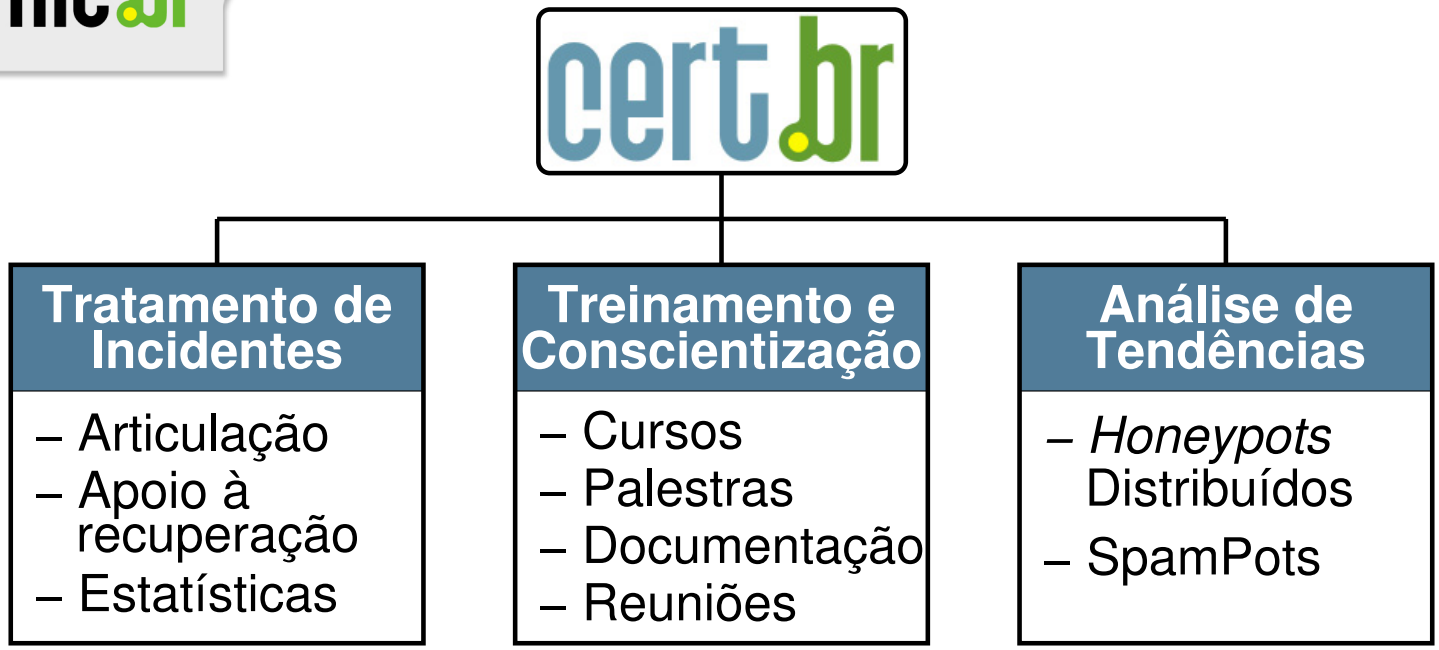
Códigos maliciosos e o (sub)mundo *das botnets*

