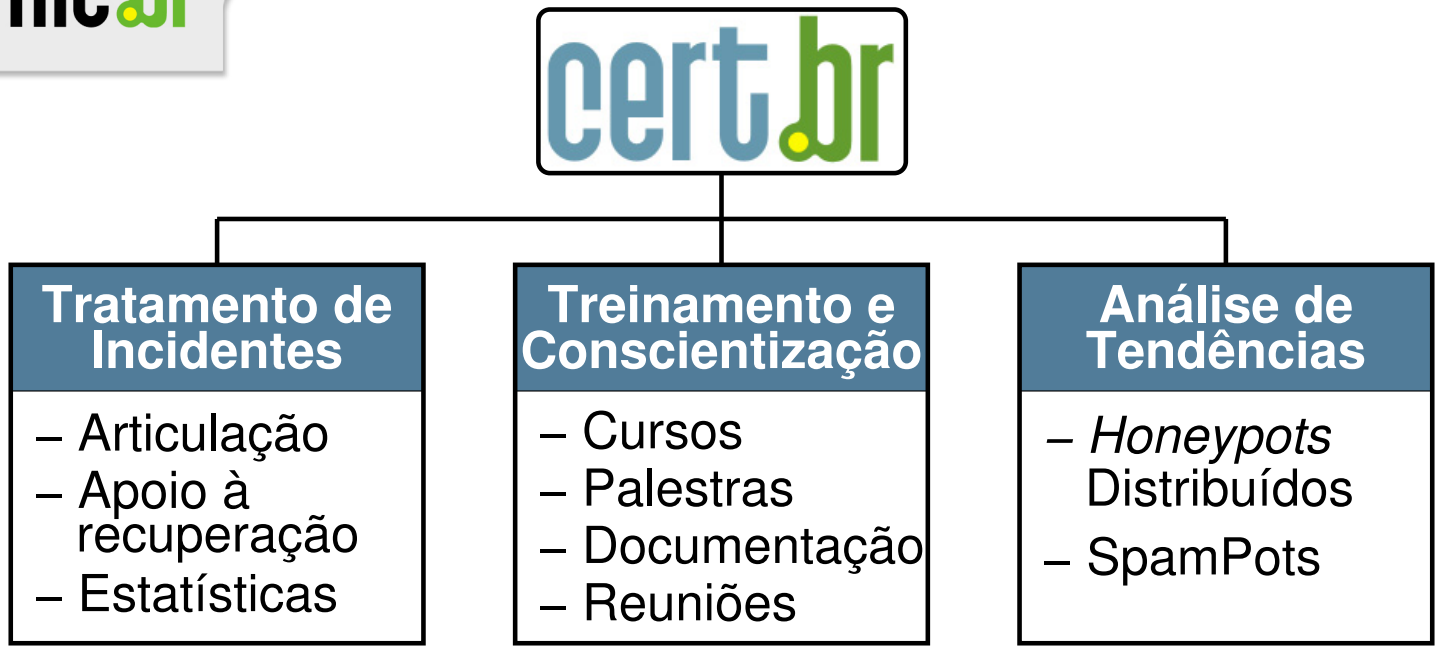
Códigos maliciosos e o (sub)mundo *das botnets*

