

Códigos maliciosos e o (sub)mundo *das botnets*

Lucimara Desiderá

lucimara@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil



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

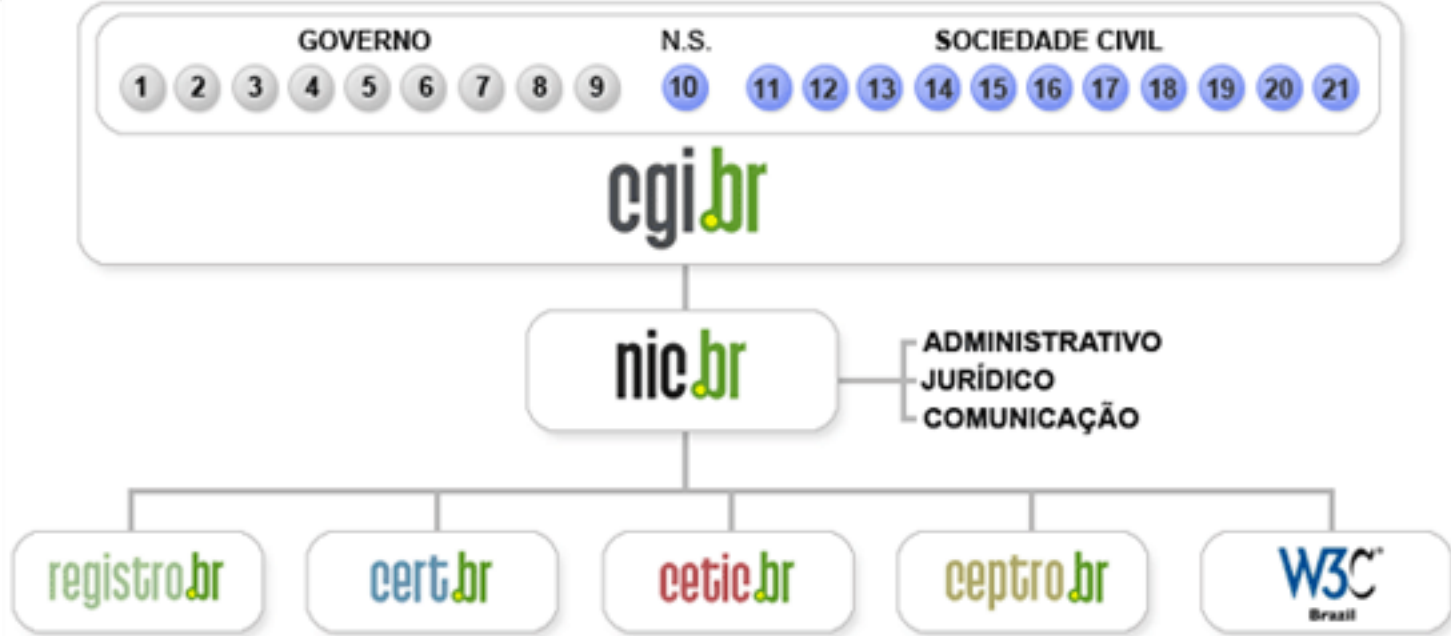


Criado em 1997 para:

- 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

<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

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/>

Agenda

- **Códigos maliciosos**
- ***Botnets***
 - **Motivações**
- **Combate a *botnets***
- **Prevenção e Boas Práticas**

Códigos maliciosos (*malware*)

Códigos Maliciosos

- **Malware:** programa especificamente desenvolvido para executar ações danosas e atividades maliciosas em um computador

Vírus

Backdoor

Worm

Trojan

Spyware

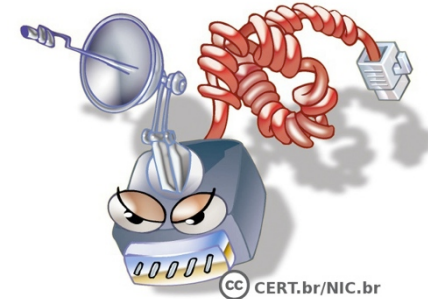
Rootkit

Bot



Bot

- Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador



- Dispõe de mecanismos de comunicação com o invasor
 - permitem que seja controlado remotamente

- Terminologia:

- Computador infectado → zumbi / bot



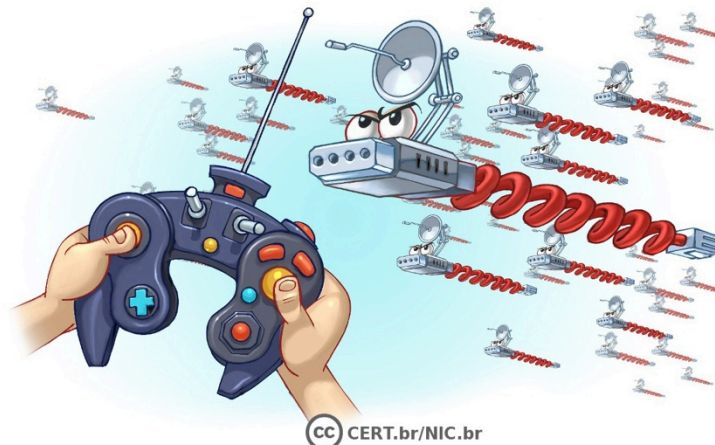
Propagação

- **Exploração de vulnerabilidades**
Ex: página *Web* com navegador vulnerável
- **Ação direta de atacantes**
- **Execução de arquivos**
 - *download* na *Web*
 - redes sociais
 - *links* ou anexos de mensagens eletrônicas (*e-mail*, *IM*)
 - compartilhamento de recursos (ex: *P2P*, mídias removíveis)
 - auto-execução de mídias removíveis infectadas

Botnets

Botnet

- Rede formada por centenas/milhares de computadores zumbis
 - remotamente controlada
 - permite potencializar a ação danosa dos *bots*
 - quanto mais *bots* mais potente é a *botnet*
- Terminologia:
 - *Herder, master* → Controlador da botnet
 - *Command and Control (C&C)* → comando e controle → computador usado para comunicação entre o controlador e os zumbis



Comando e Controle

- **Comunicação**
 - IRC
 - HTTP
 - P2P
- **Tendências de gerenciamento e defesa**
 - **Novos mecanismos de troca de mensagens**
 - *DNS covert channel*
 - *ICMP*
 - **Twitter / Facebook**
 - **Criptografia**
 - **Ofuscação**
 - **Autenticação**
 - *Fast-flux service networks*
 - *Domain Generation Algorithms (DGA)*

Usos



- **Coleta de informações**

- dados pessoais
- espionagem

- **Ataques de negação de serviço (DDoS)**

- ativismo político
- extorsão

- **Envio de *spam* e *phishing***



- **Propagação de código malicioso**

- *Pay per Install (PPI)*
- *Trojan, worm, spyware, adware*

- ***Click Fraud***



Motivações

Motivações

- Desejo de autopromoção
- Política / Ideológica
- **FINANCEIRA**
 - mercado negro

```
12:31 < > /\ Selling Dumps Track 1 & 2 With Pin /\ Selling Shop Admin US With Big
& Samll Daily Order /\ Selling Serial Camfrog & Paltalk /\ Selling
Software Find Fresh Maillist Perfect /\ Selling Shell C99 /\ Selling Root
/\ ~ I ACCEPT ONLY .
12:31 * Chkon msr206 msg now
12:32 < > selling Account SMTP inbox (send to your inbox for test)...also selling US
& UK maillist...selling Host Support Cpanel+Ftp...selling SMTP scanner &
Ssh Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY for serious buyer
payment only ( RIPPER ) !!!
12:32 < > - Set your timers on , using => " /timer 0 50 /msg your message here
" Enjoy your stay!!
12:32 * Selling Fresh Dumps, Cvv2 & Fullz. USA / CAN / UK / Europe. Spammed &
Hacked Shop Admin. Accepting + + .
12:32 * I Can CASHOUT Uk Cvv With DOB,
12:32 < > selling Account SMTP inbox (send to your inbox for test)...also selling US
& UK maillist...selling Host Support Cpanel+Ftp...selling SMTP scanner &
Ssh Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY for serious buyer
payment only ( RIPPER ) !!!
```

Motivações - Mercado Negro (cont.)

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

Motivações - Mercado Negro (cont.)

