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

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”

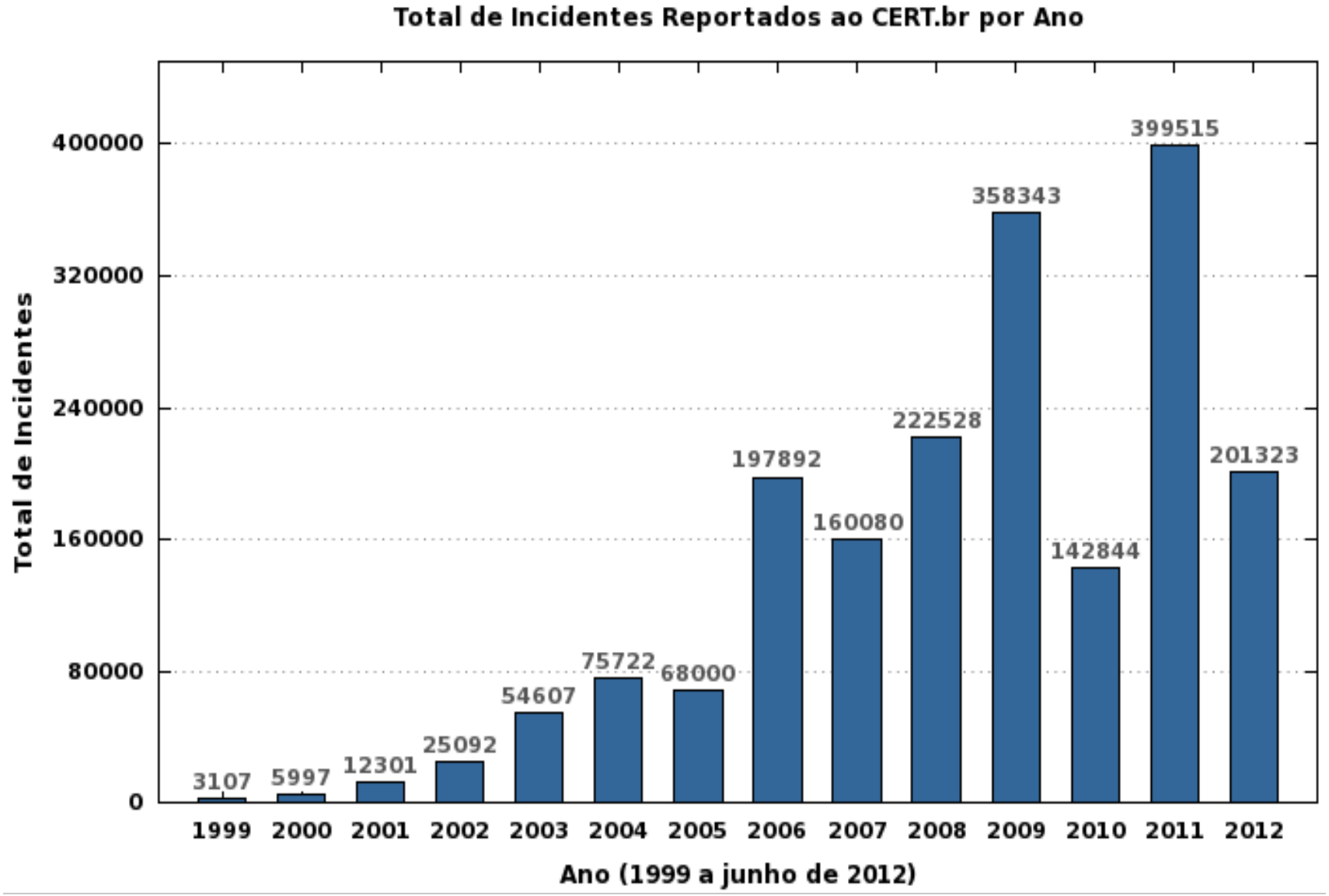
diariosp.com.br

Segurança da Informação - Motivação

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

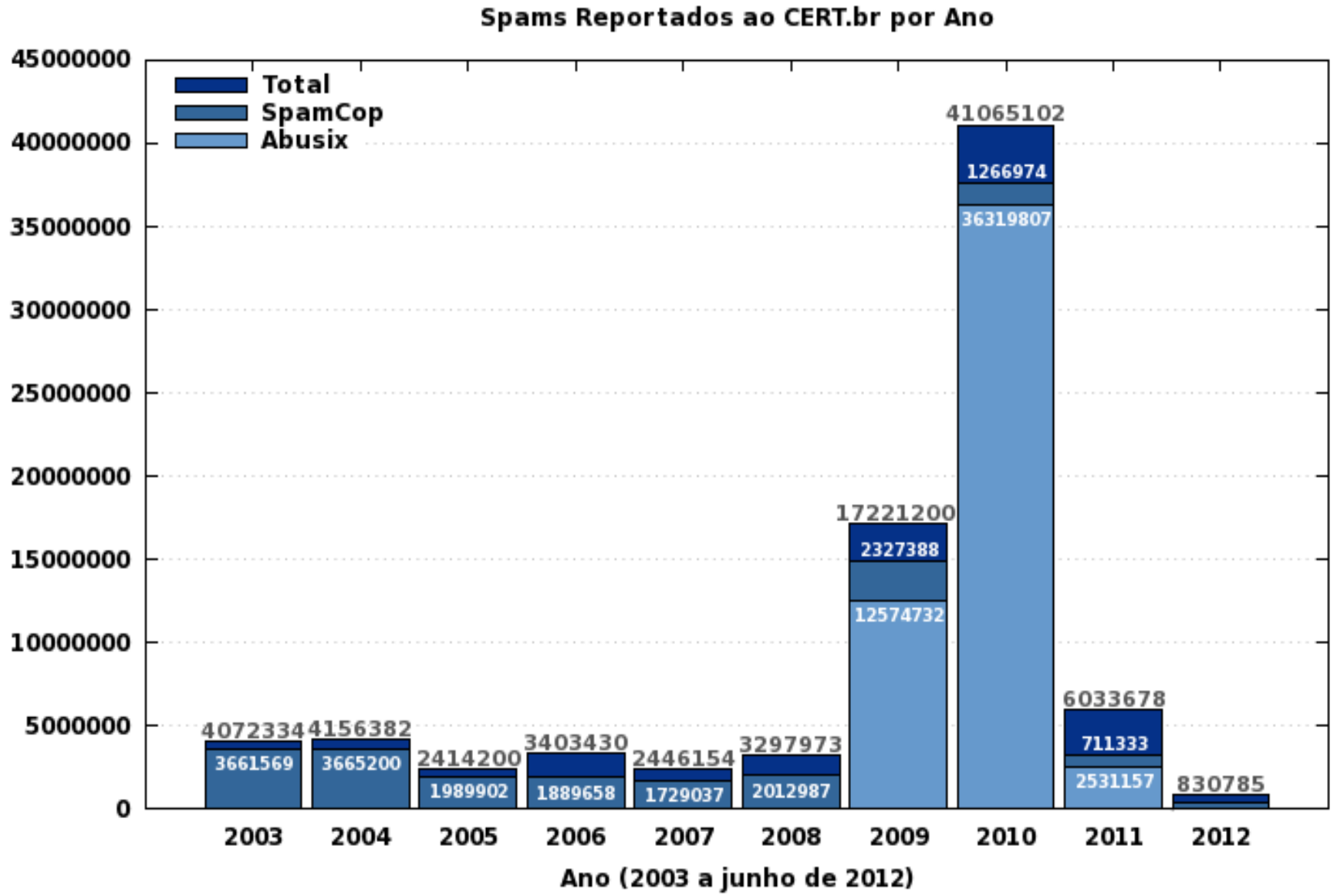
