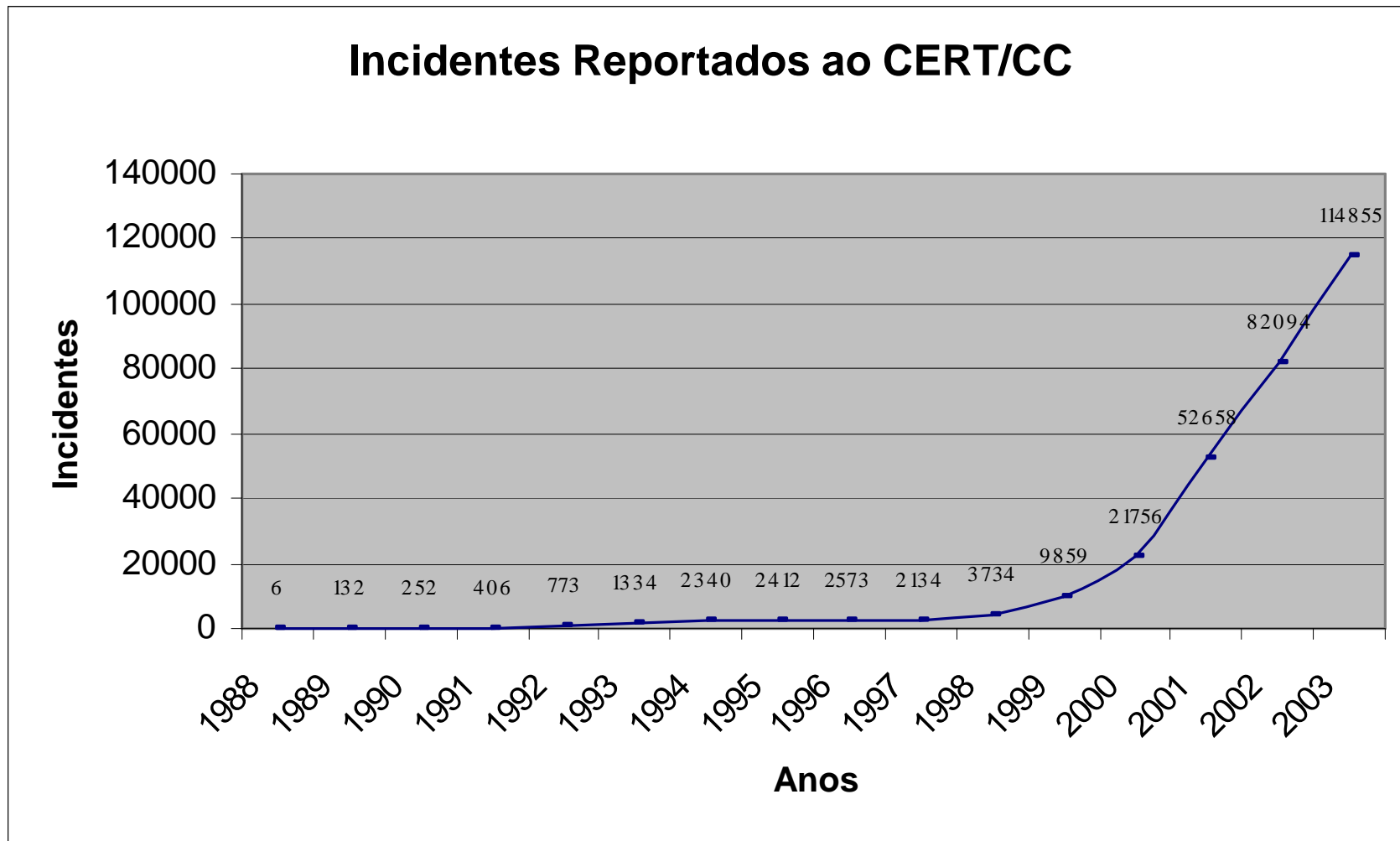


Estatísticas 2003





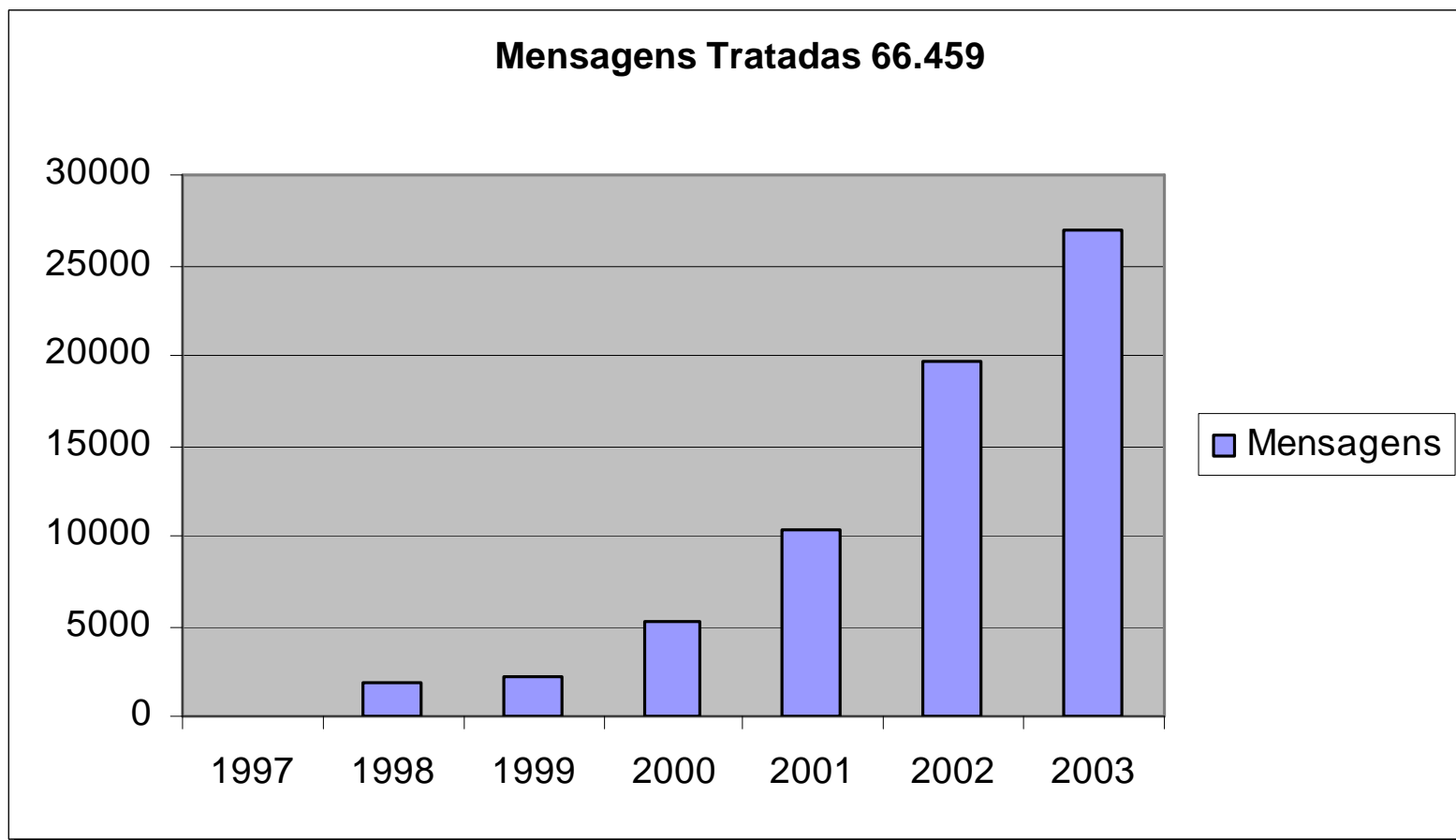
Estatísticas 2003



Retrospectiva na área de segurança

