Segurança na Internet: Tendências e Desafios

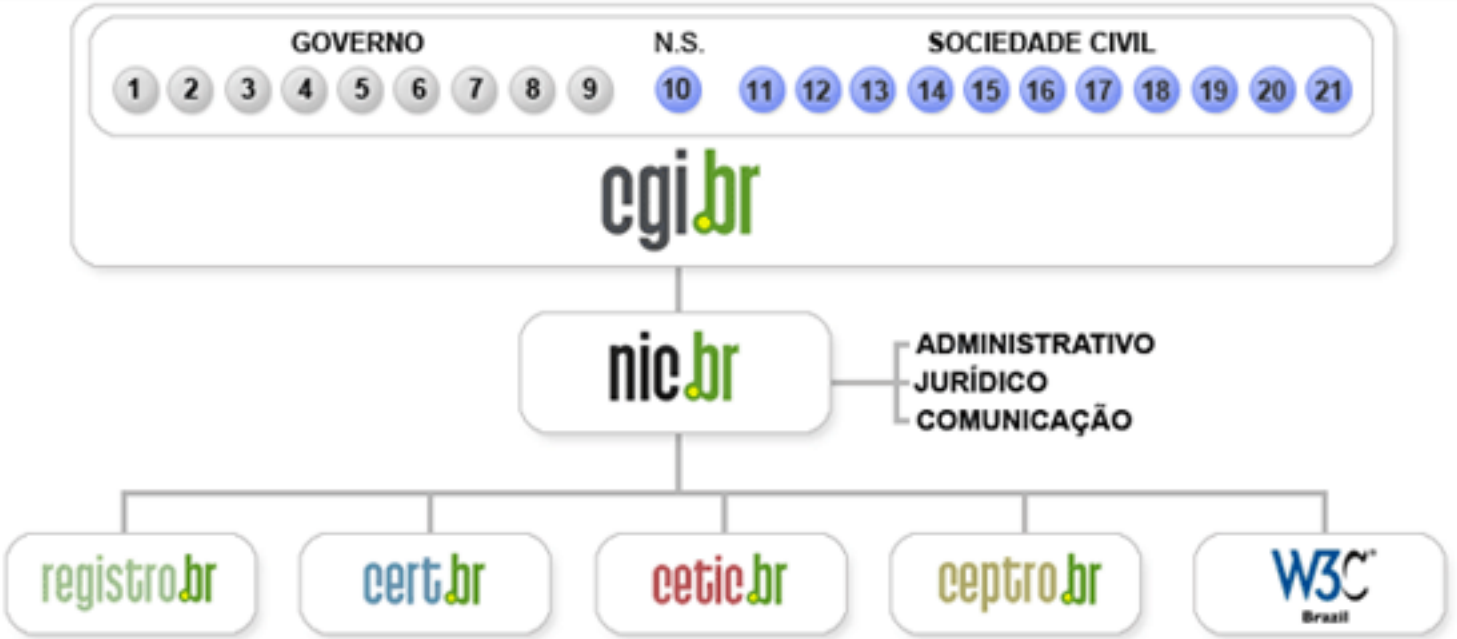
Miriam von Zuben
miriam@cert.br

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