Lucimara Desiderá

lucimara@cert.br

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



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

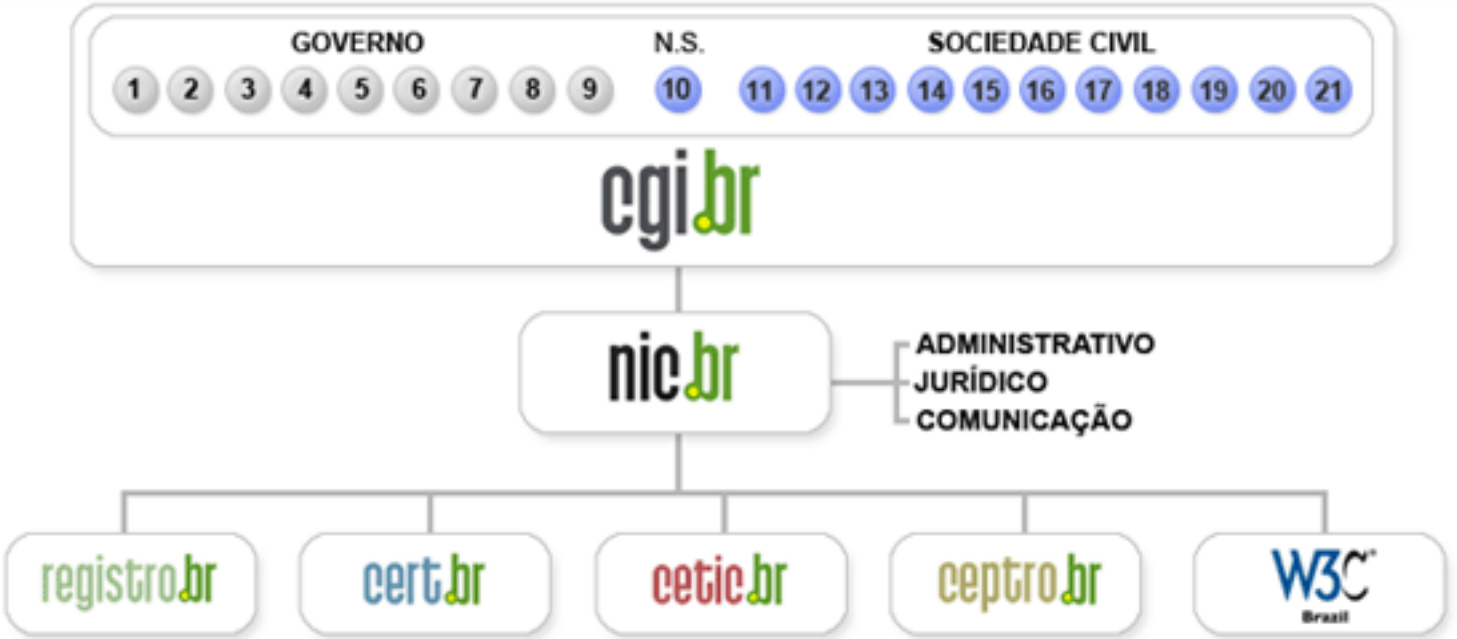
The Honeynet PROJECT

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**

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

Worm

Spyware

Bot

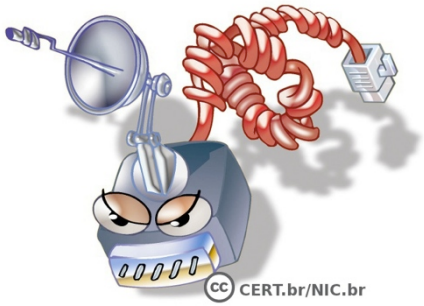
Backdoor

Trojan

Rootkit

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**

Propagação

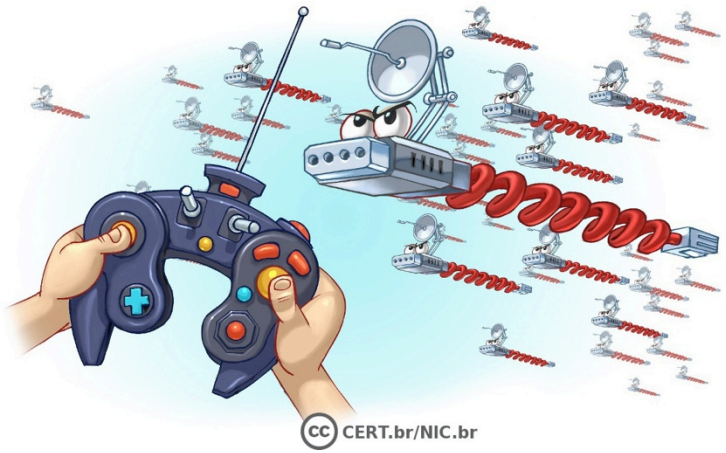
- **Exploração de vulnerabilidades**

