RELATÓRIO ANUAL

Destaques do Tratamento de Incidentes em 2010

RNP

1 Introdução

Sobre a RNP

Responsável pela introdução da Internet no Brasil, em 1992, a RNP opera a rede acadêmica nacional, a rede Ipê. Sua missão é promover o uso inovador de redes avançadas no país. Mantida pelos Ministérios da Ciência e Tecnologia, da Educação e da Cultura, atua no desenvolvimento e na prestação de serviços em três áreas: infraestrutura de redes de alto desempenho, aplicações avançadas e formação de recursos humanos em redes. A rede Ipê é uma infraestrutura de alto desempenho para colaboração e comunicação em educação e pesquisa que alcança os 26 estados da federação e o Distrito Federal. A RNP está conectada às redes acadêmicas latino-americana (RedCLARA), europeia (Géant) e norte-americana (Internet2), além de ter conexão própria à Internet mundial.

Sobre o CAIS

Criado em 1997, o CAIS atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica nacional (rede Ipê). Em seu site (www.rnp.br/cais), o CAIS disponibiliza uma série de informações para alertar os internautas sobre as ameaças da rede. Além disso, mantém um canal de contato com seus clientes através do endereço cais@cais.rnp.br, para onde devem ser enviados relatos de incidentes de segurança relacionados à rede Ipê. No campo internacional, o CAIS mantém relações com as principais organizações atuantes no setor de segurança na Internet. É filiado desde setembro de 2001 ao Forum of Incident Response and Security Teams (FIRST) e, desde setembro de 2005, também é parceiro de pesquisa do APWG (Anti-Phishing Working Group).

Objetivo

O presente relatório tem como propósito apresentar uma análise estatística do processo de atendimento a incidentes realizado na RNP. No documento, produzido pela primeira vez, constam dados do atendimento a incidentes em 2010, as tendências observadas no período e a descrição de iniciativas relevantes que impactaram positivamente no processo de resposta a incidentes.

2 Resumo do ano

Apesar de 2010 ter sido um ano de menos incidentes em comparação a 2009, o CAIS registrou um crescimento vertiginoso nas notificações enviadas a partir de outubro do ano passado por conta da ativação do Gerenciador de Envio de Incidentes e de Contatos de Segurança (GENICS), da reativação de parcerias e do processamento de dados recebidos de grupos de pesquisa em segurança. A ferramenta de envio automático de notificações entrou em operação em agosto de 2010, mas atingiu seu pleno funcionamento em outubro, dando vazão a uma grande quantidade de e-mails enviados diariamente.

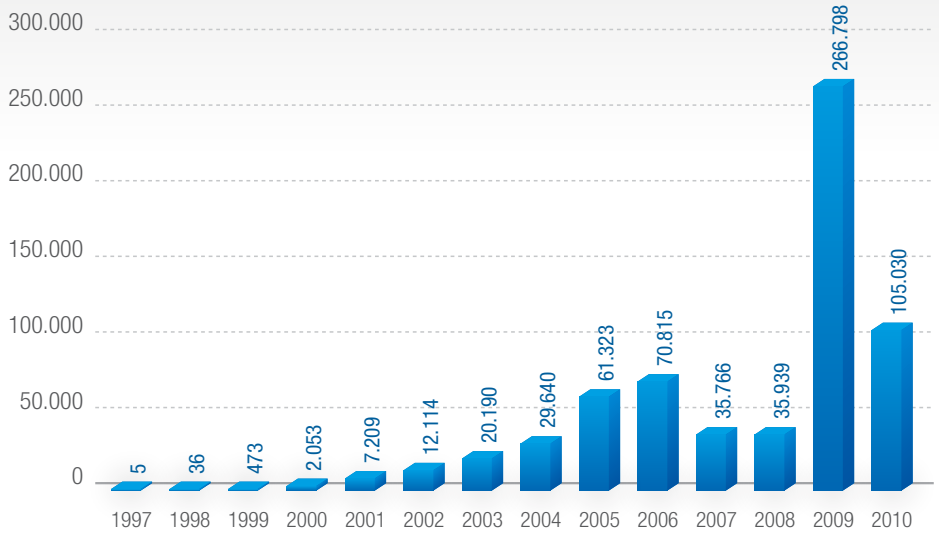
Com a GENICS em funcionamento, iniciou-se o processamento de dados de diversos parceiros, que fornecem informações sobre máquinas infectadas por vírus, envio de spams, sistemas participantes de botnets , entre outros. A reativação destas parcerias e a análise destes dados propiciaram a identificação em maior escala de problemas em sistemas conectados à rede da RNP.