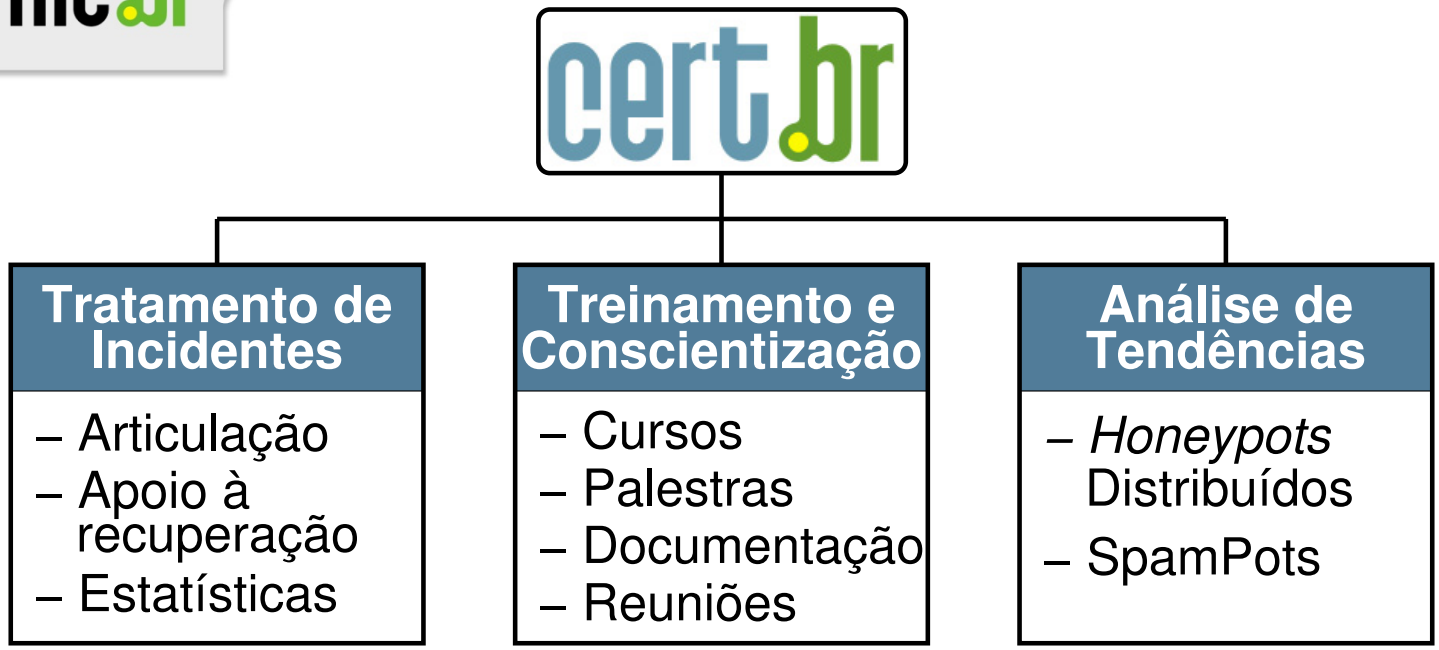
- CERT.br
- Cenário atual
- Tendências
- Desafios
- Recomendações

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