  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

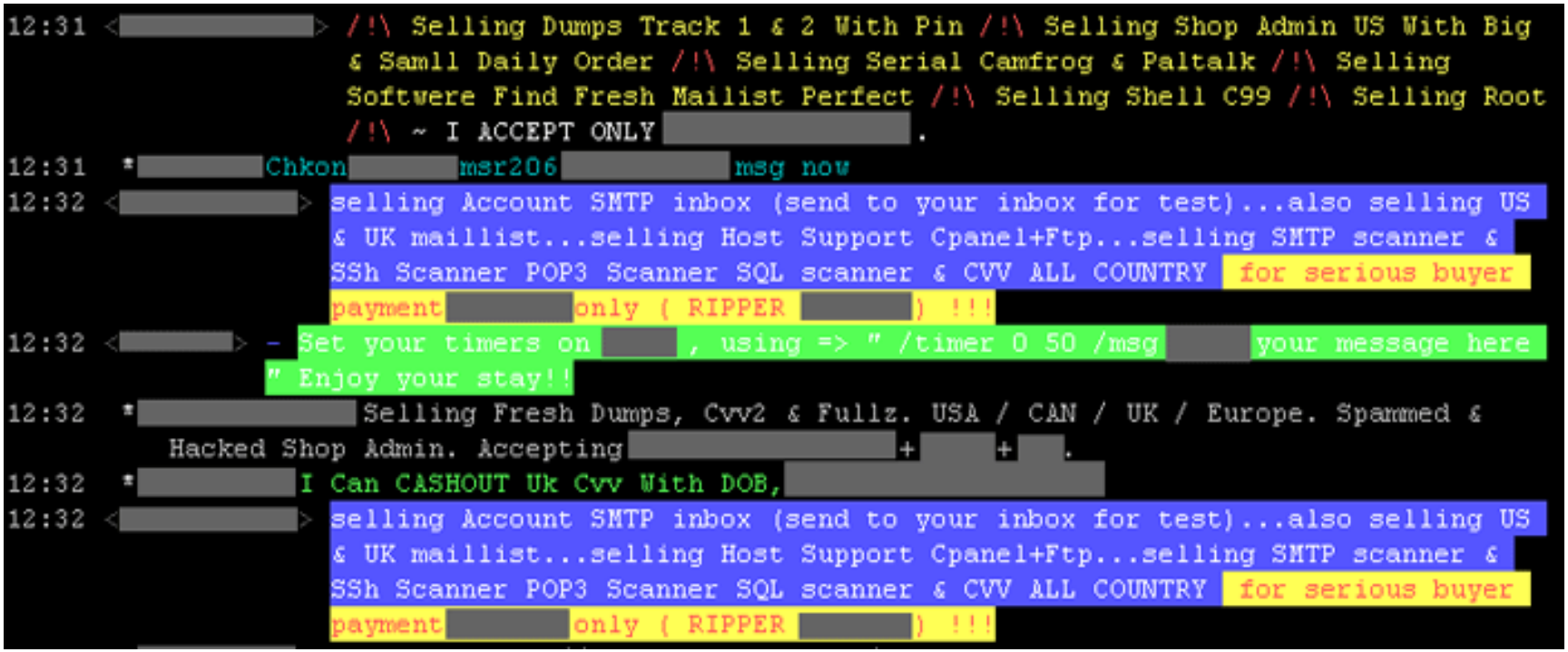
- **Coleta de informações**
  - **dados pessoais**
  - **espionagem**
- **Ataques de negação de serviço (DDoS)**
  - **ativismo político**
  - **extorsão**
- **Envio de *spam* e *phishing***

- **Propagação de código malicioso**
  - ***Pay per Install (PPI)***
  - ***Trojan*, *worm*, *spyware*, *adware***
- ***Click Fraud***

Motivações

Motivações

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



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.)