Miriam von Zuben

miriam@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

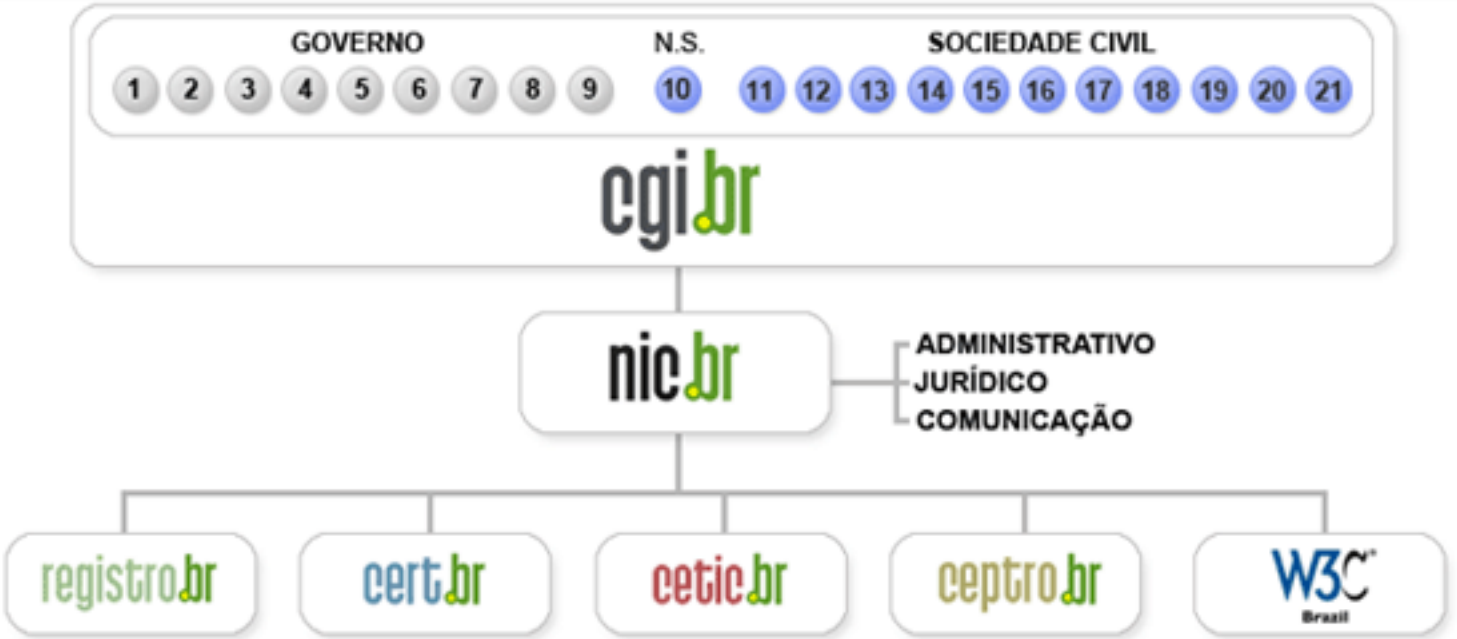
The Honeynet PROJECT

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;**

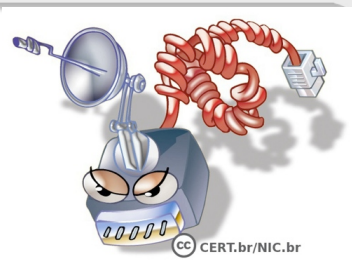
http://www.cgi.br/sobre-cg/

Agenda

- *Bots e Botnets*
  - definição
  - funcionamento básico
- Mercado negro
- Combate a *botnets*
- Boas práticas
  - administradores de redes
  - usuários finais

Bots e Botnets

Bot (1/2)



- **Tipo de código malicioso**
  - ***malware*: programa especificamente desenvolvido para executar ações danosas e atividades maliciosas em um computador**
    - **outros exemplos: vírus, *worm*, *spyware*, *backdoor* e *rootkit***
- **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**
  - **similar ao *worm* porém com capacidade de comunicação**
- **Terminologia:**
  - **Computador infectado ➔ zumbi**

Bot (2/2)

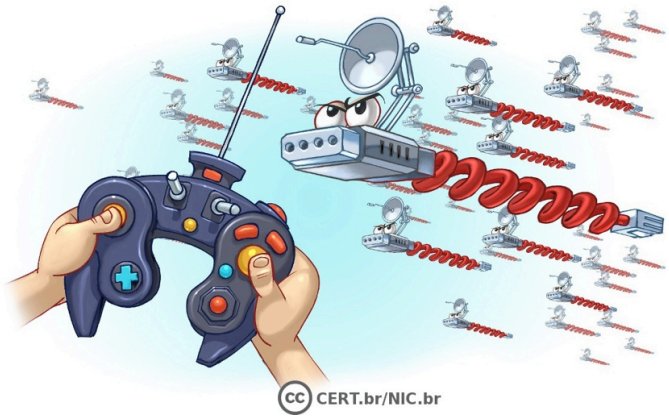
- **Zumbis podem ser:**
  - **computadores pessoais**
  - **dispositivos móveis (*tablets*, *smartphones*, celulares)**
  - **equipamentos de rede (roteadores, *modems)***

