

Grupo de Resposta a Incidentes de Segurança

Conhecendo Segurança da Informação

Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

Grupo de Resposta a Incidentes de Segurança



Quem somos?

Conhecendo Segurança da Informação

[←](#) [→](#) [↺](#) [www.gris.dcc.ufrj.br/documentos/artigos](#) [☆](#) [🔍](#) [🔧](#)

 **GRIS** **Grupo de Resposta a Incidentes de Segurança**

[Acessar](#)

[Buscar](#)
☐ apenas nesta seção

[Informações](#) [Documentos](#) [Projetos](#) [Serviços](#) [Eventos](#) [Notícias](#)

Menu
[Página Inicial](#)
[Informações](#)
[Documentos](#)
[Artigos](#)
 [Rootkits - Survey](#)
 [Técnicas de Engenharia Social - Survey](#)
 [Fundamentos da Criptologia Parte I - Introdução e Histórias](#)
 [Fundamentos da Criptologia Parte II - Criptografia Simétrica](#)
 [Fundamentos da Criptologia Parte III - Criptografia Simétrica \(continuação\)](#)
 [Como Escolher uma Senha](#)
 [A ICP-Brasil e o Poder Regulador do ITI](#)
 [Phishing Scam - A fraude do século XXI](#)
 [Definições e Referências sobre CSirts](#)
 [Buffer Overflow](#)
 [Google - Ferramenta de Ataque e Defesa de](#)

Você está aqui: [Página Inicial](#) > [Documentos](#) > [Artigos](#)

Artigos

Aqui são disponibilizados os artigos de segurança da informação produzidos pelo GRIS

Rootkits - Survey

Na maioria dos ataques a sistemas de informação, o objetivo do invasor é ter acesso ao nível administrativo. Uma vez transposta a barreira para conseguir esse privilégio, o novo objetivo é manter o poder e apagar os indícios da invasão. Um rootkit é um conjunto de programas utilizados para impedir a detecção de atividades maliciosas no sistema, como a presença de usuários não autorizados. Costumam ser usados por invasores de sistemas para manterem acesso após um ataque bem sucedido, sem que precisem subverter o sistema novamente.

[rootkits.pdf](#) — PDF document, 298 kB (305624 bytes)

Técnicas de Engenharia Social - Survey

A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

[Tecnicas_de_Engenharia_Social.pdf](#) — PDF document, 97 kB (99742 bytes)

Fundamentos da Criptologia Parte I - Introdução e Histórias

Iniciando a série "Fundamentos da Criptologia", este artigo visa introduzir o leitor no mundo da criptografia e criptoanálise, apresentando fatos históricos e curiosidades sobre o tema.

[criptologia_parte1.pdf](#) — PDF document, 913 kB (934976 bytes)

Fundamentos da Criptologia Parte II - Criptografia Simétrica

Continuando a série "Fundamentos da Criptologia", este artigo aborda a criptografia de chave simétrica, apresentando cifras de substituição como a ROT-X, Vigenère, entre outras mono e polialfabéticas, com exemplos