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

Fonte:Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

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**

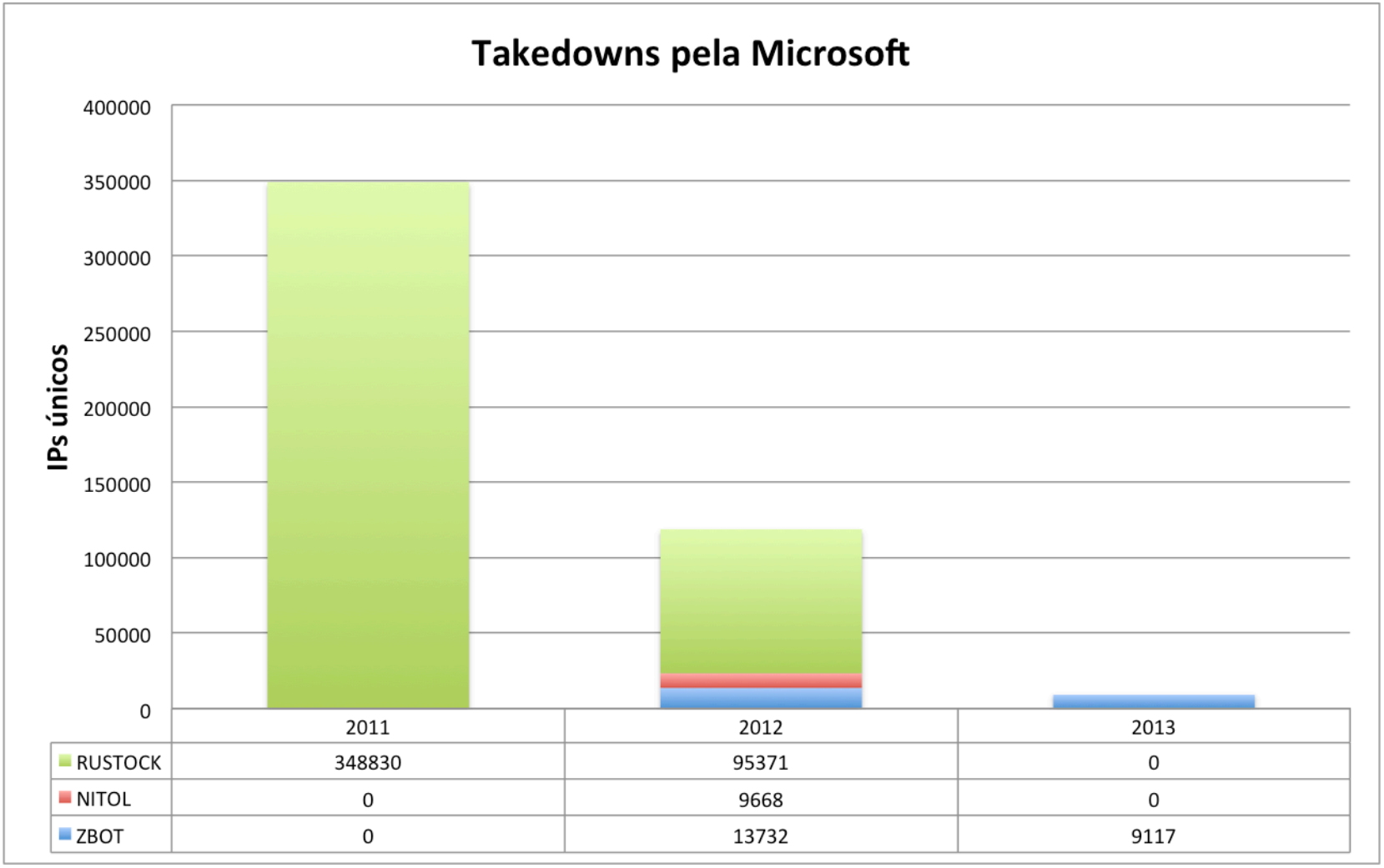
Atividades de mitigação no Brasil

- Campanha de Gerencia de Porta 25 e Antispam.br
  - http://antispam.br/porta25/
  - Brasil não está mais no topo da lista CBL
    http://cbl.abuseat.org/country.html
    http://www.nic.br/imprensa/clipping/2013/midia182.htm

- Registro.br: ações contra domínios maliciosos
  - Ex: bloqueio do registro de domínios usados por variantes do Conficker