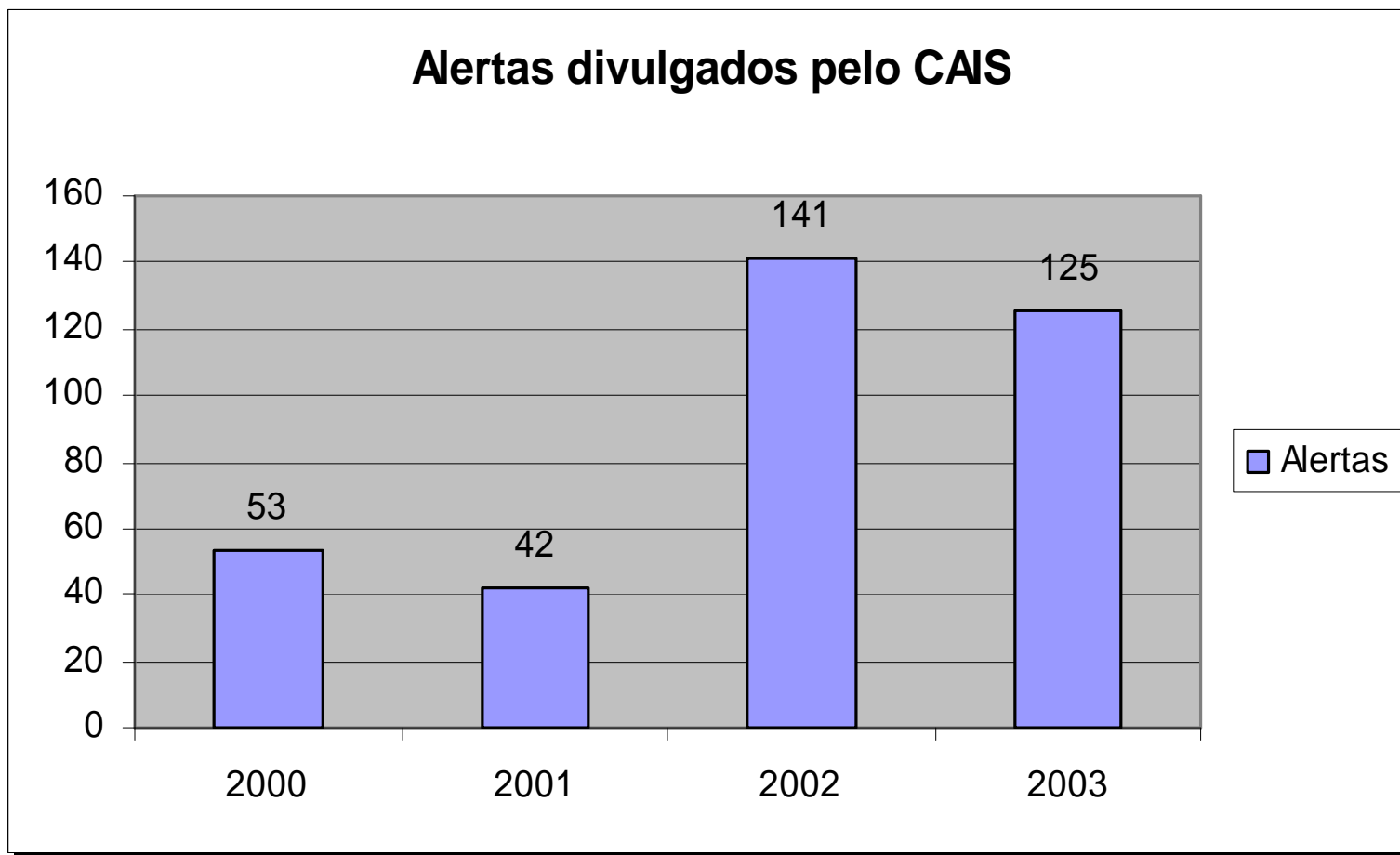


Estatísticas 2003





Estatísticas 2003



Retrospectiva na área de segurança



2003: "O Ano da Fraude"



Retrospectiva na área de segurança



O quê se espera de 2004?

- ⌘ Pressão Internacional contra o Brasil
- ⌘ Spam
- ⌘ Novos Worms
- ⌘ BlackHats x WhiteHats



