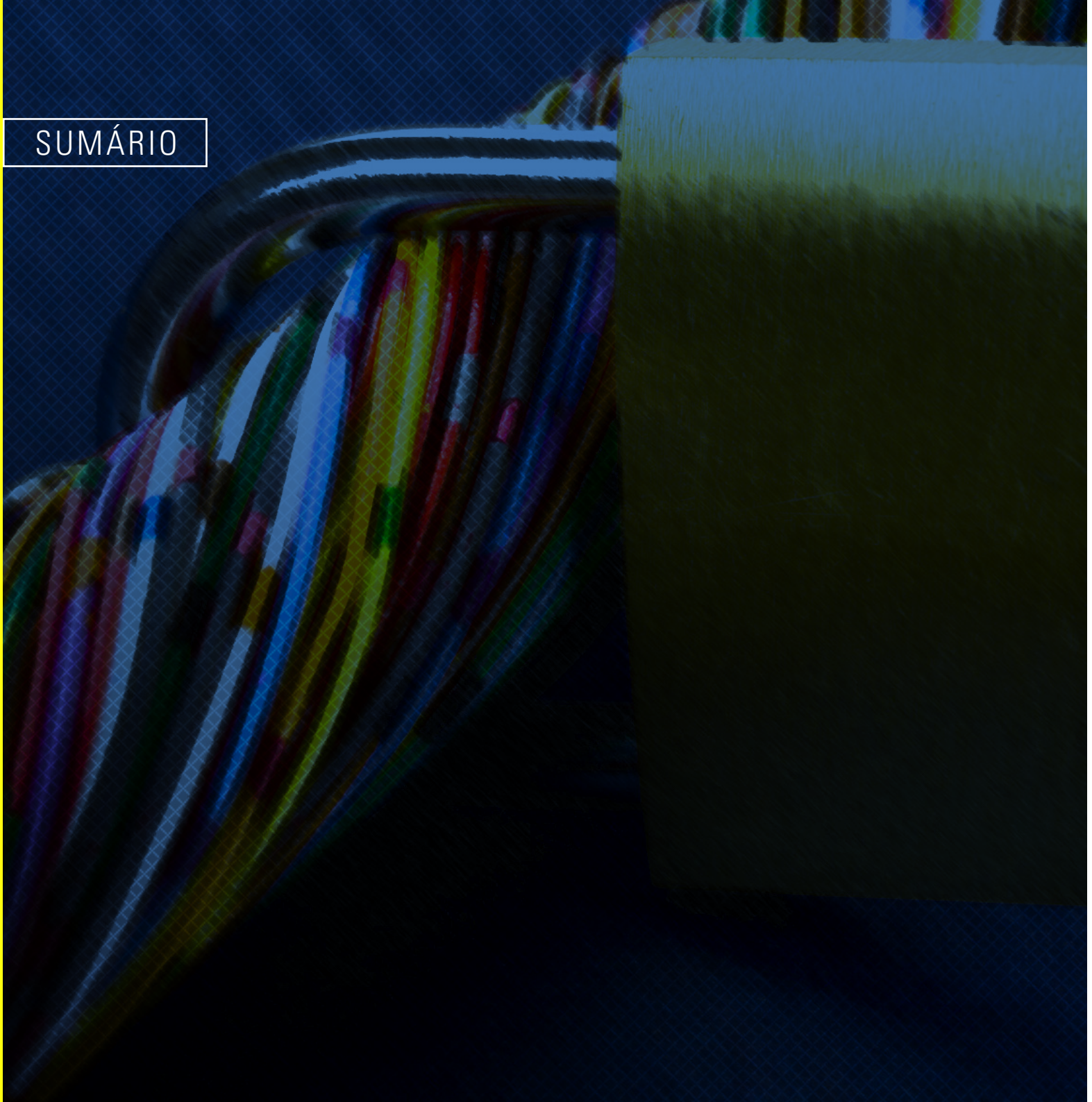
CAIS

RELATÓRIO ANUAL
INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 2013

RNP



SUMÁRIO

A RNP

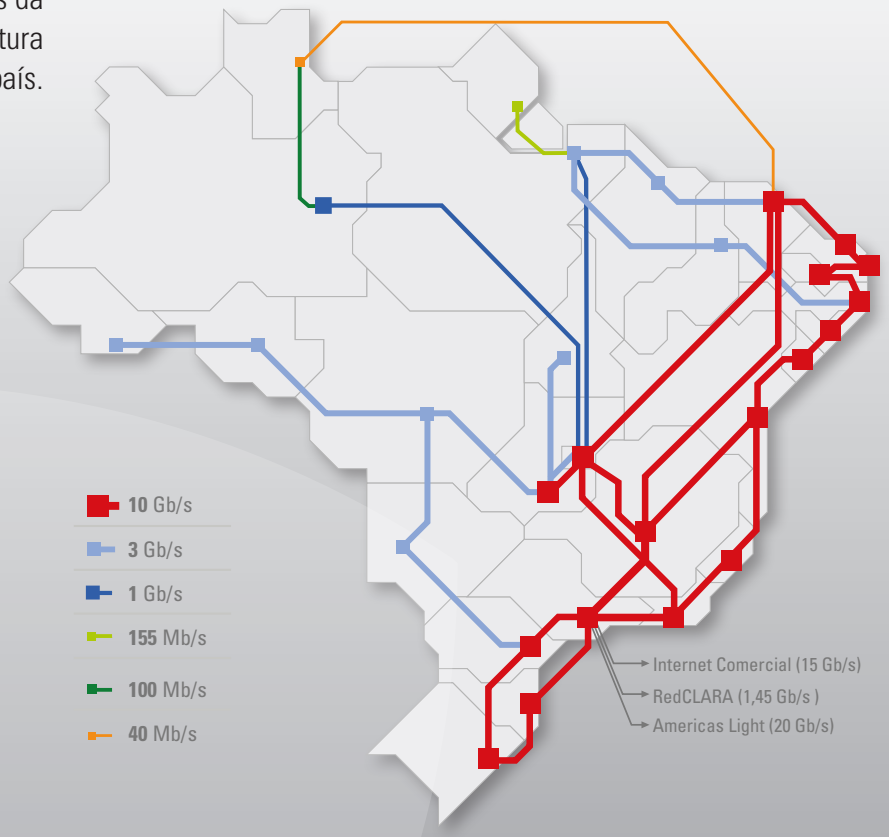
A RNP - Rede Nacional de Ensino e Pesquisa foi criada em 1989 pelo Ministério da Ciência e Tecnologia (MCT) com o objetivo de construir uma infraestrutura de rede Internet nacional para a comunidade acadêmica. Como primeira rede de acesso à Internet no Brasil, a RNP integra atualmente 1166 instituições de ensino e pesquisa no país, conectando mais de 3,5 milhões de usuários.