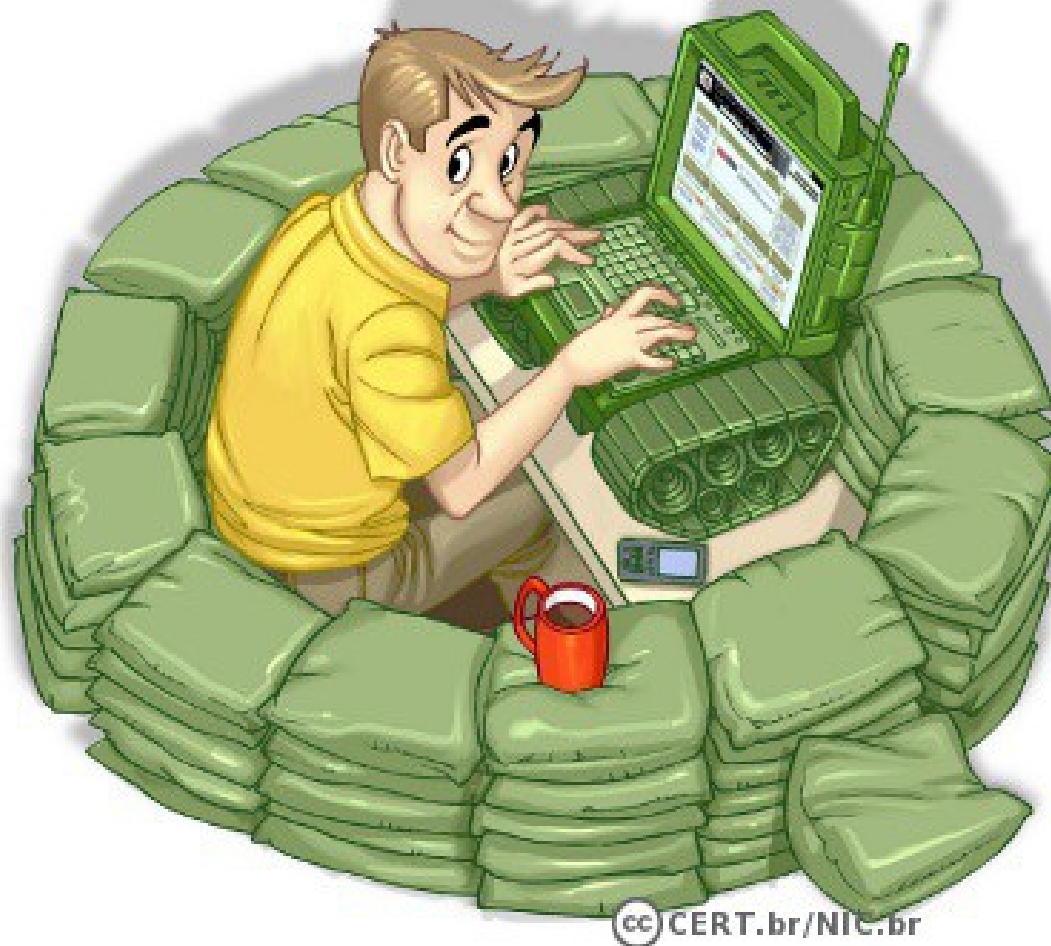
Redes Sociais
  

Dia Internacional de Segurança da Informação


Notícias
[Aprovados no Processo Seletivo de 2012/1](#)
20/07/2012
[Garantindo a segurança de suas crianças na Internet](#)
18/07/2012

gris.dcc.ufrj.br

Conhecendo Segurança da Informação



Motivação

Conhecendo alguns ataques

Conceitos

Boas Práticas

Segurança da Informação - Motivação