- **Formas de propagação**
  - **exploração de vulnerabilidades**
  - **ação direta de atacantes**
    - **contas/computadores/equipamentos invadidos**
  - **execução de arquivos**
    - ***download* na *Web***
    - **redes sociais**
    - ***links* ou anexos de mensagens eletrônicas (*e-mail*, IM, SMS)**
    - **compartilhamento de recursos (P2P, mídias removíveis)**
    - **auto-execução de mídias removíveis infectadas**

Botnet (1/2)

- **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***

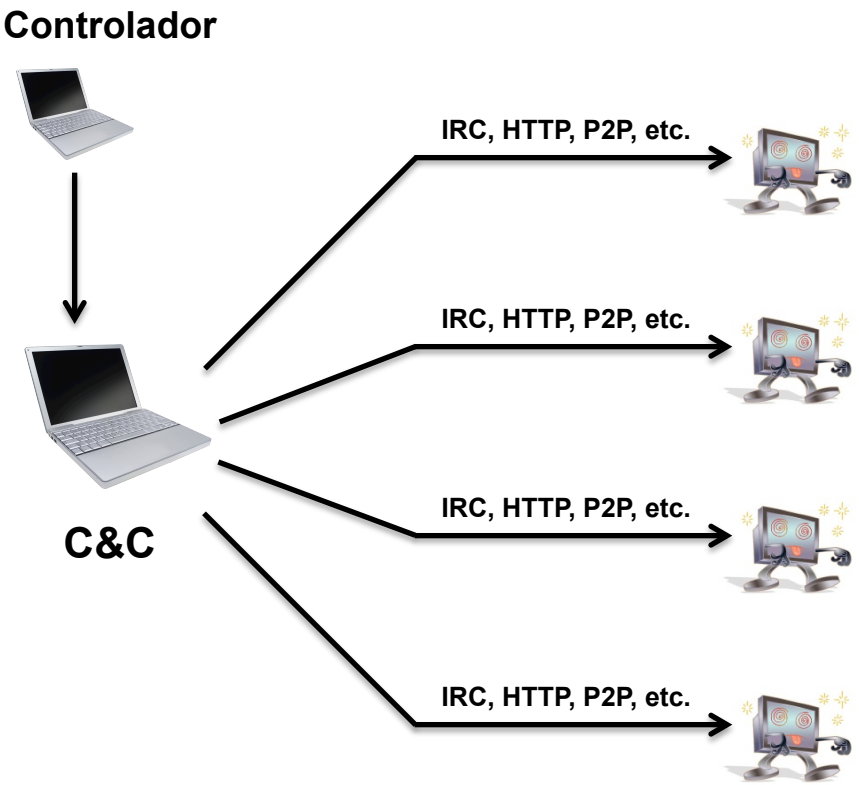
- **Terminologia*:***
  - **invasor ➔ controlador, *herder*, *master***
  - ***Command and Control* (C&C) ➔ comando e controle ➔ computador usado para comunicação entre o controlador e os zumbis**



Botnet (2/2)

