Estratégias de Defesa Contra Ataques de Negação de Serviço

GTS 26 – São Paulo/SP – 11/dez/2015

Gustavo Rodrigues Ramos
grramos@uoldiveo.com

Agenda

- Introdução
- Tipos de Ataques de Negação de Serviço
- Planejamento
- Detecção
- Contra-medida

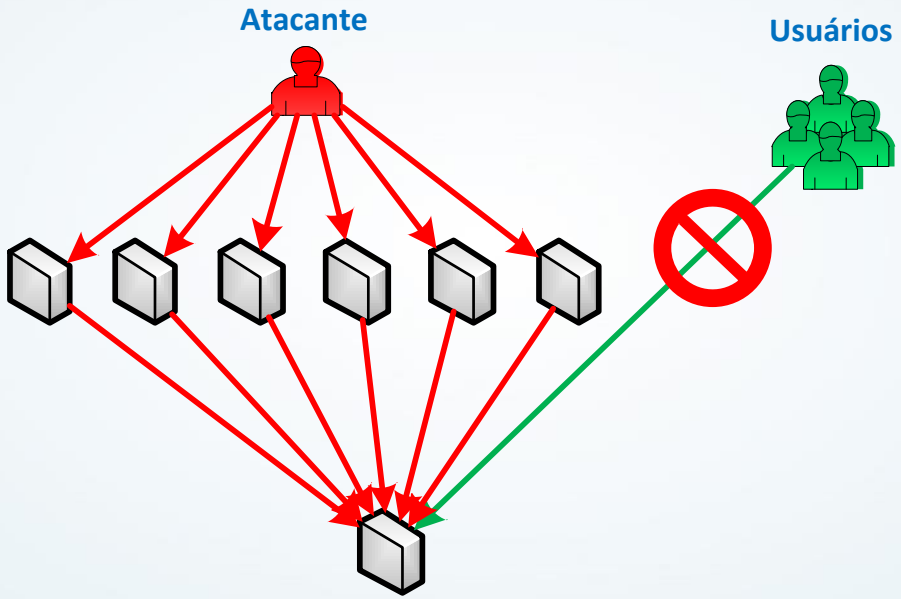
UOL DIVEO SER

Introdução

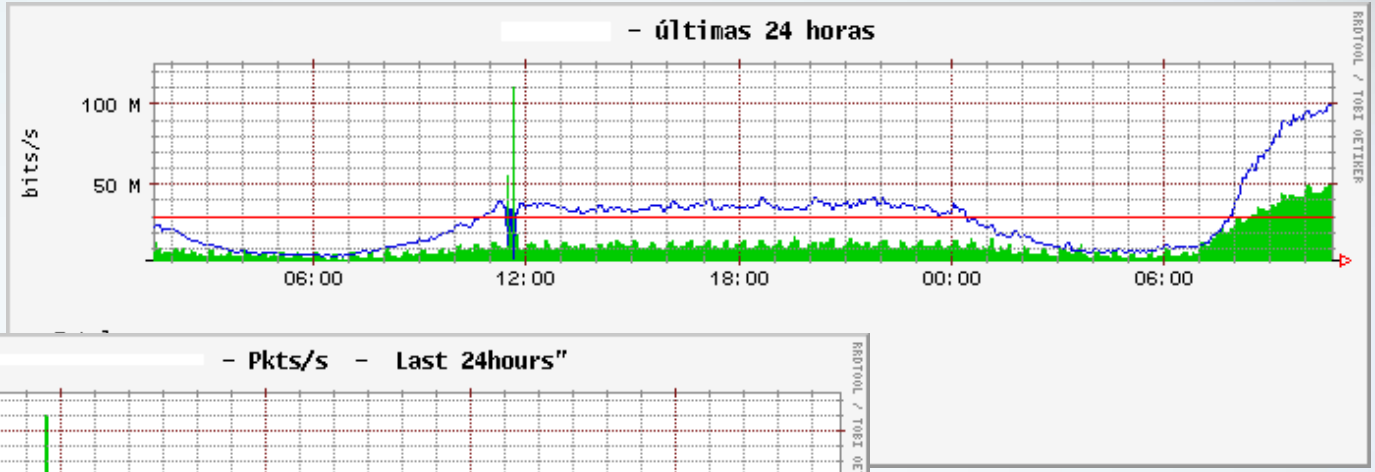
