Spywares, *Worms*, *Bots* e Boas Práticas de Segurança

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

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
– Articulação – Apoio à recuperação – Estatísticas	– Cursos – Palestras – Documentação – Reuniões	– *Honeypots* Distribuídos – SpamPots

SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

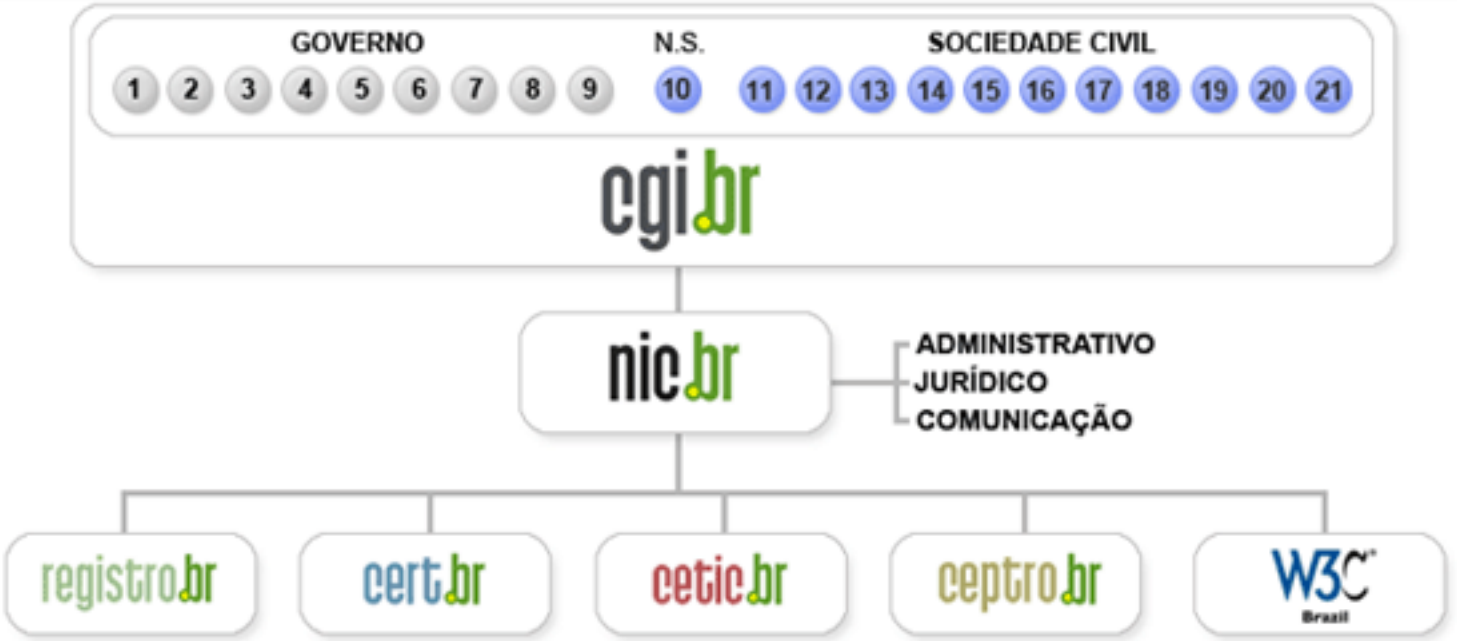
The Honeynet PROJECT

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**
  - **Histórico**
  - **Principais Tipos**
  - **Resumo Comparativo**
- **Boas Práticas de Segurança**

Códigos Maliciosos

Códigos Maliciosos (1/3)

Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador

- **principais tipos:**

Vírus	***Backdoor***
Worm	***Trojan***
Spyware	***Rootkit***
Bot	***Botnet***

Códigos Maliciosos (2/3)

- **Infecção ocorre por meio:**
  - **ação direta de atacantes**
  - **acesso a páginas *Web* vulneráveis**
  - **auto-execução de mídias removíveis infectadas**
  - **execução de arquivos previamente infectados**
  - **exploração de vulnerabilidades nos programas instalados**

- **Ações executadas:**
  - **de acordo com as permissões do usuário**

Códigos Maliciosos (3/3)