**“Novos vírus bancários driblam
sistema de proteção dos bancos”**

totalsecurity.com.br

**“Novo trojan para Mac se instala
sem autorização do usuário”**

techtudo.com.br

**“Hackers invadem e tiram do ar site
do Bradesco”**

diariosp.com.br



Segurança da Informação - Motivação



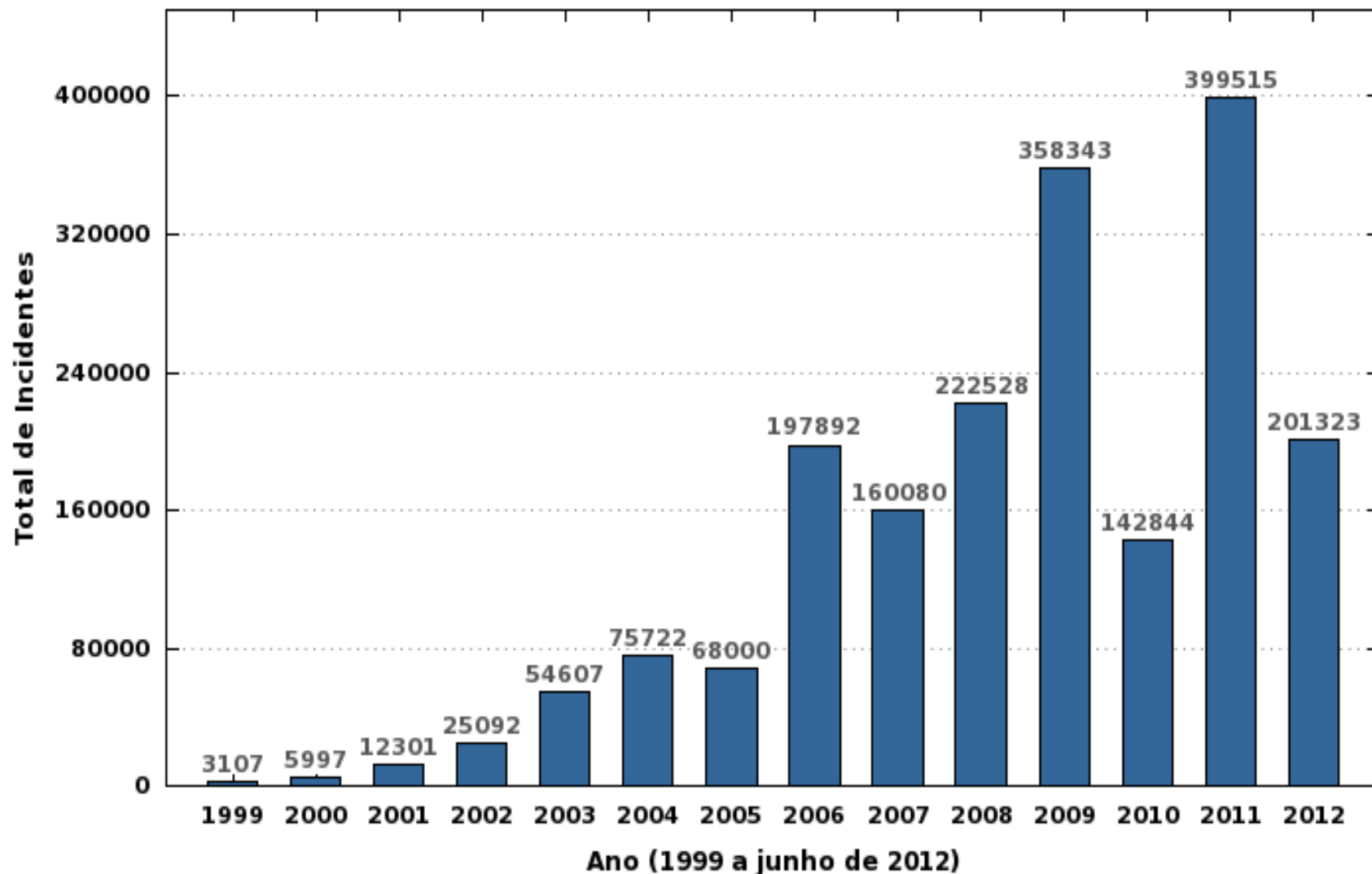
“Brasil tem aumento de 53% nas notificações de golpes na internet, informa organização”