Definição

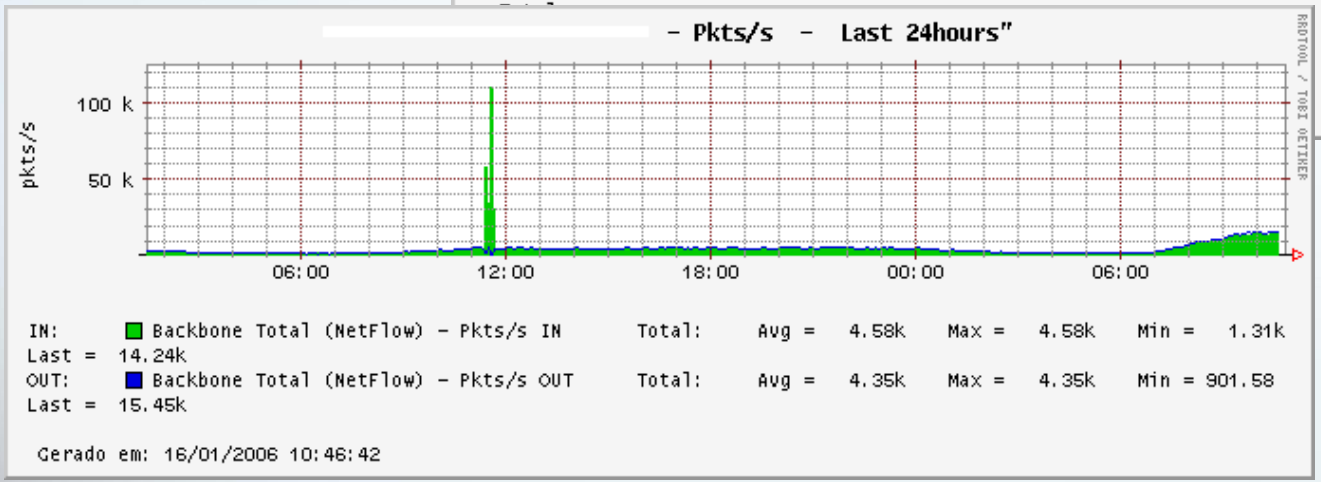
- **Ataque de Negação de Serviço** (*Denial-of-serice – DoS*): Uma tentativa de indisponibilizar um recurso ou serviço aos seus usuários, tal como impossibilitar o acesso à um website na Internet.
- Versão 2.0: Ataque de Negação de Serviço **Distribuído** ou DDoS.

Ataque de Negação de Serviço Distribuído (DDoS)

