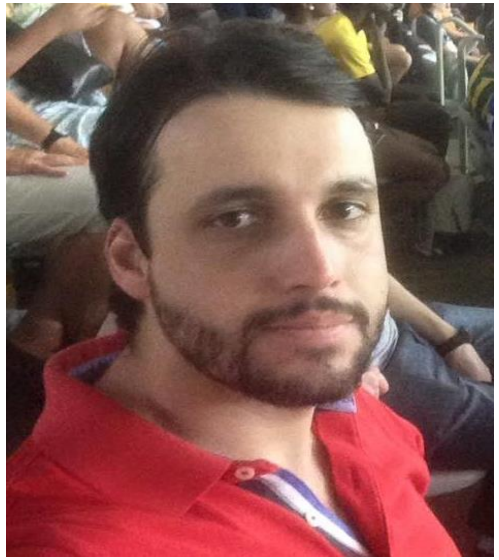
Ataques DDoS
Panorama, Mitigação e Evolução

Wilson Rogério Lopes

LACNIC 26 / LACNOG 2016

09/2016

Wilson Rogério Lopes



- Especialista em arquitetura e segurança de redes, com 12 anos de atuação em grandes provedores do mercado de internet no Brasil.
- Pós-graduado pela Universidade de São Paulo – USP.
- Palestrante frequente no GTER e GTS – Grupo de trabalho de engenharia e segurança de redes no Brasil.
- Áreas de Interesse - Arquitetura e Segurança de Redes, IaaS, SDN, DNS, DNSSEC.

Contato – wilsonlopes00@gmail.com
https://br.linkedin.com/in/wrlopes

Disclaimer

As informações e opiniões contidas nesta apresentação não representam o meu empregador. Todas as informações e estatísticas apresentadas são de domínio público, coletadas de blogs e sites de notícias na internet.

Agenda

- DDoS - Panorama atual e Evolução
- Mitigação – Opções e aplicabilidade
- Recomendações gerais

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

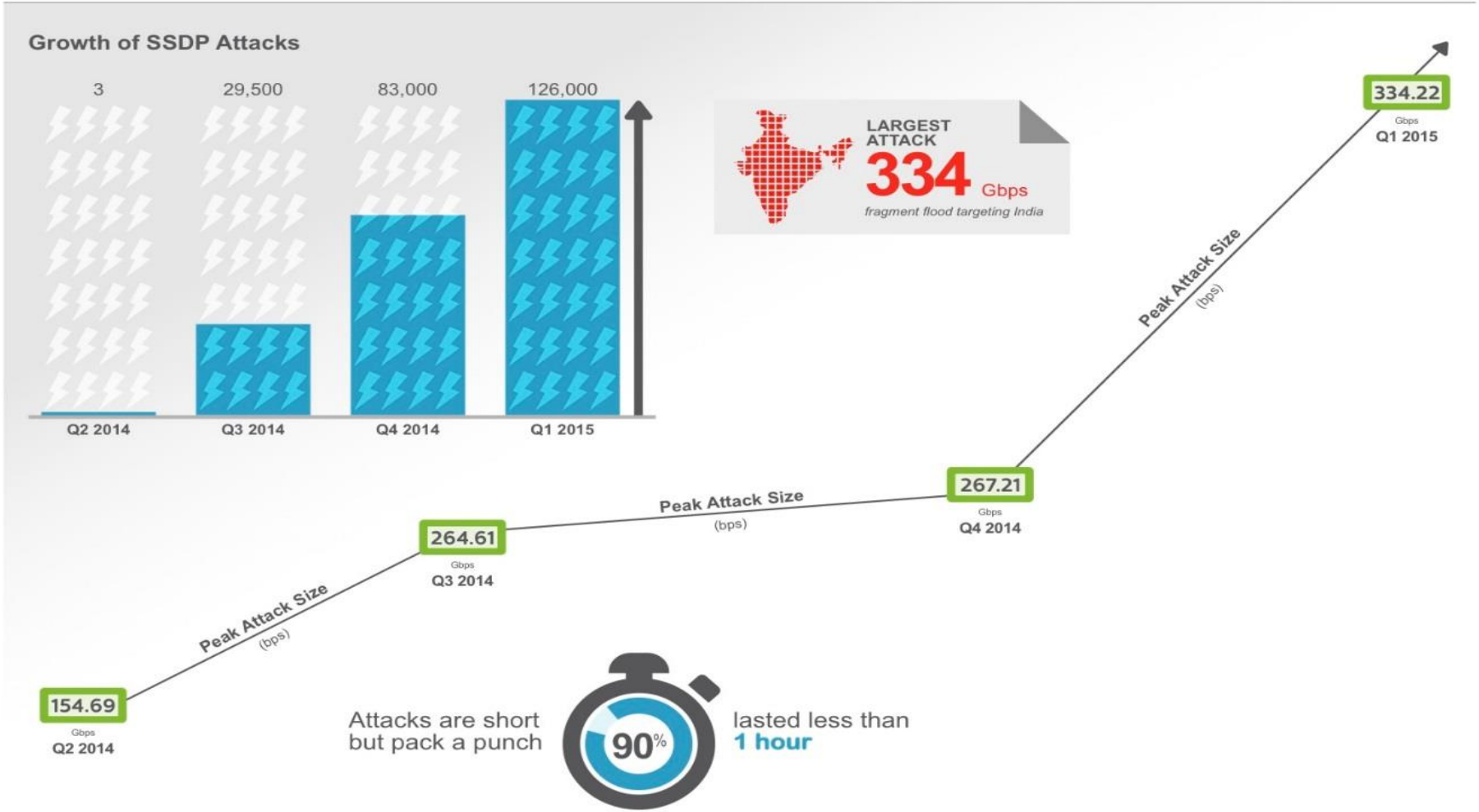
Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