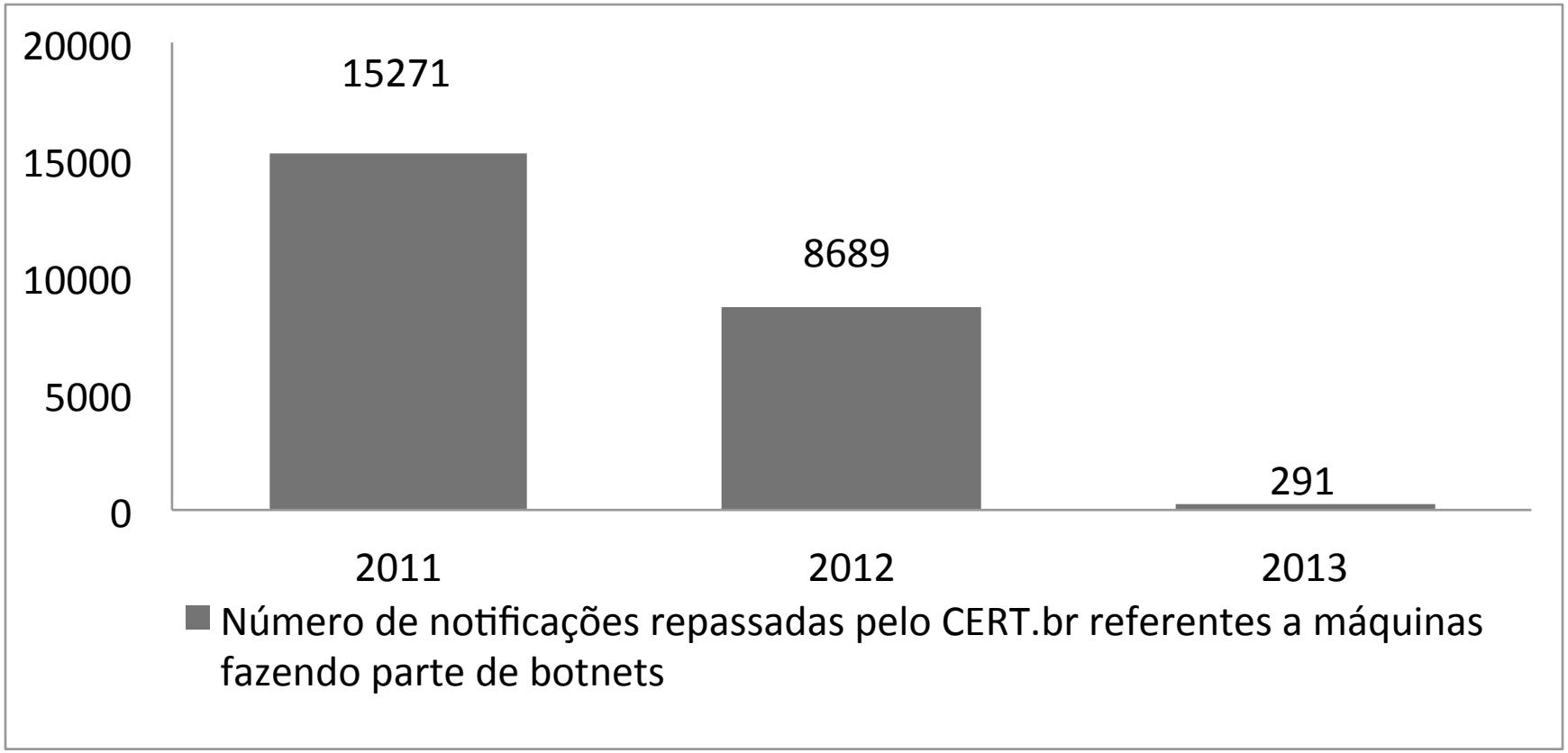
- CERT.br: notificação de redes participantes em atividades relacionadas bots
  - através da rede de honeypots
  - como parte de operações de takedown