- SOCKS bot (to get around firewalls): \$100
- Email spam: \$10 per one million emails
- Email spam (using a customer database): \$50-\$500 per one million emails
- SMS spam: \$3-\$150 per 100-100,000 messages
- ZeuS source code: \$200-\$500
- Windows rootkit (for installing malicious drivers): \$292
- Hacking Facebook or Twitter account: \$130
- Hacking Gmail account: \$162
- Hacking corporate mailbox: \$500

Distributed Denial-of-Service Service Prices

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

Botnet Prices

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

Pay-per-Install Service Prices

Offering	Price per 1,000 Downloads
Australia (AU)	US\$300-550
Great Britain (UK)	US\$220-300
Italy (IT)	US\$200-350
New Zealand (NZ)	US\$200-250
Spain (ES), Germany (DE), or France (FR)	US\$170-250
United States (US)	US\$100-150
Global mix	US\$12-15
European mix	US\$80
Russia (RU)	US\$100

Combate a *botnets*

Técnicas de mitigação mais conhecidas

- **Foco na disruptura das comunicações entre C&C e bots**
 - **Contramedidas baseadas em DNS**
 - ***Takedown* de servidores *Command-and-Control***
 - **Filtragem de pacotes**
- **Foco no bloqueio das ações dos zumbis**
 - **Listas de bloqueio de enderecos IPs infectados**
 - **Gerenciamento de Porta 25**

Atividades de mitigação no Brasil

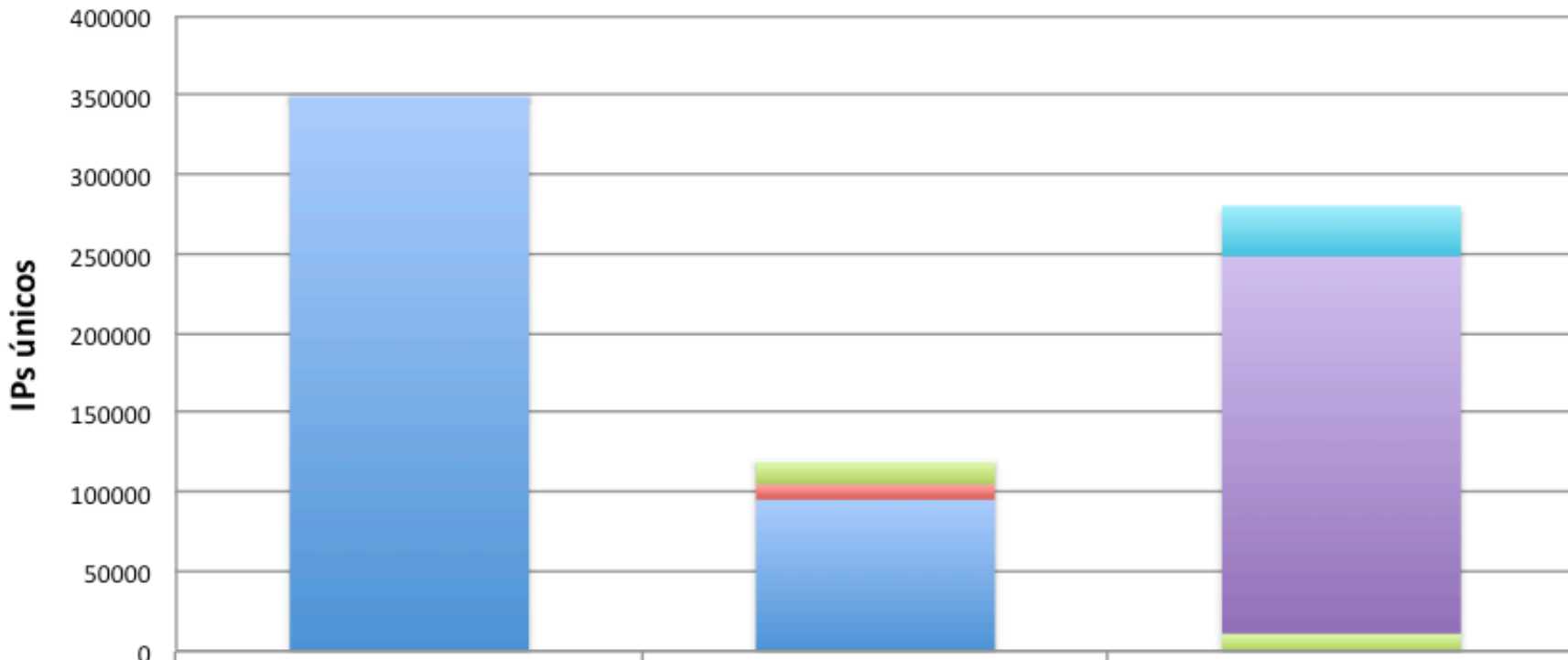
- Campanha de Gerencia de Porta 25 e Antispam.br
 - <http://antispam.br/porta25/>
 - Brasil não está mais no topo das listas de *spammers*:
 - **CBL**: <http://cbl.abuseat.org/country.html>
 - 2009: 2º Nov 2012: 3º Dez 2013: 19º (31º em Ago/2013)
 - **Cisco**:
 - 2009: Artigo da Forbes: “*Brazil: The New Spam King*”
 - 2014 Annual Security Report – não está na lista
 - **Dirty Dozen – Sophos** (<http://nakedsecurity.sophos.com/tag/dirty-dozen/>)
 - Q3-2010: 2º Q1-2013: não está na lista
 - **Kaspersky**
 - Q3-2012: 5º Q3-2013: não está entre os Top 20
 - Spam in Q3 2012 http://www.securelist.com/en/analysis/204792251/Spam_in_Q3_2012
 - Spam in Q3 2013 http://www.securelist.com/en/analysis/204792311/Spam_in_Q3_2013