tecnologia.uol.com.br



Segurança da Informação - Motivação

Total de Incidentes Reportados ao CERT.br por Ano

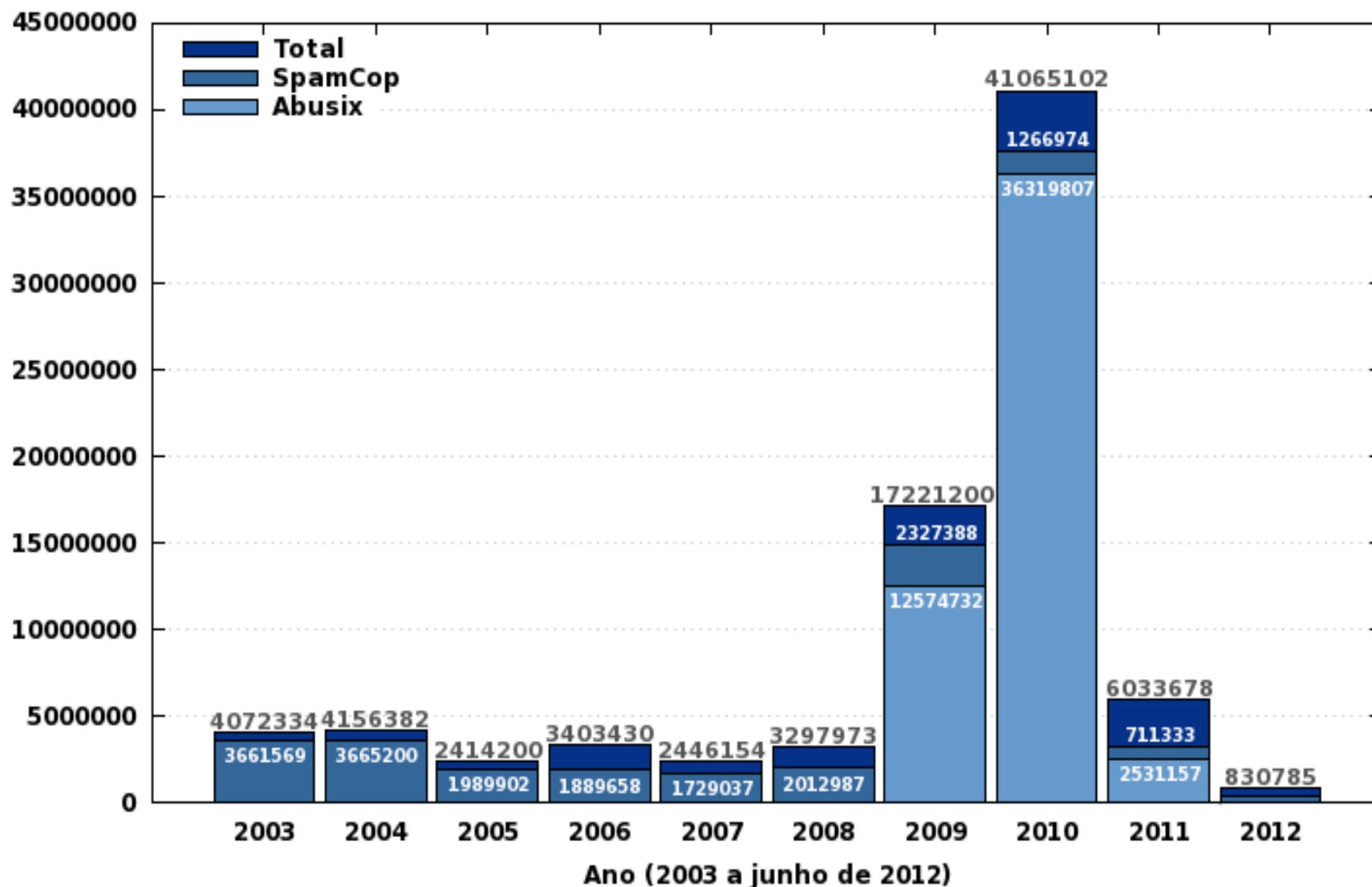


<http://www.cert.br/stats/incidentes/>



Segurança da Informação - Motivação

Spams Reportados ao CERT.br por Ano



<http://www.cert.br/stats/spam/>



Segurança da Informação - Motivação

Hacktivismo



Segurança da Informação?



Segurança da Informação - Conceito



CID

Confidencialidade



Integridade



Disponibilidade



Segurança da Informação - Conceito



~~CID~~



Segurança da Informação - Conhecendo os ataques

Spam

Trojans

Rootkits

DoS e DDoS

Engenharia Social

Botnets

SQL injection

Worms

**Adware e
Spywares**

Backdoor

Vírus

Keyloggers



Segurança da Informação - Conhecendo os ataques



Spam

O termo spam se refere basicamente à mensagens de e-mail não solicitadas. Vale observar que um spam não necessariamente contém vírus, porém todo cuidado é pouco!



Segurança da Informação - Conhecendo os ataques



Os trojans na informática, assim como o "Presente Grego" , tem como finalidade executar funções geralmente maliciosas, sem a percepção do usuário, juntamente com as funções reais do programa.

Trojans



Segurança da Informação - Conhecendo os ataques

Vírus

Software, que tal como um vírus biológico, faz cópia de si mesmo e se propaga para diversos computadores.



Segurança da Informação - Conhecendo os ataques



Rootkits

Rootkit é um pedaço de programa que pode ser instalado e escondido em seu computador sem sua percepção. Não necessariamente são programas maliciosos, contudo eles podem esconder atividades maliciosas.



Segurança da Informação - Conhecendo os ataques



Em um ataque DoS, um atacante tem como objetivo impedir que os usuários acessem suas informações e serviços de várias formas. Caso o ataque seja bem sucedido, o atacante pode impedir que você acesse seu e-mail, conta de banco online, sites na Internet, e vários outros serviços que o computador infectado poderia realizar.