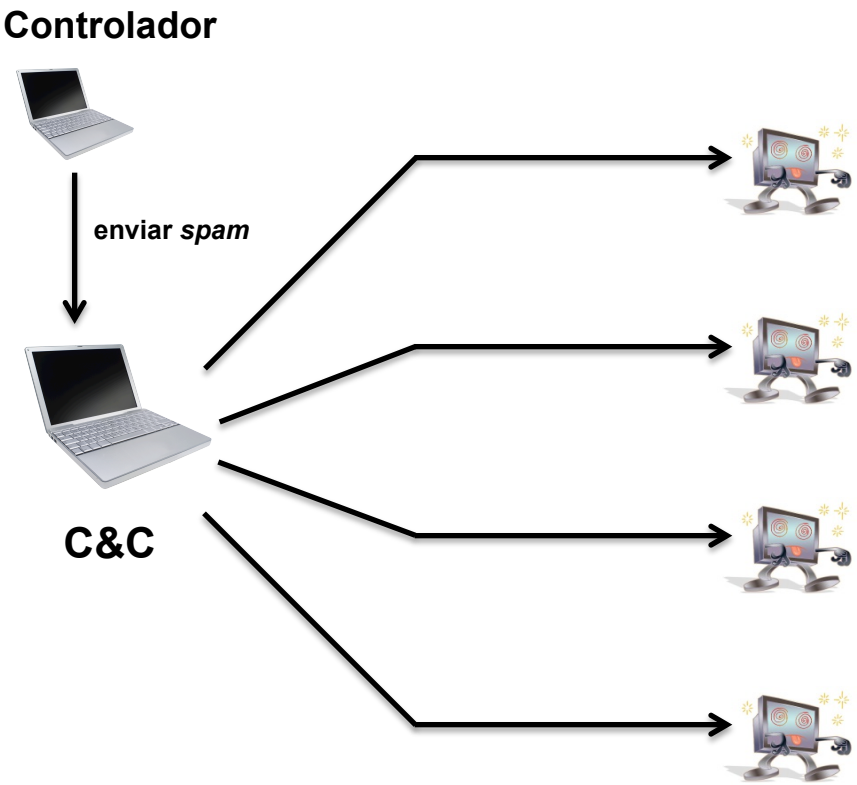
- **Atividades maliciosas:**
  - **coleta de informações pessoais**
  - **envio de *spam* e *phishing***
  - **propagação de códigos maliciosos**
  - ***click-fraud***
  - **desativação de mecanismos de segurança**
    - **antivírus*, antimalware, antispam***
  - **ataques de negação de serviço (DDoS)**
    - **ativismo político**
    - **extorsão**

Funcionamento básico (1/4)



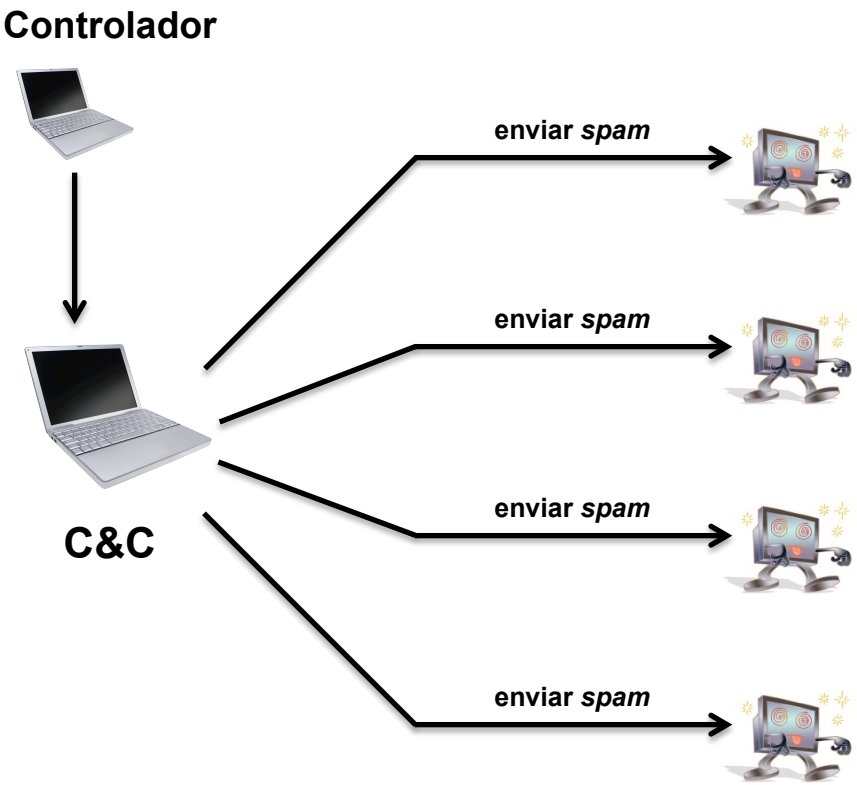
1. Zumbis ficam à espera dos comandos a serem executados

Funcionamento básico (2/4)



