Ataques DDoS
Panorama, Mitigação e Evolução

Wilson Rogério Lopes

GTER 39

05/2015

“DDoS is a new spam…and it’s everyone’s problem now.”

Preston Hogue

CERT.br registra aumento de ataques de negação de serviço em 2014

"...223.935 notificações, um número 217 vezes maior que o registrado em 2013."

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

13 Feb 2014 by Matthew Prince

http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

"To generate approximately 400Gbps of traffic, the attacker used 4,529 NTP servers running on 1,298 different networks. On average, each of these servers sent 87Mbps of traffic to the intended victim on CloudFlare's network. Remarkably, it is possible that the attacker used only a single server running on a network that allowed source IP address spoofing to initiate the requests."

NTP Monitoring List

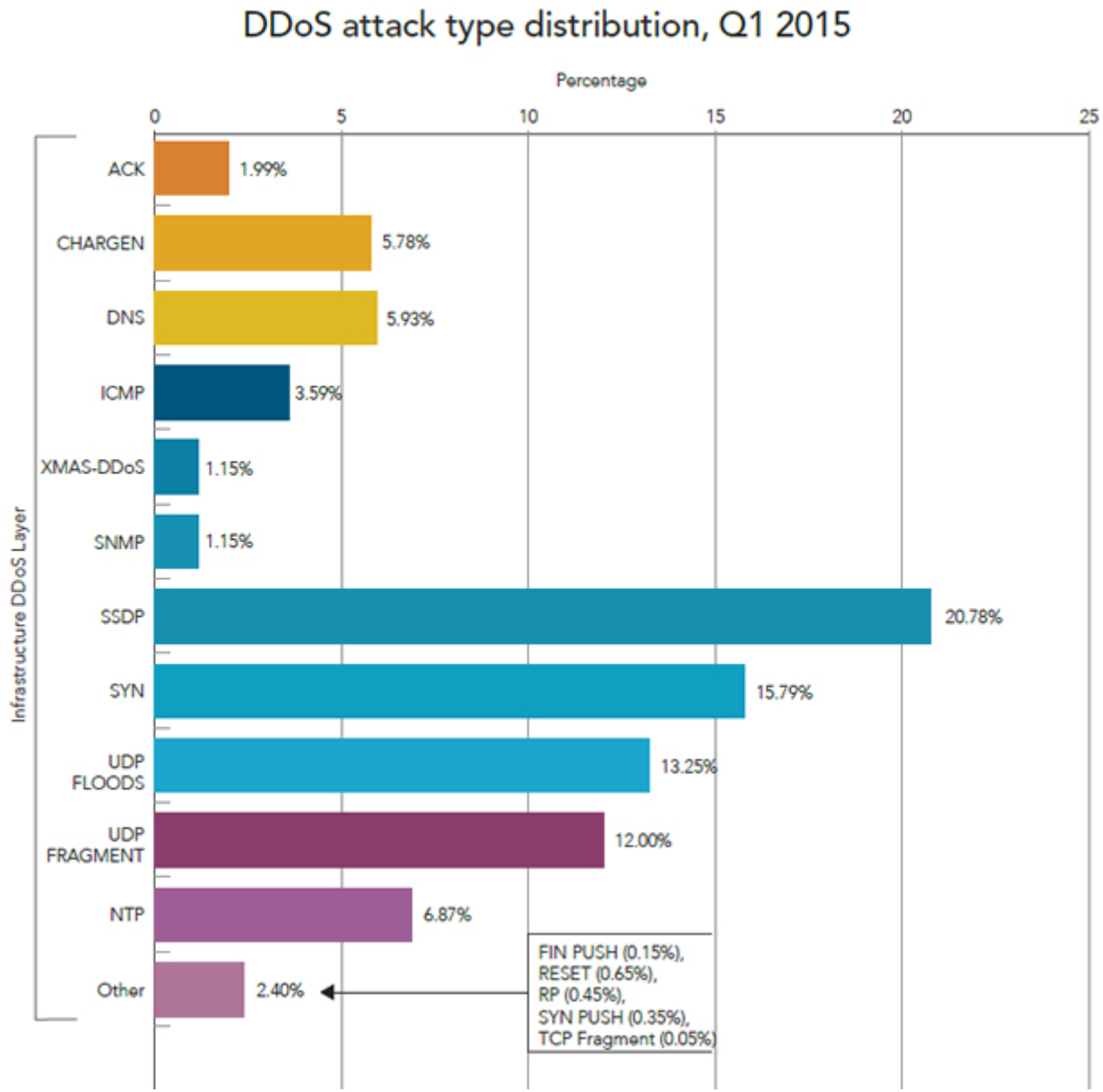
$ntpdc –c monlist 200.xxx.xxx.1