tecnologia.uol.com.br

Segurança da Informação - Motivação



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

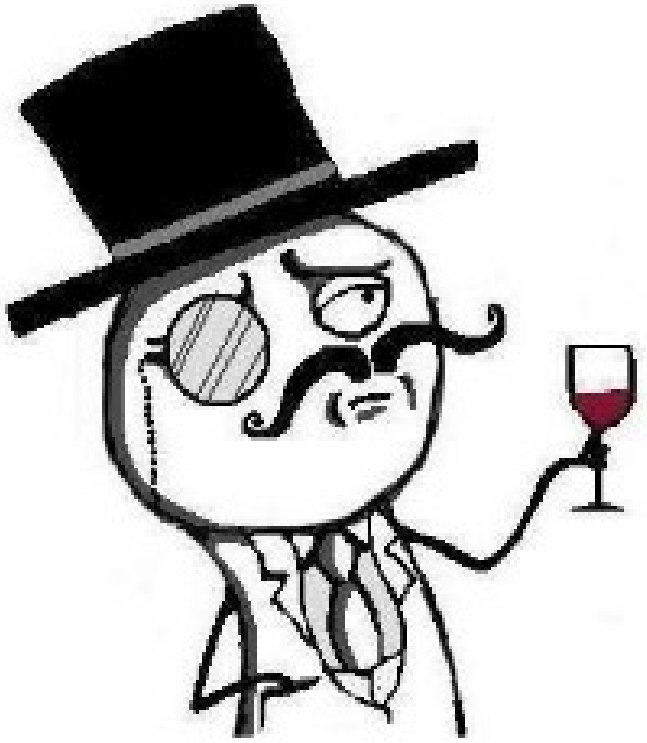
Segurança da Informação - Motivação



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

Worms

Adware e Spywares

Backdoor