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

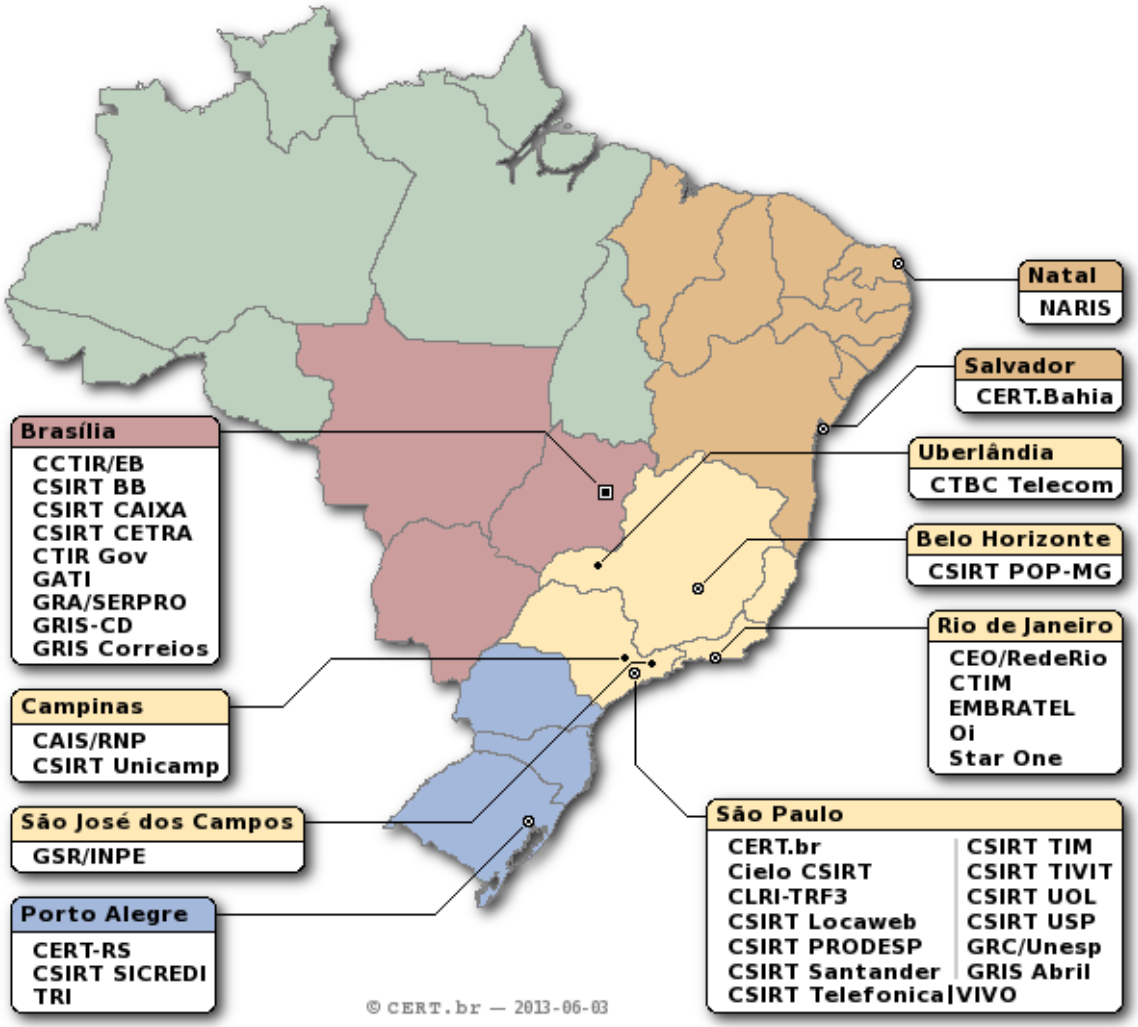
- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar 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/