No.	Time	Source	Destination	Protocol	Length	Info
665	*REF*	10.114.1.118	1[redacted]9	NTP	234	NTP Version 2, private
666	0.144916000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
667	0.146839000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
668	0.148329000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
669	0.150853000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
670	0.152744000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
671	0.155101000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
672	0.156374000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
673	0.158604000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
674	0.160587000	1[redacted]9	10.114.1.118	NTP	482	NTP Version 2, private
675	0.160924000	1[redacted]9	10.114.1.118	NTP	122	NTP Version 2, private

600 ips

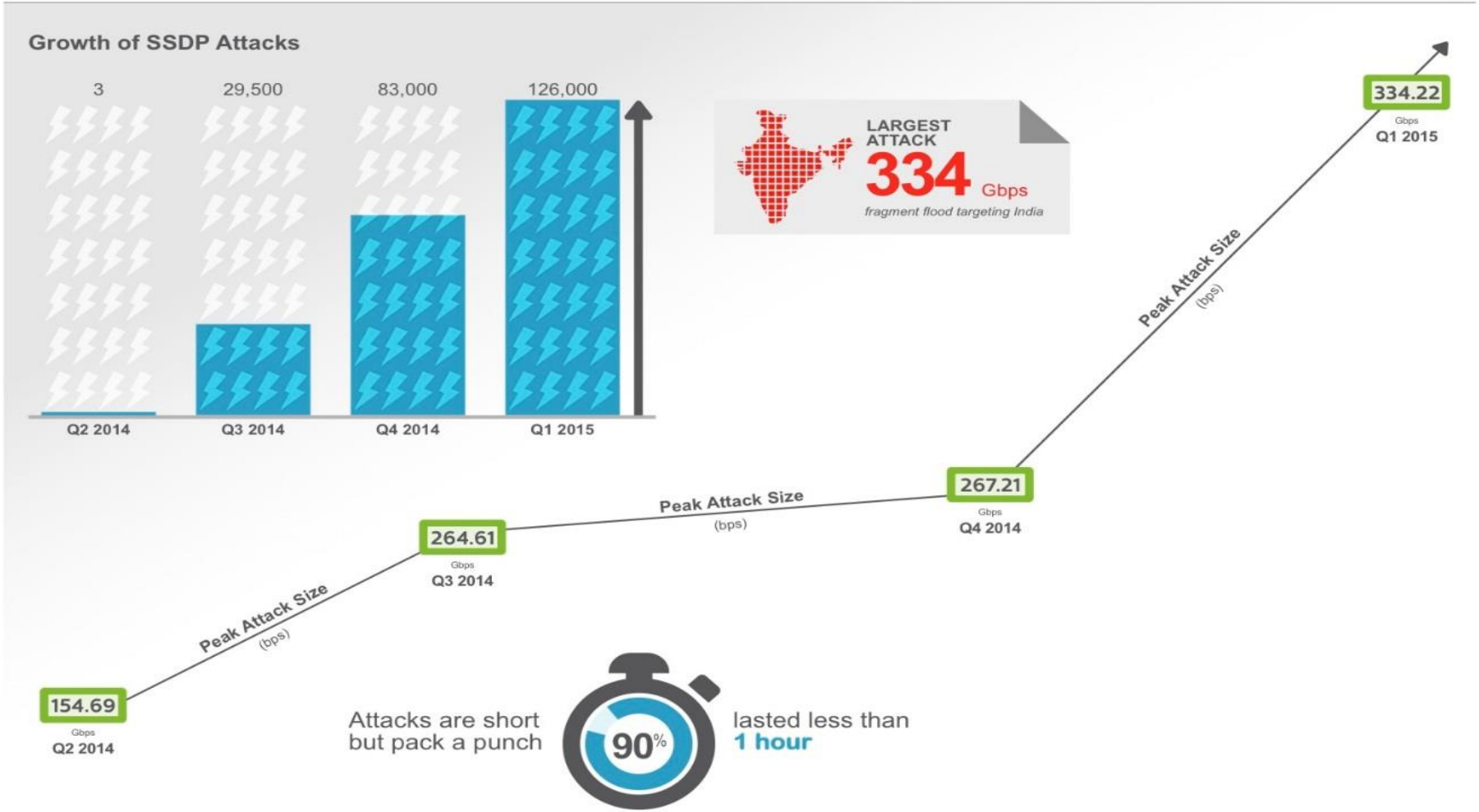
Resposta de 48K para 234 bytes da consulta