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."

DDoS Attack Trends in Q1 2015



Fonte: Atlas Arbor Networks

Top 20 Countries With Open SSDP

Country	Total
China	2,640,200
Russian Federation	477,586
Argentina	389,663
United States	362,416
Vietnam	302,993
Malaysia	300,232
Brazil	239,750
Taiwan	238,272
Turkey	230,286
Venezuela	221,203
Japan	210,542
Ukraine	200,419
Korea, Republic of	190,986
Spain	180,269
India	167,808
Greece	141,244
Canada	126,731
Colombia	124,072
Italy	91,285
Thailand	65,674

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

SSDP - Simple Service Discovery Protocol

- UDP porta 1900
- “Search” Request
- Fator de amplificação – 30x
- 8 milhões de dispositivos abertos

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.99	192.168.2.1	SSDP	122	M-SEARCH * HTTP/1.1
2	0.009361000	192.168.2.1	192.168.2.99	SSDP	270	HTTP/1.1 200 OK
3	0.000864000	192.168.2.1	192.168.2.99	SSDP	342	HTTP/1.1 200 OK
4	0.000001000	192.168.2.1	192.168.2.99	SSDP	279	HTTP/1.1 200 OK
5	0.001079000	192.168.2.1	192.168.2.99	SSDP	334	HTTP/1.1 200 OK
6	0.000001000	192.168.2.1	192.168.2.99	SSDP	279	HTTP/1.1 200 OK
7	0.000303000	192.168.2.1	192.168.2.99	SSDP	318	HTTP/1.1 200 OK
8	0.000049000	192.168.2.1	192.168.2.99	SSDP	350	HTTP/1.1 200 OK
9	0.000331000	192.168.2.1	192.168.2.99	SSDP	279	HTTP/1.1 200 OK
10	0.000002000	192.168.2.1	192.168.2.99	SSDP	338	HTTP/1.1 200 OK
11	0.004177000	192.168.2.1	192.168.2.99	SSDP	344	HTTP/1.1 200 OK
12	0.001284000	192.168.2.1	192.168.2.99	SSDP	332	HTTP/1.1 200 OK
13	0.000043000	192.168.2.1	192.168.2.99	SSDP	254	HTTP/1.1 200 OK

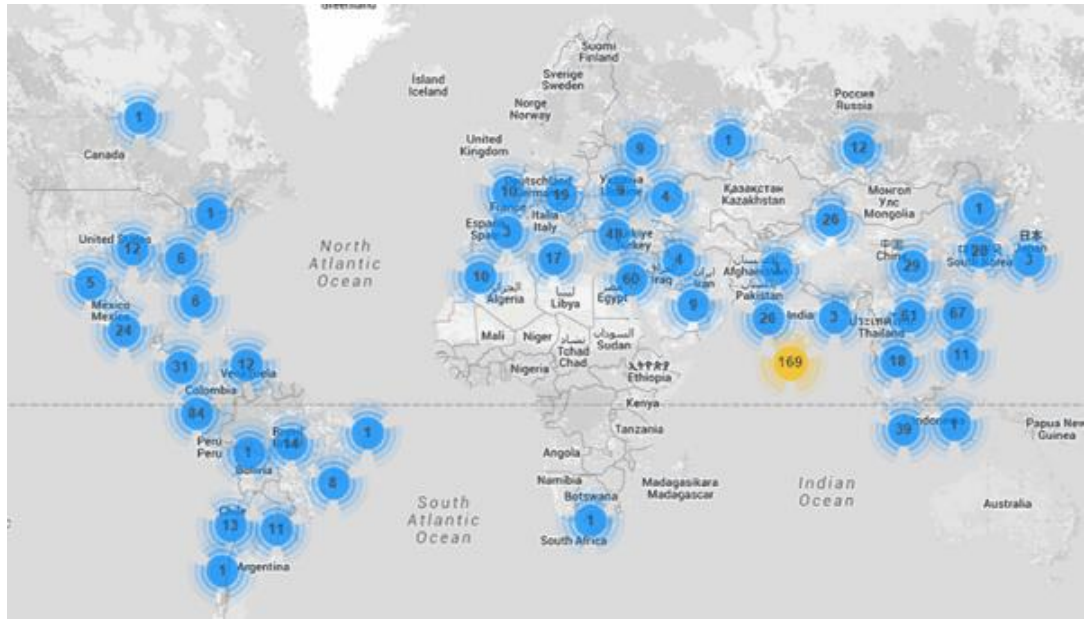
2016 - IoT – CCTV Botnet

- CCTV devices – telnet, admin com senha default
- Mesmo firmware em pelo menos 70 vendors
- Lizard Squad – Bot LizardStresser
- **400Gbps de volumetria – sem amplificação**

HTTP Request flood, tcp connections flood, udp flood

Fonte: https://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser/

```
0 ::ffff:10.0.0.21:telnet       ::ffff:60.x.x.57:41238     ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:85.x.x.175:42836    ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:31.x.x.114:21833    ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:14.x.x.49:4344      ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:36.x.x.70:33348     ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:222.x.x.237:49593   ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:201.x.x.157:42611   ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:60.x.x.90:51354     ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:88.x.x.139:42413    ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:219.x.x.139:55355   ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:49.x.x.29:44295     ESTABLISHED
0 ::ffff:10.0.0.21:telnet       ::ffff:60.x.x.111:50127    ESTABLISHED
```

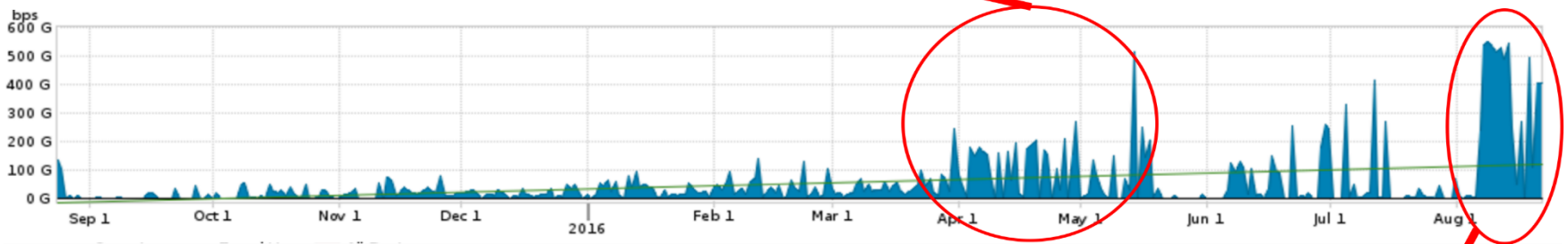


2016 – Olimpíada Rio de Janeiro

2015 | 2016

ARBOR

Início atividade IoT botnet



Rio 2016 Olympic Games

```
Frame 1: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits)
Ethernet II, Src: CiscoInc_e5:47:09 (64:12:25:e5:47:09), Dst: ArborNet_a0:ca:c0 (00:50:49:a0:ca:c0)
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
Generic Routing Encapsulation (Transparent Ethernet bridging)
  Flags and Version: 0x0000
  Protocol Type: Transparent Ethernet bridging (0x6558)
Ethernet II, Src: 77:e7:b5:c8:52:6c (77:e7:b5:c8:52:6c), Dst: 92:bf:07:08:7c:a1 (92:bf:07:08:7c:a1)
Internet Protocol Version 4, Src: [redacted] Dst: [redacted]
User Datagram Protocol, Src Port: 34109 (34109), Dst Port: 17880 (17880)
Data (512 bytes)
  Data: b9709c7211c10b6d31cd5f4264e108297e15d990f239ef24...
  [Length: 512]
```

- 540Gbps de volume sustentados durante horas
- Alvos – Governo, Patrocinadores, Instituições Financeiras
- Uso de GRE para bypass das mitigações

Fonte: https://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser/

2016 – 21/09 - Retaliação

- vDOS Israelense identificado e proprietários presos
- Noticiado pelo repórter **Brian Krebs** - http://krebsonsecurity.com/about/
- **665Gbps – 143Mpps – Sem amplificação !**

briankrebs @briankrebs · 21 de set

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

775 1,1 mil

briankrebs @briankrebs · 21 de set

per the last tweet, they threw it all at my site; SYN Flood, GET Flood, ACK Flood, POST Flood, GRE Protocol Flood]; 665.00 Gbps;143.50 Mpps

124 158

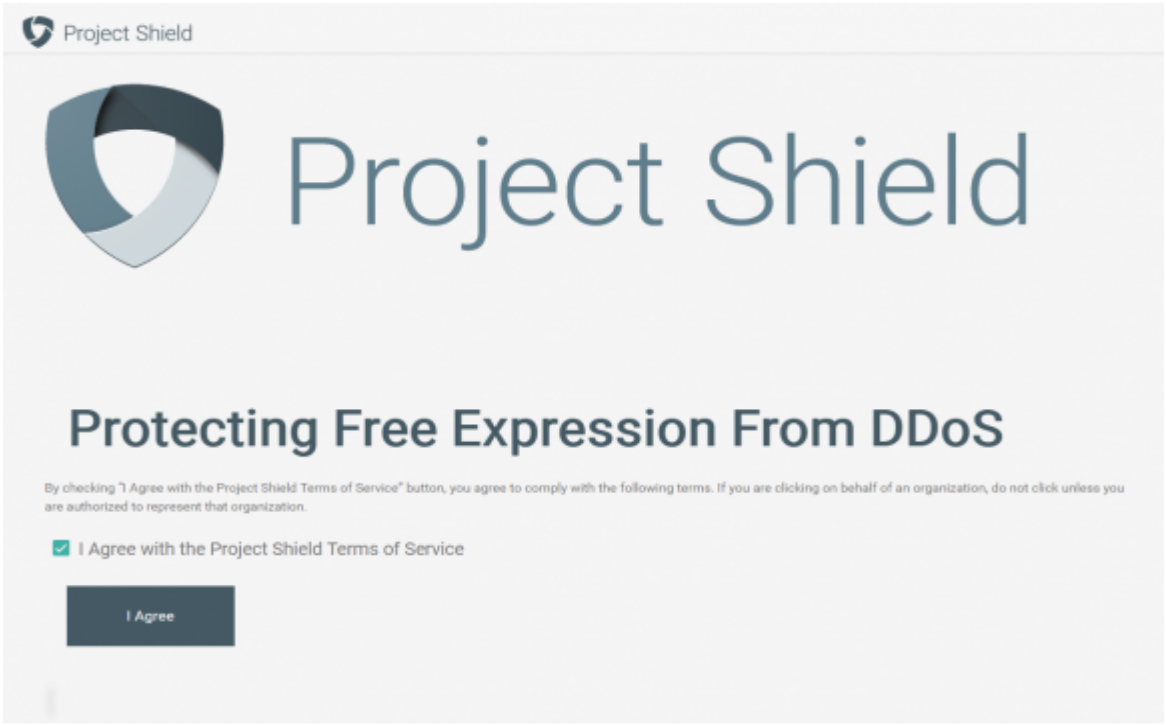
briankrebs @briankrebs · 22 de set

It's looking likely that KrebsOnSecurity will be offline for a while. Akamai's kicking me off their network tonight.

745 644

2016 – 25/09 – Google Project Shield

Today, I am happy to report that the site is back up — this time under Project Shield, a free program run by **Google** to help protect journalists from online censorship. And make no mistake, DDoS attacks — particularly those the size of the assault that hit my site this week — are uniquely effective weapons for stomping on free speech, for reasons I'll explore in this post.



Google's Project Shield is now protecting KrebsOnSecurity.com

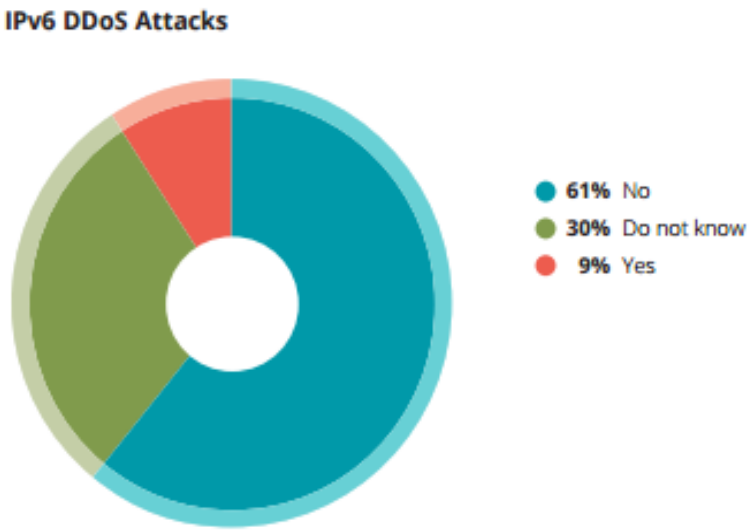
Protecting news from digital attacks

Project Shield is a free service that uses Google technology to protect news sites and free expression from DDoS attacks on the web.