- **Principais motivações dos atacantes:**
  - **vandalismo**
  - **desejo de autopromoção**
  - **coleta de informações confidenciais**
  - **obtenção de vantagens financeiras**
  - **prática de golpes**
  - **realização de ataques**
  - **disseminação de *spams***

Histórico

Histórico (1/2)

	1971-1980	1981-1990	1991-2000
Principais características	surgimento dos primeiros vírus e antivírus (específicos)	surgimento do primeiro *worm*, dos vírus maliciosos e dos antivírus genéricos	Popularização da Internet; grande quantidade de vírus (*kits* de criação)
Objetivos	demonstrar conhecimento científico	demonstrar conhecimento científico; causar danos	vantagens financeiras; extorsão; furto de informações; envio de *spams*
Propagação		*disquetes e e-mails*	*e-mails*
Principais alvos		DOS	Windows e aplicativos

Histórico (2/2)

	2001-2010	2011-2012
Principais características	atacantes com pouco conhecimento técnico; explosão no número de códigos maliciosos (múltiplas funcionalidades); popularização das redes sociais, *antimalware*	popularização dos dispositivos móveis e das redes sociais; uso de *botnets* para ataques ideológicos
Objetivos	demonstrar conhecimento científico	demonstrar conhecimento científico e causar danos
Propagação	*e-mails*; mídias removíveis e redes sociais	*e-mails* e redes sociais
Principais alvos	usuários finais	usuários finais; sistemas industriais e alvos específicos

Principais Tipos de Códigos Maliciosos

Vírus

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos

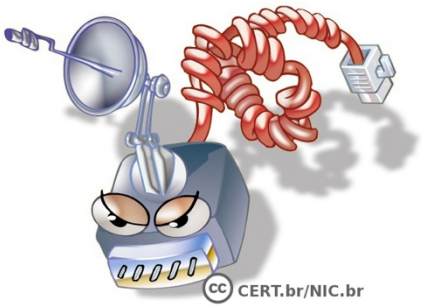
- **depende da execução do programa ou arquivo infectado para se tornar ativo e continuar o processo de infecção**
- **meios de propagação: mídias removíveis**
- **principais tipos:**
  - ***boot*: infectam o setor de inicialização do disquete/disco rígido**
  - **programas: infectam arquivos executáveis**
  - **macro: infectam arquivam lidos por programas que usam macros**

Worm

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

- **meios de propagação:**
  - **execução direta de suas cópias**
  - **exploração automática de vulnerabilidades existentes em programas instalados em computadores**
- **consomem grandes quantidades de recursos**
  - **afetam a utilização de computadores e redes**

Bot

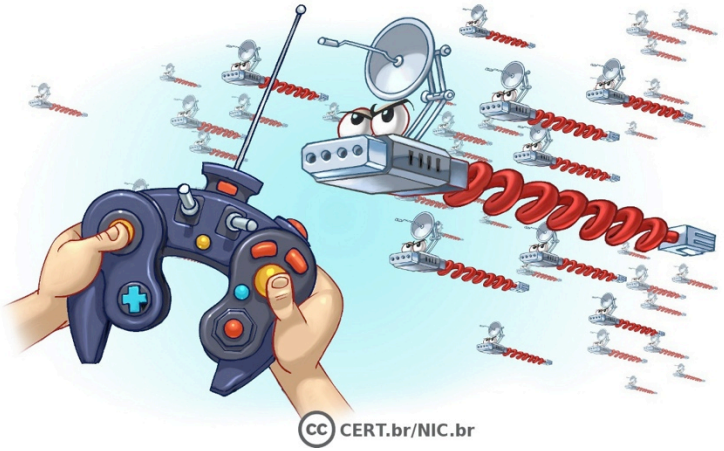


Programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente

- **processo de infecção e propagação similar ao do *worm***
- **comunicação com o invasor via: canais de IRC, servidores *Web* e redes do tipo P2P, entre outros**
- **computador zumbi: controlado remotamente, sem o conhecimento do dono**
- **ações maliciosas executadas:**
  - **ataques na Internet**
  - **furto de dados**
  - **envio de *spam***