Vírus

Keyloggers

SQL injection

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 sí 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

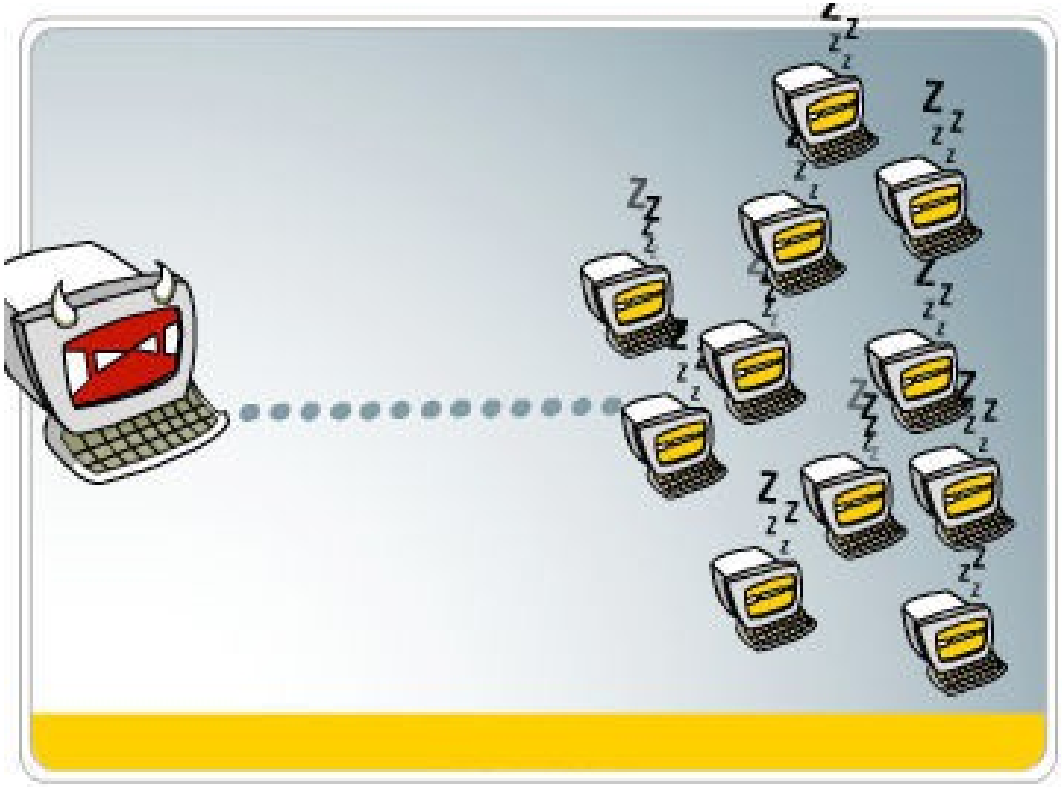
Segurança da Informação - Conhecendo os ataques

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.