CSIRTs Brasileiros

34 times com serviços anunciados ao público

Setor	CSIRTs
Escopo Nacional	CERT.br
Governo	CLRI-TRF-3, CSIRT Prodesp, CTIR Gov, GATI, GRA/SERPRO, GRIS-CD
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CERT-Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



http://www.cert.br/csirts/brasil/

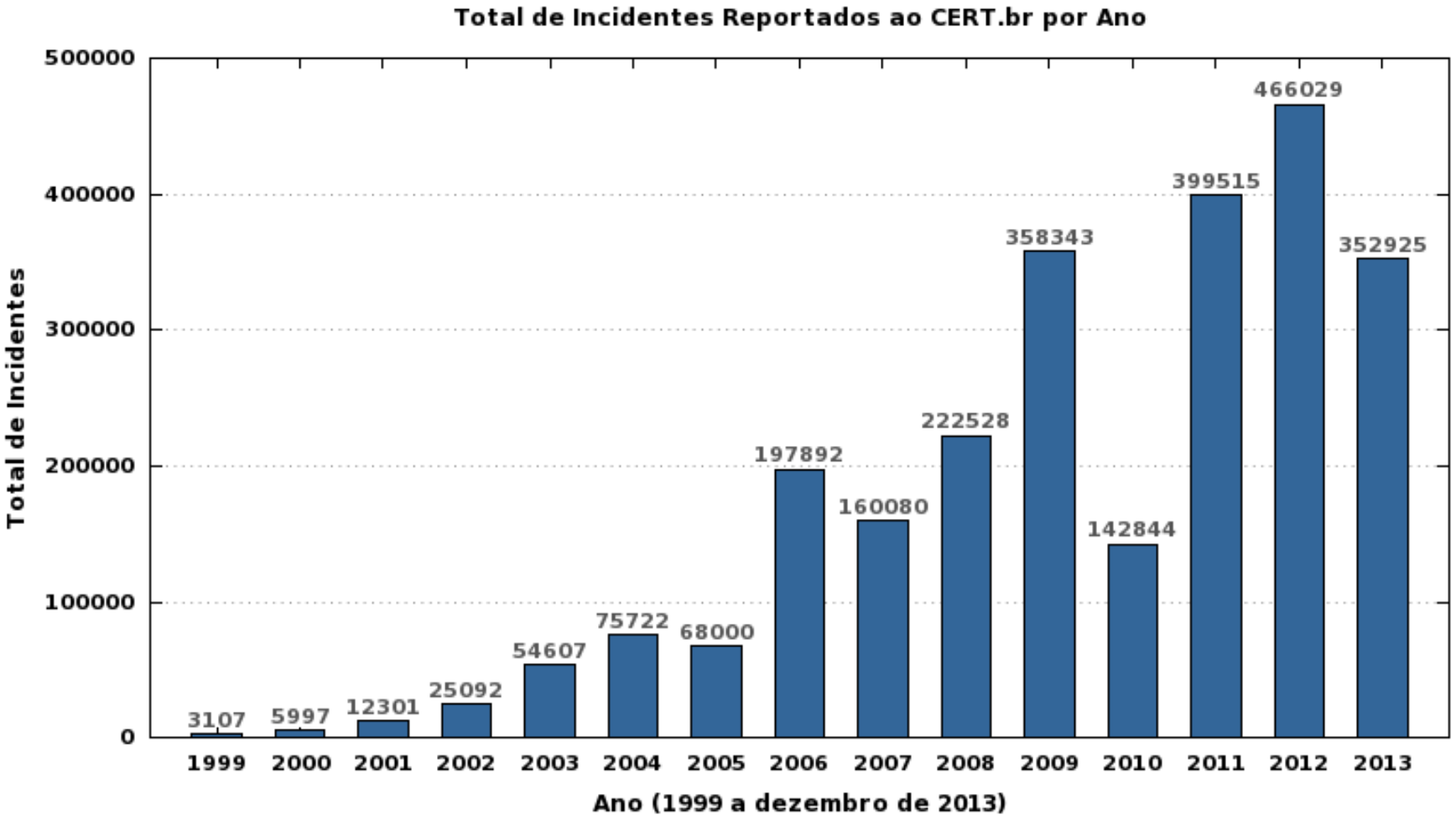
Projeto *Honeypots* Distribuídos

- **Rede de sensores (*honeypots**), instalados em diversas redes conectadas à Internet no Brasil, capazes de observar ataques a eles direcionados**
- **Objetivo: aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro**
  - **47 instituições parceiras, entre academia, governo, indústria, instituições financeiras e redes militares**
    - **ANSP, Unicamp, Unesp, USP, INPE**
  - **baseado em trabalho voluntário**
  - **http://honeytarg.cert.br/honeypots/**
- **Utilização dos dados coletados para:**
  - **notificação das redes originadoras dos ataques**
  - **geração de estatísticas públicas**

* *Honeypot* é um tipo de sensor usado para simular serviços e registrar as atividades maliciosas.
Fonte: http://www.cert.br/docs/whitepapers/honeypots-honeynets/

Cenário Atual

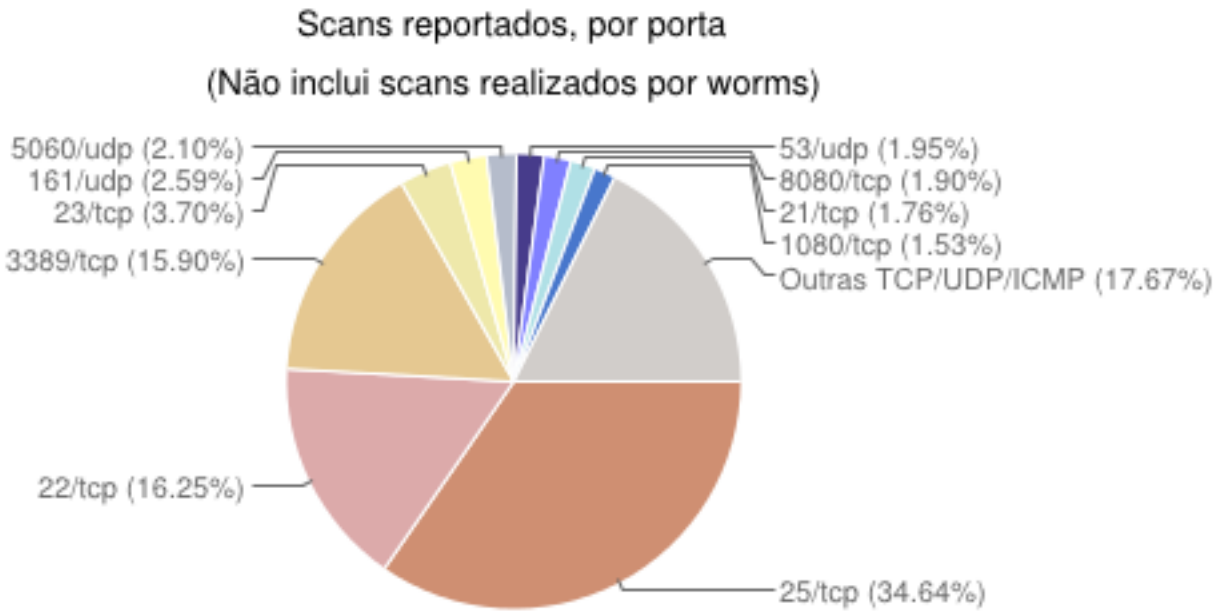
Incidentes reportados ao CERT.br



Tipos de ataque – 2013

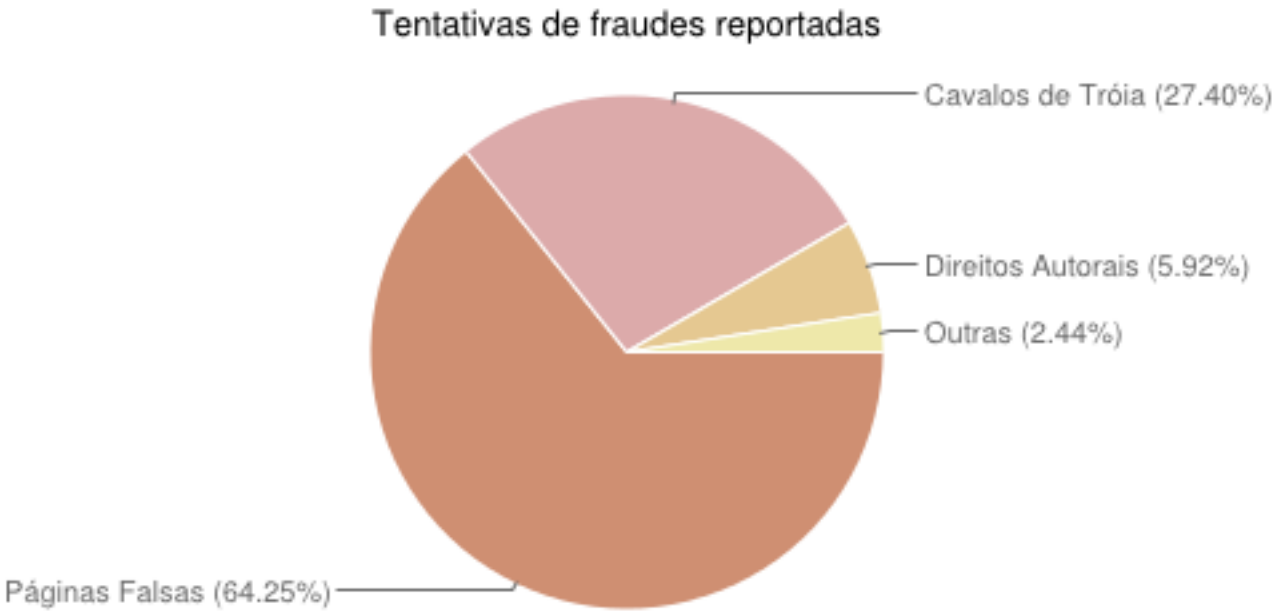
- **Contra usuários finais**
  - **mais fácil e rentável**
  - **motivações: financeira, espionagem, sabotagem**
  - **aplicações Web vulneráveis com rápido crescimento nos últimos anos**
  - ***drive-by download: sites* principais da Vivo, Oi e Ambev**

Scans reportados – 2013



- **Força bruta**
  - **contra serviços de rede: SSH, FTP, Telnet, VNC, etc.**
  - **alvos: senhas fracas, senhas padrão, contas temporárias**
  - **acesso a servidores, roteadores, *modems* banda larga, etc.**
  - **pouca monitoração permite ao ataque perdurar por horas/dias**

Tentativas de fraudes – 2013



- **Retorno de páginas falsas**
  - **via *spams* em nome de instituições financeiras e/ou *de e-commerce***
  - **muitas envolvem alteração do arquivo *hosts* das máquinas**
- ***Spams* em nome de diversas entidades/temas variados**
  - ***links* para *trojans* hospedados em diversos *sites***
  - **vítima raramente associa o *spam* com a fraude**

Tendências

Uso de *botnets*

- **Base muito grande de computadores com *software* desatualizado/ vulnerável sendo ativamente abusada por criminosos**
  - **especialmente em países em desenvolvimento**
- **Uso de *botnets:***
  - **DDoS**
  - **extorsão**
  - ***download* de outros tipos de *malware***
  - **furto de informações**
  - **proxies abertos**
    - **envio de *spam***
    - **navegação anônima**

Ataques a servidores Web

- **Muitas vulnerabilidades de *software***
  - ***softwares* de CMS desatualizados**
    - **Wordpress, Joomla**
  - **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**
  - **"Aumente a segurança de websites com Wordpress"**

    http://www.security.unicamp.br/artigos/23-seguranca-site-wordpress.html

2º Fórum Brasileiro de CSIRTs

www.cert.br/forum2013/agenda/

Reader

Anatomy of Operation Ababil - DDoS attacks targeting US Banks [

[Slides]

André Corrêa, Senior Security Analyst

PhishLabs Security Operations

iosos na Rede do Gover

ação e Comunicação do Pa

Using Joomla? Your website might ha... taken part in DDoS attack – HKCERT

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

Reader

Security Blog

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

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

Reader

ars technica

HEAD TO TOE GUIDE OF THE SEASON

MAIN MENU ▾ MY STORIES: 24 ▾ FORUMS SUBSCRIBE JOBS ARSCOIN STORE

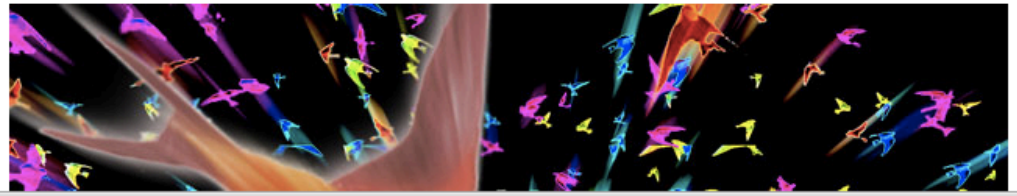
RISK ASSESSMENT / SECURITY & HACKTIVISM

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



Outros ataques em rápido crescimento (1/2)

- "*Modems*" e roteadores banda larga (CPEs)
  - *botnets* usadas para ataques diversos
    - comprometidos via força bruta (telnet)
    - vários modelos permitem reset via WAN – Post na porta TCP/80
  - comprometimento para alteração do serviço DNS para
    - fraudes financeiras
    - redirecionamento para obter "cliques" de propaganda
    - DDoS

- Dispositivos com sistema Android
  - *botnets*
  - fraudes e outros tipos de *malware*
  - *Pocket Botnets*

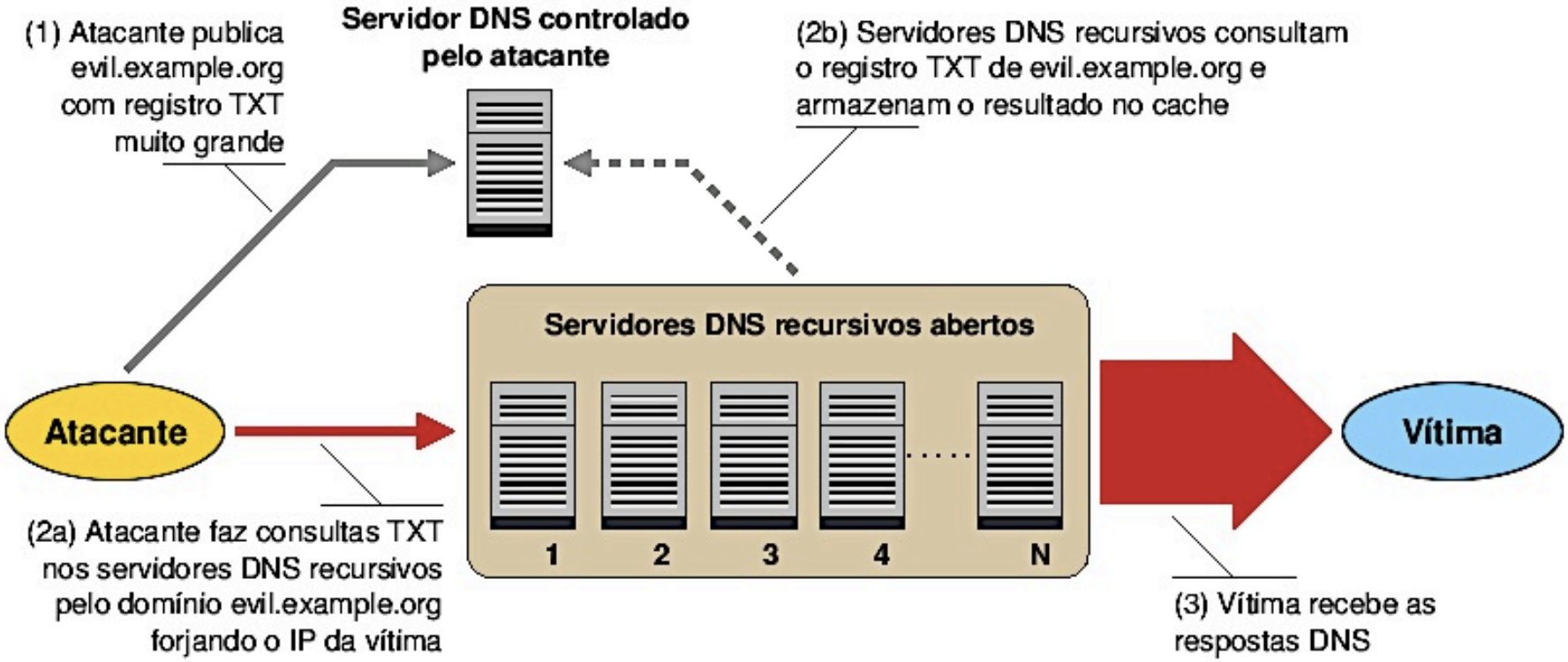
Outros ataques em rápido crescimento (2/2)

- **Ataques a serviços de rede:**
  - **não tão frequentes, mas com grande impacto por serem contra a infra-estrutura 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**

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

Foco dos ataques continua sendo

Serviços *Online*

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

Foco dos ataques continua sendo

Clientes/Usuários

- Internet passou a fazer parte do dia-a-dia
- Usuários não são especialistas
- Grande base
  - de dispositivos vulneráveis
  - com banda disponível
- Mais fáceis de atacar
- Grande exposição de dados pessoais
- Possuem dados de valor
  - dados financeiros
  - endereços de *e-mail* válidos
  - credenciais de acesso
- BYOD
- Dispositivos podem ser usados para ataques (*spam*, *botnets)*

Desafios

Reais Causas dos Problemas (1/2)

- **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**

Reais Causas dos Problemas (2/2)

- **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"**

- **Dificuldade de identificação dos ataques:**
  - **ataques partem de vítimas na maioria absoluta dos casos**

- **Criminosos estão apenas migrando para onde os negócios estão**

Mercado negro (1/2)

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

Mercado negro (2/2)

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**

"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 up

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

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**
  - **profissional com sólida formação tem mais sucesso em usar 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 *trojans* instalados em sua infraestrutura**

Desafios para a Melhora do Cenário como um Todo

Desafios (1/3)

- **Só haverá melhorias quando:**
  - **o processo de desenvolvimento de *software* incluir**
    - **levantamento de requisitos de segurança**
    - **testes que incluam casos de abuso (e não somente 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**
  - **os sistemas para usuários finais forem menos complexos**
    - **mudança total de paradigma de uso da tecnologia**

Desafios (2/3)