Botnet

Rede formada por centenas/milhares de computadores zumbis



- **permite potencializar as ações danosas dos *bots***
- **quanto mais *bots* mais potente é a *botnet***
- **podem ser alugadas pelos atacantes**
- **ações maliciosas executadas:**
  - **ataques de negação de serviço (DoS)**
  - **disseminação de *spam***
  - **propagação de códigos maliciosos**
  - **coleta de informações confidenciais**

Spyware

Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros

- **pode ser usado de forma legítima ou maliciosa, dependendo:**
  - **de como é instalado**
  - **das ações realizadas**
  - **do tipo de informação monitorada**
  - **do uso que é feito por quem recebe a informação**

Tipos de *Spyware*

***Keylogger*: capaz de capturar o que é digitado pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia**

Screenlogger*: capaz de capturar o que é "digitado" via teclados virtuais, principalmente em *sites* de *Internet Banking

***Adware*: projetado para apresentar propagandas. Pode ser usado para fins legítimos ou maliciosos**

Backdoor

Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim

- **pode ser incluído:**
  - **pela ação de outros códigos maliciosos**
  - **por atacantes**
- **após incluído:**
  - **é usado para para assegurar o acesso futuro ao computador comprometido, permitindo que seja acessado remotamente**
  - **sem que seja necessário recorrer novamente aos métodos usados na infecção/invasão**

Cavalo de Tróia (*Trojan*)

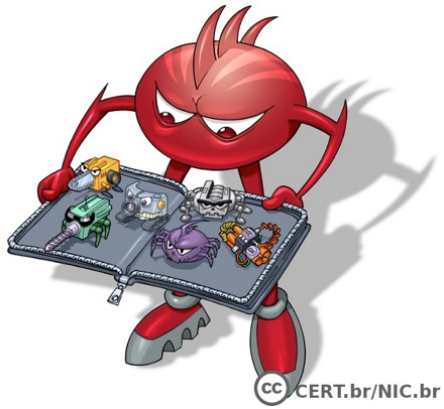
Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário

- **pode ser instalado:**
  - **pela ação do usuário: via arquivos recebidos**
  - **por atacantes: via alteração de programas já existentes**

- **tipos:**

Trojan Downloader	*Trojan Dropper*	*Trojan Backdoor*
Trojan DoS	*Trojan* Destrutivo	*Trojan Clicker*
Trojan Proxy	*Trojan Spy*	*Trojan Banker*

Rootkit



Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido

- **pode ser usado para:**
  - **remover evidências em arquivos de *logs***
  - **instalar outros códigos maliciosos**
  - **esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede, etc.**
  - **mapear potenciais vulnerabilidades em outros computadores**
  - **capturar informações da rede**

Resumo Comparativo

Resumo Comparativo (1/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔

Resumo Comparativo (2/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔

Resumo Comparativo (3/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como se propaga:							
Insere cópia de próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔

Resumo Comparativo (4/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Boas Práticas de Segurança

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 já disponíveis**
- **Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros**

Mantenha uma 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**

Proteja suas Contas e Senhas (1/2)

- **Utilize senhas contendo:**
  - **grande quantidade de caracteres**
  - **diferentes tipos de caracteres**
  - **números aleatórios**

- **Evite usar:**
  - **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.**

Proteja suas Contas e Senhas (2/2)

- **Dicas de elaboração**
  - **selecione caracteres de uma frase**
    - **“O Cravo brigou com a Rosa debaixo de uma sacada” ➔ ”?OCbcaRddus”**
  - **utilize uma frase longa**
    - **“1 dia ainda verei os aneis de Saturno!!!”**
  - **faça substituições de caracteres:**
    - **“Sol, astro-rei do Sistema Solar” ➔ “SS0l, asstrr0-rrei d0 SSisstema SS0larr”**
- **Procure trocar regularmente suas senhas**
- **Evite usar o usuário “administrador”**

Informe-se e Mantenha-se Atualizado (1/2)

Cartilha de Segurança para Internet
http://cartilha.cert.br/

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

Twitter
http://twitter.com/certbr

Informe-se e Mantenha-se Atualizado (2/2)

Portal Internet Segura

http://www.internetsegura.br/

INTERNET SEGURA.BR

Campanha Antispam.br

http://www.antispam.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/