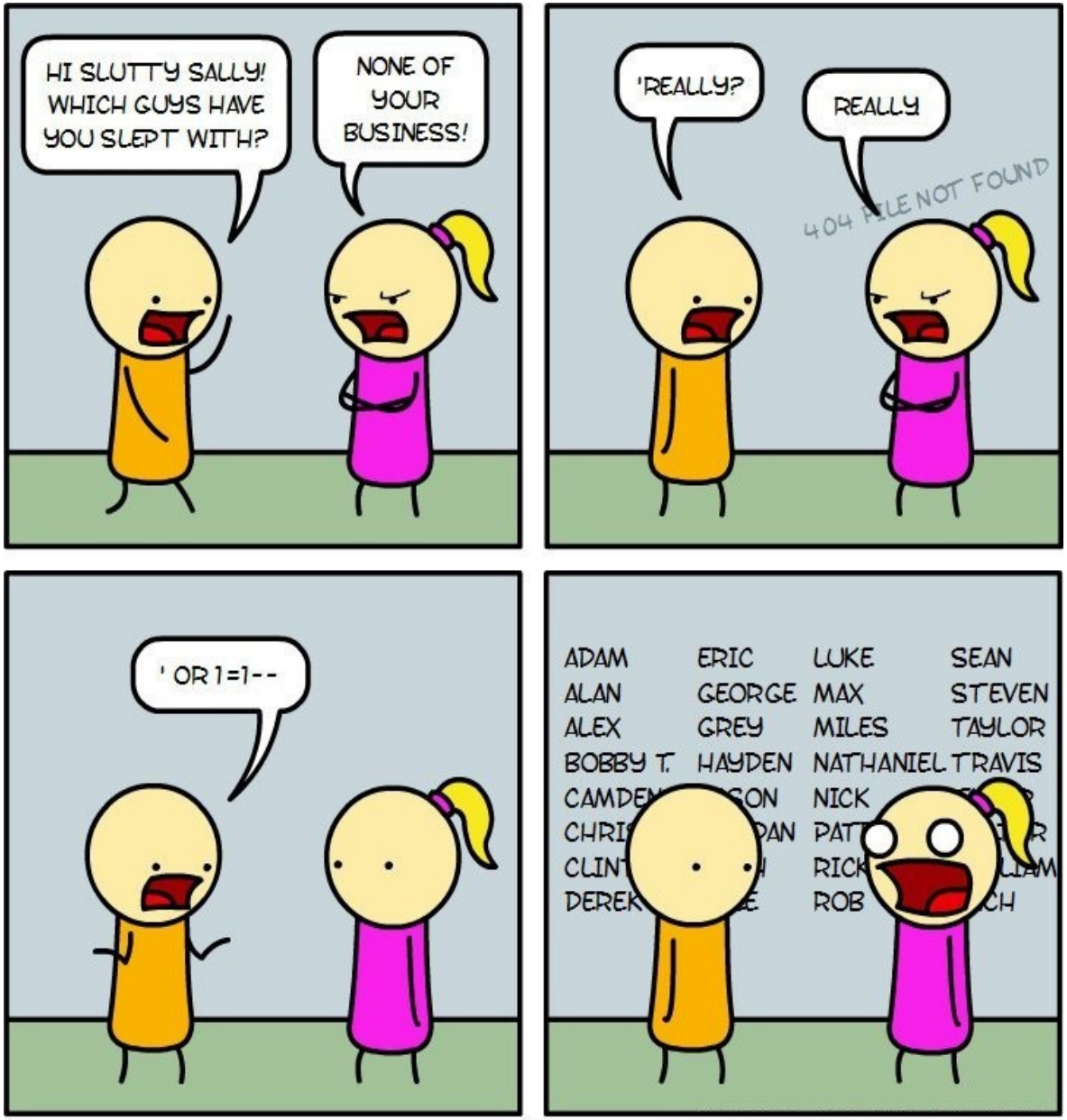
Segurança da Informação - Conhecendo os ataques

Botnets



Botnet é um termo derivado da ideia de "bot networks" . De uma forma simplificada, um bot é simplesmente um programa de computador automizado , 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!

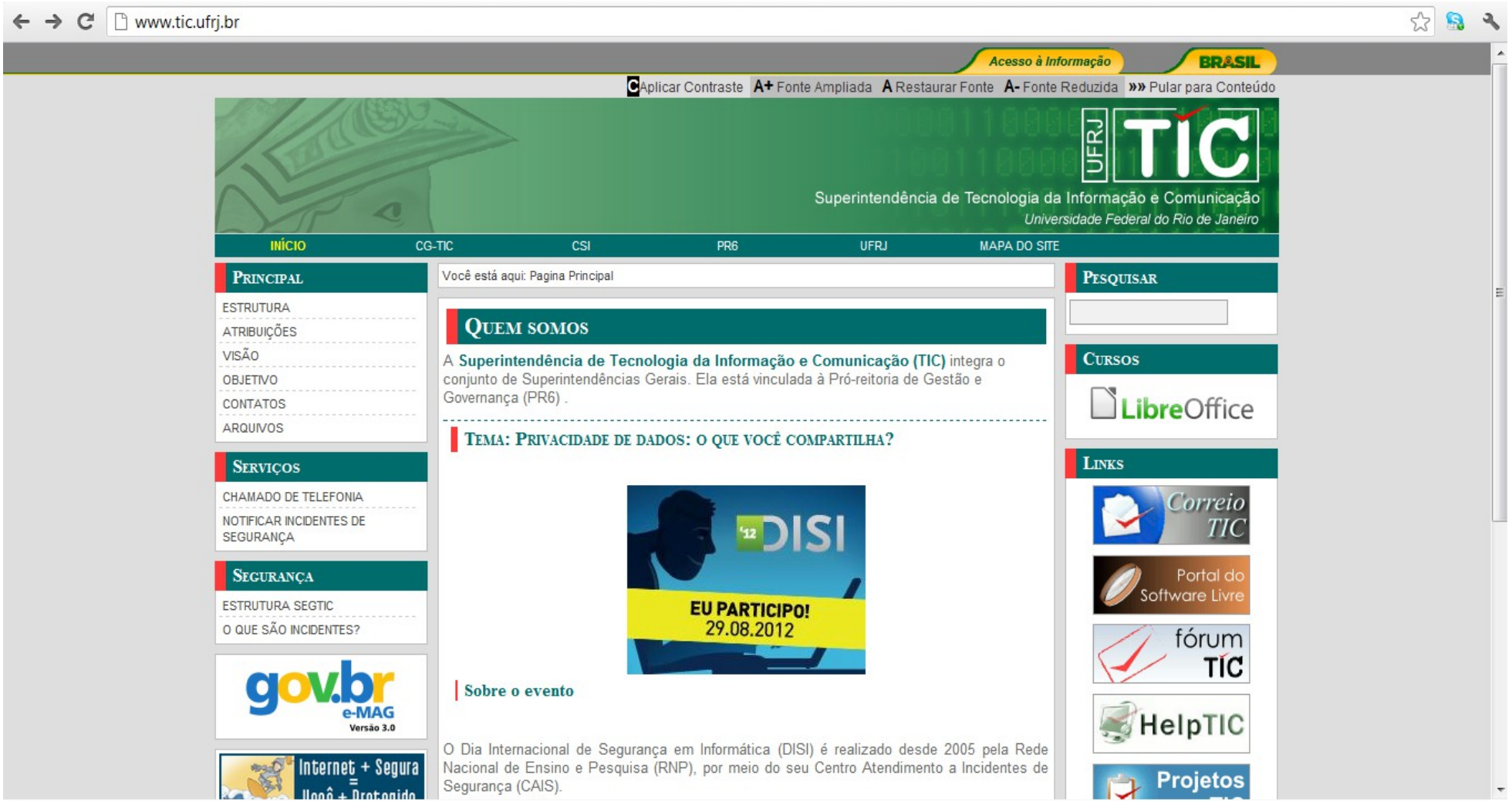
Segurança da Informação – Boas Práticas

Se mantenha atualizado nas últimas notícias e alertas sobre Segurança!

Segurança da Informação – Boas Práticas

gris.dcc.ufrj.br

Segurança da Informação – Boas Práticas



tic.ufrj.br

Segurança da Informação – Boas Práticas

cert.br

Segurança da Informação – Boas Práticas

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

Cuidado ao instalar aplicativos em dispositivos móveis

Segurança da Informação – Boas práticas

Nunca utilize softwares piratas!