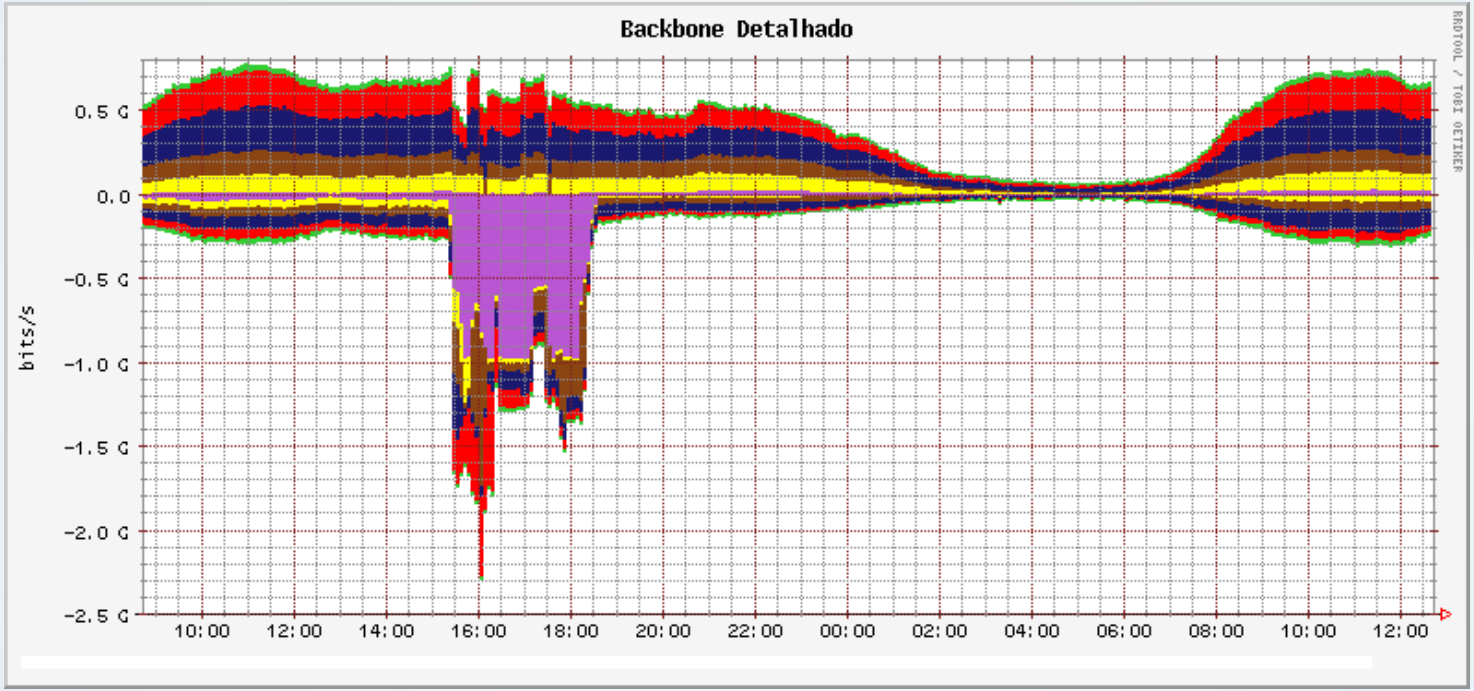


História: 2006

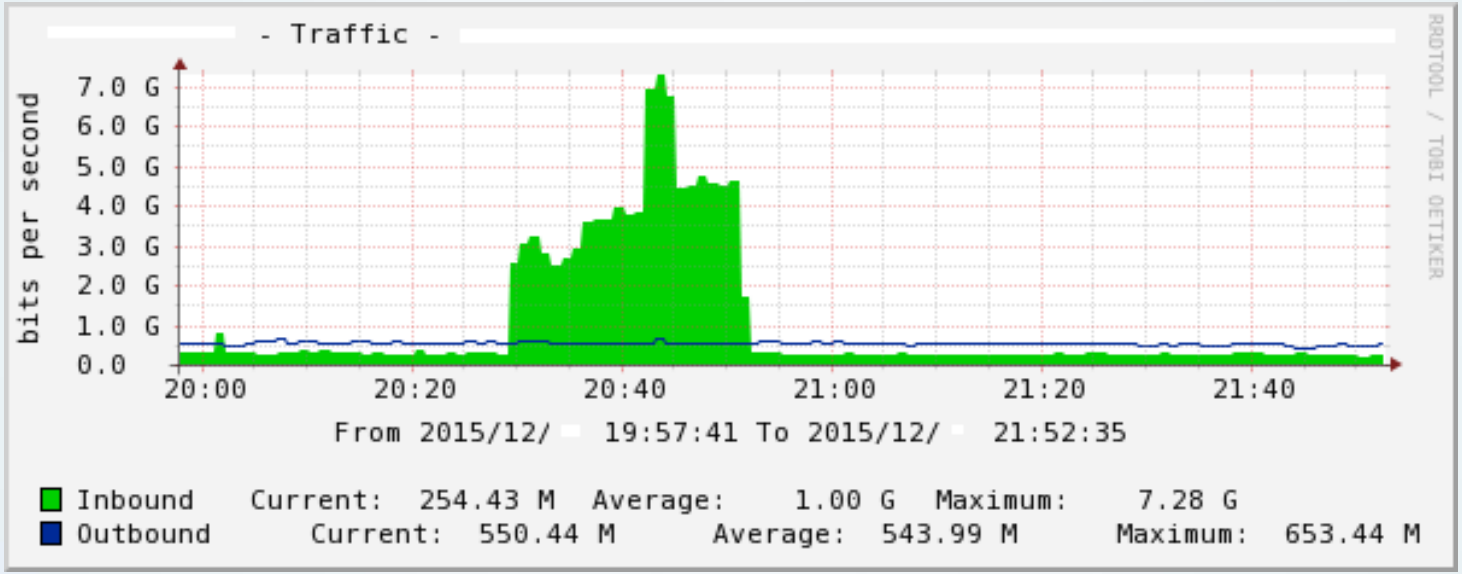




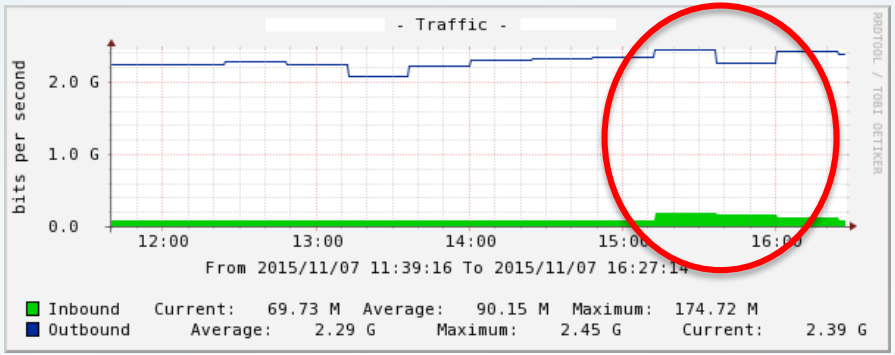
História: 2010

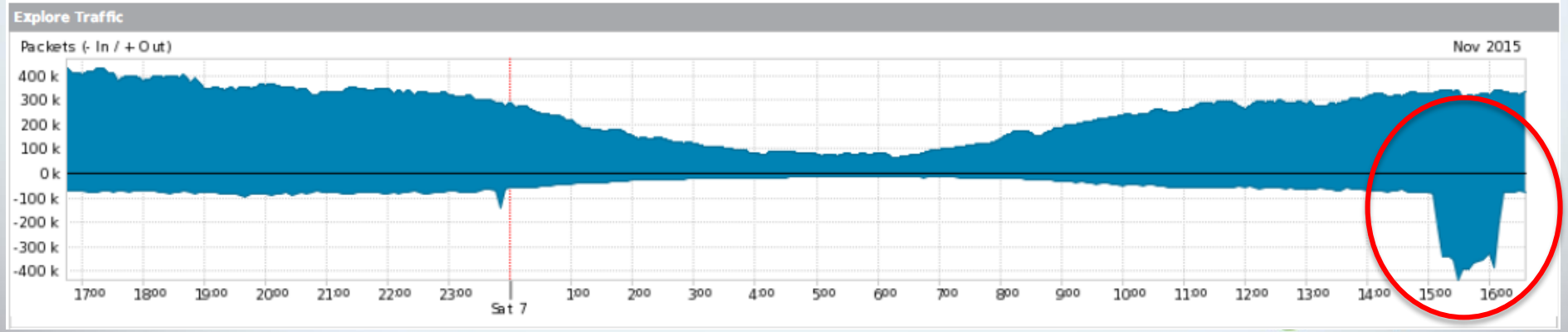


E atualmente em 2015



E atualmente em 2015





Na mídia

SECTIONS The New York Times SUBSCRIBE LOG IN

TECHNOLOGY

UltraDNS Server Problem Pulls Down Websites, Including Netflix, for 90 Minutes

By NICOLE PERLROTH OCT. 15, 2015

Email

Share

Tweet

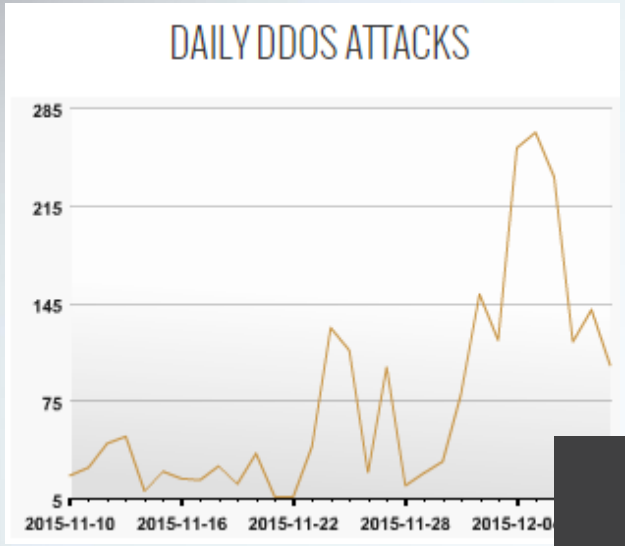
Save

SAN FRANCISCO — UltraDNS, a web content delivery service, went down Thursday afternoon, taking with it a number of popular websites, including Netflix and Expedia.

The cause of the 90-minute failure

http://www.nytimes.com/2015/10/16/technology/ultradns-server-problem-pulls-down-websites-including-netflix-for-90-minutes.html?_r=0

UOL DIVEO SER



http://www.team-cymru.org/graphs.html

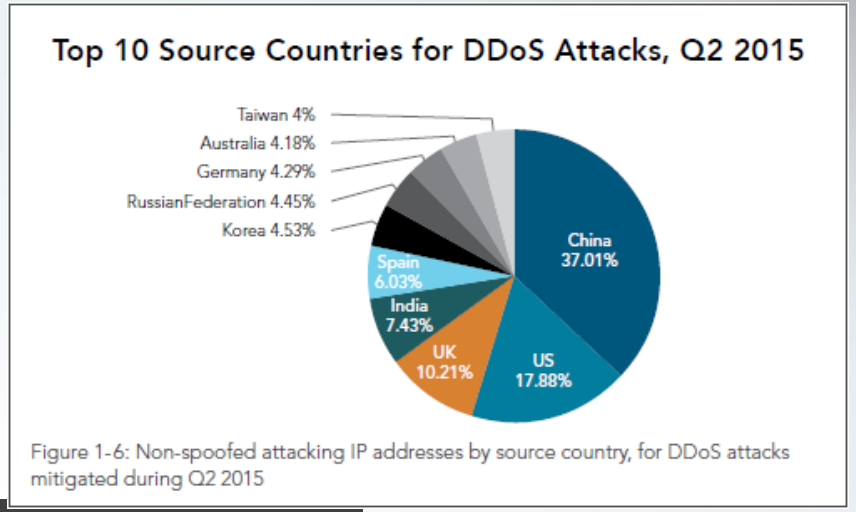
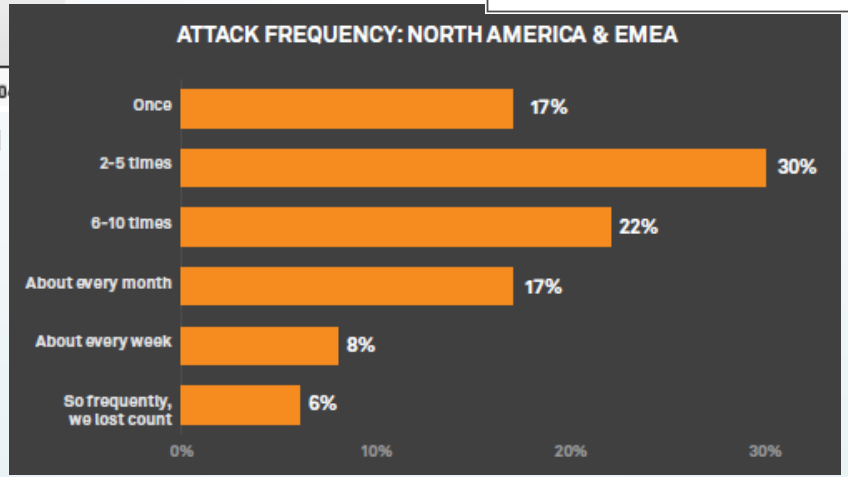


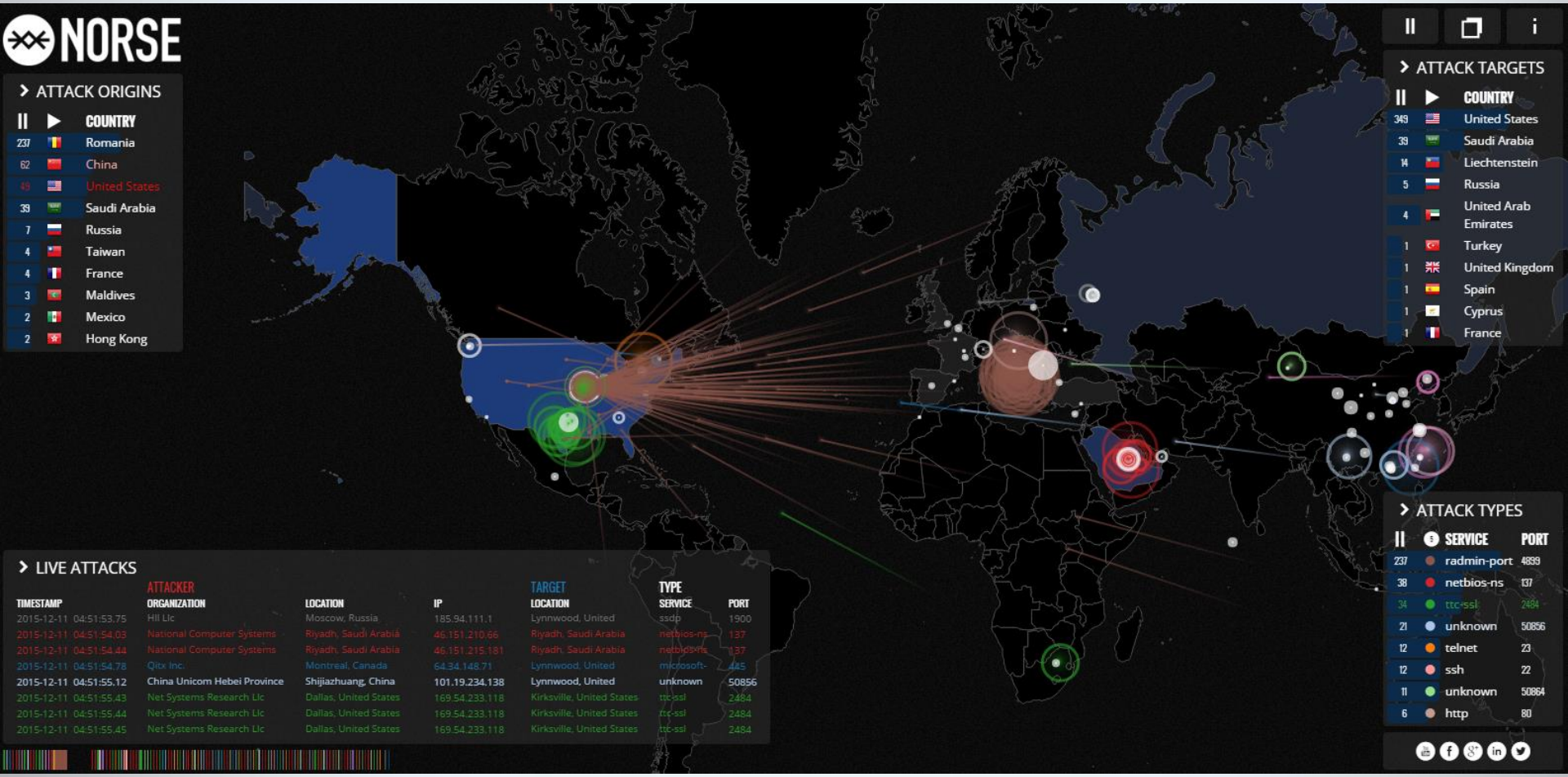
Figure 1-6: Non-spoofed attacking IP addresses by source country, for DDoS attacks mitigated during Q2 2015

AKAMAI STATE OF THE INTERNET SECURITY REPORT Q2-2015

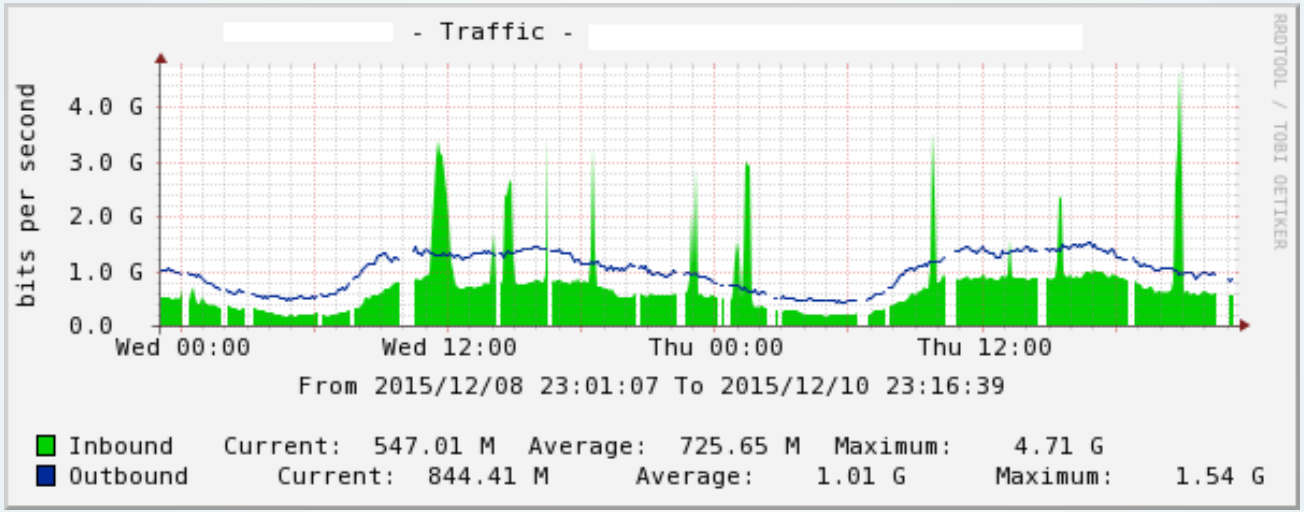


OCTOBER 2015 NEUSTAR DDOS ATTACKS & PROTECTION REPORT: NORTH AMERICA & EMEA

http://map.norsecorp.com/v1/



Um dia comum na vida...



Principais Alvos: Setores

- *Games*
- Empresas de jogos
- Jogos on-line
- Internet, Tecnologia, Software, etc
- Lojas virtuais (e-commerce)
- Serviços Financeiros

Tipos de Ataques

Tipos de Ataques DoS e DDoS

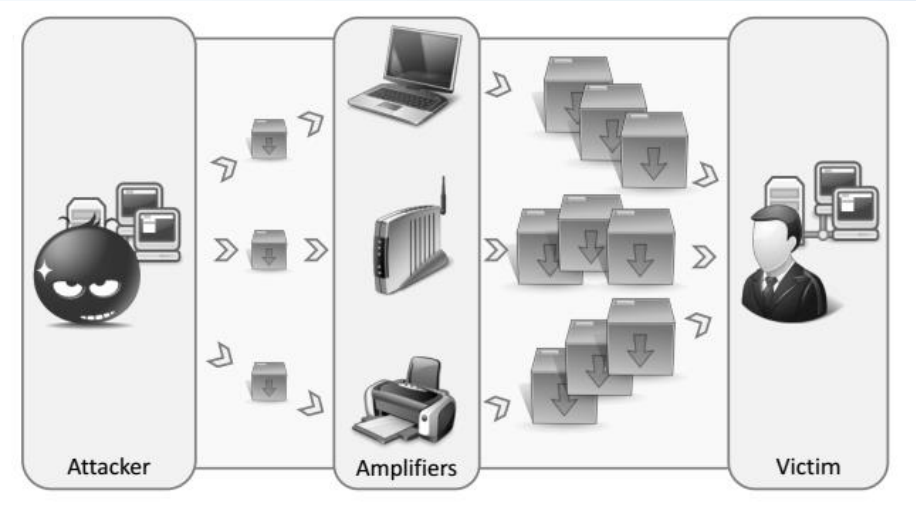
- Mais visíveis *versus* “menos visíveis”
- Flood
  - Consumo de banda / capacidade interface
    - Protocol flood (ICMP, UDP, etc)
    - **Reflexão**
  - Consumo de recursos de sistemas / protocolos
    - *Syn Flood TCP*
    - *Slowloris* para HTTP
    - Ataques DoS ao NDP IPv6
- DD4BC: *DDoS 4 Bitcoin*
  - *Mais informações: https://blog.arbornetworks.com/icymi-arbors-roland-dobbins-nanog-presentation-on-the-dd4bc-extortion-campaign/*

Ataques de Reflexão

- Principais protocolos e fator de multiplicação
  - NTP (123/udp) – 556x
  - DNS (53/udp) – 28 a 54x
  - SSDP (1900/udp) – 30x
  - RIPv1 (520/udp) – 131x
  - SNMP (161/udp) – 6x
  - Fonte: https://www.us-cert.gov/ncas/alerts/TA14-017A

- IP Source Address Spoofing ou BCP38
  - http://bcp.nic.br/
  - https://www.routingmanifesto.org/

- Importância da definição de um bom baseline para instalação de equipamentos.
  - Atenção às configurações “de fábrica”.



Planejamento

Arquitetura do Sistema

- Uma botnet *versus* o seu firewall / servidor
  - Identificar os serviços mais críticos
  - Distribuir o controle do acesso
  - Permitir o crescimento elástico e **distribuído**

- “Dividir para conquistar”
  - Anycast
  - CDN
  - GSLB (Global Server Load-balance)

Endereçamento IP

- Planejar com margem para manobras:
  - Separar alocações de infra-estrutura de alocações para clientes / serviços.
  - Alocar os clientes ou serviços “especiais” em diferentes blocos /24.

- Servidores DNS autoritativos devem estar em /24 diferentes!
  - “The name servers must be in at least two topologically separate networks. A network is defined as an origin autonomous system in the BGP routing table. The requirement is assessed through inspection of views of the BGP routing table.” - https://www.iana.org/help/nameserver-requirements
  - Alexa TOP 500 Brasil (440 websites)
    - 0,61% possui apenas um servidor DNS autoritativo
    - 26,82% possui 2 servidores DNS autoritativo
    - **8,41%** possuem todos os servidores DNS autoritativo em um mesmo bloco /24

Links de Trânsito

- Antes de contratar o seu “link de Internet”:
  - Avaliar a possibilidade de “on-demand” e planejar a interface física para suportar upgrades com menor *downtime* (link-aggregation?).
  - Contratação na modalidade *95-percentil.*
  - Communities BGP para Blackhole é obrigatório!
    - Mesmo para peering?
  - Communities BGP para controle de anúncios é recomendado.
  - Avaliar a possibilidade de acordos comerciais ($$$) para a operadora bloquear tráfego não desejado.
  - Atenção ao contratar trânsito através de um ponto de troca de tráfego: sempre implementar uma forma de controle para o tráfego do trânsito não interferir no tráfego de peering.

Equipamentos

- Avaliar a capacidade de todos os equipamentos.
  - “Meu roteador de US$ 500k está conectado em um switch de US$ 3k!!!”
- Atenção a capacidade dos sistemas em bps e pps.
- Ajustar parâmetros “default”:
  - Desabilitar serviços que não são utilizados (!!!).
  - Ajustar os parâmetros de limites do plano de controle (Cisco CoPP ou Juniper DDoS protection ou ...).
  - Ajustar o número máximo de sessões e proteções default (firewall).
  - Parâmetros de kernel e CPU/NIC Affinity (servidores e firewalls).
  - Mais informações: http://www.slideshare.net/securitysession/practical-steps-to-mitigate-ddos-attacks

UOL DIVEO SER

Detecção

Você só poderá detectar o que você pode ver!

- Visibilidade dos ativos (interna)
  - Monitoração de tráfego nas interfaces - incluindo taxa de pacotes (pps)
  - Monitoração detalhada dos equipamentos e serviços
    - CPU, memória, CPU de line card, etc e os **limites de cada hardware**
    - Número de sessões para um serviço e taxa de novas conexões
    - Número de conexões SYN_RECEIVED

- Visibilidade dos ativos (externa)
    - Uptime Robot
    - StatusCake
    - Pingdom
    - ThousandEyes

- Visibilidade do tráfego *flow (sflow, netflow, ipix, etc)
    - Free
      - cflowd / flowscan
      - https://github.com/FastVPSEestiOu/fastnetmon e http://www.enog.org/presentations/enog-9/17-FastNetMon_ENOG_pdf.pdf
      - http://nfsen.sourceforge.net/
      - http://www.sflow.org/products/collectors.php
      - https://www.telcomanager.com/en/trafip-netflow-collector-and-analyzer
    - Pagos
      - Arbor Peakflow
      - Plixer Scrutinizer
      - Manageengine Netflow Analyzer

Conhecimento

- Análise de tendência
  - Frequência dos ataques
  - Alvos preferidos
  - Protocolos mais utilizados - pelos usuários e pelos atacantes.
- Quanto maior o conhecimento da rede e dos serviços utilizados, maior serão as opções de contra-medidas disponíveis.

Contra-medidas

O ataque é **menor** que a banda disponível

- ACL e Controle de banda (bps)
  - “Disponível nos melhores equipamentos do ramo.”
- Controle de taxa de pacotes (pps)
  - Por exemplo Cisco 6880-X
  - *Feature request* para Juniper MX
- FlowSpec
  - Regras por tamanho do pacote (!!!)
- Elemento de mitigação “out-of-band”
  - Proxy de alta capacidade (para serviços específicos)
  - Appliance de rede com maior granularidade de regras
    - GeoIP
    - Assinatura do tráfego

UOL DIVEO SER

O ataque é **maior** que a banda disponível

- Aumente a banda! ☺
- Seu provedor / data center é seu amigo (???)
- Remotely-Triggered Black Hole (RTBH) – RFC5635
  - Através do BGP, sinalizar o bloqueio total para um IP
  - Salva a rede, mata um IP (ou vários)
  - Quanto melhor sua conectividade, menor sua indisponibilidade
  - Nacional *versus* internacional (e a China?)
  - Importância de peering

O ataque é **maior** que a banda disponível

- *Clean pipe*
  - Exemplos: Staminus, Black Lotus (Level 3), Imperva Incapsula
  - Problema de túneis GRE e MTU
    - Muito bom quando você é um provedor de conteúdo (requisição = 80 bytes, conteúdo = 1500 bytes)
    - Muito ruim quando você é um provedor de serviço (*download* com pacotes de 1500 bytes)
  - Importância do peering

O ataque é **maior** que a banda disponível

- Distribuir o “alvo” do ataque.
  - Anycast
  - Global Server Load-balance (GSLB)
  - CDN
- Instalar um POP na China.

Dúvidas?

GTS 26 – São Paulo/SP – 11/dez/2015

Gustavo Rodrigues Ramos
grramos@uoldiveo.com