Fator de amplificação = 206 X



Fonte: Akamai Q1 2015 Report

DDoS Attack Trends in Q1 2015



Fonte: Atlas Arbor Networks

Top 20 Countries With Open SSDP

Country	Total
China	4,526,046
United States	1,235,061
Korea, Republic of	995,107
Russian Federation	467,685
Vietnam	448,169
Japan	393,073
Brazil	392,139
Spain	307,165
Taiwan	301,583
India	290,692
Uruguay	278,198
Ukraine	247,968
Canada	241,994
Turkey	204,541
Colombia	192,923
Greece	188,477
Malaysia	187,003
Argentina	166,297
Hungary	109,875
Bulgaria	107,859

SSDP - Simple Service Discovery Protocol

- UDP porta 1900
- “Search” Request
- Fator de amplificação – 30x

Fonte: https://ssdpscan.shadowserver.org/

Chinese government linked to largest DDoS attack in GitHub history

http://www.techrepublic.com/article/chinese-government-linked-to-largest-ddos-attack-in-github-history/

26/03/2015
Man-in-the-middle – "Grande firewall da China" ?

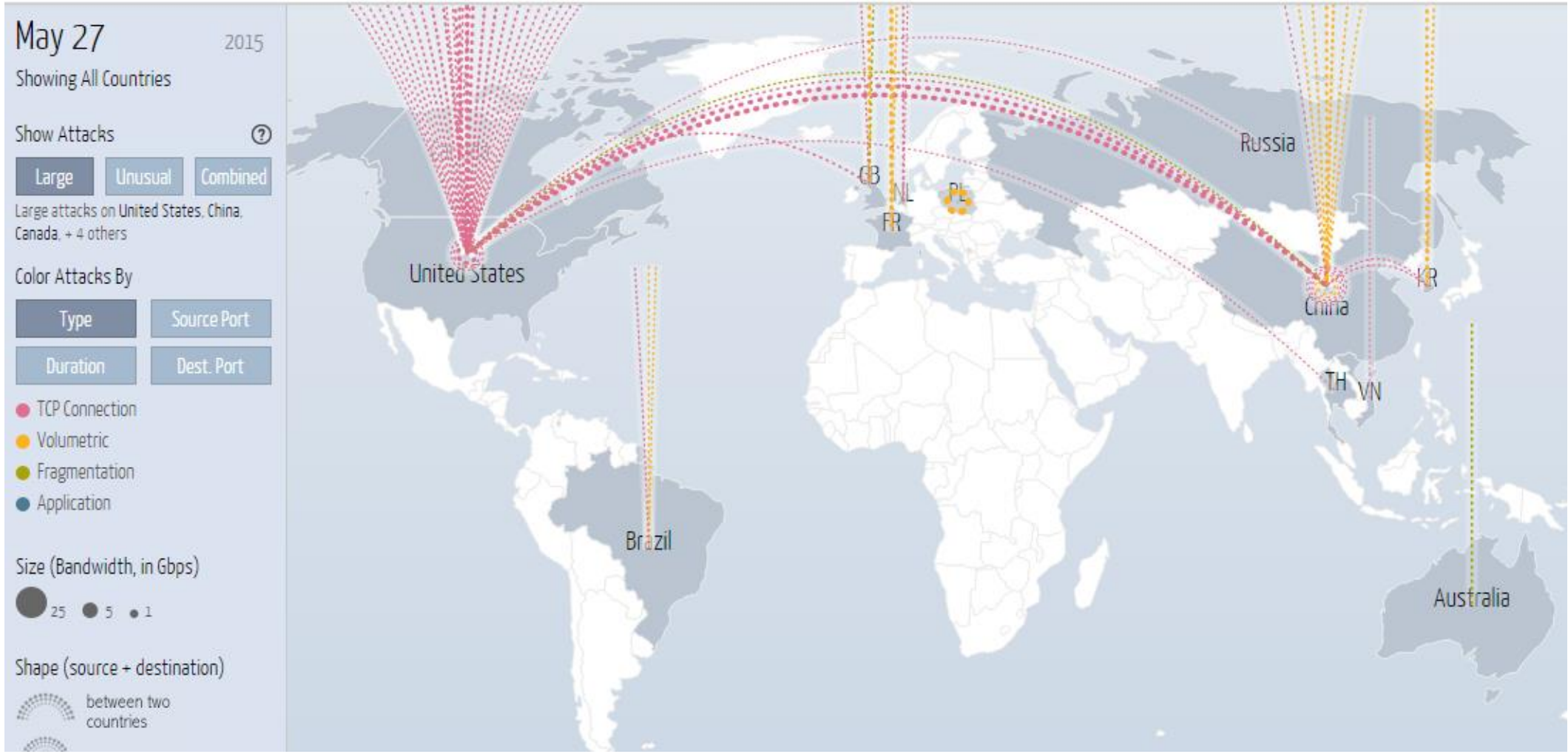
Baidu Analytics – javascript substituído

http://hm.baidu.com/h.js

Get a cada 2 segundos nas urls : https://github.com/greatfire
https://github.com/cn-nytimes

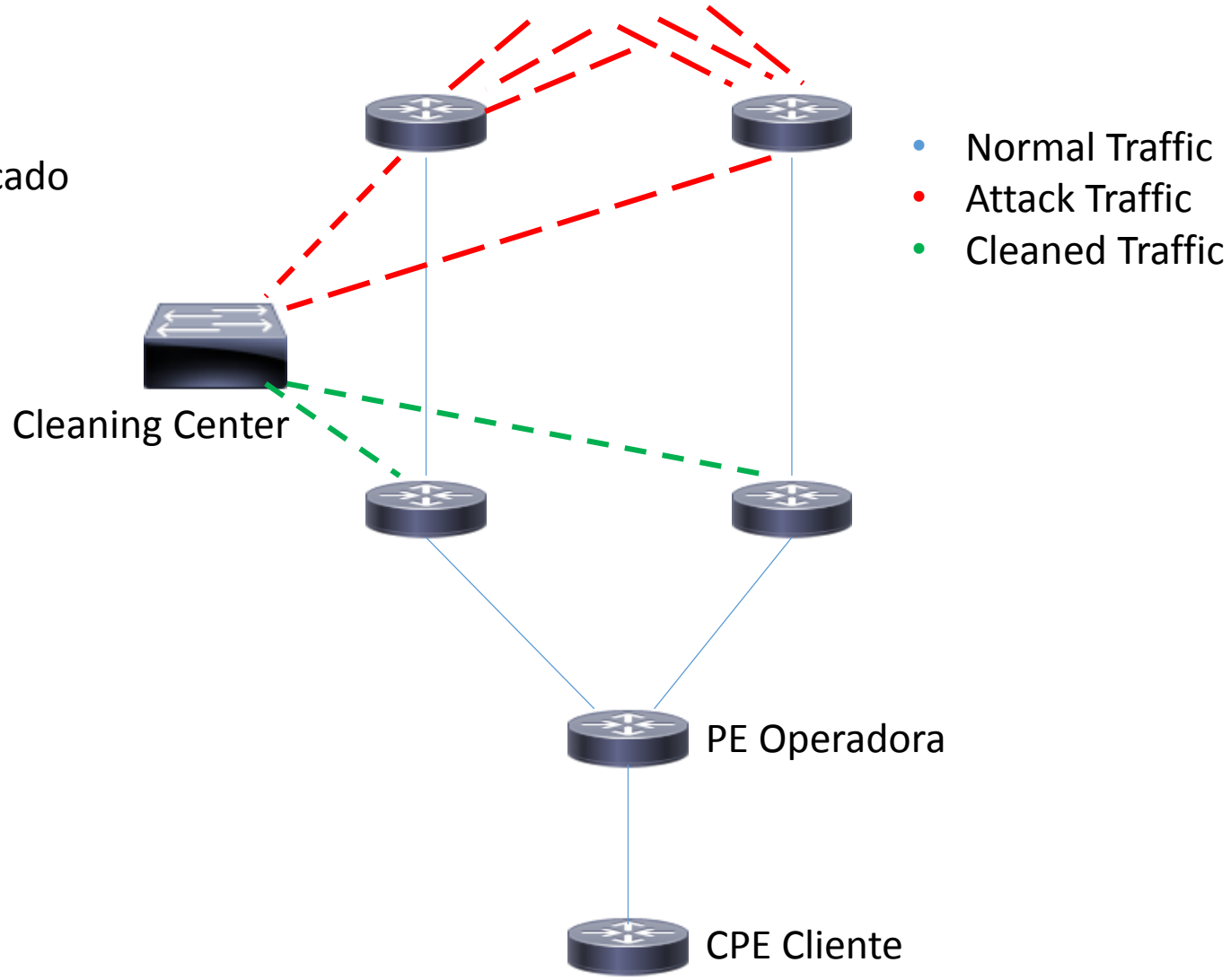
Digital Attack Map – Atlas Arbor e Google Ideas

http://www.digitalattackmap.com/



Mitigação – *Clean Pipe* Operadoras

- Detecção do ataque via Netflow
- Anúncio mais específico via BGP do ip/prefixo atacado
- “Limpeza” do tráfego
  - Syn cookies
  - Filtros estáticos: Drop UDP 1900
    Drop UDP 123
  - Rate Limit
  - Protocol Authentication
  - GeoIP



Mitigação – Cloud DDoS Service Providers

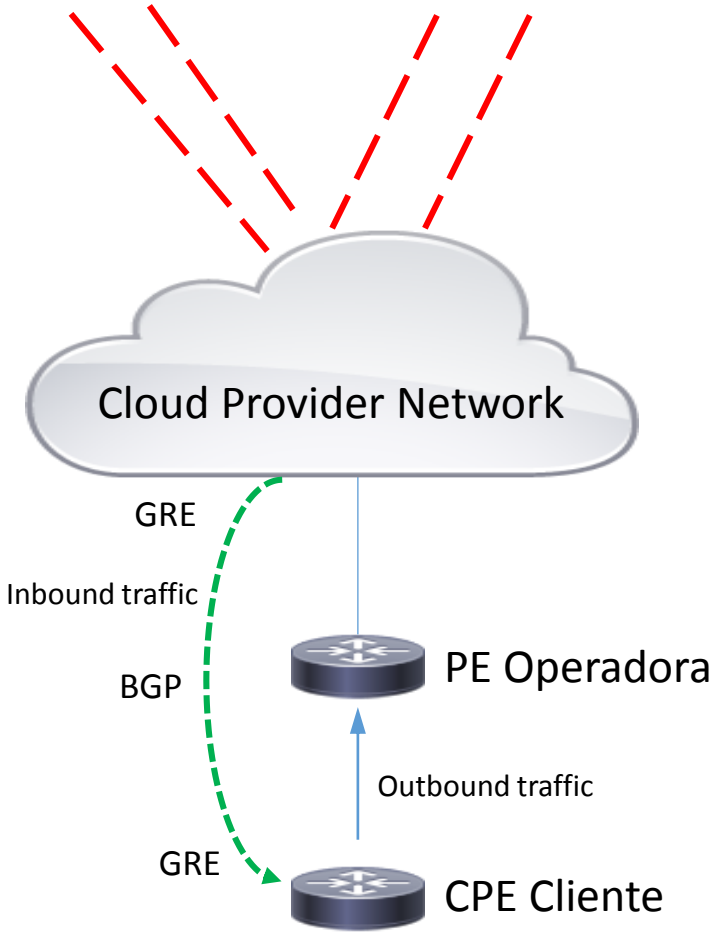
- Túnel GRE com a rede do Cloud Provider
- Sessão BGP estabelecida
- Detecção do ataque via Netflow
- Anúncio do bloco atacado via BGP
- Cloud Provider divulga o anúncio para seus upstreams
- Bloqueio de ataques de camada 3 e 4
- Serviço de Proxy / WAF HTTP/HTTPS

Prós

- Capacidade/Superfície de mitigação
- Implementação sem necessidade de adequações na infra

Contras

- Latência - anúncios fora do BR
- GRE e MSS – adequação do MSS, TCP DF bit setado



- Normal Traffic
- Attack Traffic
- Cleaned Traffic

Mitigação – Load Balancers

- **Syn Flood**

  - Syn Cookies por hardware – Centenas de milhões de syn cookies por segundo

- **L7 HTTP/HTTPS Floods**

  - Análise header HTTP

    Check de User Agent
    Check de Referer

  - Rate limit IP/URL/URI

  - Inserção de cookies

  - Inserção de js

  - Inserção de captcha

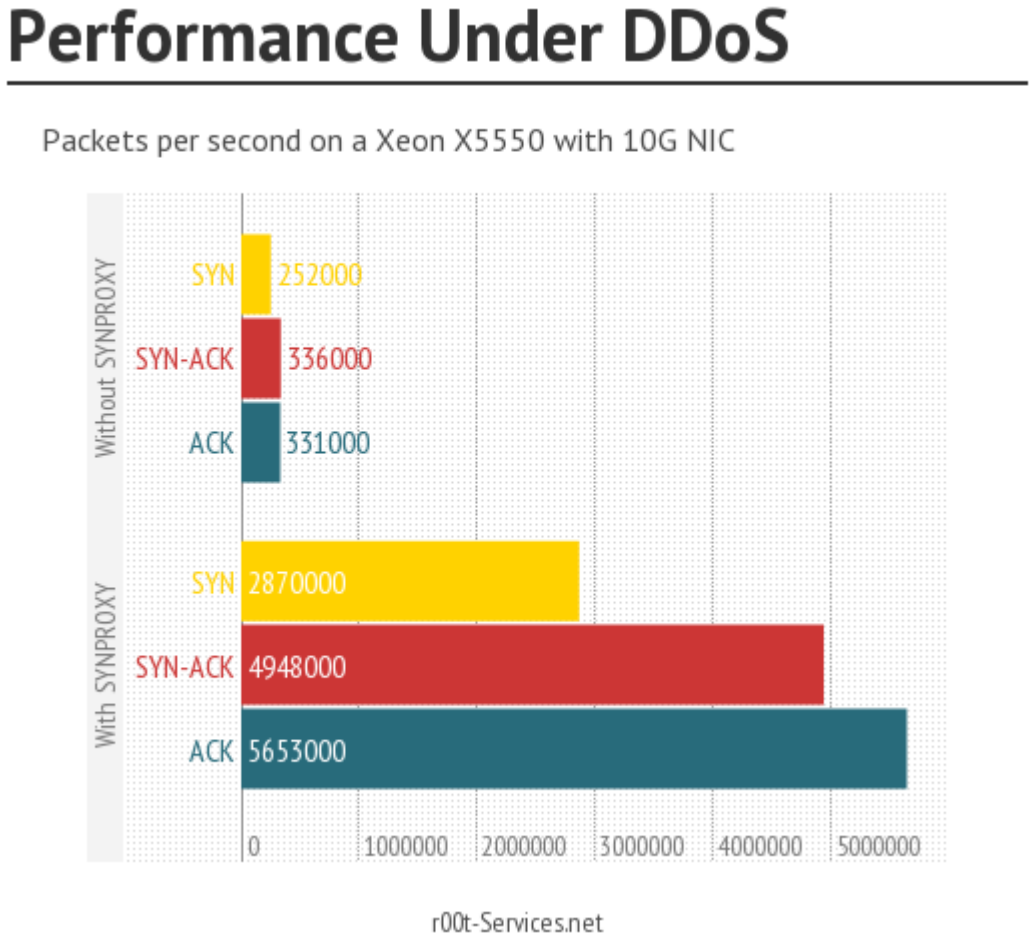
Mitigação – Home Made

- **Iptables SynProxy**

  Kernel 3.13, Red Hat 7

iptables -t raw -I PREROUTING -p tcp -m tcp --syn -j CT –notrack

iptables -I INPUT -p tcp -m tcp -m conntrack –ctstate UNTRACKED -j SYNPROXY --sack-perm --timestamp --wscale 7 --mss 1460



Mitigação – Home Made

- **Mod Evasive**

Limita número de requests baseado na URL, URI, ip de origem e intervalo de tempo

DOSPageCount 2
DOSSiteCount 50
DOSPageInterval 1
DOSSiteInterval 1
DOSBlockingPeriod 60
DOSEmailNotify admin@example.org

Mitigação – Home Made

- **Mod Security**

WAF – Monitoração, log e bloqueio

OWASP Core rules - https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

Violação de protocolo
RBL
Bloqueio de floods e slow attacks