Infelizmente esse quadro só tende a piorar!

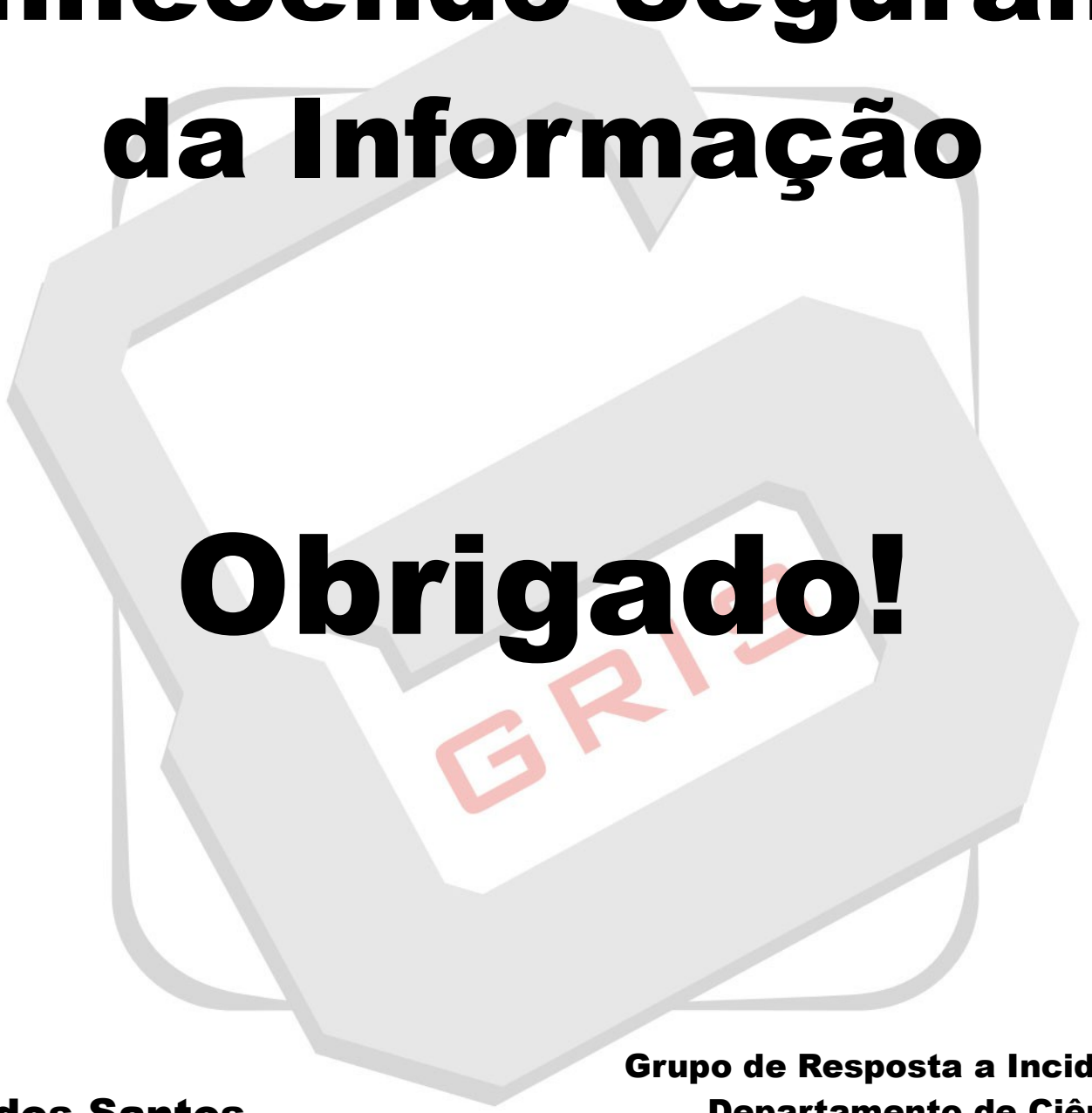
Conhecendo Segurança da Informação

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