DoS e DDoS



Segurança da Informação - Conhecendo os ataques

Engenharia Social

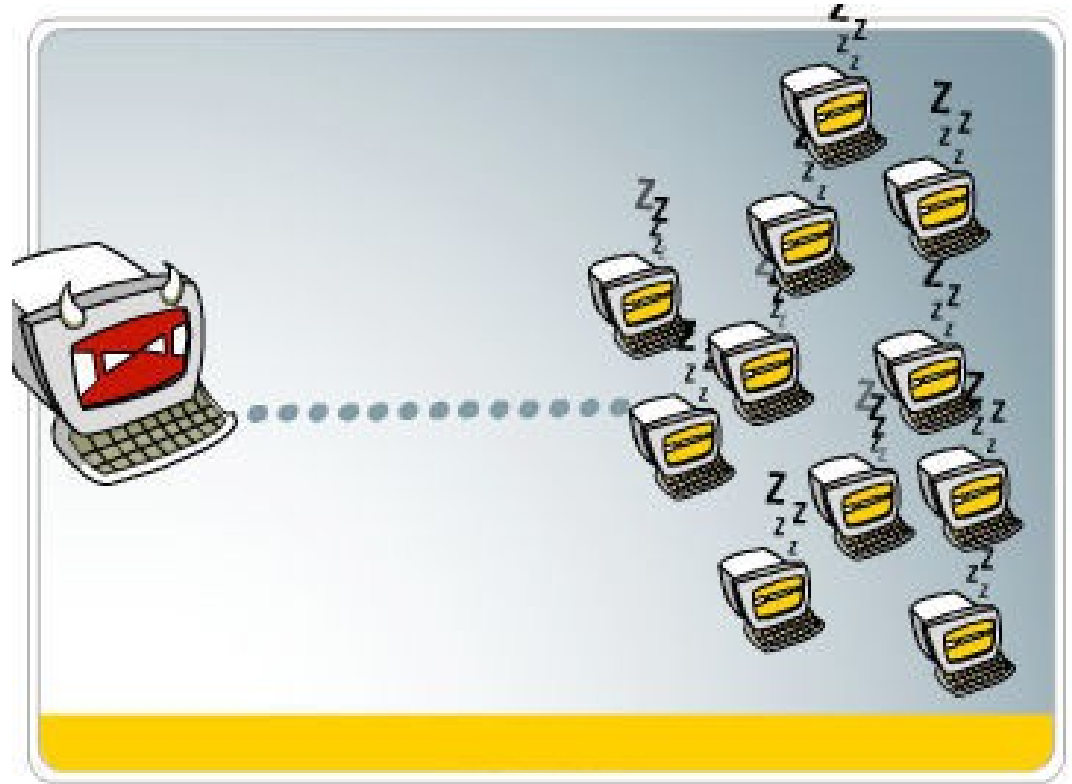


A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação.



Segurança da Informação - Conhecendo os ataques

Botnets

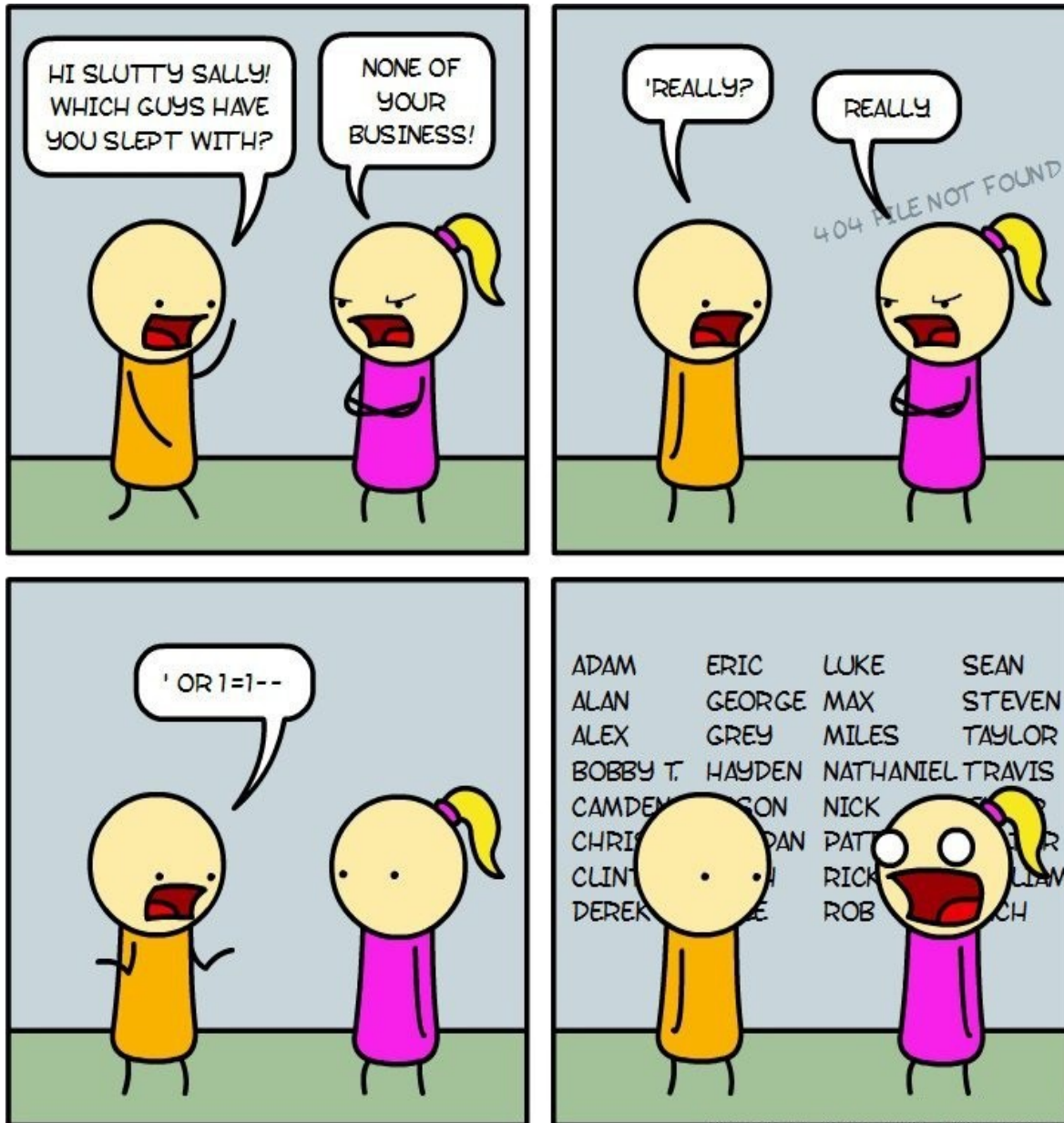


Botnet é um termo derivado da ideia de “bot networks” . De uma forma simplificada, um bot é simplesmente um programa de computador automatizado , ou um robô. No contexto dos Botnets, bots são computadores que são capazes de serem controlados por uma, ou várias, fontes externas.

