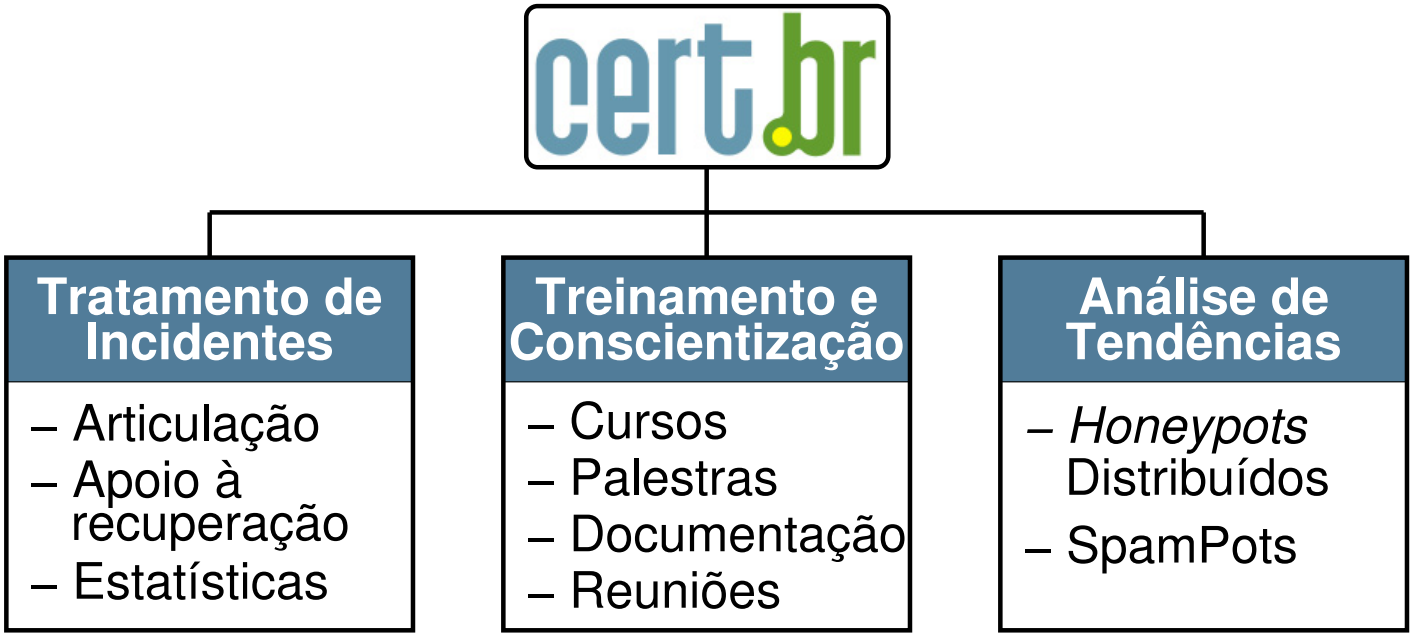
nic.br cgi.br | cert.br

Café Cinfotec da Unicamp
Campinas, SP
16 de março de 2016

Segurança em Aplicações Web: Como mitigar os riscos

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

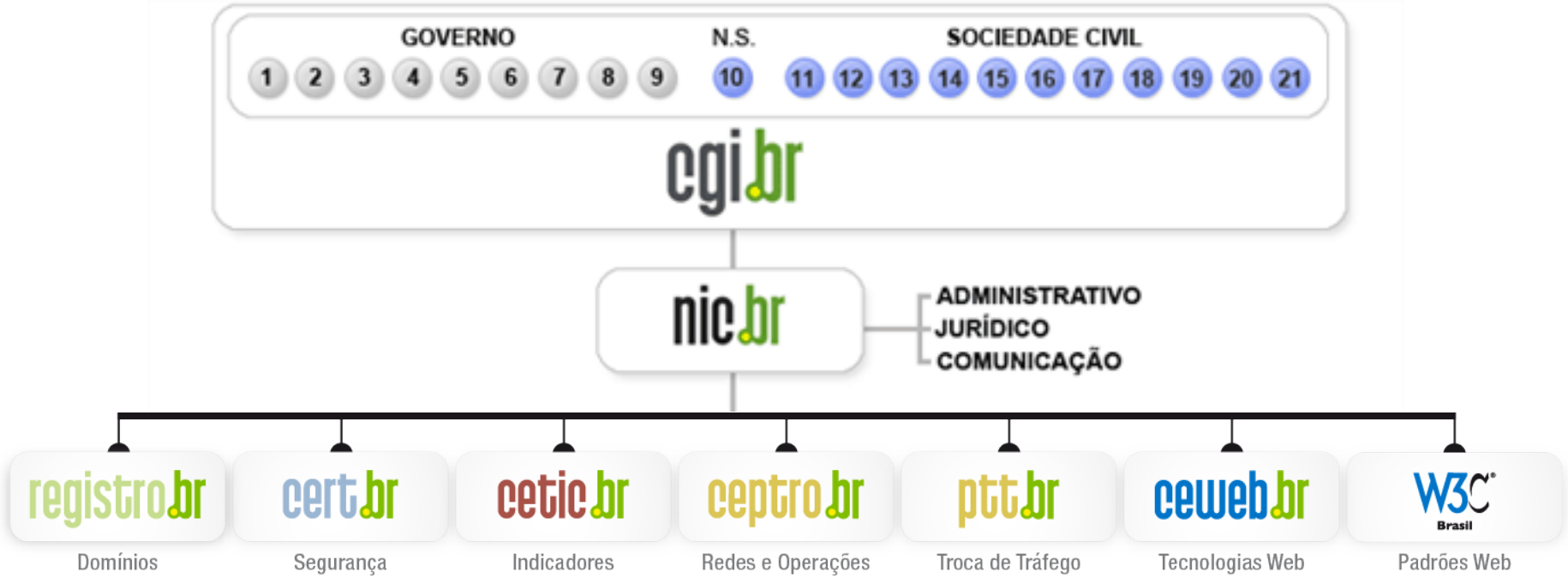
The Honeynet PROJECT

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:

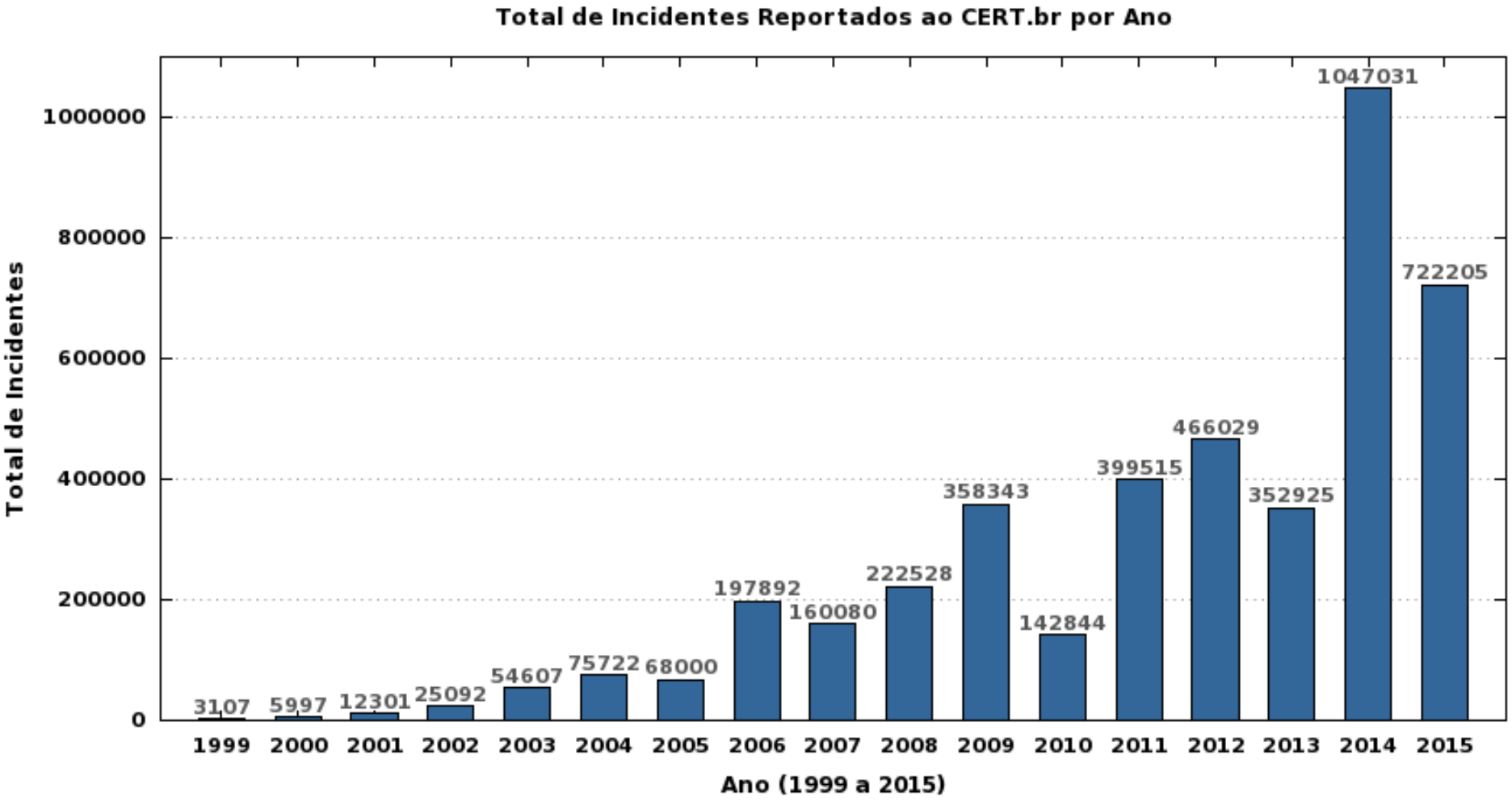
- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **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/

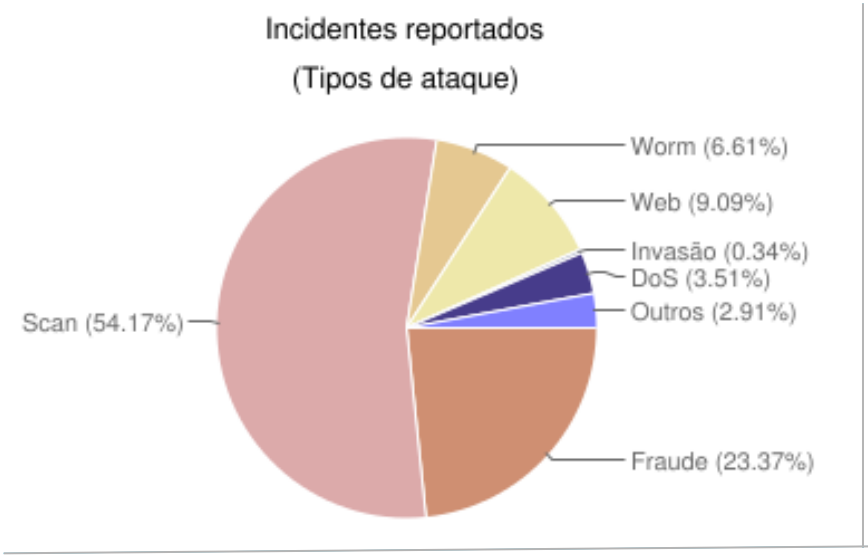
Agenda

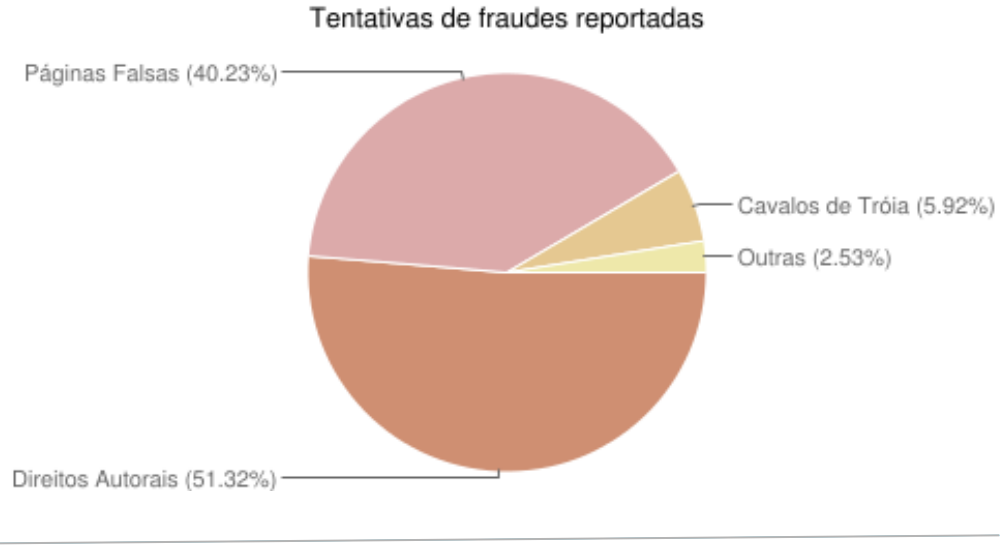
- **Estatísticas gerais**
- **Ataques a servidores Web**
  - Motivação dos ataques
  - Cenário atual
- **Mitigando os riscos**
  - Boas práticas para desenvolvedores
  - Boas práticas para administradores
- **Referências**

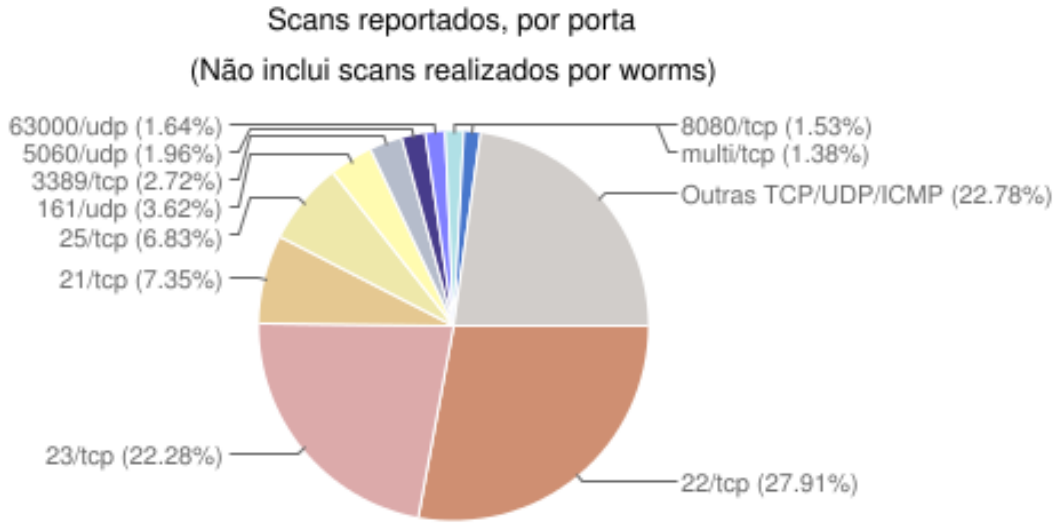
Estatísticas CERT.br – 1999 a 2015



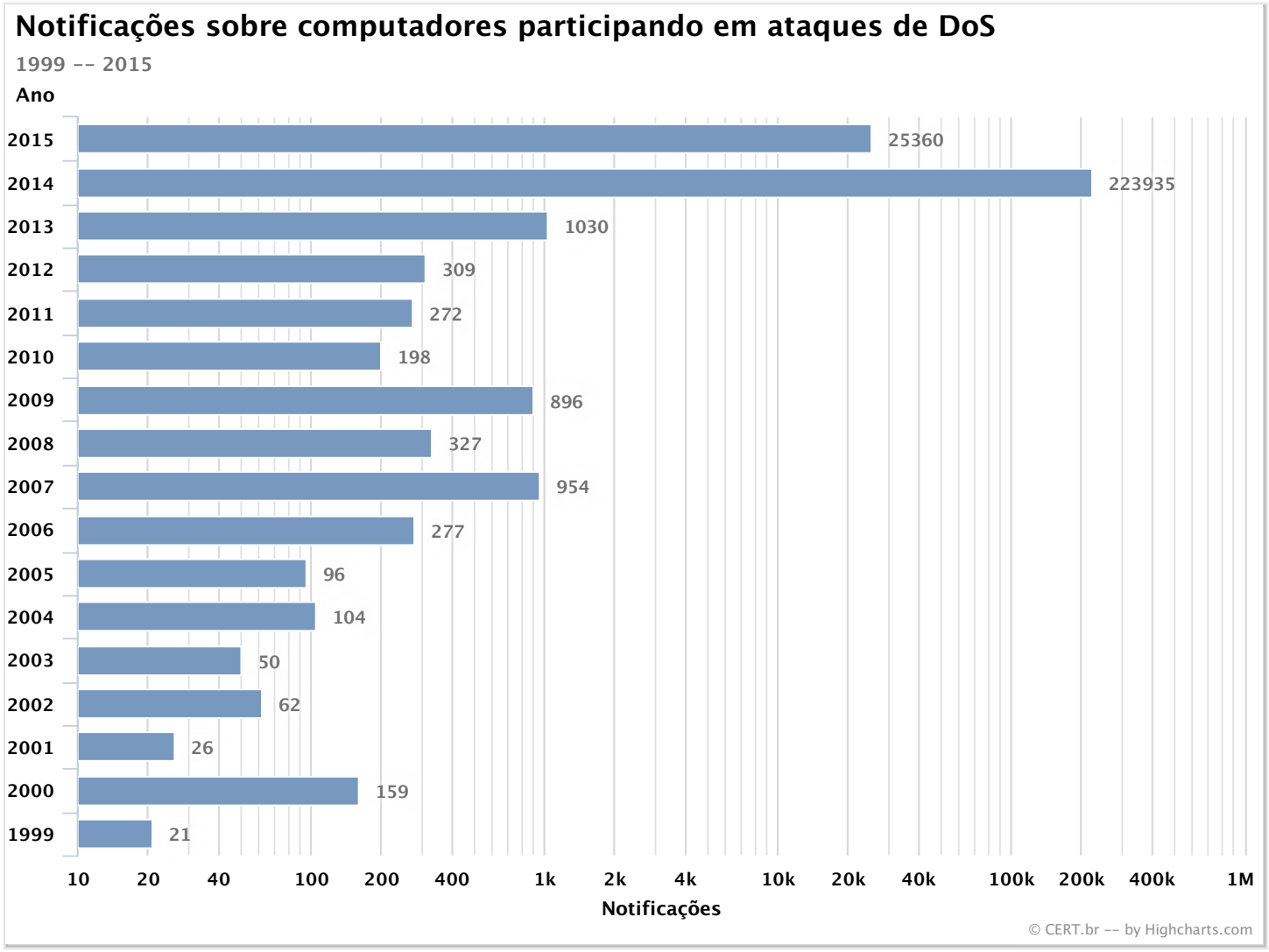
Estatísticas CERT.br – 2015



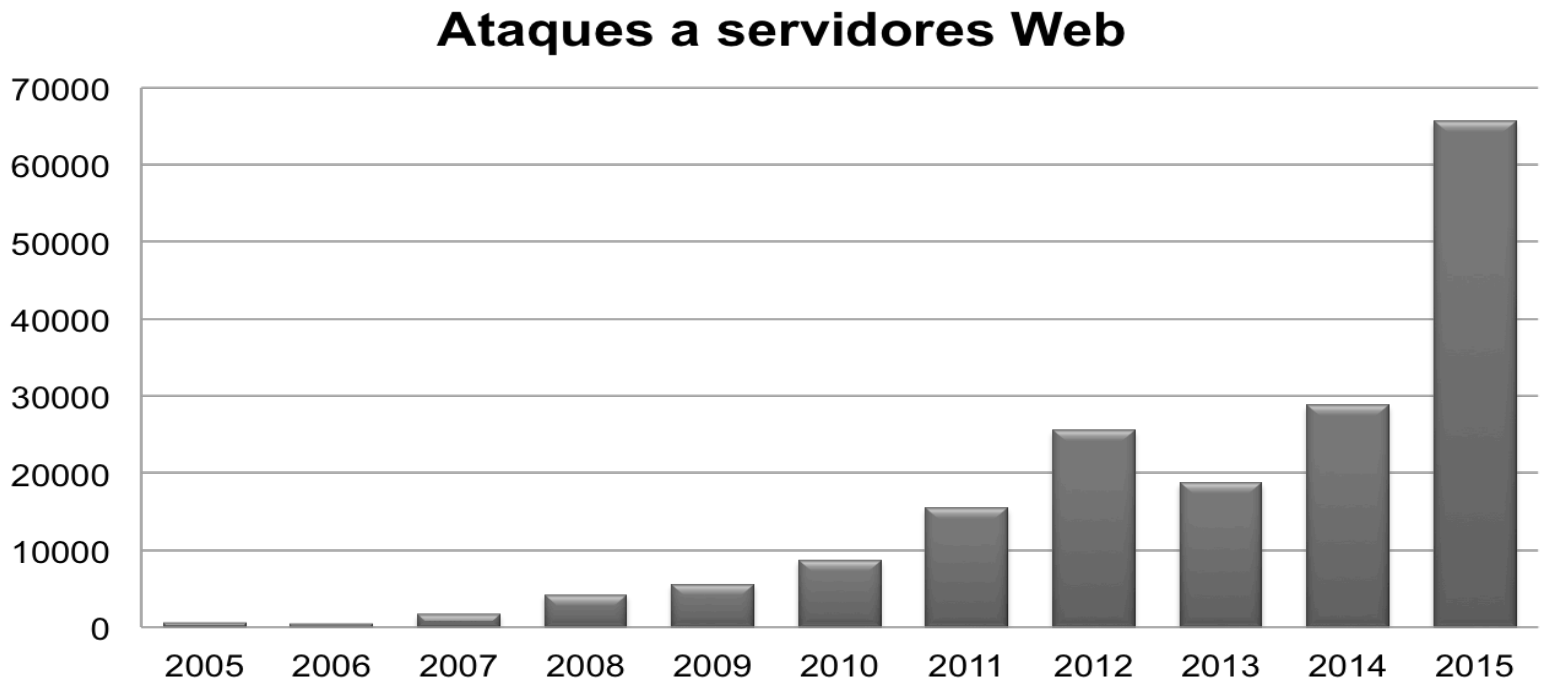




Estatísticas CERT.br – 1999 a 2015



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/

Motivação dos ataques

cert.br nic.br cgi.br

Motivação dos ataques (1/3)

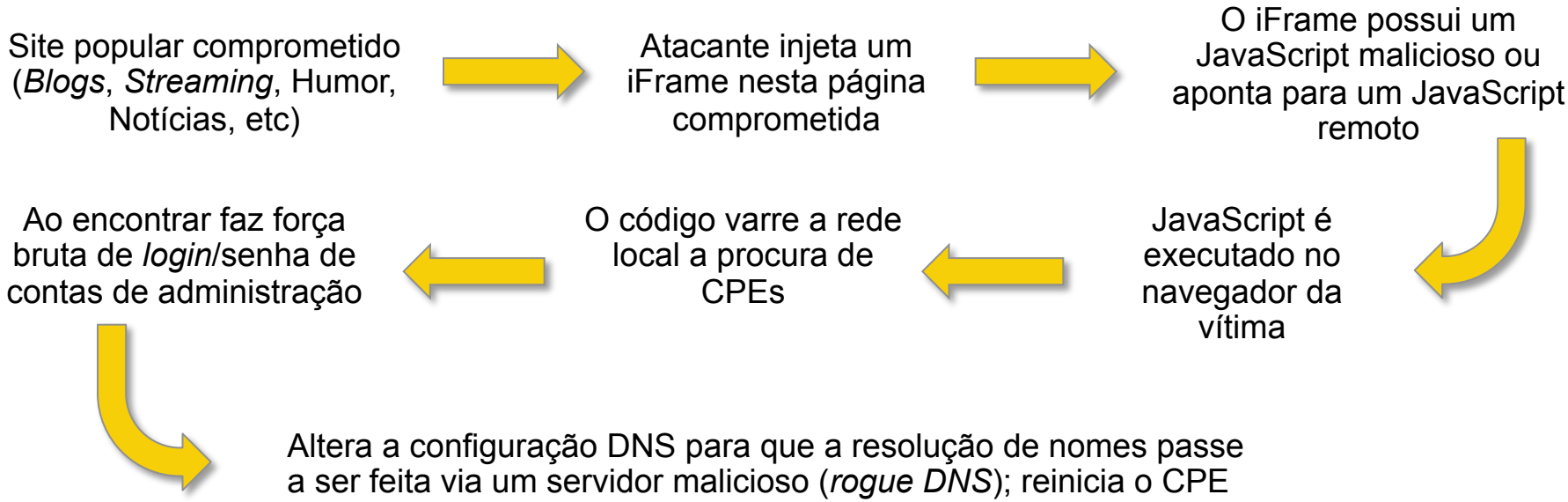
- **Autopromoção**
- **Motivos políticos e ideológicos**
- **Coleta de dados**
- **Repositório de dados**
- **Motivos econômicos**
- ***Phishing***
- **Instalação de códigos maliciosos**
- **Venda de *exploits* e *zero-days***

Motivação dos ataques (2/3)

- **Ataques DDoS**
  - servidores Web usados para gerar ataques
    - mais poderosos, mais banda de Internet, alta disponibilidade
  - aplicações como alvo de ataques
    - ataques a camada 7
    - procuram explorar características específicas de uma aplicação
      - saturar recursos
      - exceder número máximo de sessões de um banco de dados
      - fazer consultas complexas aos sistemas
    - mais difíceis de serem detectados
      - podem ser confundidos com problemas de implementação
      - não necessitam de muitos recursos e tráfego

Motivação dos ataques (3/3)

- **Disparar outros ataques e golpes**
  - Fraude de Boleto Envolvendo CPEs e DNS
  - Objetivo: adulterar o boleto para beneficiar o fraudador
  - Veículo: comprometimento de CPEs
    - forçar uso de DNS malicioso que aponta para página falsa de geração de boleto ou instala malware para alterar boleto



Cenário atual

cert.br nic.br cgi.br

Cenário atual (1/3)

- **Empresas/instituições:**
  - segurança não é parte dos requisitos
    - ou uma das primeiras a serem cortadas para redução de custos
  - dificuldade em:
    - entender, lidar com os problemas (descrédito)
      - “Segurança é paranoia. Nada vai acontecer”
    - avaliar os riscos
      - informações cada vez mais valiosas disponibilizadas via Web

Cenário atual (2/3)

- **Aplicações:**
  - cada vez mais complexas
  - com muitas vulnerabilidades
  - não são testadas adequadamente
  - pressão econômica para lançar, mesmo com problemas
  - precisam estar acessíveis
    - inclusive as de infraestrutura crítica
  - uso indiscriminado de certificados digitais auto-assinados

- **Desenvolvedores:**
  - falta de capacitação para desenvolver com requisitos de segurança
    - não aprendem, ou
    - aprendem nos últimos anos da graduação
  - alguns que sabem cobram mais caro pelo desenvolvimento seguro

Cenário atual (3/3)

- **Ferramentas:**
  - de segurança: não conseguem remediar os problemas
  - de ataque: “estão a um clique de distância”

- **Administradores:**
  - precisam correr atrás dos prejuízos
  - instalação / configuração “*default*”
    - senhas fracas / padrão
  - falta de manutenção
    - atualizações
    - correções de erros

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/

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/

Infusion Pumps

www.hospira.com/en/products_and_services/infusion_pumps

Reader

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Contact Hospira

Our focused line of infusion systems includes general infusion and pain management pumps:

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Advisory (ICSA-15-161-01)

More Advisories

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

Exploração de vulnerabilidades

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

Ataques a Servidores Web / CMS – *Plugins*

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 – *Core*

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

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/

Mitigando os Riscos

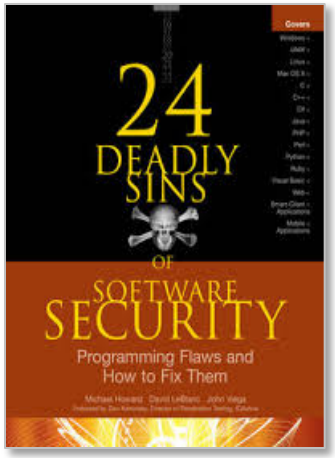
cert.br nic.br cgi.br

Boas Práticas para Desenvolvedores Web

cert.br nic.br cgi.br

Boas Práticas para Desenvolvedores Web (1/3)

- **Pensar em segurança desde os requisitos**
  - requisitos de confidencialidade, integridade e disponibilidade
  - pensar também nos casos de ABUSO (o ambiente é HOSTIL)



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

Boas Práticas para Desenvolvedores Web (2/3)

- **Segurança deve ser implementada no lado do servidor**
  - checagens via Javascript podem ser desabilitadas

- **Uso de certificados digitais assinados**
  - ICPEdu
    - certificados assinados pela GlobalSign
    - reconhecidos pelos principais navegadores e sistemas
  - garantir que a checagem do certificado esta sendo feita
    - ambiente de teste / produção

Boas Práticas para Desenvolvedores Web (3/3)

- **Efetuar testes de carga (*over provision*)**

- **Usar ferramentas de teste**
  - OWASP ZAP
  - *proxy* que:
    - analisa o comportamento da aplicação e
    - mostra possíveis vulnerabilidades
  - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

- **Considerar o uso de *Web Application Firewall***
  - deve ser uma camada extra de segurança
  - não pode substituir outros cuidados

Boas Práticas para Administradores

cert.br nic.br cgi.br

Servidores Web

- **Manter o computador atualizado (processo contínuo)**
  - sistema operacional
  - *software* do web/app *server*, *plugins*
- **Monitorar *logs*, eventos, etc**
- **Fazer *backup* e teste de restauração**
  - única solução efetiva contra *ransomware*
- **Sincronizar as máquinas via NTP**

Servidores Web

- ***Hardening* do servidor**
  - desabilitar:
    - a listagem de diretórios no servidor Web
    - módulos e serviços desnecessários
    - diretiva que mostra informações do servidor (versão, caminho do sistema, nome de banco de dados, etc)
    - métodos TRACE e TRACK, pois eles permitem “debugar” informações e expõem dados contidos em *cookies*

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

Política de contas e senhas

- **Não instalar/executar serviços com usuário privilegiado**
- **Criar usuários distintos para diferentes serviços**
  - Web/app server, banco de dados
  - privilégios mínimos
- **Ser criterioso nas permissões de arquivos e diretórios**
- **Usar senhas fortes**
  - considerar o uso de verificação em duas etapas
- **Não reutilizar senhas**
  - basta descobrir a senha de um serviço para invadir outros que usam a mesma senha
- **Ter política de desligamento de funcionários**
  - trocar as senhas compartilhadas
  - cancelar contas, revogar acessos externos

Gerenciadores de conteúdos – CMS

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

Em caso de invasão...

cert.br nic.br cgi.br

...tire a mão do teclado!!!

O que fazer (1/2)

- **Bloquear acesso ao *site***
  - bloquear no firewall, parar o serviço
- **Fazer *backup* da máquina**
  - para preservar as evidências
- **Investigar a origem do comprometimento**
- **Tentar definir as ações do invasor**
- **Procurar por outras máquinas que também possam estar comprometidas ou vulneráveis**
  - mesma senha
  - mesma vulnerabilidade
  - mesma versão de CMS, etc.

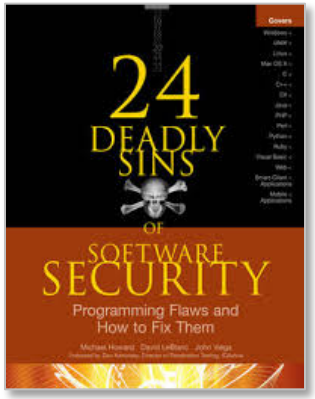
O que fazer (2/2)

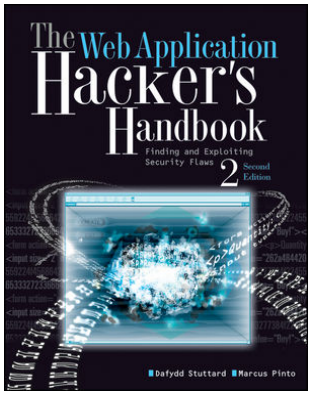
- **Corrigir a falha explorada**
  - trocar as senhas
  - atualizar os sistemas
  - atualizar *plugins*
  - alterar configurações
- **Se necessário reinstalar a máquina**
  - nem sempre é possível mapear todas as ações do invasor
- **Notificar o incidente**

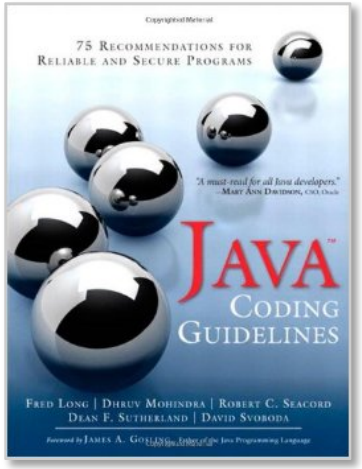
Referências

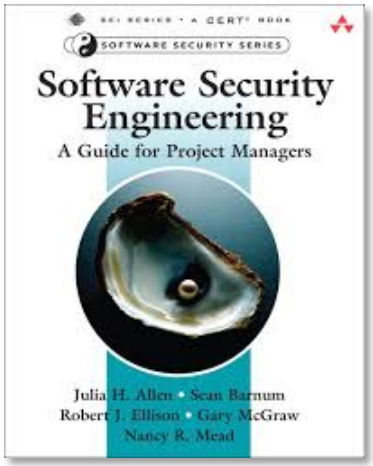
cert.br nic.br cgi.br

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/

Obrigada

www.cert.br

miriam@cert.br

@certbr

16 de março de 2016

nic.br cgi.br

www.nic.br | www.cgi.br