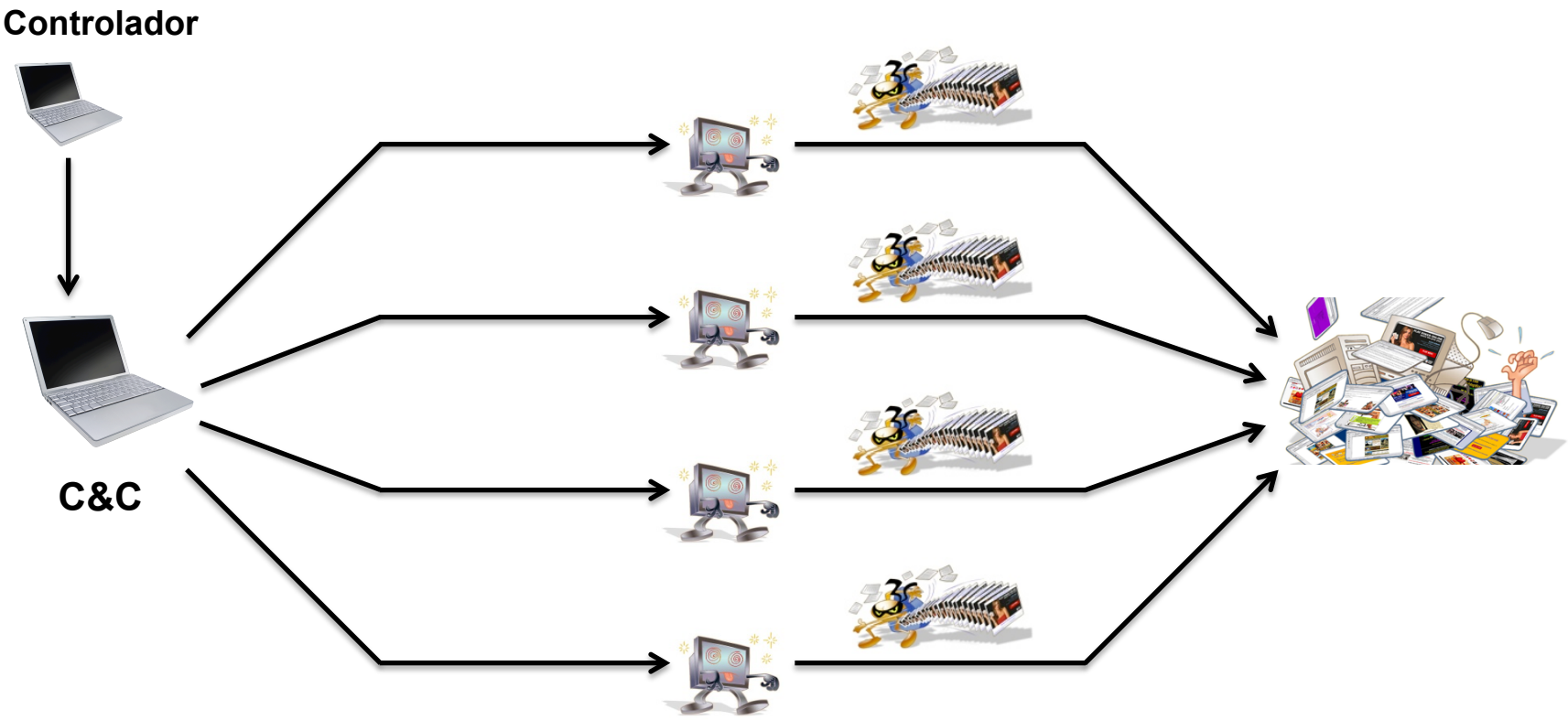
1. Zumbis ficam à espera dos comandos a serem executados
2. **Controlador envia ao C&C os comandos a serem executados (exemplo: envio de *spam*)**

Funcionamento básico (3/4)



1. Zumbis ficam à espera dos comandos a serem executados
2. Controlador envia ao C&C os comandos a serem executados (exemplo: envio de *spam*)
3. **C&C repassa os comandos aos zumbis**

Funcionamento básico (4/4)



1. Zumbis ficam à espera dos comandos a serem executados
2. Controlador envia ao C&C os comandos a serem executados (exemplo: envio de *spam*)
3. C&C repassa os comandos aos zumbis
4. **Zumbis executam os comandos pelo tempo determinado**

Tendências

- C&C
  - gerenciamento
    - DNS *covert channel*
    - *ICMP*
    - P2P (cada vez mais popular)
    - Twitter / Facebook
  - defesa:
    - criptografia, ofuscação, autenticação
    - *fast-flux service networks*
    - *Domain Generation Algorithms (DGA)*
- Exploração de CPEs
  - senhas padrão

Mercado Negro

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)

- 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

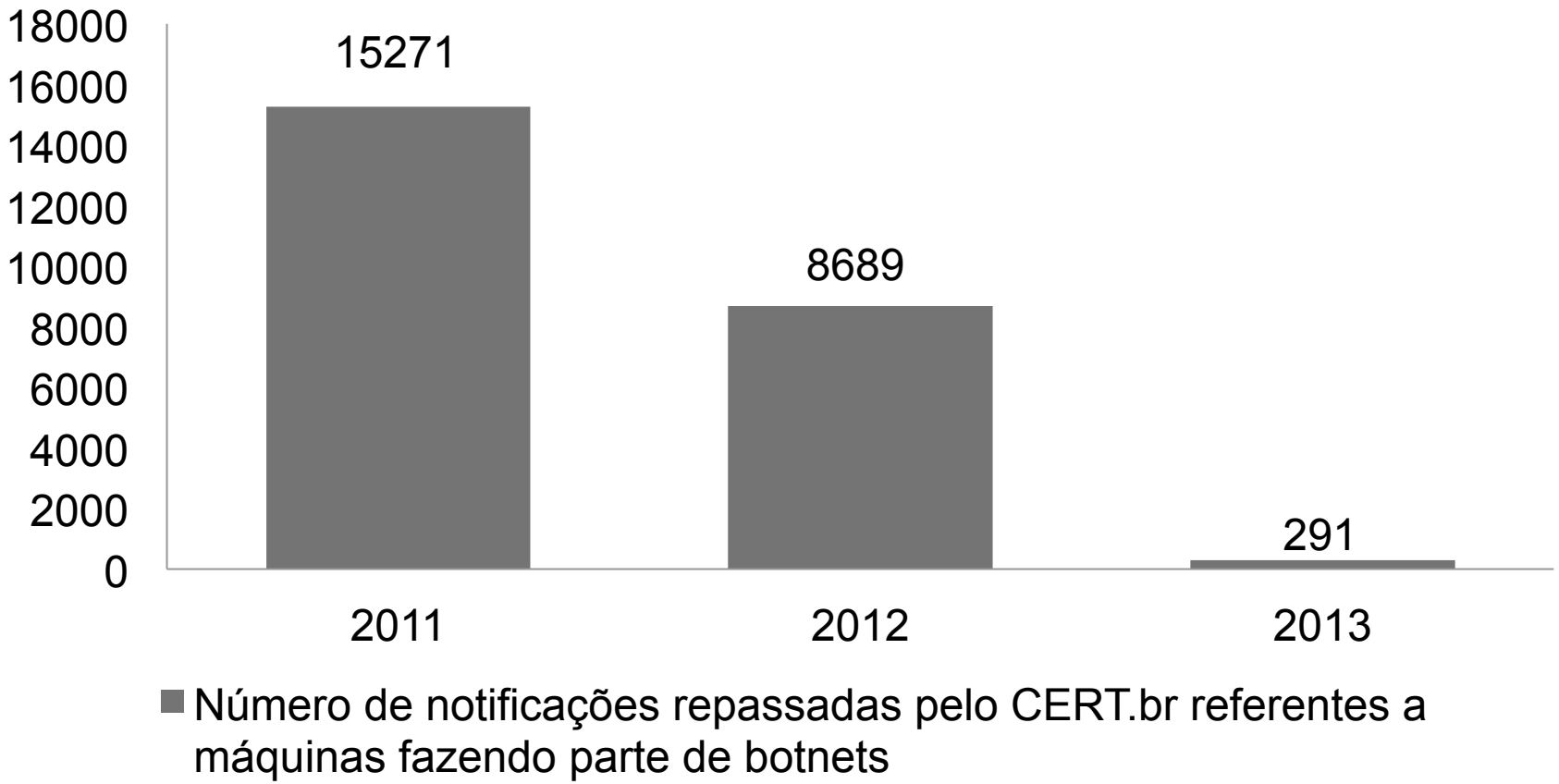
Combate a *botnets*

Takedown

- **Iniciativas de diversas empresas para desativar *botnets***
- **B*otnets* desativadas envolvidas no envio massivo de *spam***
- **Associado à redução da quantidade global de *spam***
- **O que fazer com a *botnet?***

2013	Bamital
2013	Virut
2012	Zeus
2011	Rustock
2011	Kelihos
2010	Mariposa
2010	Pushdo/Cutwail
2010	Bradolab
2010	Wadelac
2010	Mega-D/Ozdok
2009	Aurora

Notificações repassadas pelo CERT.br



Boas práticas

Proteção

- **A potência das *botnets* está diretamente associada com a quantidade de zumbis que as compõem**
  - **quanto menos zumbis**
    - **menos potentes elas serão**
    - **menores poderão ser os danos causados**
  - **prevenção depende de ação conjunta**
    - **administradores de redes**
    - **usuários finais, etc.**

Faça a sua parte!!!!

Combate a *botnets*

- **Detectar infecções:**
  - **acompanhar *flows* de rede**
    - **identificar zumbis se comunicando com o C&C**
  - ***postmortem***
    - **detectar outras máquinas infectadas (C&C)**

- **Mitigar as atividades maliciosas:**
  - **implementar BCP 38**
    - **impedir a participação dos zumbis em:**
      - **ataques de amplificação**
      - **outros ataques que usem pacotes *spoofados***

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

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

Proteção aos equipamentos de rede

- Administradores e usuários finais
- Alterar, se possível, a senha padrão
  - verificar em contrato se isso é permitido
  - utilizar senhas bem elaboradas
    - guardar a senha original
    - lembrar de restaurá-la quando necessário
- Desabilitar o gerenciamento via Internet (WAN)
  - funções de administração (interface de configuração) acessíveis somente via rede local
    - atacante externo não será capaz de promover mudanças de segurança

Dicas para usuários finais (1/3)

- **Manter computadores e dispositivos móveis seguros:**
  - **com todas as atualizações aplicadas**
  - **com todos os programas instalados com as versões mais recentes**
- **Usar:**
  - **mecanismos de segurança**
    - ***firewall* pessoal, *antimalware, antiphishing*, *antispam***
    - **complementos, extensões, *plugins***
  - **apenas programas originais**
  - **configurações de segurança já disponíveis**
- **Instalar aplicativos**
  - **de fontes confiáveis**
  - **bem avaliados pelos usuários**
  - **com permissões coerentes**

Dicas para usuários finais (2/3)

- **Manter postura preventiva**
  - **não acessar *sites* ou seguir *links***
    - **recebidos de mensagens eletrônicas**
    - **em páginas sobre as quais não se saiba a procedência**
  - **não confiar apenas no remetente da mensagem**
    - **ela pode ter sido enviada de:**
      - **máquinas infectadas**
      - **contas falsas ou invadidas**

Dicas para usuários finais (3/3)

- **Proteger contas e 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**
- **Evitar usar o usuário "administrador"**

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

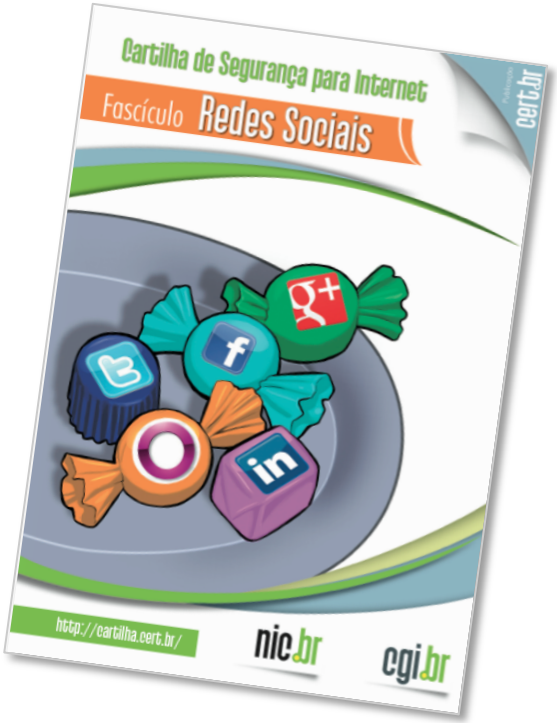
- *Creative Commons* (CC BY-NC-ND 3.0)

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

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?

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/