Bot, crowler e scan detection

Mitigação – Recomendações

- **Mitigação híbrida – Tenha o controle nas mãos para não morrer pela vacina**

  Bloqueio de ataques l3/l4 no provedor
  Bloqueio local de ataques de aplicação

- **Monitoração com foco específico para DDoS**

  Monitorações do NOC geralmente não atendem à agilidade que a mitigação de um DDoS necessita

- **Bom e velho Anycast**

- **Fuja de controles statefull na borda**

- **Não bloqueie tcp 53 e pacote dns udp maior que 512. Não, esta não é a RFC ☺**

Referências

- **Arbor Networks Detects Largest Ever DDoS Attack in Q1 2015 DDoS Report**
http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5405-arbor-networks-records-largest-ever-ddos-attack-in-q1-2015-ddos-report

- **Akamai Q1 2015 SOTI Security Preview: 7 Attack Vectors**
https://blogs.akamai.com/2015/05/q1-2015-state-of-the-internet-security-report-released.html

- **Mod Evasive - http://www.zdziarski.com/blog/?page_id=442**

- **Mod Security - https://www.modsecurity.org/**

- **Iptables SynProxy - http://rhelblog.redhat.com/2014/04/11/mitigate-tcp-syn-flood-attacks-with-red-hat-enterprise-linux-7-beta/**