Atividades de mitigação no Brasil (cont.)

- **Registro.br: ações contra domínios maliciosos**
 - Ex: bloqueio do registro de domínios usados por variantes do Conficker
- **CERT.br: notificação de redes participantes em atividades relacionadas bots**
 - através da rede de honeypots
 - Ex: identificação de botnet com C&C em uma grande rede no Brasil
 - como parte de operações de takedown

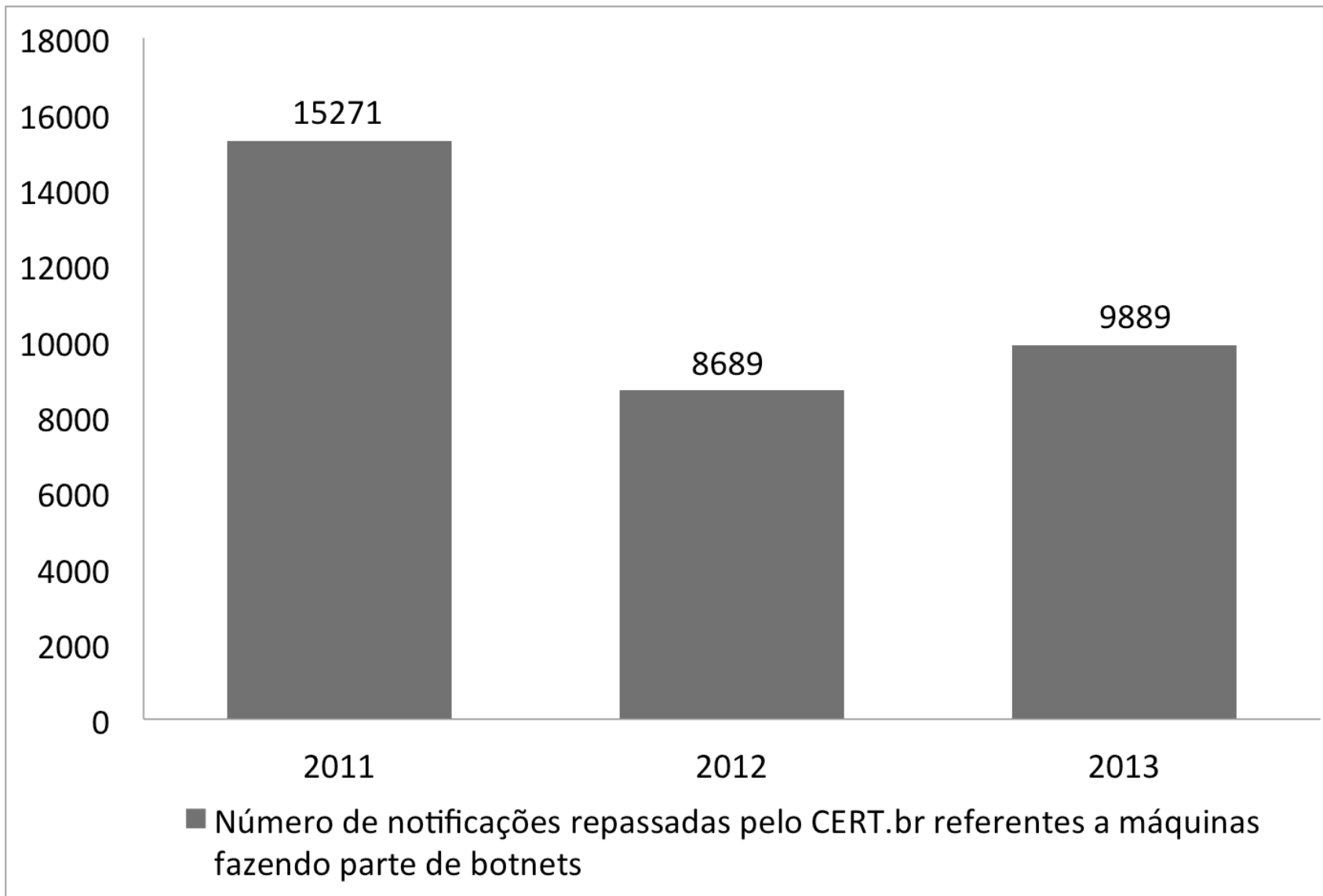
Combate – notificações recebidas da Microsoft

Takedowns pela Microsoft

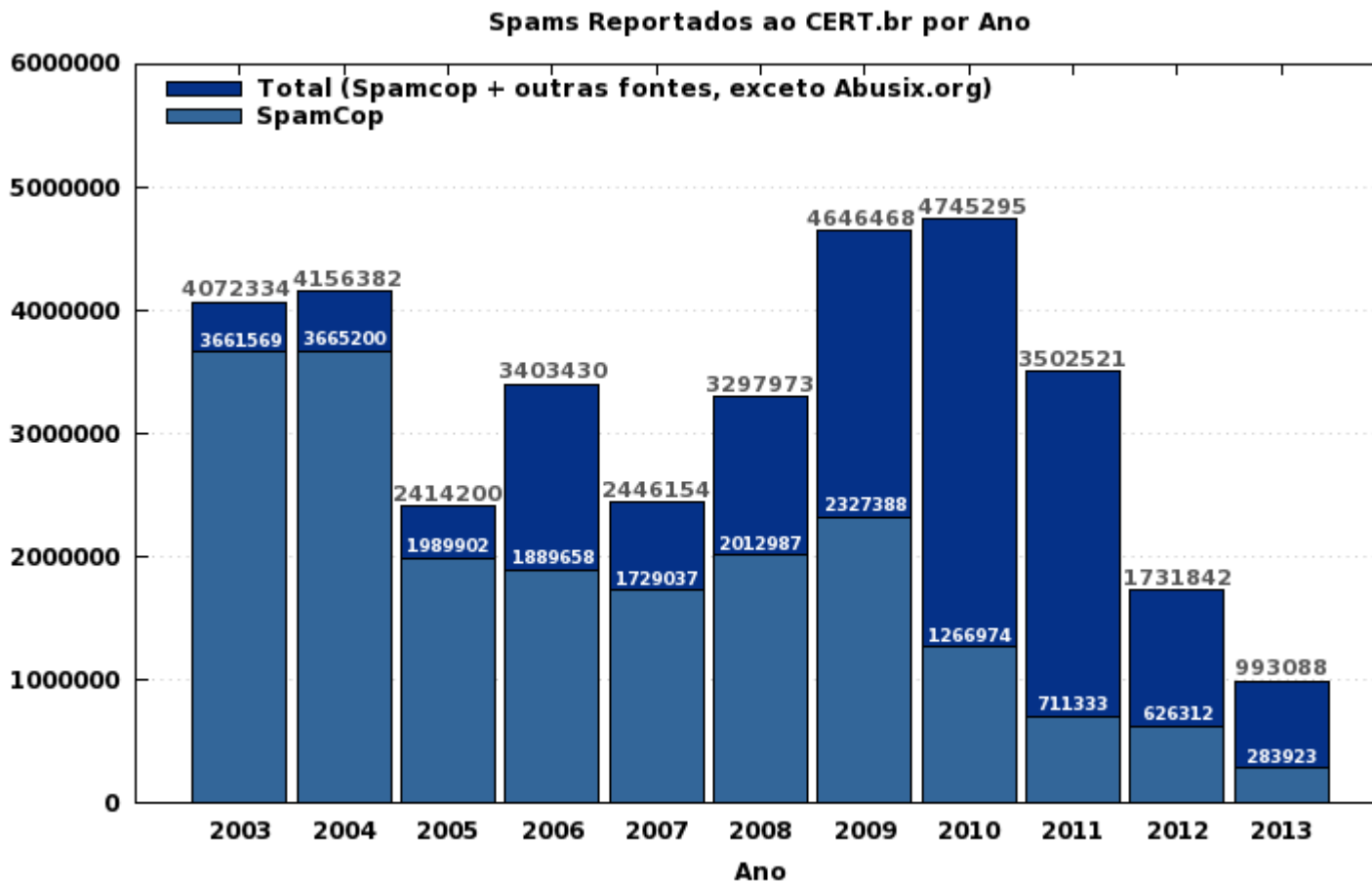


	2011	2012	2013
ZeroAccess	0	0	31757
Citadel	0	0	237626
Zbot	0	13732	10903
Nitol	0	9668	0
Rustok	348830	95371	0

Notificações repassadas pelo CERT.br



Combate



Fonte: Estatísticas CERT.br – <http://www.cert.br/stats/spam/>

Redução no volume de *spam* pode ser consequência do combate às botnets

<http://idgnow.uol.com.br/internet/2013/01/23/derrubada-de-botnets-diminui-drasticamente-numero-de-spams/>

Prevenção e Boas Práticas



Proteção

- **Técnicas correntes de mitigação não são suficientes:**
 - usuários continuam infectados
 - prevenção depende de ação conjunta
 - administradores de redes
 - usuários finais, etc.

Faça a sua parte!!!!

Administrador: Mitigar as atividades maliciosas

- **Implementar melhores práticas:**
 - **BCP 38 / BCP 84**
 - filtrar pacotes com endereços “*spoofados*”
 - impedir a participação dos zumbis em:
 - ataques de DDoS, amplificação
 - outros ataques que usem pacotes *spoofados*

<http://bcp.nic.br/entenda-o-antispoofing/>
 - **Gerência de Porta 25**
 - impedir que zumbis sejam usados para entrega direta de *spam*
 - detectar máquinas infectadas

<http://www.antispam.br/admin/porta25/>
 - **Configuração adequada de servidores DNS recursivo**
 - Mitigar ataques como envenenamento de cache e negação de serviço/ amplificação.

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

Usuário: Proteja seu Computador

- **Mantenha seu computador seguro:**
 - com todas as atualizações aplicadas
 - com todos os programas instalados com as versões mais recentes
- **Use mecanismos de segurança**
 - *firewall* pessoal, *antimalware*, *antiphishing*, *antispam*
 - complementos, extensões, *plugins*
- **Use apenas programas originais**
- **Use as configurações de segurança disponíveis**
- **Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros**

Usuário – Mantenha Postura Preventiva

- **Não acesse *sites* ou siga *links***
 - recebidos de mensagens eletrônicas
 - em páginas sobre as quais não se saiba a procedência
- **Não confie apenas no remetente da mensagem, pois ela pode ter sido enviada de:**
 - máquinas infectadas
 - contas falsas ou invadidas
- **Proteja sua privacidade, evite divulgar:**
 - dados pessoais ou de familiares e amigos
 - informações sobre seu cotidiano
 - informações sensíveis, como:
 - senhas
 - números de cartão de crédito

Usuário: Proteja suas Contas e Senhas

- **Evitar usar o usuário “administrador”**
- **Ao elaborar senhas:**
 - **utilizar:**
 - grande quantidade de caracteres
 - diferentes tipos de caracteres
 - números aleatórios
 - **não utilizar:**
 - sequências de teclado
 - dados pessoais:
 - nome, sobrenome, contas de usuário, números de documentos, placas de carros, números de telefones
 - informações que possam ser coletadas em *blogs* e redes sociais
 - palavras que façam parte de listas
 - nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc.
- **Trocar regularmente as senhas**
- **Não utilizar a mesma senha para todos os serviços**

Cartilha de Segurança para Internet

- Livro (PDF e ePub) e conteúdo no *site* (HTML5)
- Licença Creative Commons

<http://cartilha.cert.br/>

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



Twitter

<http://twitter.com/certbr>



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/>



Perguntas?

Lucimara Desiderá - lucimara@cert.br

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



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