Segurança da Informação - Conhecendo os ataques

SQL Injection

SQL Injection costuma ser feito em aplicações (como PHP, Java ou ASP), e o objetivo do ataque é extrair informação relevante da base de dados.



Segurança da Informação - Conhecendo os ataques

Keyloggers

Programas capazes de capturar e armazenar as teclas digitadas pelo usuário, geralmente afim de roubar senhas de email, facebook, ou até mesmo de bancos.



Segurança da Informação - Conhecendo os ataques

Backdoor



Quando um cracker invade um computador através de malwares, ele geralmente deixa “buracos”(do inglês “Backdoors”) no computador para que ele possa ter livre acesso ao dispositivo infectado em outras ocasiões.



Segurança da Informação - Conhecendo os ataques

Adware (Advertising software) é um tipo de software especificamente projetado para apresentar propagandas. Já Spyware é o termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.



Adware e Spywares



Segurança da Informação - Conhecendo os ataques



Ouch!

Segurança da Informação – Boas Práticas

Se mantenha atualizado nas últimas notícias e alertas sobre Segurança!



Segurança da Informação – Boas Práticas





GRIS
Grupo de Resposta a Incidentes de Segurança

Buscar no Site
☐ apenas nesta seção

Informações

Documentos

Projetos

Serviços

Eventos

Notícias

Menu

[Página Inicial](#)

[Informações](#)

[Documentos](#)

[Artigos](#)

[Rootkits - Survey](#)

[Técnicas de Engenharia Social - Survey](#)

[Fundamentos da Criptologia Parte I - Introdução e Histórias](#)

[Fundamentos da Criptologia Parte II - Criptografia Simétrica](#)

[Fundamentos da Criptologia Parte III - Criptografia Simétrica \(continuação\)](#)

[Como Escolher uma Senha](#)

[A ICP-Brasil e o Poder Regulador do ITI](#)

[Phishing Scam - A fraude do século XXI](#)

[Definições e Referências sobre CSirts](#)

[Buffer Overflow](#)

[Google - Ferramenta de Ataque e Defesa de](#)

Você está aqui: [Página Inicial](#) > [Documentos](#) > [Artigos](#)

Artigos

Aqui são disponibilizados os artigos de segurança da informação produzidos pelo GRIS

Rootkits - Survey

Na maioria dos ataques a sistemas de informação, o objetivo do invasor é ter acesso ao nível administrativo. Uma vez transposta a barreira para conseguir esse privilégio, o novo objetivo é manter o poder e apagar os indícios da invasão. Um rootkit é um conjunto de programas utilizados para impedir a detecção de atividades maliciosas no sistema, como a presença de usuários não autorizados. Costumam ser usados por invasores de sistemas para manterem acesso após um ataque bem sucedido, sem que precisem subverter o sistema novamente.

 [rootkits.pdf](#) — PDF document, 298 kB (305624 bytes)

Técnicas de Engenharia Social - Survey

A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

 [Tecnicas_de_Engenharia_Social.pdf](#) — PDF document, 97 kB (99742 bytes)

Fundamentos da Criptologia Parte I - Introdução e Histórias

Iniciando a série "Fundamentos da Criptologia", este artigo visa introduzir o leitor no mundo da criptografia e criptoanálise, apresentando fatos históricos e curiosidades sobre o tema.

 [criptologia_parte1.pdf](#) — PDF document, 913 kB (934976 bytes)

Fundamentos da Criptologia Parte II - Criptografia Simétrica

Continuando a série "Fundamentos da Criptologia", este artigo aborda a criptografia de chave simétrica, apresentando cifras de substituição como a ROT-X, Vigenère, entre outras mono e polialfabéticas, com exemplos