A RNP oferece conexão gratuita à Internet para instituições federais de ensino superior ligadas ao Ministério da Educação (MEC), unidades de pesquisa federais ligadas ao Ministério da Ciência, Tecnologia e Inovação (MCTI), agências de ambos os ministérios e outras instituições de ensino e de pesquisa públicas e privadas. Um universo estimado em cerca de três milhões e meio de usuários da comunidade acadêmica brasileira se beneficia dessa infraestrutura que estimula o progresso da ciência e da educação superior no país.

A REDE IPÊ

A rede Ipê, como é chamado o Backbone da RNP, é uma infraestrutura de rede Internet voltada para a comunidade brasileira de ensino e pesquisa. Nela conectam-se as principais universidades e institutos de pesquisa do país, servindo como um canal de comunicação rápido e com suporte a serviços e aplicações avançadas.

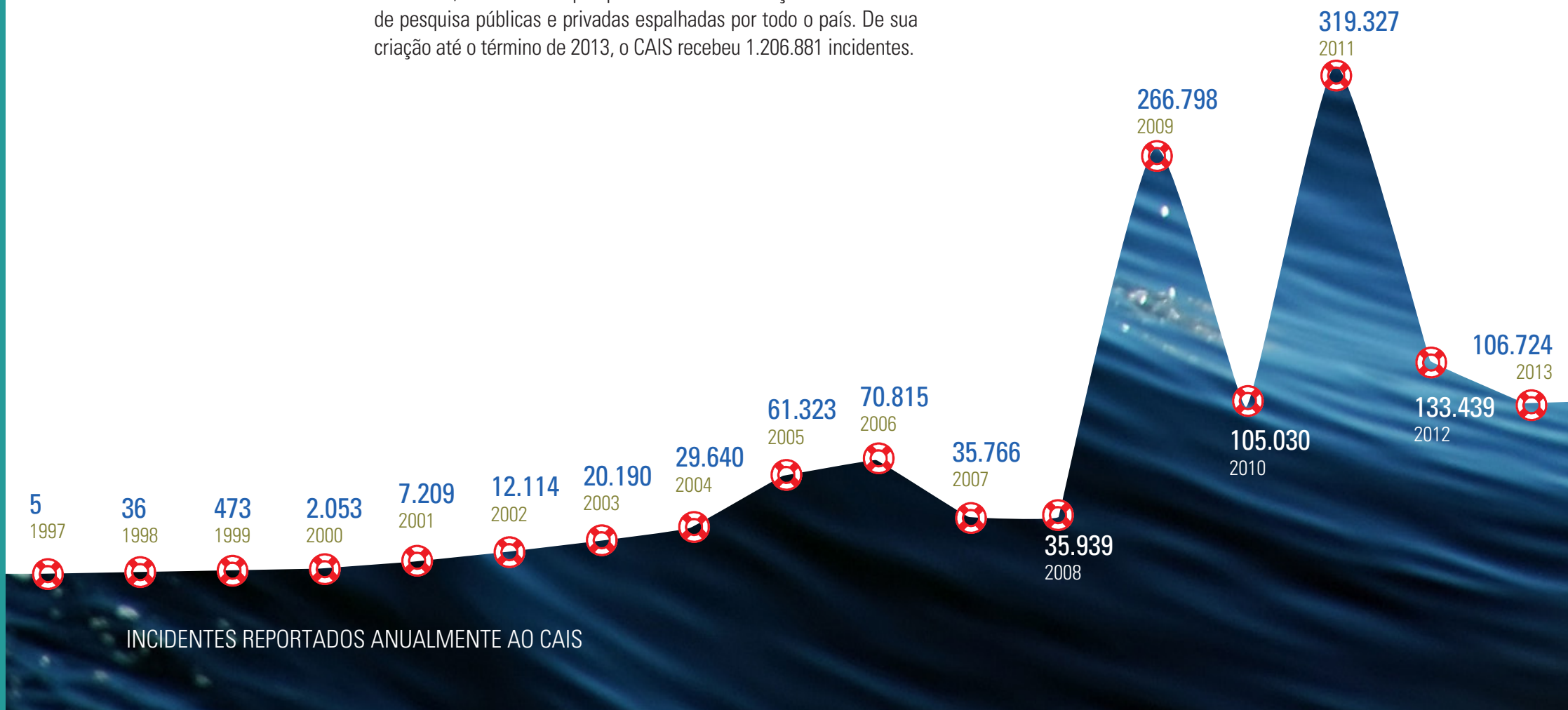
Baseada em tecnologia de transmissão óptica, a rede Ipê está entre as mais avançadas do mundo e possui conexão com redes acadêmicas estrangeiras, tais como RedClara (América Latina), Internet2 (Estados Unidos) e Géant (Europa).