De todos os incidentes tratados, o ano de 2010 se destacou pela quantidade de máquinas infectadas com códigos maliciosos, principalmente do tipo bot . A ação do Conficker e de bots como o Zotob mostrou-se bastante intensa na rede da RNP, e foi responsável por grande parte das notificações enviadas. Também ocorreram, com bastante freqüência, incidentes envolvendo o envio de spam, o download de material protegido por direitos autorais e casos de fraudes online.

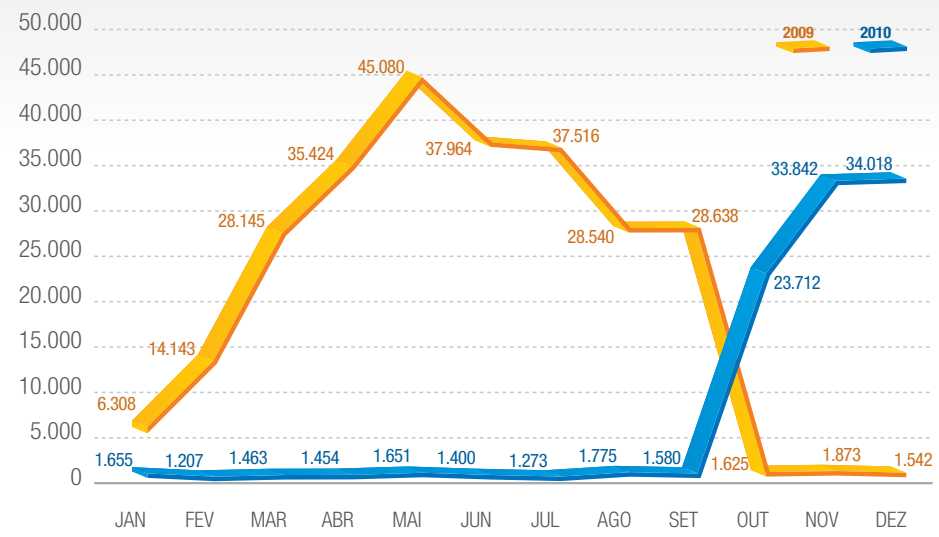
3 Quantidade de incidentes volta a crescer na RNP