Redes Sociais



Dia Internacional de Segurança da Informação



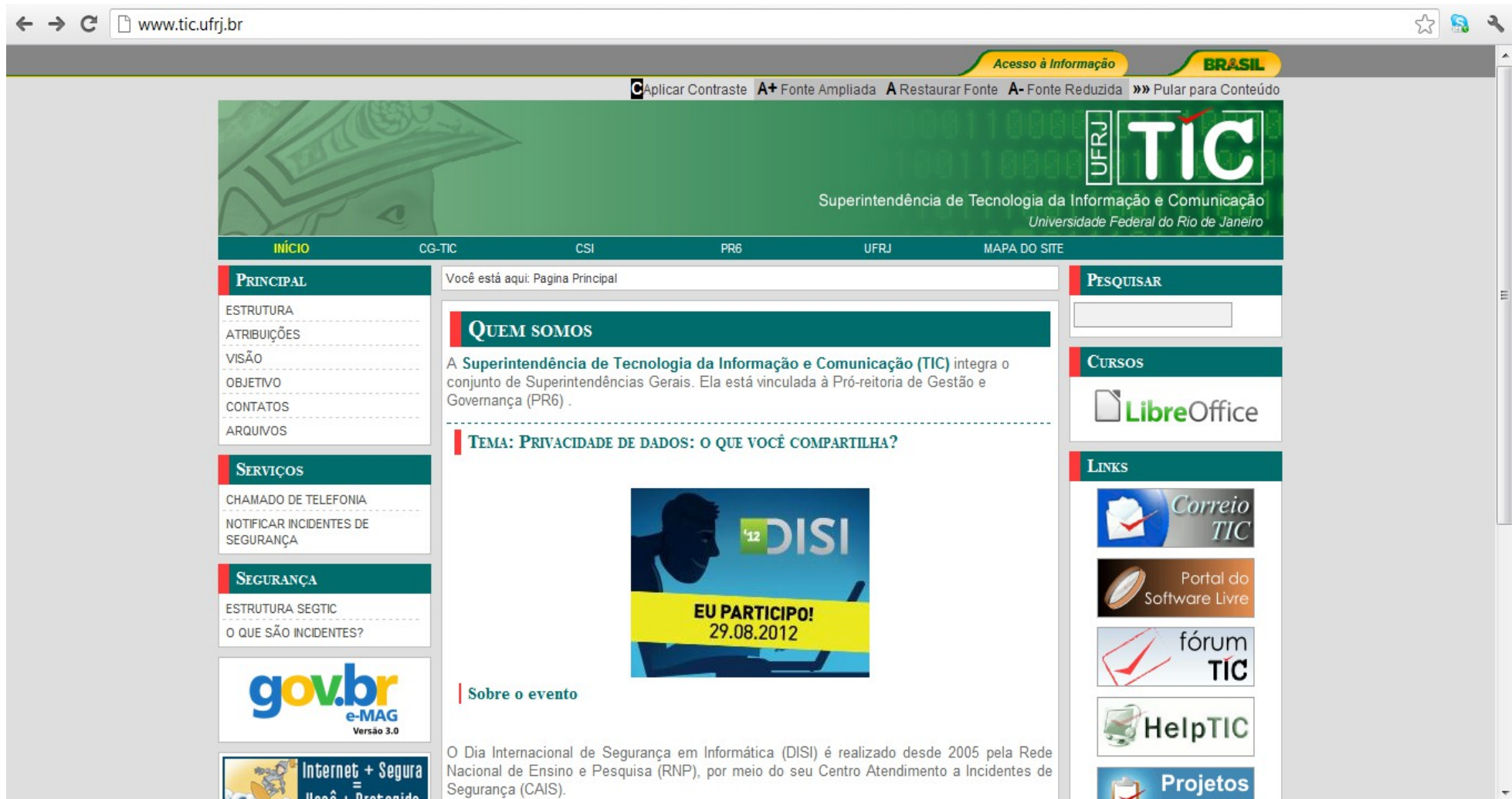
Notícias

[Aprovados no Processo Seletivo de 2012/1](#)
20/07/2012

[Garantindo a segurança de suas crianças na Internet](#)
18/07/2012

gris.dcc.ufrj.br

Segurança da Informação – Boas Práticas



tic.ufrj.br

Segurança da Informação – Boas Práticas

The screenshot shows the website www.cert.br/sobre/. The page is titled "Núcleo de Informação e Coordenação do Ponto BR" and includes a navigation bar with links to CGL.br, NIC.br, Registro.br, CERT.br, CETIC.br, CEPTR0.br, and W3C.br. The main content area is titled "Sobre o CERT.br" and describes the organization's role in responding to security incidents in Brazil. It mentions that CERT.br is a group of response to security incidents for the Brazilian Internet, maintained by NIC.br, the Internet Management Committee in Brazil. It is responsible for treating security incidents in computers that involve networks connected to the Brazilian Internet. The page also lists the strategic objectives of CERT.br, which are to increase the levels of security and the capacity to treat incidents in networks connected to the Internet in Brazil. The page is organized into sections: "Sobre o CERT.br", "Principais Atividades", and "Treinamento e Conscientização". The "Principais Atividades" section is divided into "Tratamento de Incidentes" and "Treinamento e Conscientização". The "Tratamento de Incidentes" section lists three main activities: providing support to the recovery and analysis of attacks and compromised systems; establishing a collaborative work with other entities, such as CSIRTs, companies, universities, providers of access and Internet services and backbones; and maintaining public statistics of incidents treated and of spam complaints received. The "Treinamento e Conscientização" section lists three main activities: offering trainings in the area of treatment of security incidents, especially for members of CSIRTs and for institutions that are creating their own group; developing documentation of support for administrators of Internet networks and users; and realizing meetings with various sectors of the Internet in Brazil, in order to articulate cooperation and implementation of good security practices.