- **Há falta de pessoal treinado no Brasil para lidar com Redes e com segurança em IPv4**
  - **a falta de pessoal com essas habilidades em IPv6 é ainda mais gritante**
  - **IPv6 não pode mais ser ignorado**
- **Vencer a cultura de que é melhor investir em tecnologia do que treinamento e implantação de boas políticas**
  - **quantas instituições realmente implementam tecnologias com base em uma análise de risco?**
- **Ir além do "*compliance*"**
  - **Target**
- **Investir em treinamento e conscientização de usuários finais**

Desafios (3/3)

- São necessários novos métodos de detecção
  - Foco atual do mercado é:
    - no que entra em uma rede, ou
    - no que é conhecidamente malicioso
      - "*Intrusion Detection*"
        - » IDS / IPS, *Firewall,* Antivírus
  - Foco precisa ser:
    - no que sai, ou
    - no tráfego interno:
      - "*Extrusion Detection*"
        - » *Flows, Honeypots, Passive* DNS
        - » Notificações de incidentes
        - » *Feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)

Recomendações

Ataques de força bruta

- Reduzir o número equipamentos com serviço aberto
  - quanto mais máquinas expostas maior o risco
  - implementar rede de gerência
- Implementar filtragem de origem
  - permitir o acesso apenas de máquinas pré-determinadas
- Mover o serviço para uma porta não padrão
  - medida paliativa, não definitiva
  - permite reduzir a quantidade de ataques
- Elaborar política de senhas
- Permitir acesso somente via chaves públicas
- Aumentar a monitoração

Sugestões para defesa contra ataques de força bruta para SSH
http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/

Abuso de máquinas de usuários

- **Definição de política de uso aceitável**
- **Monitoração:**
  - **pró-ativa de fluxos**
  - **das notificações de abusos**
- **Ação efetiva junto ao usuário nos casos de:**
  - **detecção de *proxy* aberto ou**
  - **máquina comprometida**
- **Gerência de saída de tráfego com destino à porta 25/TCP para redução de *spam***

  http://www.antispam.br/admin/porta25/

Criar um CSIRT

- A redução do impacto de um incidente é consequência da:
  - agilidade de resposta
  - redução no número de vítimas
- O sucesso depende da confiabilidade
  - nunca divulgar dados sensíveis nem expor as vítimas
- O papel do CSIRT e dos profissionais de segurança é:
  - auxiliar a proteção da infra-estrutura e das informações
  - prevenir incidentes e conscientizar sobre os problemas
  - responder incidentes
  - retornar o ambiente ao estado de produção
- A pessoa que responde a um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - seguir políticas e preservar evidências

Acompanhamento de notificações

- Criar *e-mails* da RFC 2142 (security@, abuse@)
- Manter os contatos de Whois atualizados
  - o contato técnico deve ser um profissional que:
    - tenha contato com as equipes de abuso, ou
    - saiba para onde redirecionar notificações e reclamações
- Endereço do grupo de resposta a incidentes de segurança deve ser anunciado junto à comunidade
- Contas que recebem notificações de incidentes/abusos não podem barrar mensagens, pois:
  - antivírus podem impedir a notificação de *malware*
  - regras *antispam* podem impedir notificações de *spam* e *phishing*

Iniciativas de Conscientização

Portal Internet Segura

http://www.internetsegura.br/

INTERNET SEGURA.BR

Campanha Antispam.br

http://www.antispam.br/

Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no *site* (HTML5)
Dica do dia no *site*, via *Twitter* e RSS
http://cartilha.cert.br/

Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- *Internet Banking*
- Computadores
- Códigos Maliciosos

Acompanhados de *Slides* de uso livre para:

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**

Outros Materiais para Usuários Finais

Portal Internet Segura

- Reúne todas as iniciativas conhecidas de educação de usuários no Brasil

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/

Cartilha de Segurança para Internet – Dica do Dia

RSS

http://cartilha.cert.br/rss/cartilha-rss.xml

Twitter

http://twitter.com/certbr

Site

http://cartilha.cert.br/

Cartilha de Segurança para Internet – Tradução

- Site em espanhol
- Fascículos:
  - Redes Sociales
  - Contraseñas
  - Privacidad

Perguntas?

Miriam von Zuben
miriam@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

cgi.br
Comitê Gestor da Internet no Brasil