O CAIS

Criado em 1997, o Centro de Atendimento a Incidentes de Segurança – CAIS foi criado para agir como CSIRT (*Computer Security Incident Response Team*), atuando na detecção, resolução e prevenção de incidentes de segurança na rede Ipê (rede acadêmica brasileira), além de elaborar, promover e disseminar práticas de segurança em redes na RNP e nas demais instituições a ela vinculadas.

Atualmente o CAIS atende 1166 instituições, em sua maioria centros de ensino, institutos de pesquisa e outras instituições de ensino e de pesquisa públicas e privadas espalhadas por todo o país. De sua criação até o término de 2013, o CAIS recebeu 1.206.881 incidentes.



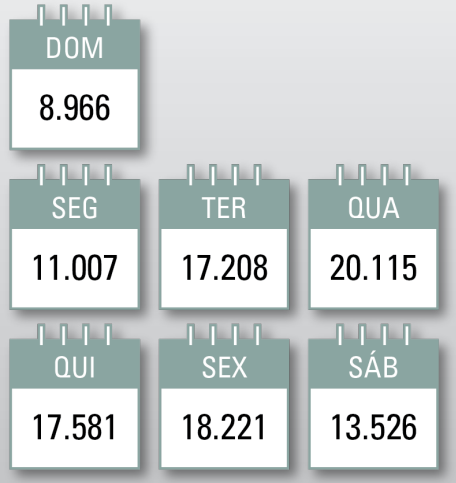
INCIDENTES REPORTADOS ANUALMENTE AO CAIS

O RELATÓRIO

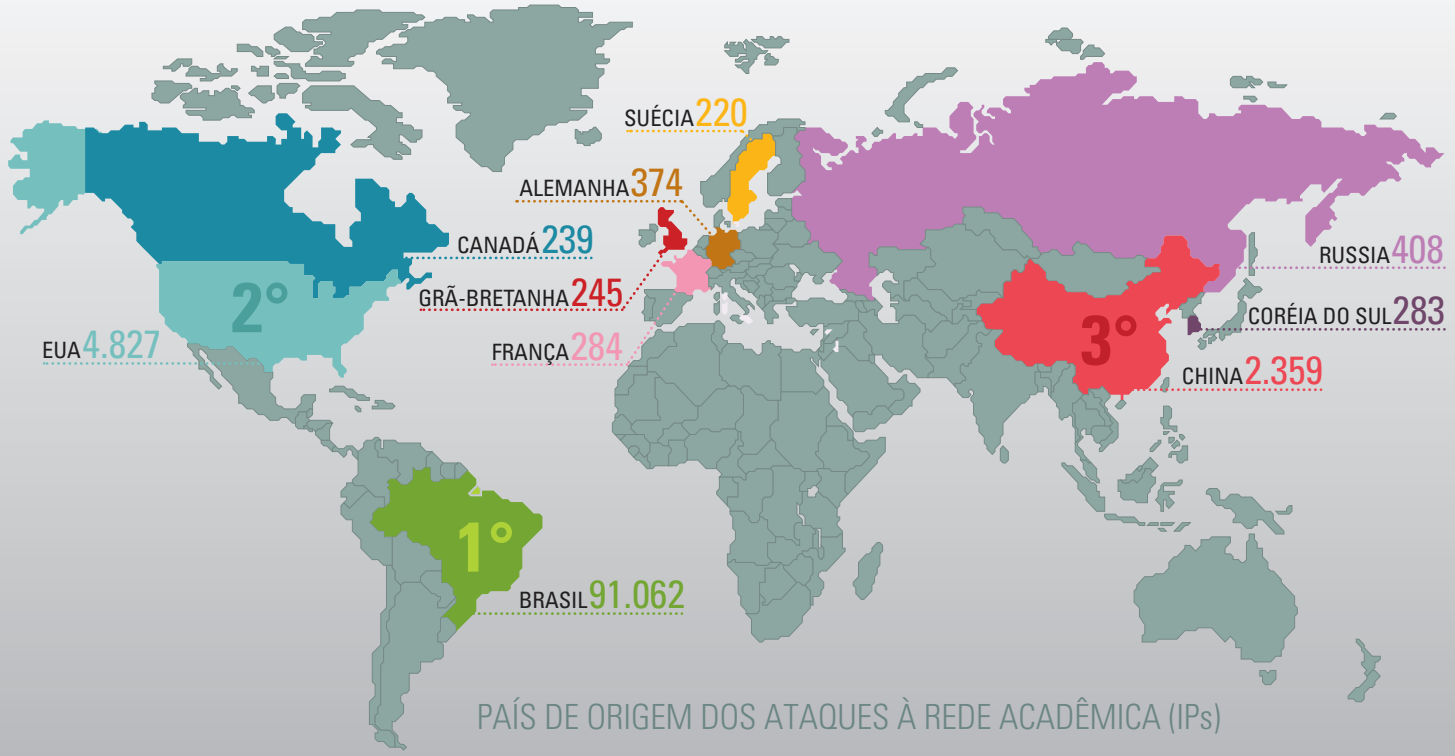
Nesta edição do Relatório Anual de Incidentes, a RNP oferece dados sobre os principais destaques de incidentes ocorridos em 2013 na rede Ipê (rede acadêmica brasileira), tais como o aumento considerável de ataques de negação de serviço (DDoS) e a redução no número geral de incidentes no ano.