Retrospectiva na área de segurança

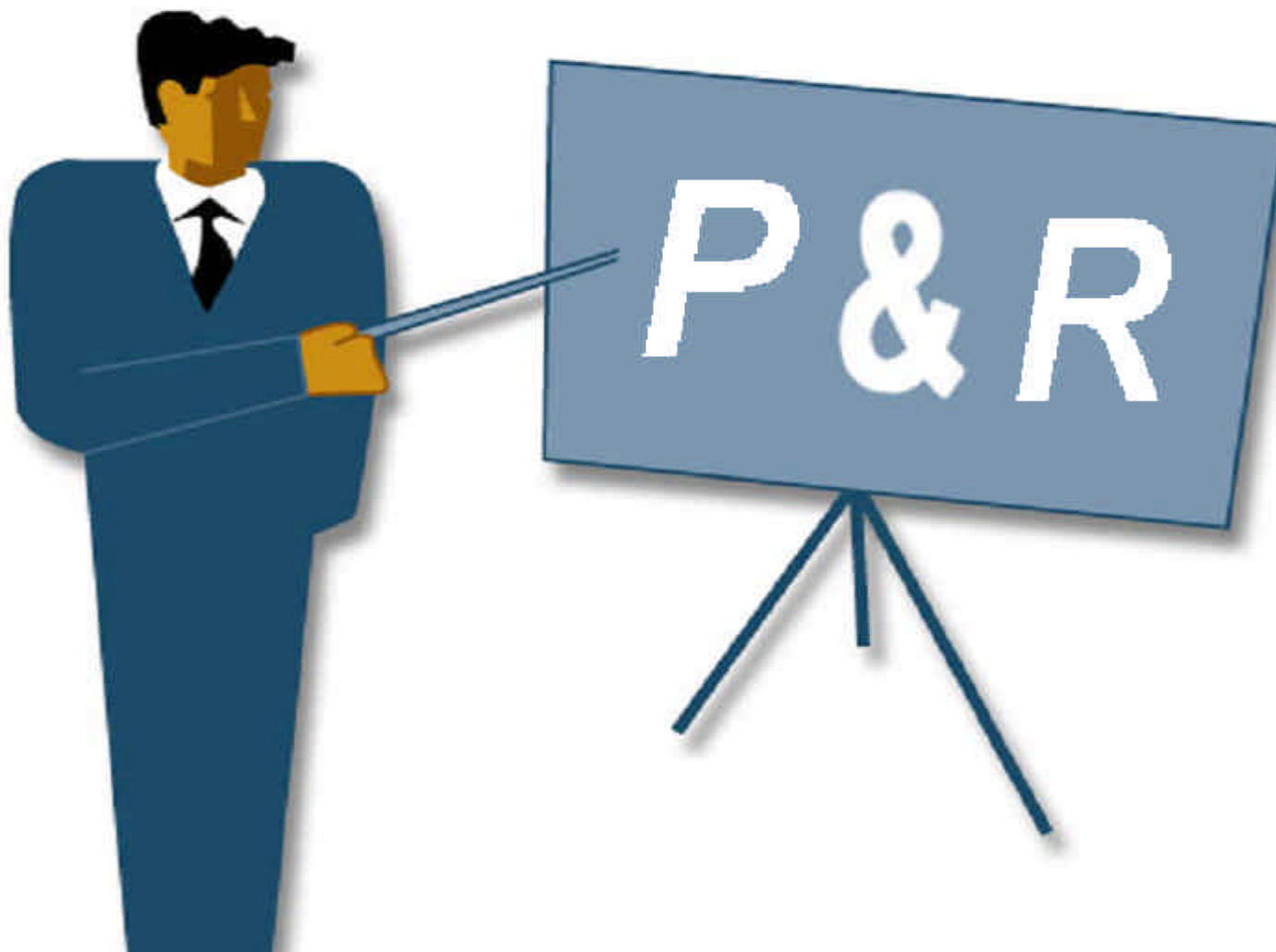


Referências

- ⌘ CAIS/RNP: <http://www.rnp.br/cais>
- ⌘ NBSO: <http://www.nbso.nic.br/>
- ⌘ CERT/CC: <http://www.cert.org/>
- ⌘ SANS: <http://www.sans.org/>
- ⌘ CVE: <http://cve.mitre.org/>
- ⌘ SecurityFocus: <http://www.securityfocus.com/>
- ⌘ Incidents: <http://www.incidents.org/>
- ⌘ Zone-h: <http://www.zone-h.org/>
- ⌘ FIRST: <http://www.first.org/>
- ⌘ Mi2G: <http://www.mi2g.com/>

Retrospectiva na área de segurança

Perguntas?



Retrospectiva na área de segurança



Contatos

Centro de Atendimento a Incidentes de Segurança – CAIS

cais@cais.rnp.br - <http://www.rnp.br/cais>



Jacomo Dimmit Boca Piccolini – jacomo@cais.rnp.br