Combate – notificações recebidas da Microsoft

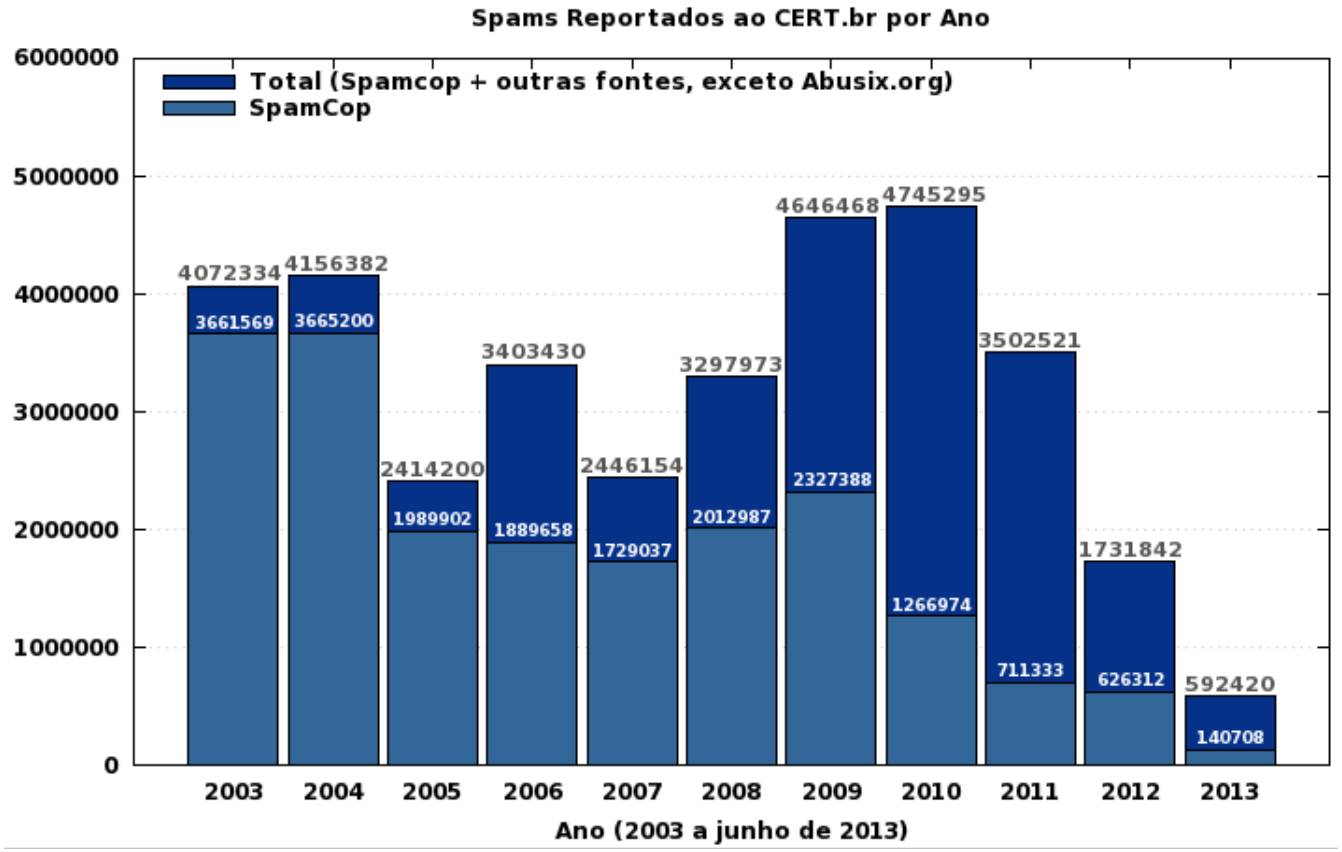


	2011	2012	2013
RUSTOCK	348830	95371	0
NITOL	0	9668	0
ZBOT	0	13732	9117

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

Informe-se e Mantenha-se Atualizado

Portal Internet Segura

http://www.internetsegura.br/

INTERNET SEGURA.BR

Campanha Antispam.br

http://www.antispam.br/

Cartilha de Segurança para Internet 4.0

2ª Edição do Livro

Novas recomendações, em especial sobre:

- segurança e privacidade em redes sociais
- segurança no uso de dispositivos móveis

Reestruturada

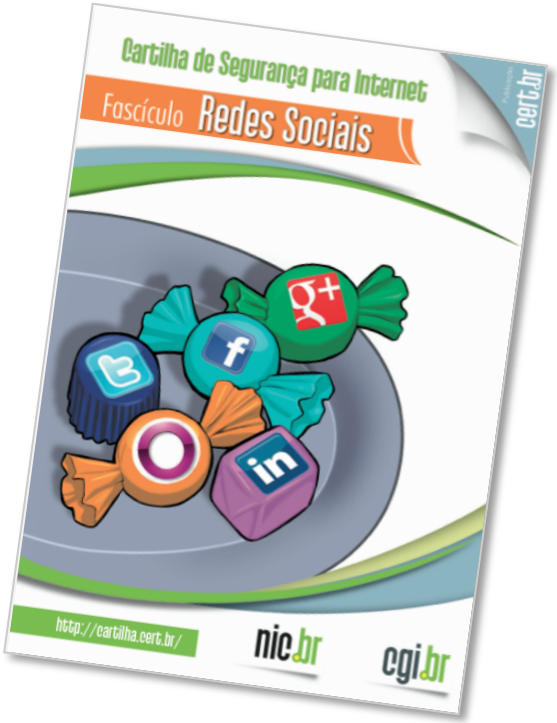
- ilustrada
- em HTML5
- formato EPub

Nova licença

- *Creative Commons* (CC BY-NC-ND 3.0)

Cartilha de Segurança para Internet – Fascículos

Organizados e diagramados de forma a facilitar a difusão de conteúdos específicos



***Slides* de uso livre para:**

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**
- **licença CC BY-NC-SA 3.0 Brasil**

Redes Sociais – 08/2012

Senhas – 10/2012

Comércio Eletrônico – 11/2012

Privacidade – 02/2013

Dispositivos Móveis – 04/2013

Internet Banking – 06/2013

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/

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/