DESTAQUES

2013 foi um ano de destaque no âmbito de Segurança da Informação no Brasil e no mundo. Notícias envolvendo *botnets*, ataques de negação de serviço distribuído (DDoS), roubo e vazamento de informações e as revelações do ex-analista da NSA, Edward Snowden, sobre os programas de vigilância norte-americanos, trouxeram à tona discussões sobre o quão seguras realmente estão as informações trafegadas na web e a que riscos estão expostos dados corporativos e pessoais. Outro fato relevante foi a exploração de vulnerabilidades de serviços essenciais de rede como o NTP e o DNS.



QUANTIDADE DE INCIDENTES
POR DIA DA SEMANA - 2013



PAÍS DE ORIGEM DOS ATAQUES À REDE ACADÊMICA (IPs)

Analisando os dados gerais dos incidentes reportados ao CAIS em 2013, destaca-se a diminuição de 20% no total de incidentes comparado a 2012. Em 2013, o CAIS registrou 106.724 incidentes, enquanto que, em 2012, foram registrados 133.439 incidentes.

Esta redução ocorreu principalmente nos ataques das categorias *Fraude*, com uma queda de 42,8% e *Código Malicioso*, com uma queda de 23,8%.

Como principais motivadores dessa diminuição podemos citar:

A desativação de *botnets* como a Rustock, Citadel e a ZeroAccess [1] (parcialmente desativada);

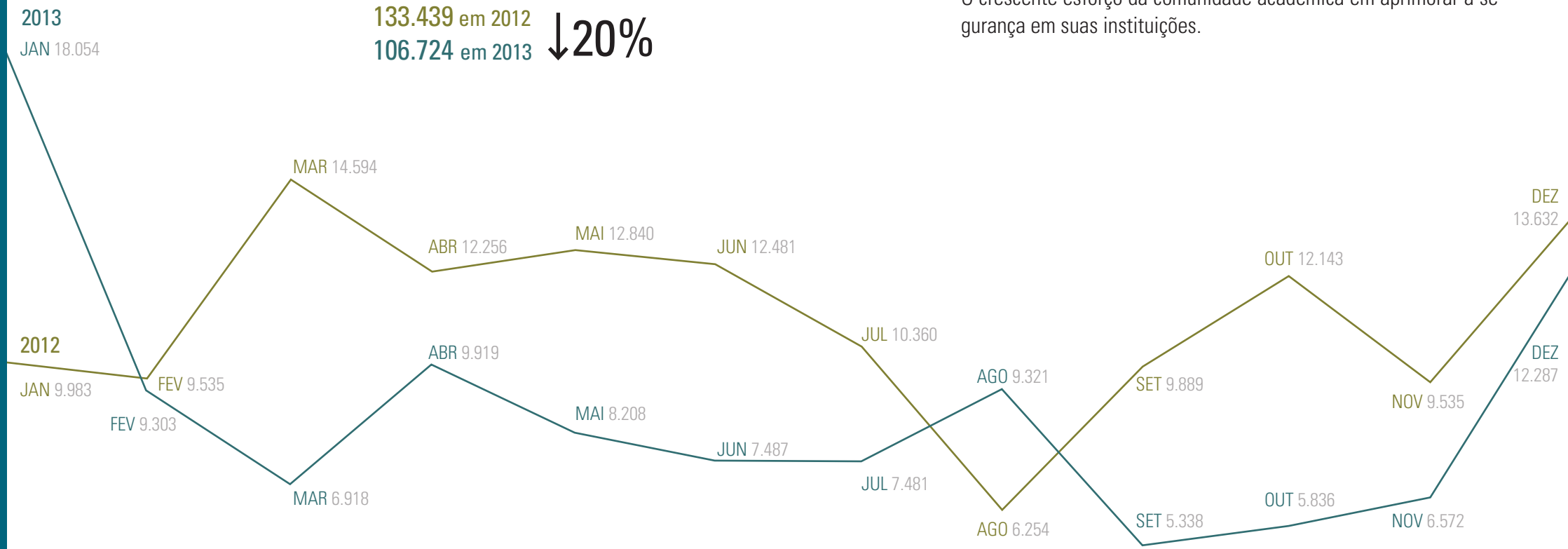
A melhoria no processo de triagem de incidentes do CAIS, que vem sendo refinada no decorrer dos anos com a aplicação de novos recursos e processos no tratamento das notificações;

O trabalho contínuo do CAIS junto à comunidade acadêmica na detecção e tratamento de incidentes e as ações de conscientização de segurança da informação;

O crescente esforço da comunidade acadêmica em aprimorar a segurança em suas instituições.

TOTAL DE INCIDENTES

133.439 em 2012
106.724 em 2013 ↓20%



QUANTIDADE DE INCIDENTES POR MÊS – COMPARATIVO 2012 E 2013

QUANTIDADE DE INCIDENTES POR CATEGORIA– COMPARATIVO 2012 E 2013

Em contrapartida, as categorias *Prospecção por informações*, *Tentativa de intrusão* e *Indisponibilidade de serviço ou informação* tiveram um aumento expressivo de 151,4%, 75,8% e 135%, respectivamente.

O aumento de incidentes envolvendo as categorias *Prospecção por Informações* e *Tentativa de Intrusão* ocorreu principalmente devido ao crescimento no número de incidentes envolvendo a exploração de vulnerabilidades dos serviços DNS e NTP, principalmente no quarto trimestre de 2013.

Já na categoria *Indisponibilidade de serviço*, várias máquinas conectadas à rede Ipê, por estarem infectadas, foram utilizadas em diversos ataques DRDoS (*Distributed Reflector Denial of Service*) contra algumas instituições bancárias americanas.[2] Outro fator para o aumento desse tipo de ataque está também relacionado à exploração de vulnerabilidades encontradas nos serviços DNS[3] e NTP[4], possibilitando ataques do tipo DRDoS.

[1] CITADEL
http://www.pcworld.com/article/2045282/microsoft-almost-90-percent-of-citadel-botnets-in-the-world-disrupted-in-june.html

RUSTOCK
http://www.theregister.co.uk/2011/03/23/rustock_takedown_analysis/

ZEROACCESS
http://nakedsecurity.sophos.com/2014/01/07/have-we-seen-the-end-of-the-zeroaccess-botnet/

[2] Ataques DRDoS contra bancos utilizando servidores DNS abertos
http://www.bankinfosecurity.com/are-ddos-attacks-against-banks-over-a-5801/op-1

[3] http://www.darkreading.com/attacks-breaches/misconfigured-open-dns-servers-used-in-r/240151862

[4] Ataques DRDoS utilizando má configuração de servidores NTP
http://www.darkreading.com/attacks-breaches/attackers-wage-network-time-protocol-bas/240165063

CÓDIGO MALICIOSO

Bot e *Botnet*

Bot é um código - na maioria das vezes malicioso - que tem por objetivo permitir que o atacante controle remotamente o computador ou dispositivo que o hospeda, este torna-se um hospedeiro utilizado na disseminação de *malwares*, envio de *spams* ou mesmo em ataques de negação de serviço (DoS). Os *Bots* são de difícil detecção, pois não seguem um padrão de desenvolvimento e podem se comportar de várias formas no dispositivo infectado, além de se conectarem à *Botnet* utilizando diversos protocolos.

Botnet é uma rede de *bots*, um conjunto de dispositivos em rede (computadores, tablets, smartphones e outros) infectados com *bots* e controlados pelo atacante com direcionamento e fins específicos. Quanto maior o número de *bots*, mais poderosa é considerada a botnet, já foram registradas *botnets* com até 2 milhões de *bots*. Atualmente é possível encontrar serviços de "aluguel de *botnets*" para ataques de negação de serviço, coleta de informações confidenciais, disseminação de *spam*, propagação de códigos maliciosos, entre outros.

O worm/*bot Conficker* foi o que teve maior destaque na rede acadêmica em 2013, com 40.814 incidentes. O CAIS vem promovendo ações de combate desde 2009, no entanto a presença desse *bot* ainda é muito expressiva.

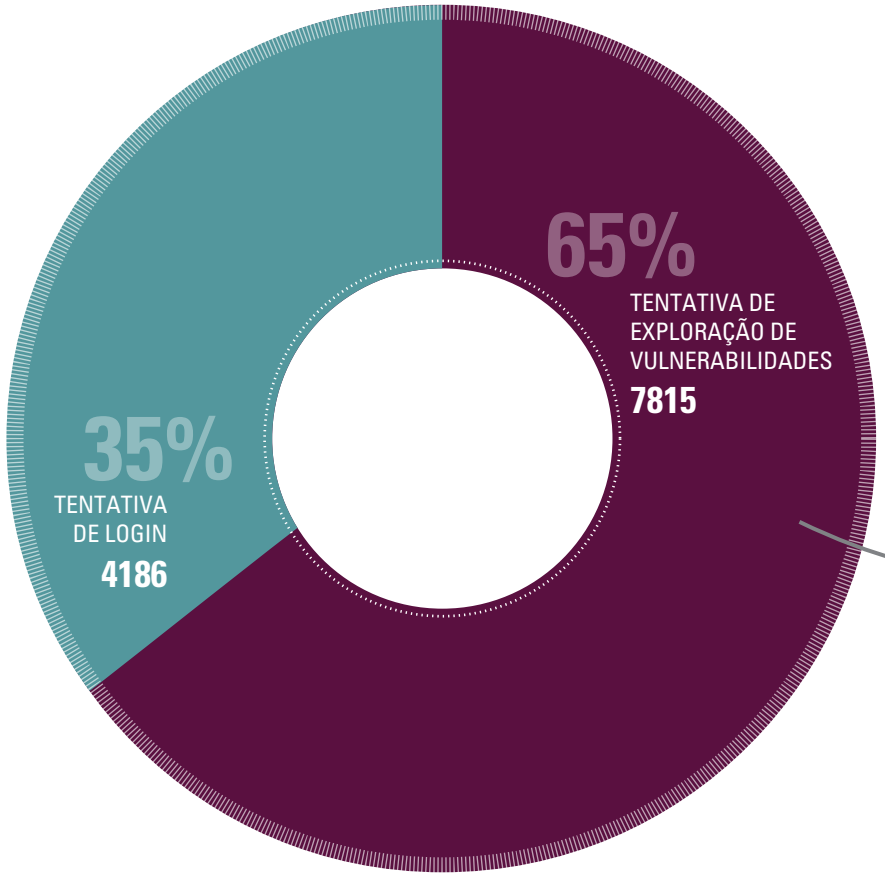
Em 2013, o *Conficker* foi o *Bot* que mais se destacou, com **40.814** incidentes.

TENTATIVA DE INTRUSÃO

Tentativa de exploração de vulnerabilidades

Os incidentes de tentativa de exploração de vulnerabilidade estão associados a *scan*. O *Scan* é um processo de varredura em redes de computadores, que tem como objetivo localizar serviços ou portas lógicas que estão ativas e podem ser exploradas. Funciona como uma busca de alvos para outros ataques, com base nas vulnerabilidades associadas a cada uma dessas portas ou serviços.

Nos meses de novembro e dezembro de 2013, o número de incidentes de tentativas de exploração de vulnerabilidades subiu exponencialmente. Em 2013 tivemos 12.001 incidentes, o que representa um aumento de 75,8% comparado a 2012, que teve 6.827 incidentes nessa categoria.



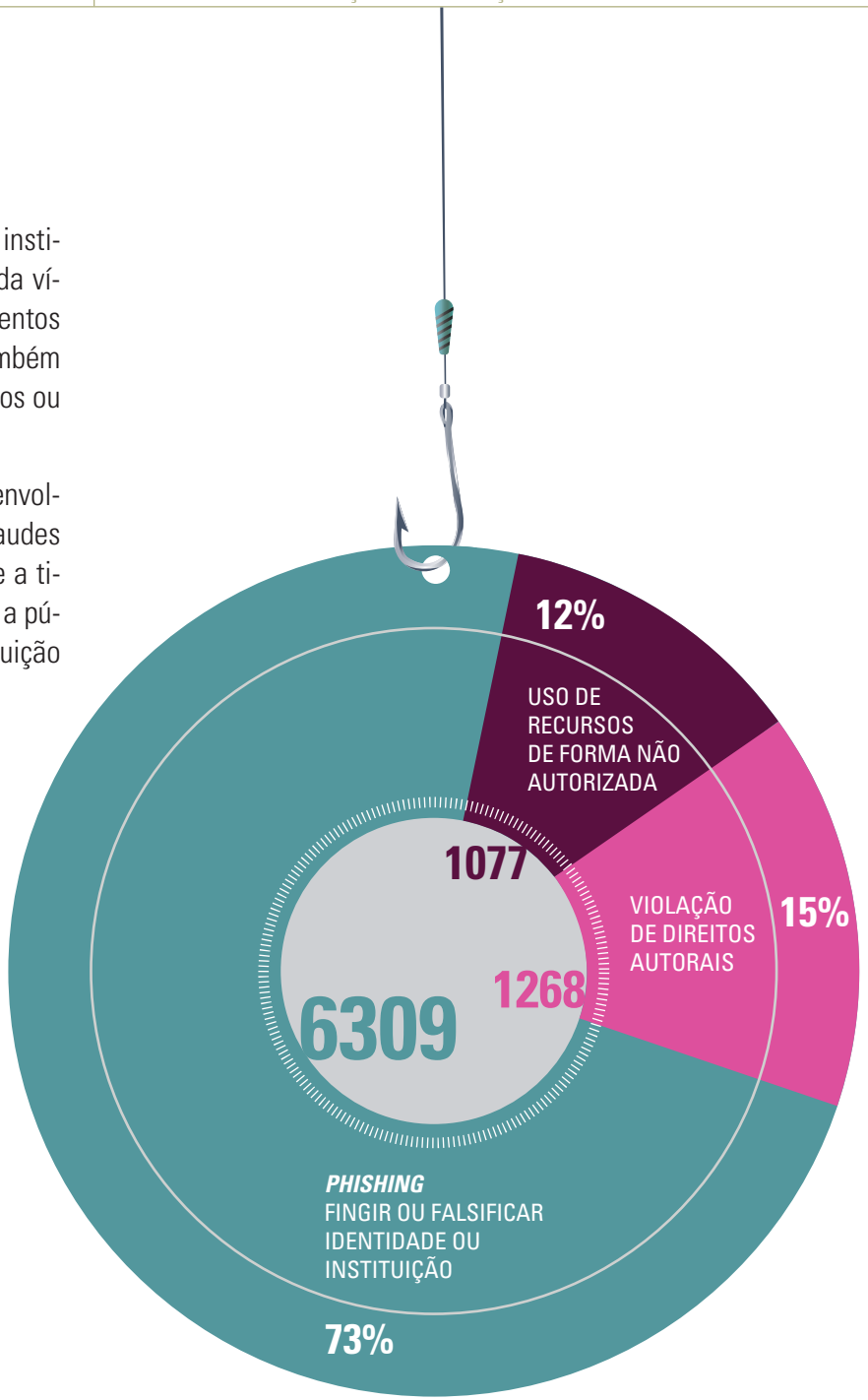
Aumento de **75,8%** comparado a 2012

FRAUDE

Phishing

Técnica onde o atacante tenta se passar por outra pessoa ou instituição para obter informações pessoais e senhas de acesso da vítima. Esses ataques muitas vezes se aproveitam de procedimentos comuns como cobrança de dívida e promoções sazonais, também exploram assuntos de destaque na mídia como grandes eventos ou escândalos envolvendo celebridades.

Em 2013, o CAIS recebeu 8.653 incidentes de fraudes, que envolveram falsidade ideológica, violação de direitos autorais e fraudes financeiras. Mais de 70% dos casos identificados referiam-se a tipos de *phishing*, como o Spear Phishing (*phishing* direcionado a públicos definidos, como por exemplo, funcionários de uma instituição ou clientes de uma empresa).



Mais de **1.300** incidentes relacionados a *spam* tratados em um único mês

CONTEÚDO ABUSIVO

Spam

Amplamente conhecida, a técnica de *spam* é utilizada com o intuito de enviar e-mails não solicitados em massa.

Se por um lado temos uma notável diminuição de incidentes de segurança envolvendo *spams* no ano de 2013, por outro se constata que mecanismos de ataque mais sofisticados e direcionados são incorporados nos *spams* enviados, na maior parte explorando a ingenuidade e curiosidade de muitos internautas interessados em assuntos e notícias recentes.

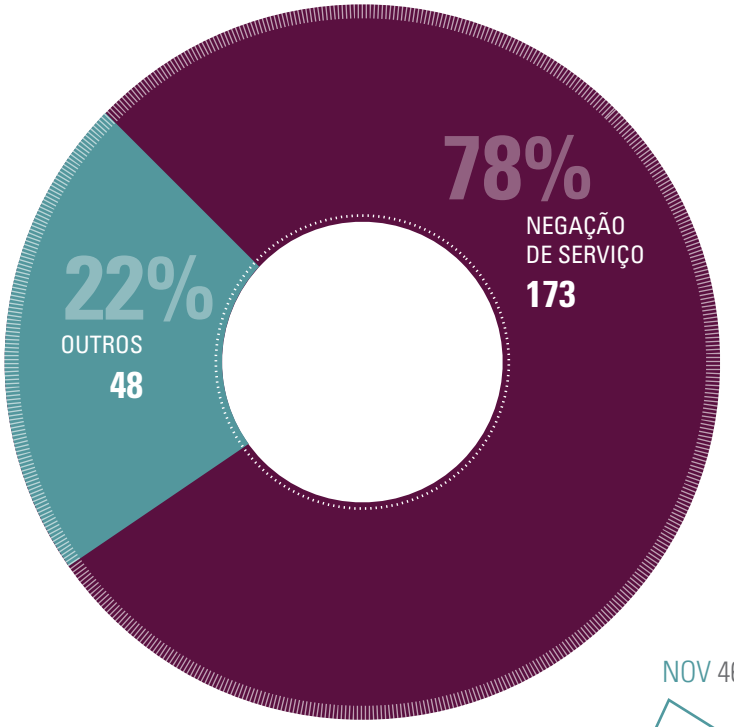
A busca pela informação atualizada, a curiosidade da suposta foto ou vídeo publicado com algum escândalo ou fato chocante torna a vítima mais vulnerável. Somente no mês de abril o CAIS tratou mais de 1.300 incidentes de *spam*, muitos deles associados às notícias do atentado na Maratona de Boston, por exemplo.

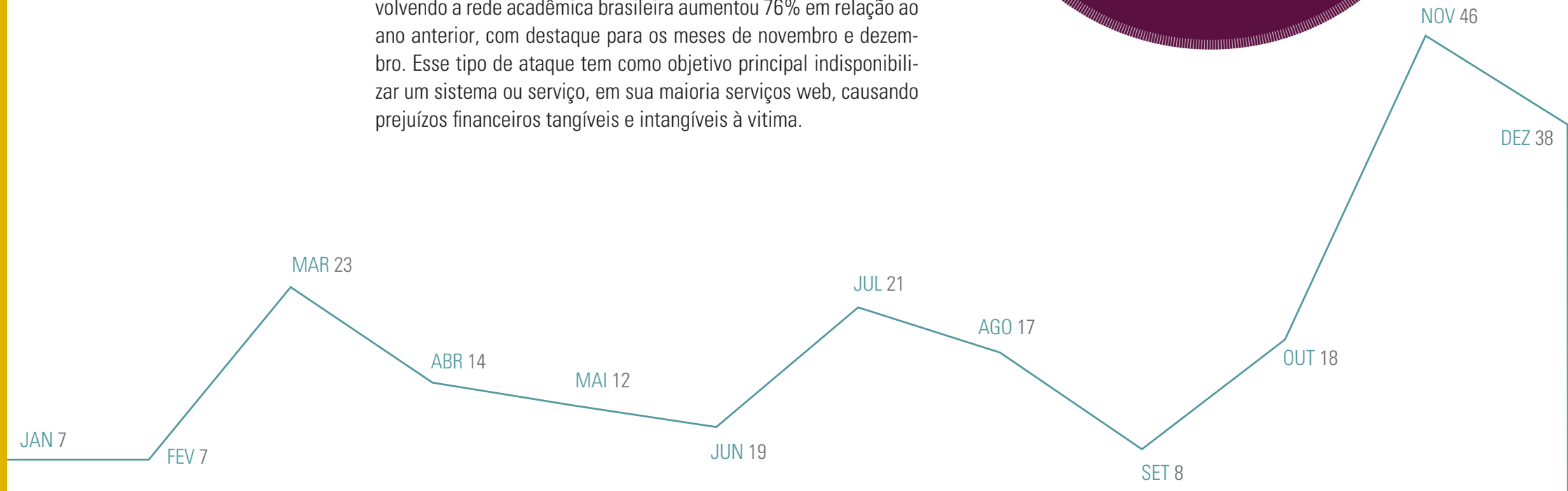
INDISPONIBILIDADE DE SERVIÇO OU INFORMAÇÃO

Ataques de Negação de Serviço (DDoS - *Distributed Denial of Service*)

Os ataques de negação de serviço ganham cada vez mais espaço no meio cibernético. Isso devido a sua capacidade de degradar e indisponibilizar sistemas, redes ou serviços. Basicamente, os ataques DDoS são orquestrados por um atacante que aciona diversas máquinas anteriormente infectadas (que fazem parte de uma *botnet*), ou ainda de máquinas vulneráveis ou mal configuradas e conectadas à internet. Essas máquinas então enviam comandos de conexão ou consumo de serviço do alvo atacado, gerando uma demanda insustentável pelo mesmo.

No ano de 2013, o número de ataques de negação de serviço envolvendo a rede acadêmica brasileira aumentou 76% em relação ao ano anterior, com destaque para os meses de novembro e dezembro. Esse tipo de ataque tem como objetivo principal indisponibilizar um sistema ou serviço, em sua maioria serviços web, causando prejuízos financeiros tangíveis e intangíveis à vitima.





TENDÊNCIAS EM INCIDENTES DE SEGURANÇA NA REDE ACADÊMICA BRASILEIRA E NO MUNDO

Prever os ataques que terão maior destaque em 2014 não é uma tarefa fácil, mas algumas tendências são muito fortes e merecem destaque:

- Apesar do número de ataques de malwares diminuir nos últimos anos (vide página 06 deste relatório), apontando a tendência de queda em 2014, a severidade desses ataques será ainda maior e os alvos cada vez mais específicos. Ou seja, embora o número de ataques diminua, o risco a eles associados aumenta ainda mais.
- Com base nas estatísticas dos anos de 2012 e 2013, os *exploit kits* continuarão sendo a principal ameaça para sistemas operacionais. No caso da Microsoft, mesmo com os esforços para elevar o padrão de segurança de seu sistema operacional, o placar ainda é desfavorável.
- Em 2014 o Windows XP completa 13 anos de existência e deixa de receber atualizações e suporte da Microsoft, tornando-se um grande alvo de ataques, uma vez que ele ainda é bastante utilizado.
- Os ataques do tipo ransomware serão mais frequentes. Nessa modalidade, o atacante criptografa arquivos da vítima e essas informações só são liberadas mediante pagamento "de resgate", seja em moeda convencional ou virtual (como Bitcoin).
- Os ataques aos dados em nuvem aumentarão. Com a prática cada vez maior de armazenamento de dados e disponibilização de serviços na nuvem, a escolha dos cibercriminosos por esses alvos também aumentará.
- O *Conficker* ainda estará presente em 2014. Com base em dados de incidentes de 2013 na rede acadêmica brasileira, estima-se que há ainda uma quantidade considerável de computadores hospedando o *conficker*. Pesquisas recentes também mostram que o *Conficker* tem uma grande presença no Brasil, o que indica uma falha generalizada em seguir as boas práticas de segurança (atualização do sistema operacional, utilização eficiente de antivírus entre outras).
- Vulnerabilidades em dispositivos móveis serão ainda mais exploradas pelo fenômeno cada vez mais comum no meio corporativo e acadêmico BYOD ("Bring Your Own Device", em português: traga seu próprio dispositivo). Isso, somado à relativa imaturidade em segurança móvel, fará com que o usuário introduza, inadvertidamente, malwares nas redes em que se conectar.
- A contratação de *Botnets* aumentará em 2014. A possibilidade de pagar por um serviço de *Botnet* (sem a necessidade de desenvolver e disseminar malwares) atrairá interessados em atacar redes ou serviços web, principalmente para ataques com fins comerciais.

Com todo esse cenário, o CAIS reforça a necessidade de se estabelecer um programa de segurança da informação eficiente, destacando-se algumas iniciativas:

- Implementação estruturada de controles de segurança
- Estabelecimento de um plano efetivo de segurança da informação
- Implementação de soluções tecnológicas integradas a processos maduros, aliados a políticas de segurança formalmente estabelecidas e aplicadas a todos os usuários
- Estabelecimento de um processo de avaliação contínua de riscos
- Implementação de um programa de conscientização de segurança eficiente

Em 2014, não apenas a evolução dos ataques deve ser assistida, mas também a melhoria nos processos e tecnologias que englobam a segurança da informação. O CAIS continuará presente nesse cenário atuando na prevenção, detecção e tratamento desses incidentes, assim como em iniciativas para a diminuição de riscos e conscientização em segurança da informação.

CRÉDITOS

RNP
Rede Nacional de Ensino e Pesquisa

Nelson Simões
Diretor Geral

José Luiz Ribeiro Filho
Diretor de Serviços e Soluções

Realização:

CAIS
Centro de Atendimento a Incidentes de Segurança da RNP

Liliana Velásquez Solha
Gerente de Segurança da Informação

Edilson Lima
Coordenador de Gestão de Incidentes de Segurança

Equipe técnica:
Alan Santos
Rildo Souza

Contribuições:
Ana Carolina Fukushima
André Landim
Carla Freitas
Júlio Henrique
Ronald Huppers
Thais Godinho
Vanessa Suzuki
Yuri Alexandro

Projeto gráfico e diagramação:
Tecnodesign

Para maiores informações sobre a RNP, o CAIS e Incidentes de Segurança da Informação, visite:

www.rnp.br/cais

CAIS

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

GOVERNO FEDERAL

BRASIL

PAÍS RICO É PAÍS SEM POBREZA