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Núcleo de Informação e Coordenação do Ponto BR

CGL.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTR0.br - W3C.br

Você está em: [CERT.br](#) > Sobre o CERT.br

Sobre o CERT.br

O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo [NIC.br](#), do [Comitê Gestor da Internet no Brasil](#). É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs no Brasil.

Estas atividades têm como objetivo estratégico aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

As atividades conduzidas pelo CERT.br fazem parte das [atribuições do CGL.br](#) de:

- I - estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
- IV - promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
- VI - ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;

Bem como dos objetivos do NIC.br, conforme seu [Estatuto](#):

- IV - atender aos requisitos de segurança e emergências na Internet Brasileira em articulação e cooperação com as entidades e os órgãos responsáveis;
- VII - promover ou colaborar na realização de cursos, simpósios, seminários, conferências, feiras e congressos, visando contribuir para o desenvolvimento e aperfeiçoamento do ensino e dos conhecimentos nas áreas de suas especialidades.

Principais Atividades

Tratamento de Incidentes

- Dar suporte ao processo de recuperação e análise de ataques e de sistemas comprometidos;
- Estabelecer um trabalho colaborativo com outras entidades, como outros CSIRTs, empresas, universidades, provedores de acesso e serviços Internet e backbones;
- Manter estatísticas públicas dos incidentes tratados e das reclamações de spam recebidas.

Treinamento e Conscientização

- Oferecer treinamentos na área de tratamento de incidentes de segurança, especialmente para membros de CSIRTs e para instituições que estejam criando seu próprio grupo;
- Desenvolver documentação de apoio para administradores de redes Internet e usuários;
- Realizar reuniões com setores diversos da Internet no Brasil, de modo a articular a cooperação e implantação de boas práticas de segurança.

Busca

Buscar em CERT.br

W3C XHTML 1.0 W3C CSS

Acessibilidade do site

cert.br

Segurança da Informação – Boas Práticas

← → ↻ www.us-cert.gov/alerts-and-tips/ ☆



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOMESECURITY PUBLICATIONSALERTS AND TIPSRELATED RESOURCESABOUT USGFIRST

Information for

Home and Business

Information for system administrators and technical users about latest threats.

Government Users

Resources for information sharing and collaboration among government agencies.

Control Systems Users

Information for industrial control systems owners, operators, and vendors.



STOP | THINK | CONNECT™

Cybersecurity is a shared responsibility. For additional tips and resources for all age groups, visit the Department of Homeland Security's [Stop.Think.Connect.™](#) Campaign.

National Cyber Awareness System

Four products in the National Cyber Awareness System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips.



Current Activity

Provides up-to-date information about high-impact types of security activity affecting the community at large.



Alerts

Provide timely information about current security issues, vulnerabilities, and exploits.



Bulletins

Provide weekly summaries of new vulnerabilities. Patch information is provided when available.



Tips

Provide advice about common security issues for the general public.

A subscription to any or all of the National Cyber Awareness System products ensures that you have access to timely information about security topics and threats. To learn more or to subscribe, visit the [subscription system](#). You can also visit our [Mailing Lists and Feeds](#) page to learn more about how to subscribe or use our syndicated feeds.

us-cert.gov

Segurança da Informação – Boas práticas

123456789

mengao123

minhasenhaedificil123

5deoutubro



**Utilize
senhas fortes!**

?!@iU98oJjLm

Po945kL??s8

nnBb123@@sxZ



Segurança da Informação – Boas práticas

**Atualize SEMPRE
seu Sistema
Operacional e
programas**



Segurança da Informação – Boas práticas



**Desconecte-se quando
não estiver usando**



Segurança da Informação – Boas práticas



**Evite compartilhar
suas informações
pessoais!**



Segurança da Informação – Boas práticas



**Trave seu computador
sempre que sair de
perto**



Segurança da Informação – Boas práticas

Não seja um clicador compulsivo!



Segurança da Informação – Boas práticas



**Cuidado ao usar
computadores
públicos**



Segurança da Informação – Boas práticas

Cuidado ao instalar aplicativos em dispositivos móveis



Segurança da Informação – Boas práticas



**Nunca utilize
softwares piratas!**



Infelizmente esse quadro só tende a piorar!



Conhecendo Segurança da Informação



Dúvidas?

Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

Conhecendo Segurança da Informação



Obrigado!

Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro