

Reflexões sobre o Estado Atual da Segurança na Internet

Cristine Hoepers, D.Sc.

cristine@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

Agenda

- **Contextualização**
 - Internet no Brasil
 - CERT.br / NIC.br / CGI.br
- **Ataques mais frequentes**
- **Desafios**
- **Considerações finais**
- **Leituras recomendadas**
 - livros, sites, blogs

Internet no Brasil

Evolução da Internet no Brasil

1989 – Criação e delegação do código de país (ccTLD) “.br” à FAPESP

1991 – Primeira conexão TCP/IP brasileira, realizada entre a FAPESP e a *ESNet*

1995 – Portaria MC/MCT nº 147, de 31 de maio, cria o CGI.br

- **coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados**

1995 – Criação do Registro.br

1997 – Criação do CERT.br (à época NBSO)

2005 – Criação do NIC.br

entidade sem fins lucrativos para executar as diretrizes do CGI.br e prestar serviços para a estabilidade e segurança da Internet no Brasil

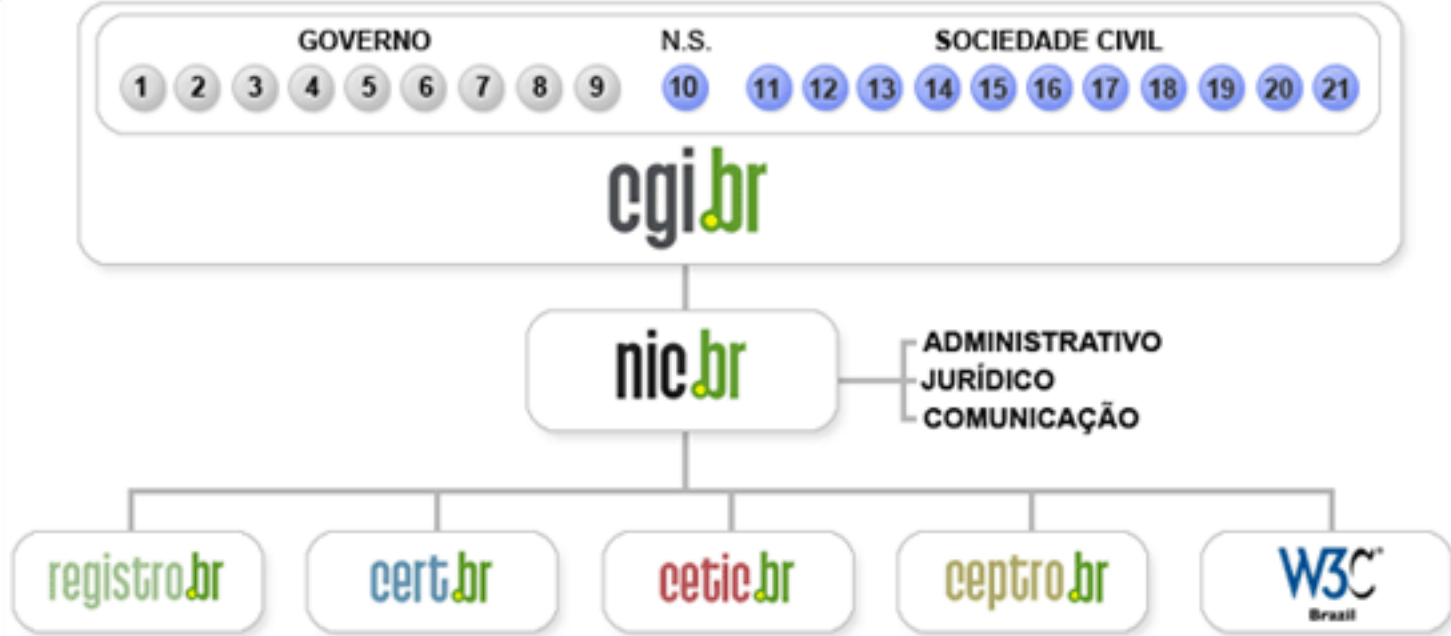
Comitê Gestor da Internet no Brasil – CGI.br

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-cg/>

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



Tratamento de Incidentes
<ul style="list-style-type: none"> – Articulação – Apoio à recuperação – Estatísticas

Treinamento e Conscientização
<ul style="list-style-type: none"> – Cursos – Palestras – Documentação – Reuniões

Análise de Tendências
<ul style="list-style-type: none"> – <i>Honeypots</i> Distribuídos – SpamPots



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/>

Ataques mais Comuns

Ataques a usuários finais

- **Fruto da mudança no enfoque dos atacantes**
 - é mais fácil e “rentável” atacar um usuário
- **Fraudes financeiras**
 - páginas falsas estão voltando a ter números significativos
 - *drive-by downloads* sendo usados intensamente no Brasil
 - casos publicados na mídia incluem:
sites principais da Vivo, da Oi e da Ambev
- **Outras motivações**
 - espionagem, sabotagem
 - nesses casos chamados de APTs (“*Advanced Persistent Threats*”)
- **Casos conhecidos cujos vetores iniciais foram usuários redes de alto valor**
 - Comprometimento da DigiNotar – PKI da Holanda
 - Caso Aurora (Google, Microsoft, etc, invadidos por meses)
 - New York Times

Ataques a dispositivos

- **“Modems” e roteadores banda larga (CPEs)**
 - **Botnets** usadas para ataques diversos
 - comprometidos via força bruta (telnet)
 - vários modelos com outras vulnerabilidades
 - Ex.: *Zollard worm*, que explora vulns. de PHP
 - **Comprometimento para alteração do serviço DNS para**
 - fraudes financeiras
 - redirecionamento para obter “cliques” de propaganda
 - DDoS (negação de serviço distribuída)
- **Dispositivos com sistema Android**
 - **Botnets, fraudes e outros tipos de malware**
- **NAS e outros sistemas com storage (como DVR’s)**
 - Ex.: *Synology Bitcoin miner*

Ataques a serviços de rede

- **De força bruta (adivinhação de conta/senha) contra serviços de rede**
 - SSH, FTP, Telnet, VNC, RDP, etc
 - acesso a servidores, roteadores, CPEs, celulares, etc
- **Não tão frequentes, mas com grande impacto por serem contra a infraestrutura crítica da Internet**
 - ataques contra servidores DNS
 - contra protocolos de roteamento como o BGP
- **Sistemas SIP (VoIP)**
 - Força bruta para realização de ligações internacionais e fraudes
 - Anatomy of SIP Attacks
<https://www.usenix.org/publications/login/december-2012-volume-37-number-6/anatomy-sip-attacks>

Ataques a servidores Web

- **Muitas vulnerabilidades de *Software***
 - ***softwares* de CMS desatualizados**
 - Wordpress, Joomla, Doldfusion
 - **uso de pacotes prontos**
 - **falta de atualização dos sistemas operacionais**
 - **muitas falhas de programação:**
 - falta de validação de entrada
 - falta de checagem de erros
 - **exploração automatizada**
 - Ex.: *botnet* Brobot

2º Fórum Brasileiro de CSIRTs

www.cert.br/forum2013/agenda/

Anatomy of Operation Ababil - DDoS attacks targeting US Banks [Slides]

André Corrêa, Senior Security Analyst
PhishLabs Security Operations

Using Joomla? Your website might have already taken part in DDoS attack - HKCERT

www.hkcert.org/my_url/en/blog/13

Security Blog

Using Joomla? Your website might have already taken part in DDoS attack

ação e Comunicação do Pa

Release Date: 29 / 11 / 2013

Contents

1. Background
2. "Operation Ababil" DDoS attack
3. HKCERT operation on "brobot" cleanup in Hong Kong
4. How to detect and remove "brobot" in CMS
5. Reference

Attackers trick 162,000 WordPress sites into launching DDoS attack | Ars Technica

arstechnica.com/security/2014/03/more-than-162000-leg

ars technica HEAD TO TOE GUIDE OF THE SEASON

MAIN MENU MY STORIES: 24 FORUMS SUBSCRIBE JOBS ARSCOIN STORE

RISK ASSESSMENT / SECURITY & HACKTIVISM

Attackers trick 162,000 WordPress sites into launching DDoS attack

Technique allows lone attacker hidden in the shadows to wage crippling attacks.

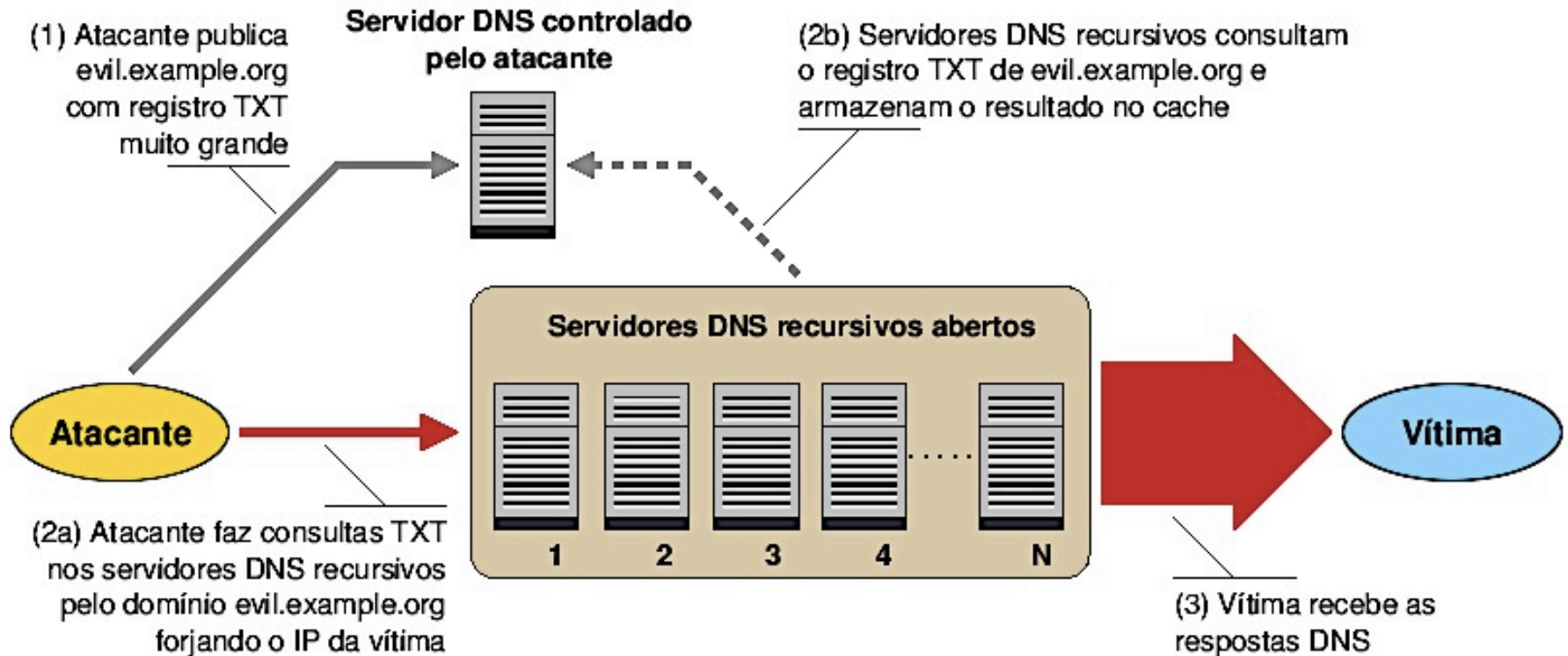
by Dan Goodin - Mar 11 2014, 1:35pm BRT

BLACK HAT INTERNET CRIME 50



DRDoS – DDoS via amplificação de tráfego UDP

Exemplo: Abuso de servidores DNS



Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

<http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>

Amplification Hell: Revisiting Network Protocols for DDoS Abuse

<http://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse>

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 infraestruturas 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

Por que são tão fáceis?

Reais Causas dos Problemas

- **Cenário atual é reflexo direto de**
 - **Aumento da complexidade dos sistemas**
 - **Softwares com muitas vulnerabilidades**
 - **Segurança não é parte dos requisitos**
 - **Falta de desenvolvedores capacitados para desenvolver com requisitos de segurança**
 - **Pressão econômica para lançar, mesmo com problemas**
 - **É uma questão de “*Economics and Security*”**
<http://www.cl.cam.ac.uk/~rja14/econsec.html>
- **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”**

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 update

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>

Desafios

Investir em treinamento e pessoal

- **Há falta de pessoal treinado para lidar com Redes e com segurança em IPv4**
 - **A falta de pessoal com essas habilidades em IPv6 é ainda mais preocupante**
 - **Sua organização já usa IPv6? :-)**
<http://ipv6.br>
- **Vencer a cultura de que é melhor investir em tecnologia do que treinamento e implantação de boas políticas**
- **Ir além do “*compliance*”**

Resiliência da infraestrutura crítica de Internet

Contínuo investimento em:

- **Ter seu próprio Sistema Autônomo (AS)**
- **Conectar-se a Pontos de Troca de Tráfego nas áreas metropolitanas – PTT.br**
- **Sistemas de redundância e mirror de DNS**
- **Adoção de DNSSEC**
 - **Novos protocolos como DANE em estudo**
- **Segurança na infraestrutura de roteamento**
 - **Roteamento dinâmico funciona por confiança nos anúncios**
 - **Em implantação o uso de RPKI e S-BGP**
 - **Em resumo: tabelas de rotas passam a ser assinadas e publicadas somente pela fonte legítima**

Mito de que só quem sabe invadir sabe proteger

- **A realidade:**
 - **Proteger é muito mais difícil que atacar**
 - especialmente contra ataques ainda não conhecidos
 - **Raríssimos os atacantes que:**
 - sabem como proteger uma rede ou corrigir um problema
 - sabem como funcionam as ferramentas que utilizam
 - **Maioria absoluta utiliza ferramentas disponíveis na Internet**
 - **Um profissional com sólida formação tem mais sucesso em utilizar as ferramentas como auxiliares nos processos de análise de risco e proteção da infraestrutura que um invasor**
- **Os riscos:**
 - **Colocar a segurança nas mãos de quem não está preparado**
 - **Ter informações confidenciais comprometidas**
 - **Ter *backdoors* e cavalos de tróia instalados em sua infraestrutura**

Recuperação adequada de incidentes

- **A redução do impacto é consequência da:**
 - agilidade de resposta
 - redução no número de vítimas
- **O sucesso depende da confiabilidade**
- **O papel do CSIRT:**
 - auxiliar a proteção da infra-estrutura e das informações
 - prevenir incidentes e conscientizar sobre os problemas
- **O CSIRT não é um investigador**
- **Tratamento de Incidentes não é perícia**
- **A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime**
 - seguir as políticas
 - preservar as evidências
 - responder incidentes – retornar o ambiente ao estado de produção

São necessários novos métodos de detecção

Foco atual do mercado é no que entra em uma rede ou no que conhecidamente é malicioso:

“Intrusion Detection”

- IDS / IPS
- *Firewall*
- Antivírus

Foco precisa mudar para o que sai ou no tráfego interno:

“Extrusion Detection”

- *Flows*
- *Honeypots*
- *Passive DNS*
- **Atuar nas notificações de incidentes**
- ***Feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)**

Desafios para a Identificação da Origem de Ataques

- Os ataques partem de vítimas na maioria absoluta dos casos
- Investigação sem contexto pode levar a graves consequências
 - e.g. Coreia do Sul x China
 - a rede usava como IPs não roteáveis (no NAT) um bloco de IPs alocado para a China – peritos viram o IP de onde veio o *malware* e anunciaram que o ataque vinha da China
- A infraestrutura usada nos ataques de alto valor pode ser a mesma do crime organizado
 - e.g. DDoS na Estônia e Georgia
 - a *botnet* usada era a mesma que há meses enviava *spams* e fazia “*DDoS for hire*”

Só haverá reais melhorias quando

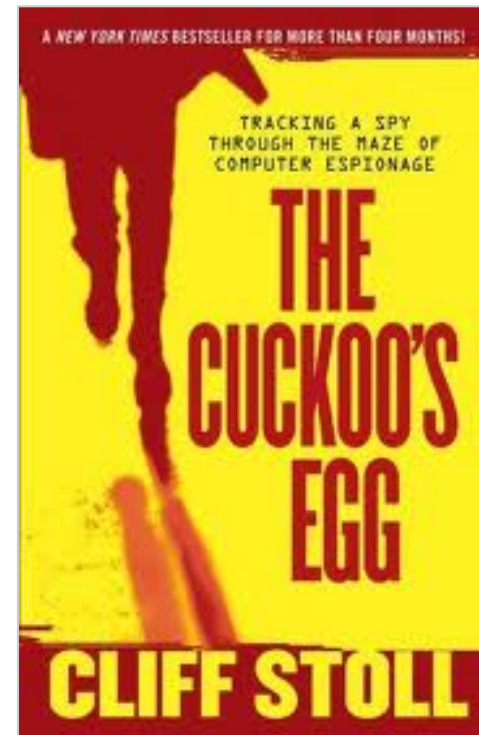
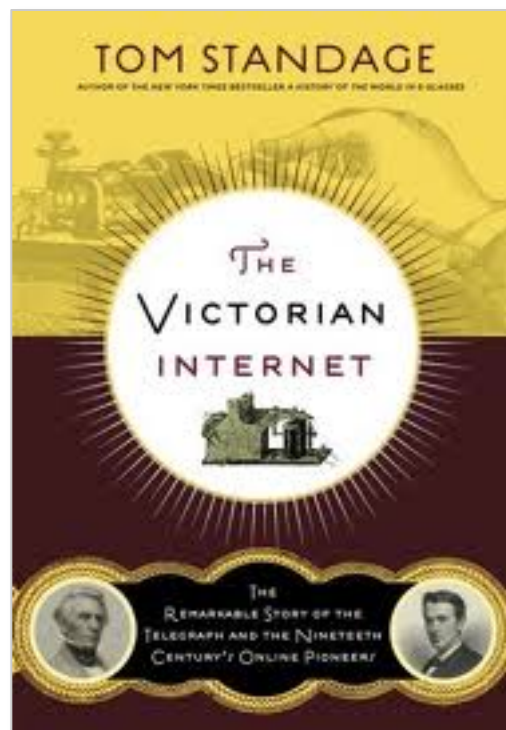
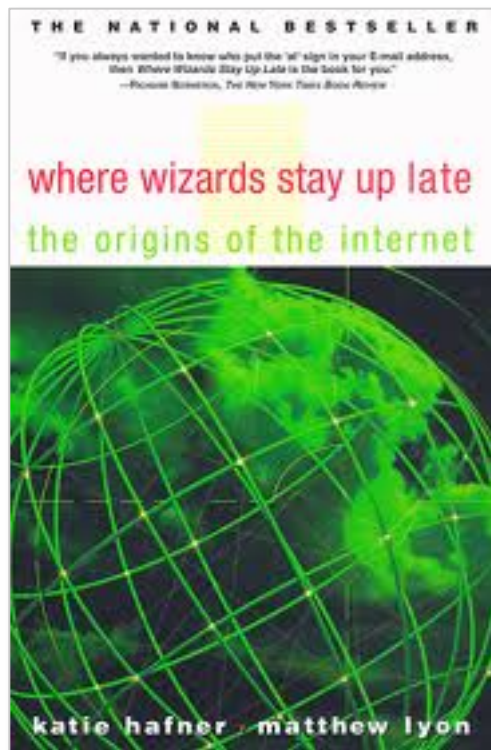
- **O processo de desenvolvimento de *software* incluir**
 - Levantamento de requisitos de segurança
 - Testes que incluam casos de abuso (e não só casos de uso)
- **Desenvolvimento seguro de *software* se tornar parte da formação de projetistas e programadores**
 - Desde a primeira disciplina de programação e permeado em todas as disciplinas
- **Provedores de acesso e serviço, operadoras e administradores de redes em geral forem mais pró-ativos**
- **Sistemas e ferramentas forem menos complexos de usar**
 - Mudança total de paradigma de uso da tecnologia

Leituras Recomendadas

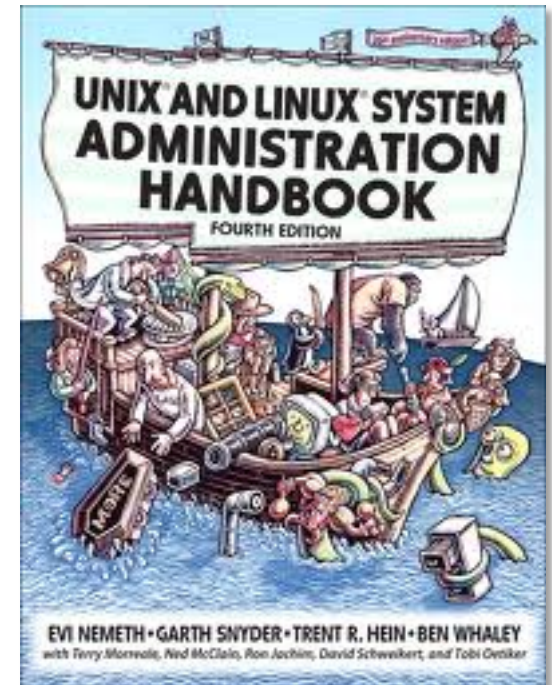
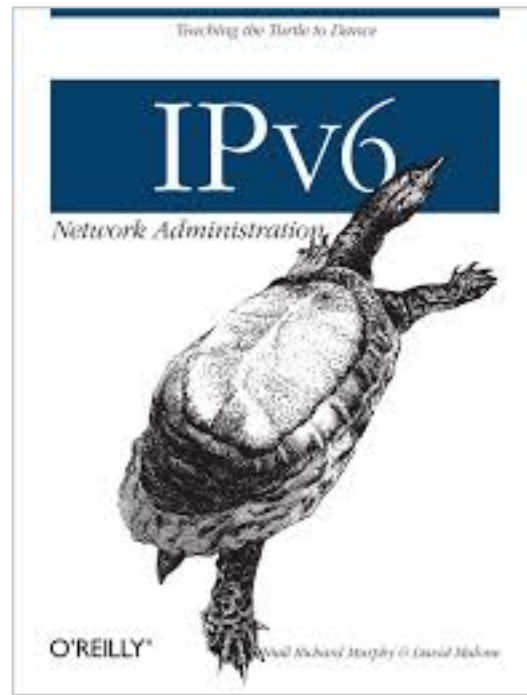
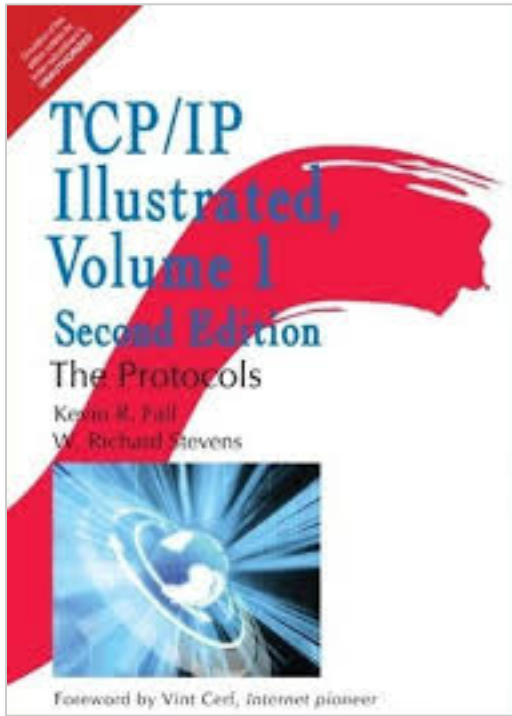
Últimas notícias e análises

- **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/>

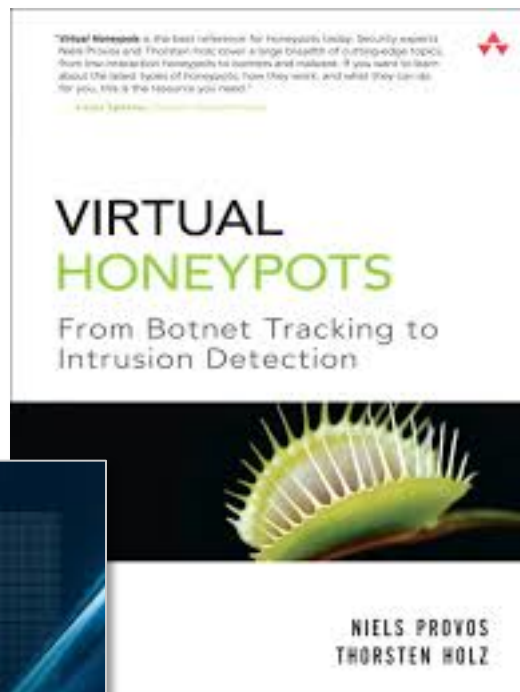
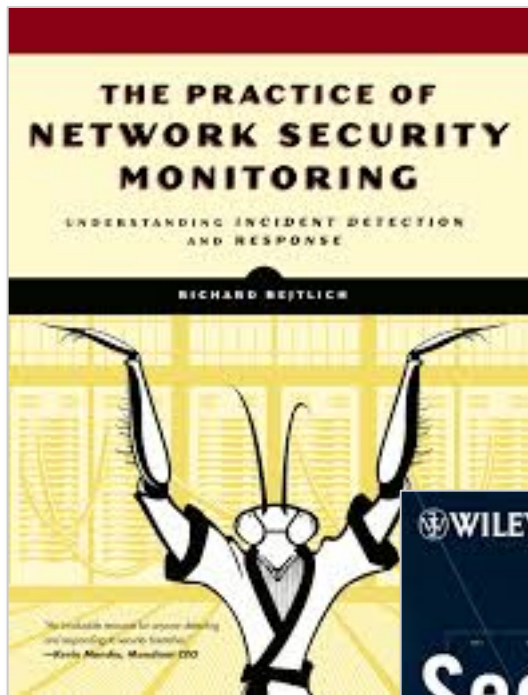
História da Internet e Primeiros Incidentes



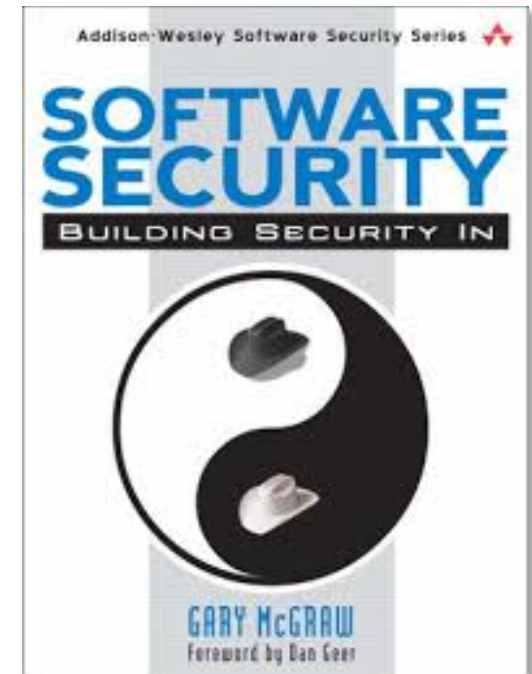
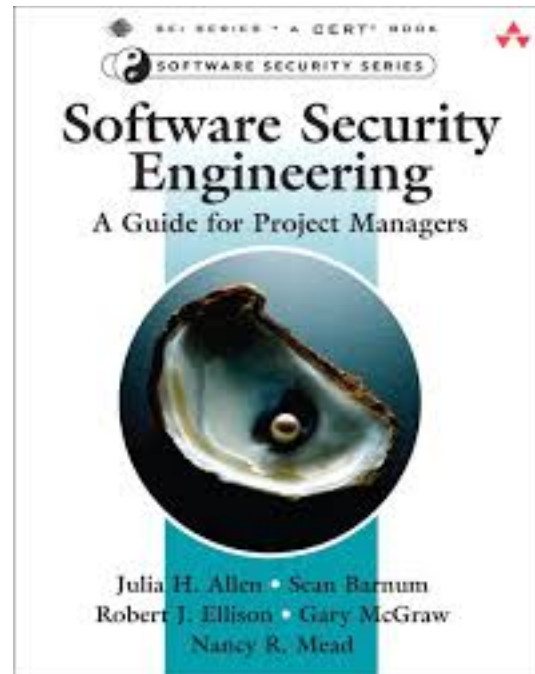
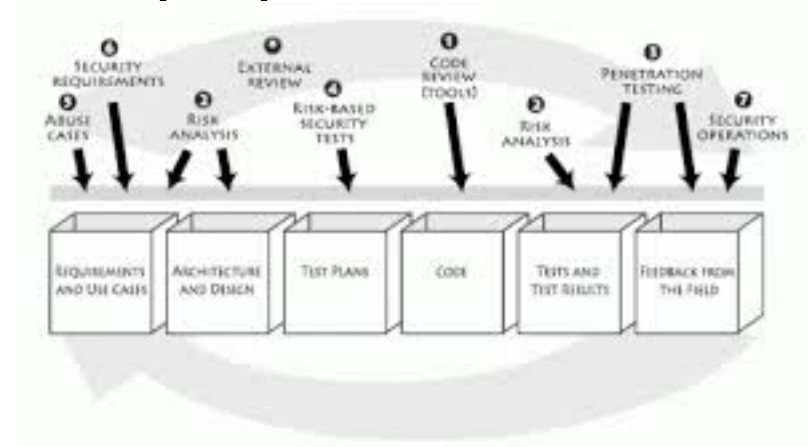
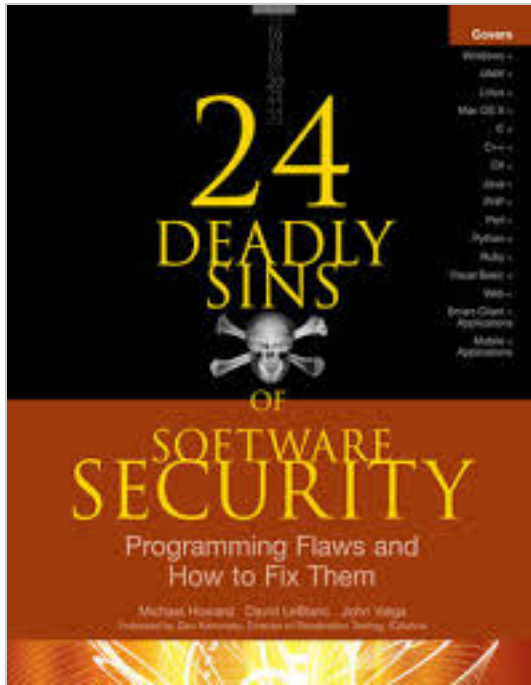
Redes e IPv6



Segurança



Segurança de Software (1/2)



Segurança de software (2/2)

- **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>

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?

Cristine Hoepers, D.Sc.
cristine@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/>
- **Cartilha de Segurança para Internet**
<http://cartilha.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

egi.br

Comitê Gestor da
Internet no Brasil

3º Fórum Brasileiro de CSIRTs – <http://cert.br/forum2014/>

- 15 e 16 de setembro
- Propostas de palestra até 27 de julho

The screenshot shows a web browser window displaying the website for the 3rd Brazilian CSIRT Forum. The browser's address bar shows the URL www.cert.br/forum2014/. The website header includes the cert.br logo and the text "Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil". The main navigation menu includes "Início", "Programação", and "Inscrições". A sidebar on the left contains links for "Keynote", "Programação", "Envio de trabalhos", "Inscrições", "Local", "Hotéis", "Informações de Interesse", and "Evento conjunto: V Seminário de Proteção à Privacidade e aos Dados Pessoais". The main content area features a section titled "Sobre o Evento" with the following text: "O Fórum Brasileiro de CSIRTs é um evento dedicado à discussão de assuntos relacionados com tratamento de incidentes e resiliência das organizações face a incidentes de segurança. O terceiro evento será realizado nos dias 15 e 16 de setembro de 2014. Haverá tradução simultânea entre Português e Inglês." Below this is a section titled "Datas Importantes" with a list of key dates:

- 27 de julho de 2014: Data limite para envio de propostas de palestras
- 11 de agosto de 2014: Anúncio das propostas aceitas
- 15 e 16 de setembro de 2014: 3º Fórum Brasileiro de CSIRTs
- 17 e 18 de setembro de 2014: Evento conjunto: V Seminário de Proteção à Privacidade e aos Dados Pessoais