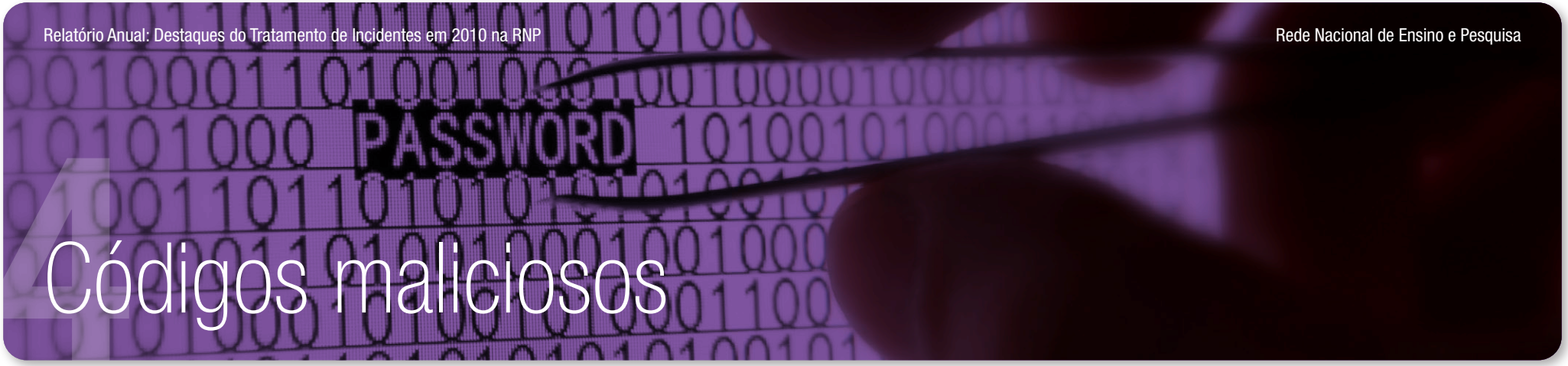
O CAIS notificou 105.030 incidentes de segurança relacionados à RNP e seus clientes no ano de 2010. Apesar da redução de 60% nas notificações enviadas se comparado a 2009, a quantidade de notificações realizadas mensalmente voltou a crescer no final do ano, consequência da ação da GENICS e dos dados recebidos de parceiros. Em outubro de 2010, as notificações chegaram a 23.000 incidentes reportados, sendo que de janeiro a setembro, a média mensal ficou em torno de 1.500 notificações. Em dezembro de 2010, atingiu-se o pico de 34.000 notificações de incidentes enviadas.

INCIDENTES NOTIFICADOS ANUALMENTE



INCIDENTES NOTIFICADOS MENSALMENTE

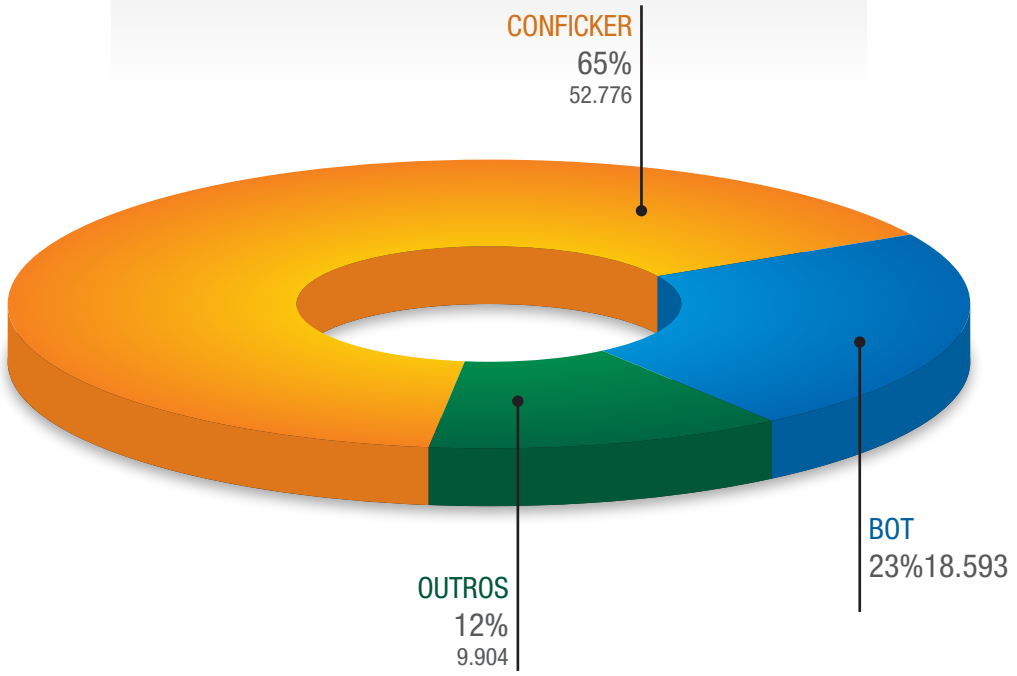




4 Códigos maliciosos

O ano de 2010 foi marcado pela presença de códigos maliciosos em sistemas conectados à rede da RNP. São considerados códigos maliciosos programas como vírus, worms, trojans, bots, spywares, entre outros, que executam tarefas no computador sem o consentimento do usuário ou que geram algum dano a ele ou ao sistema. Dos 105.030 incidentes notificados, 81.273 estavam relacionados a códigos maliciosos, o que representa 77% do total de notificações enviadas pelo CAIS no ano. Uma estimativa por tipo de código malicioso mostra que mais da metade destes casos (65%) se deve à ação do worm Conficker, ainda presente em sistemas conectados à rede acadêmica. Os incidentes reportando a presença de bots em sistemas totalizaram 23% das notificações de códigos maliciosos. Entre as variantes identificadas estão Zotob, Artro e Torpig.

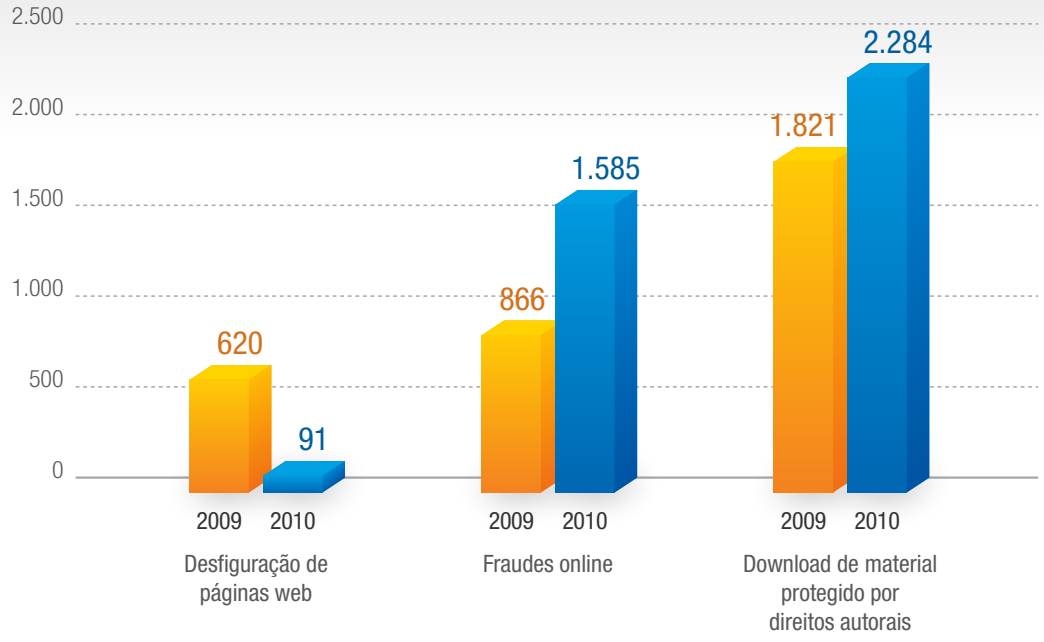
ESTIMATIVA DE INCIDENTES NOTIFICADOS
POR TIPO DE CÓDIGOS MALICIOSOS



5 Fraudes, desfiguração de páginas web e violação de direitos autorais

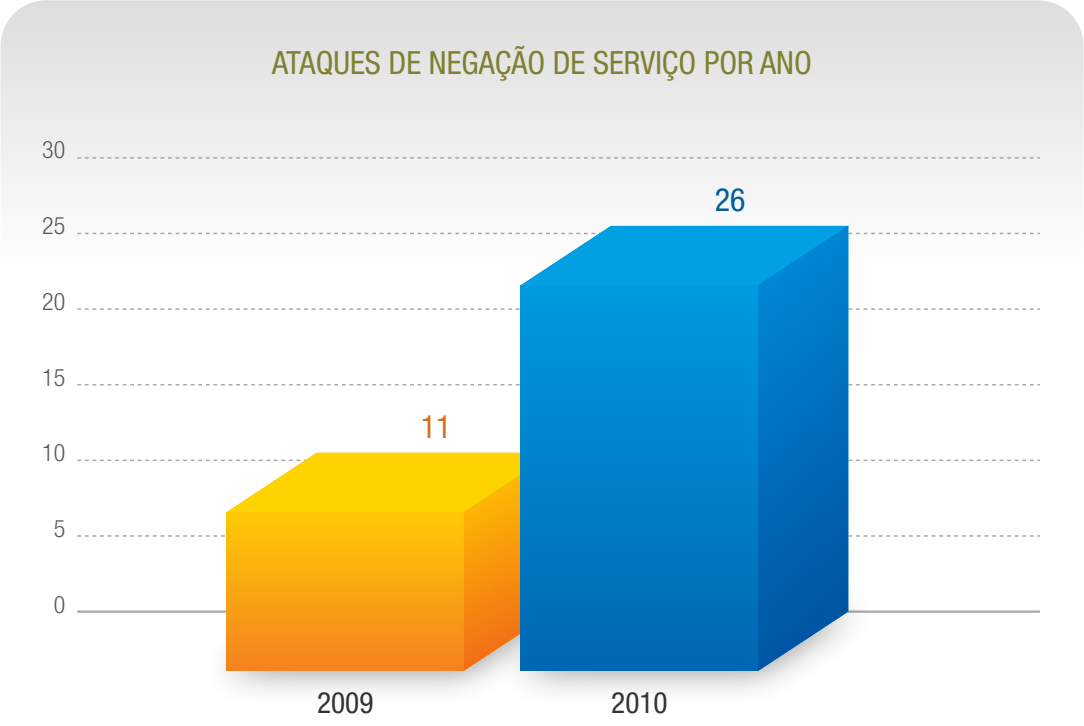
Foram notificados, no período, 3.960 incidentes relacionados ao download de material protegido por direitos autorais, fraudes online e desfiguração de páginas web, totalizando 3% dos incidentes tratados no ano. Destes, os casos de fraudes online foram os que mais cresceram de 2009 para 2010 (83%), evidenciando o aumento nos ataques contra instituições financeiras e contra a segurança de dados sigilosos dos usuários. Também houve aumento nos números de notificações de incidentes relacionados ao download de material protegido por direitos autorais: 25% comparado a 2009. Em contrapartida, foi registrada uma significativa redução de 85% nos casos de desfiguração de páginas web, incidentes estes relacionados a ataques que se utilizam de vulnerabilidades em servidores ou aplicações para modificar o texto e imagens de websites.

INCIDENTES NOTIFICADOS ANUALMENTE POR CATEGORIA



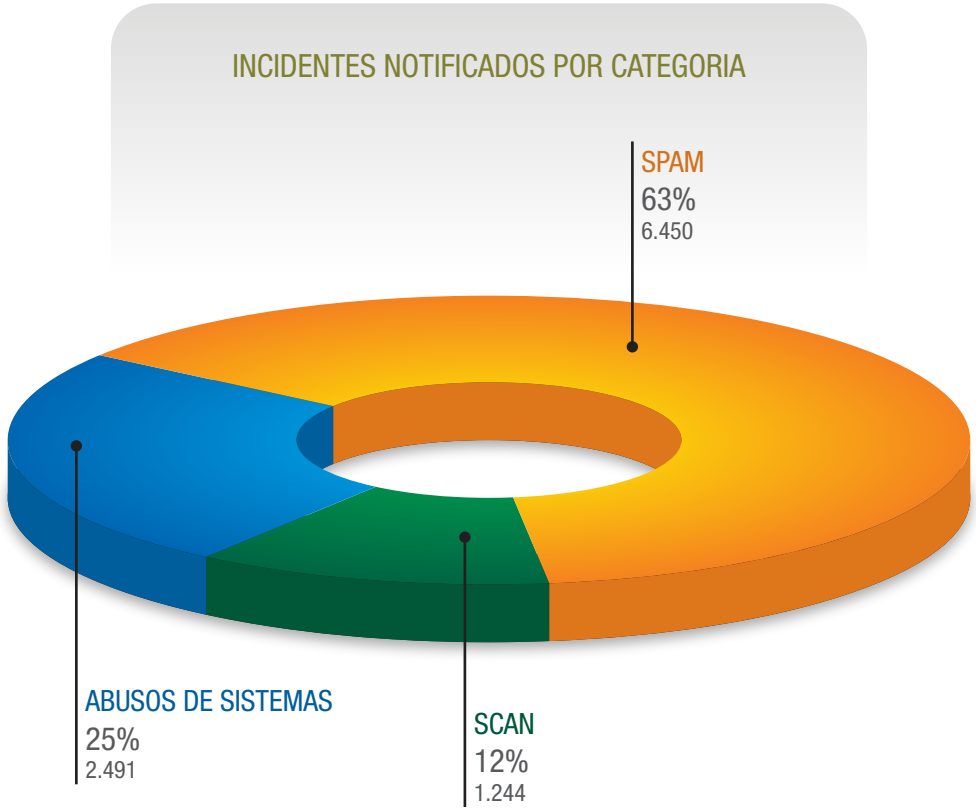
6 Ataques de negação de serviços

Os ataques de negação de serviço, cujo intuito é impedir um sistema de funcionar corretamente, minando seus recursos de hardware, software ou conexão, aumentaram em 136% na rede da RNP em 2010. Foram notificados 26 ataques de negação de serviço, sendo sete distribuídos (diversas máquinas atacantes) e 19 centralizados (uma única máquina atacante), contra um total de 11 notificações em 2009. Apesar da baixa quantidade de notificações se comparado aos casos de códigos maliciosos ou ao download de material protegido por direitos autorais, os ataques de negação de serviço são preocupantes pelo impacto que podem causar e pela dificuldade em serem contidos, quando se tratam de ataques distribuídos.



Spams, varredura por serviços abertos e abuso de sistemas

Os incidentes relacionados ao envio de spam, ao abuso de sistemas (open-relay, open-proxy) e à varredura por serviços abertos, através de testes com login e senha de usuários (SSH, FTP, etc.), totalizaram 10.185 notificações registradas pelo CAIS, com parciais de 63%, 25% e 12%, respectivamente.



CAIS

RNP

Ministério da **Cultura**

Ministério da **Educação**

Ministério da **Ciência e Tecnologia**

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Mais informações

RNP - Rede Nacional de Ensino e Pesquisa
www.rnp.br

CAIS - Centro de Atendimento a Incidentes de Segurança da RNP
www.rnp.br/cais

Incidentes de segurança relacionados à rede da RNP podem ser notificados através do endereço cais@cais.rnp.br.

Créditos

Ministério da Ciência e Tecnologia
Ministério da Educação
Ministério da Cultura

Rede Nacional de Ensino e Pesquisa
Nelson Simões
DIRETOR-GERAL

Diretoria de Serviços & Soluções
José Luiz Ribeiro Filho
DIRETOR

Centro de Atendimento a Incidentes de Segurança (CAIS)
Liliana Velásquez Solha
GERENTE

Coordenação Técnica
Atanaí Sousa Ticianelli
ANALISTA DE SEGURANÇA

Revisão
Gerência de Comunicação Corporativa

Projeto gráfico e diagramação
Tecnodesign

Contato: +55 19 3787-3300