DDoS na Rede Ipê

Contendo ataques do tipo "*all your giga links belong to us*" no backbone acadêmico brasileiro

Frederico R. C. Costa
Coordenador de segurança da informação
CAIS / RNP

GTER 33 / GTS 19
Natal – RN
Maio/2012

AGENDA

- Rede Nacional de Ensino e Pesquisa – RNP
- Centro de Atendimento a Incidentes de Segurança – CAIS
- Histórico de incidentes em 2011
- Preocupações
- Ataques e contenções aplicadas
- Conclusão

- **RNP – Rede Nacional de Ensino e Pesquisa**
  - Criada em 1989 pelo MCT
  - Primeira rede de acesso à internet no Brasil
  - Conexão de internet para instituições de ensino superior e unidades de pesquisa (Rede Ipê)
  - Desenvolvimento e uso de aplicações avançadas em rede
  - Treinamento de profissionais em redes
  - Atualmente, está no 6o estágio de desenvolvimento do backbone

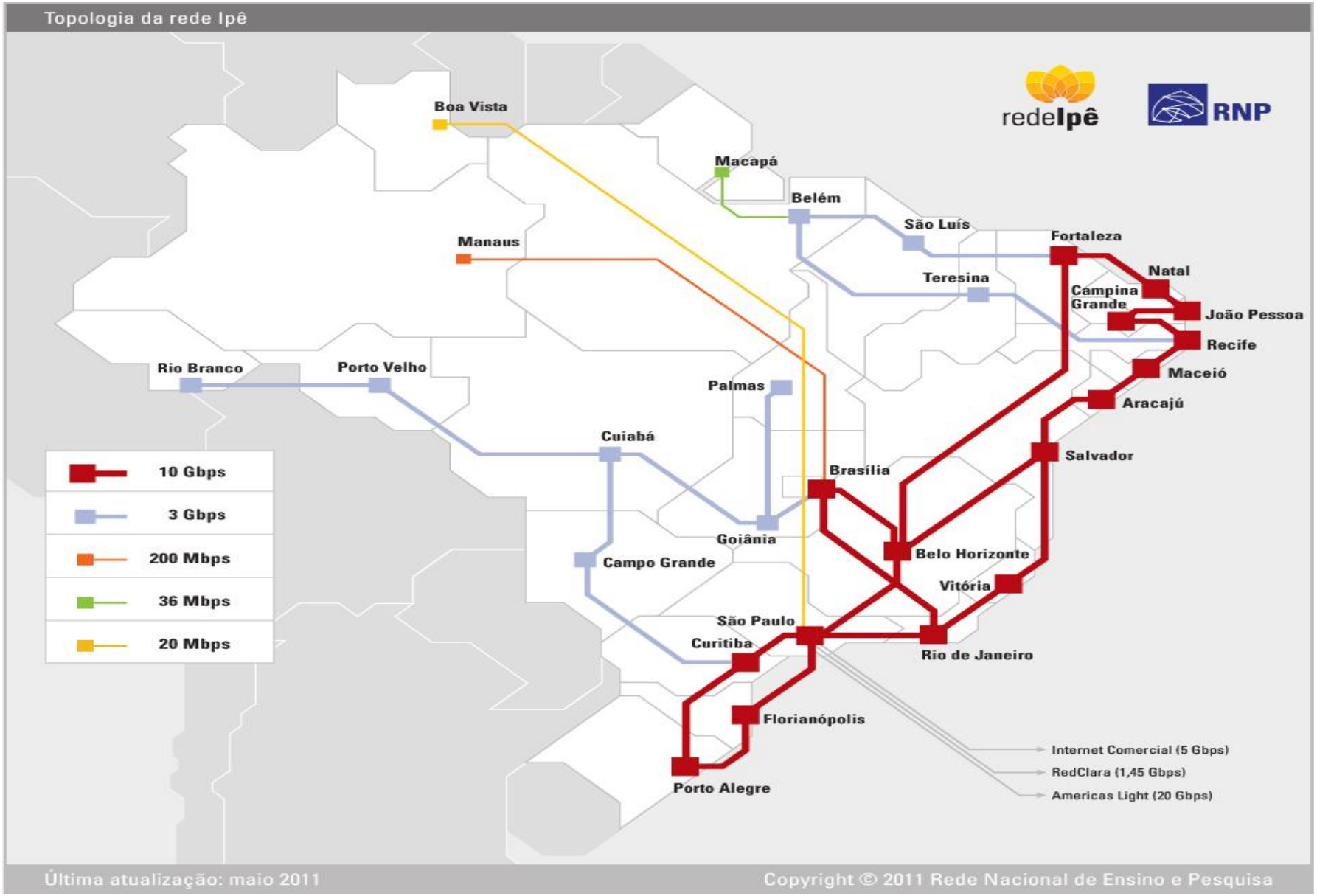
- **CAIS – Centro de Atendimento a Incidentes de Segurança**
  - Área criada em 1997 na RNP
  - Gestão de Incidentes de Segurança
  - Disseminação da Cultura de Segurança
  - Gestão de Riscos e Segurança da Informação
  - Infraestrutura e Serviços à Comunidade Acadêmica

- **Rede Ipê: sexta geração**
  - Mais de 800 instituições conectadas
  - 3,5 milhões de usuários estimados
  - 27.500 grupos de pesquisa beneficiados
  - Universidades federais, escolas agrotécnicas, centros federais de educação tecnológica, centros de pesquisa, hospitais, museus, outros.

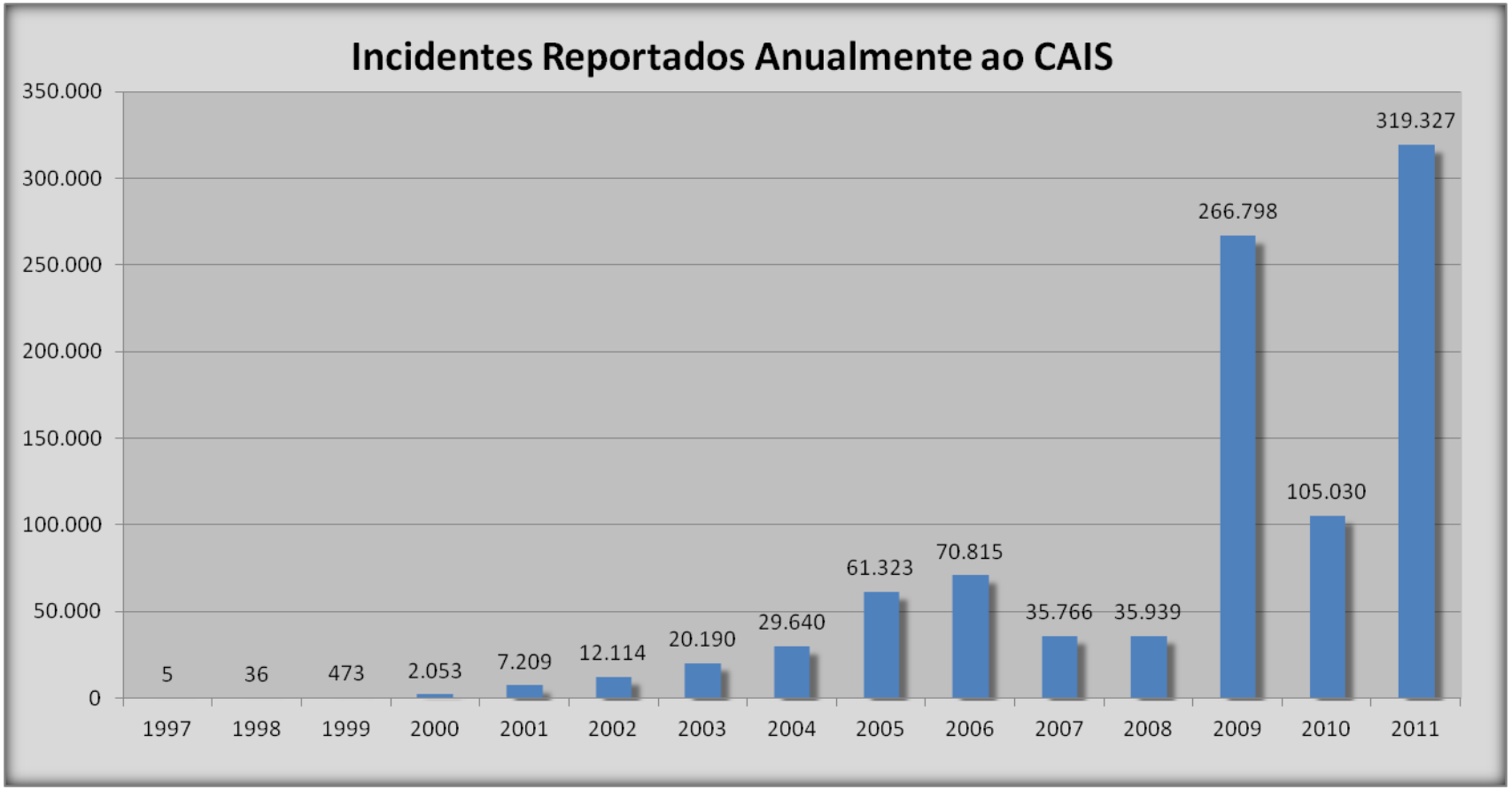
"A RNP está na ponta de lança da construção de uma sociedade do conhecimento. Depende do Plano Nacional de Banda Larga e da RNP dar suporte às instituições brasileiras de formação de capital humano."

Aloízio Mercadante – MCTI – 13/07/2011

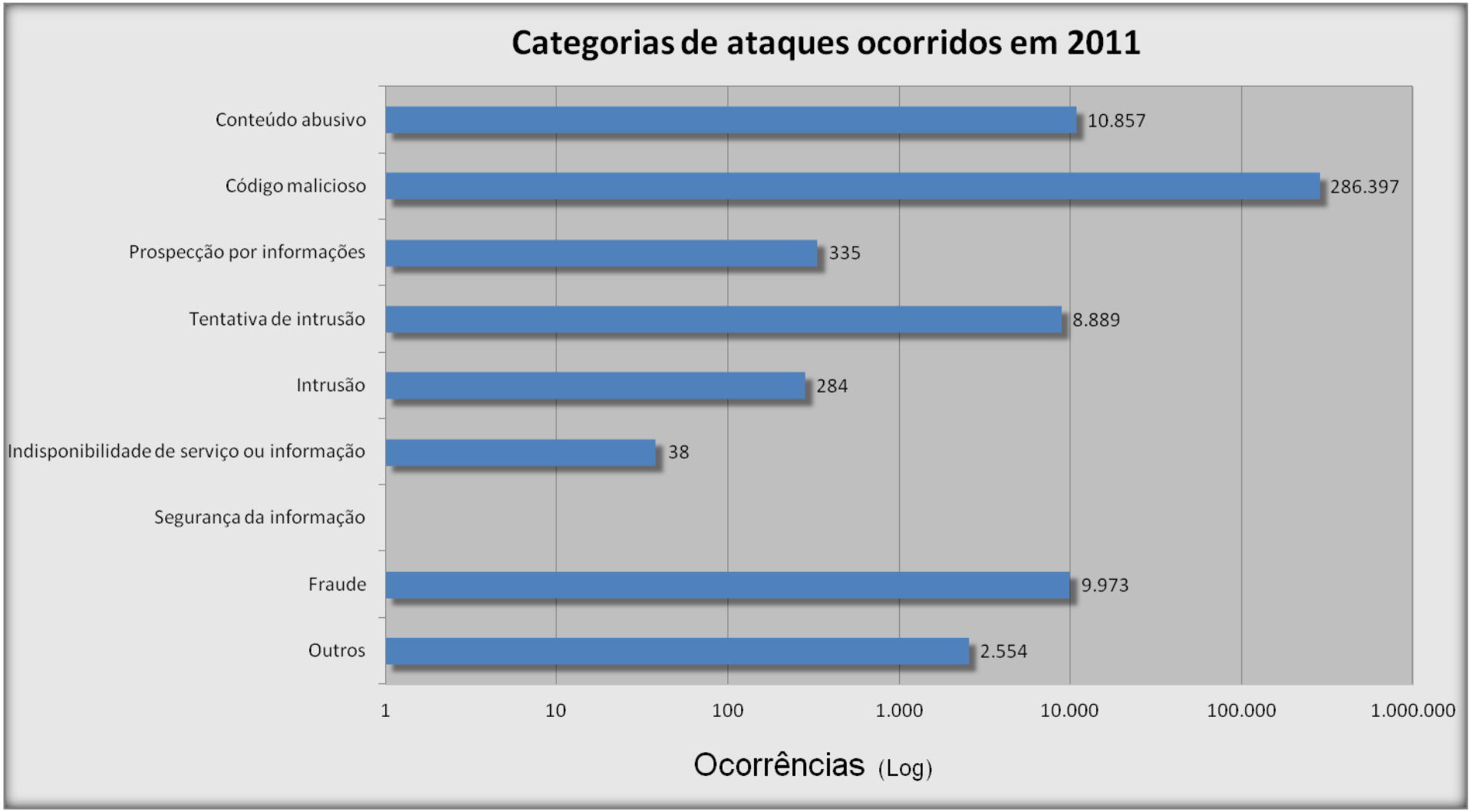
Rede Ipê


Topologia da rede Ipê
redeIpê
RNP
Boa Vista
Macapá
Belém
São Luís
Fortaleza
Manaus
Teresina
Natal
Campina Grande
João Pessoa
Recife
Rio Branco
Porto Velho
Maceió
Palmas
Aracajú
Cuiabá
Salvador
Brasília
10 Gbps
3 Gbps
200 Mbps
36 Mbps
20 Mbps
Goiânia
Belo Horizonte
Campo Grande
Vitória
São Paulo
Curitiba
Rio de Janeiro
Florianópolis
Internet Comercial (5 Gbps)
RedClara (1,45 Gbps)
Americas Light (20 Gbps)
Porto Alegre
Última atualização: maio 2011
Copyright © 2011 Rede Nacional de Ensino e Pesquisa

Histórico de incidentes



Histórico de incidentes



- **Bots em 2011**
  - **281.965** incidentes reportados
    - 53 % Downadup
    - 42% Outros
    - 3% Sality
    - 2% Conficker
    - 1 Zeus
  - **11.754** endereços IP únicos

- **Backbone com alta capacidade/disponibilidade de banda**
- **Instituições de ensino, pesquisa, cultura e saúde conectadas**
  - Enorme quantidade de computadores conectados
- **Pontos de troca de tráfego com grandes "players"**
- **IDC – Data Center da RNP**
  - Hospeda equipamentos de clientes na modalidade *colocation*, disponibilizando acesso ao backbone acadêmico
    - CAPES
    - INEP
    - CNPQ
    - FNDE
    - Entre outros

- **2011 – DDoS "fashion year"**
  - Ataques de negação de serviço se tornam "armas" para grupos hackers e para outros grupos auto-denominados de "cyberativistas";
  - Diversos grupos "recrutam" usuários pela Internet em prol de uma causa ou objetivo em comum;
  - Instituições e corporações das mais diversas áreas foram afetadas por este "movimento".

** Imagens coletadas diretamente do Twitter*

*** http://webtrends.about.com/od/profile1/tp/Rage-Faces-Internet-Meme-Faces-And-Funny-Memes.htm*

- **Ataques contra os clientes da RNP**
  - Um cliente importante sofreu um ataque de aproximadamente 700Mbps, indisponibilizando o acesso às informações em um momento crítico
    - Este ataque foi mitigado e contido
  - Uma instituição foi citada para ser atacada, em uma conversa em um canal IRC de um grupo de “cyberativistas”
    - Este ataque não chegou a ocorrer ou não foi suficientemente significativo para ser detectado

```
<hlbbit> pacota esse 150.162.2.10
* AttaXX (bels@AN-d77.tua.qj9f10.IP) has joined #LulzSecBrazil
* _0RL0FF_ (_0RL0FF_@AN-6j1.1l5.rnpprb.IP) has joined #LulzSecBrazil
<shibi> esse ip é de onde?
<hlbbit> universidade federal
<Lefioda> ufsc
<hlbbit> de santa catarina
```

- **Utilização de computadores conectados à RNP envolvidos em ataques**
  - Dados coletados em atividades de monitoramento e informações enviadas por parceiros mostram que indivíduos supostamente ligados a grupos como Anonymous e Lulzsec pretendiam utilizar o backbone da RNP em seus ataques.
    - Esta utilização do backbone não ocorreu

```
Jun 22 13:03:51 <JC_muahaha>    as conexoes do brasil, ainda que
pontuais
Jun 22 13:03:53 <JC_muahaha>    passam por backbones
Jun 22 13:04:07 <JC_muahaha>    ou seja, eles roteiam as informacoes
que entram no pais
Jun 22 13:04:54 <JC_muahaha>    podemos usar um DDOS mais potente
Jun 22 13:04:56 <JC_muahaha>    e deixar o brasil inteiro
Jun 22 13:04:57 <JC_muahaha>    isolado
Jun 22 13:04:59 <JC_muahaha>    da internet mundial
Jun 22 13:05:01 <JC_muahaha>    por exemplo
Jun 22 13:05:08 <JC_muahaha>    hackers fizeram isso na espanha
Jun 22 13:05:09 <JC_muahaha>    ha uns 6 anos
...
Jun 22 13:17:35 <pr0teus>       JC_muahaha:  ate tenho uma solucao
Jun 22 13:18:04 <pr0teus>       JC_muahaha: parte da RNP eh ligada ao
exterior por backbones proprios...
Jun 22 13:18:29 <pr0teus>       JC_muahaha: basta só ter acesso a
alguns servidores da RNP
Jun 22 13:19:19 <JC_muahaha>    pr0teus, esse eh um bom caminho
```

- **Em 2011 38 ataques críticos de negação de serviço envolvendo endereços IP da Rede Ipê foram tratados**
- **Ataques com maior impacto:**
  - TCP Flood:
    - Instituição em DF (Destino) – 682 Mbps / 2.1 Mpps (DDoS)
    - Instituição em ES (Origem) – 386.9 Mbps / 43.4 Kpps
    - Instituição em ES (Origem) – 255.9 Mbps / 25.9 Kpps
    - Instituição em RJ (Desitno) – 40.3 Mbps / 105 Kpps (Ddos)
    - Instituição em SC (Origem) – 27.1 Mbps / 65. 28 Kpps
    - Instituição em ES (Origem) – 8.19 Mbps / 19.68 Kpps
  - UDP Flood :
    - Instituição em SC (Origem) – 545.8 Mbps / 631.7 Kpps
    - Instituição em SC (Origem) – 541.2 Mbps / 626.4 Kpps
    - Instituição em SC (Origem) – 533.62 Mbps / 617.61 Kpps
    - Instituição em AM (Destino) – 352.9 Mbps / 1.5 Mpps (DDoS)
    - Instituição em CE (Destino) – 143.42 Mbps

- ***"Remember… Remember… The 5th November."***
  - Diversos grupos anunciaram ataques contra corporações e instituições no dia 05 de Novembro, em uma alusão a data citada no filme "V de Vingança";
  - Durante o dia foram detectados 10 ataques na Rede Ipê;
  - Ataques iniciaram por volta das 15h30 e tiveram duração de 40 minutos;
  - Cerca de 1.9 Gbps de tráfego malicioso foi detectado durante o período

** http://www.salon.com/2011/07/27/lulzsec_topiary_arrest/*

*** http://www.inquisitr.com/156983/2011-guy-fawkes-day-celebrated-by-occupy-protesters/*

- **Mitigação X Término do Ataque**

  - A média de tempo entre a detecção de um ataque e sua mitigação é em torno de 30 minutos;
    - Tempo de análise do ataque (evitar falsos positivos) + aplicação de filtro
    - Ataques identificados no dia 05 de novembro, individualmente, não duraram o suficiente, dispensando qualquer ação de mitigação..
  - As ações de mitigação são tomadas em conjunto com as equipes de engenharia e operações de rede
  - Detecção por monitoramento e/ou solicitações das instituições impactadas/envolvidas nos ataqes

• Mitigação X Término do Ataque

– Alguns ataques continuam por dias, após a aplicação dos filtros aplicados.

– Um determinado ataque contra uma instituição durou cerca de 09 dias seguidos;

– Responsável pelo equipamento que originava os ataques estava de férias!!! Nenhum outro analista foi autorizado a desativar o equipamento. =(

- UDP flood – 143.42 Mbps
  - Inicio: 09/09/11 – 14:04
  - Mitigação: 09/09/11– 15:38 (filtro aplicado)
  - Término: 19/09/2011 – 11:20 (máquina retirada da rede pelo adm)

- **A detecção deste tipo de tráfego é possível através de um monitoramento constante de amostras do tráfego do backbone (flows)**
- **A integração da equipe de segurança, engenharia e operações do backbone é fundamental para a contenção dos ataques**
- **O apoio de outros grupos de segurança é fundamental para a detecção de hosts infectados**
  - http://www.enisa.europa.eu/activities/cert/support/proactive-detection
- **Campanhas para "limpeza" da fauna de bots são necessárias de tempos em tempos**
  - Conficker (2009) – diminuição de 40% de hosts infectados

Obrigado!!!

Centro de Atendimento a Incidentes de Segurança CAIS/RNP

http://www.rnp.br/cais/

@caisrnp

http://www.facebook.com/caisRNP

http://www.orkut.com.br/Main#Profile?uid=15632011403178010 54

Notificação de Incidentes

Para encaminhar incidentes de segurança envolvendo redes conectadas à RNP:

1. E-mail: cais@cais.rnp.br

Para envio de informações criptografadas use a chave PGP pública do CAIS: http://www.rnp.br/cais/cais-pgp.key

2. Formulário para Notificação de Incidentes de Segurança: http://www.rnp.br/cais/atendimento_form.html

Hotline INOC-DBA (Inter-NOC Dial-By-ASN): 1916*800

Atendimento Emergencial: Para contato fora do horário comercial (09:00 - 18:00 - Horário de Brasília) por favor utilize o telefone (61) 226-9465.

Alertas do CAIS: O CAIS mantém a lista rnp-alerta@cais.rnp.br. Assinatura aberta à comunidade de segurança. Inscrição através do formulário em:

http://www.rnp.br/cais/alertas/