#dig krebsonsecurity.com.
krebsonsecurity.com. 246 IN A 130.211.45.45

CIDR: 130.211.0.0/16
NetName: GOOGLE-CLOUD

Ataques DDoS – IPv6



- 354 Service Providers entrevistados
- 70% responderam ter IPv6 implementado

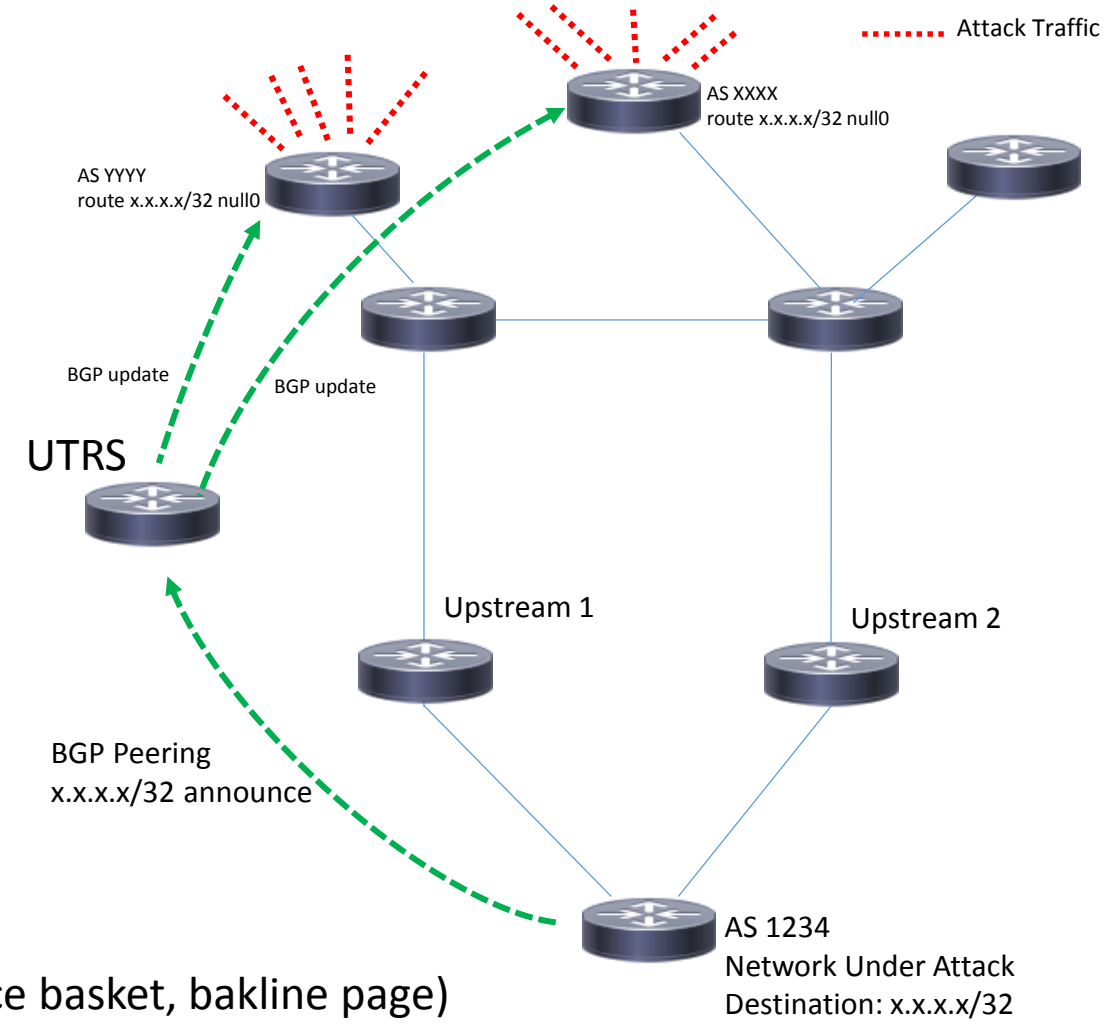
  2015 – 2% reportaram ter sofrido pelo menos 1 ataque DDoS
  2016 – 9%

  Ataque de maior volumetria - 6Gbps

Fonte: Arbor 2016 Worldwide Infrastructure Security Report

Mitigação – Team Cymru UTRS

- UTRS - Unwanted Traffic Removal Service
- Destination RTBH multihop – BGP
- AS vítima anuncia o ip atacado
- Verificação da autenticidade – whois e peering db
- Bloqueio do ataque no AS de origem
- Restrito a prefixo /32
- Quanto maior o número de ASs, maior a eficácia



Recomendado

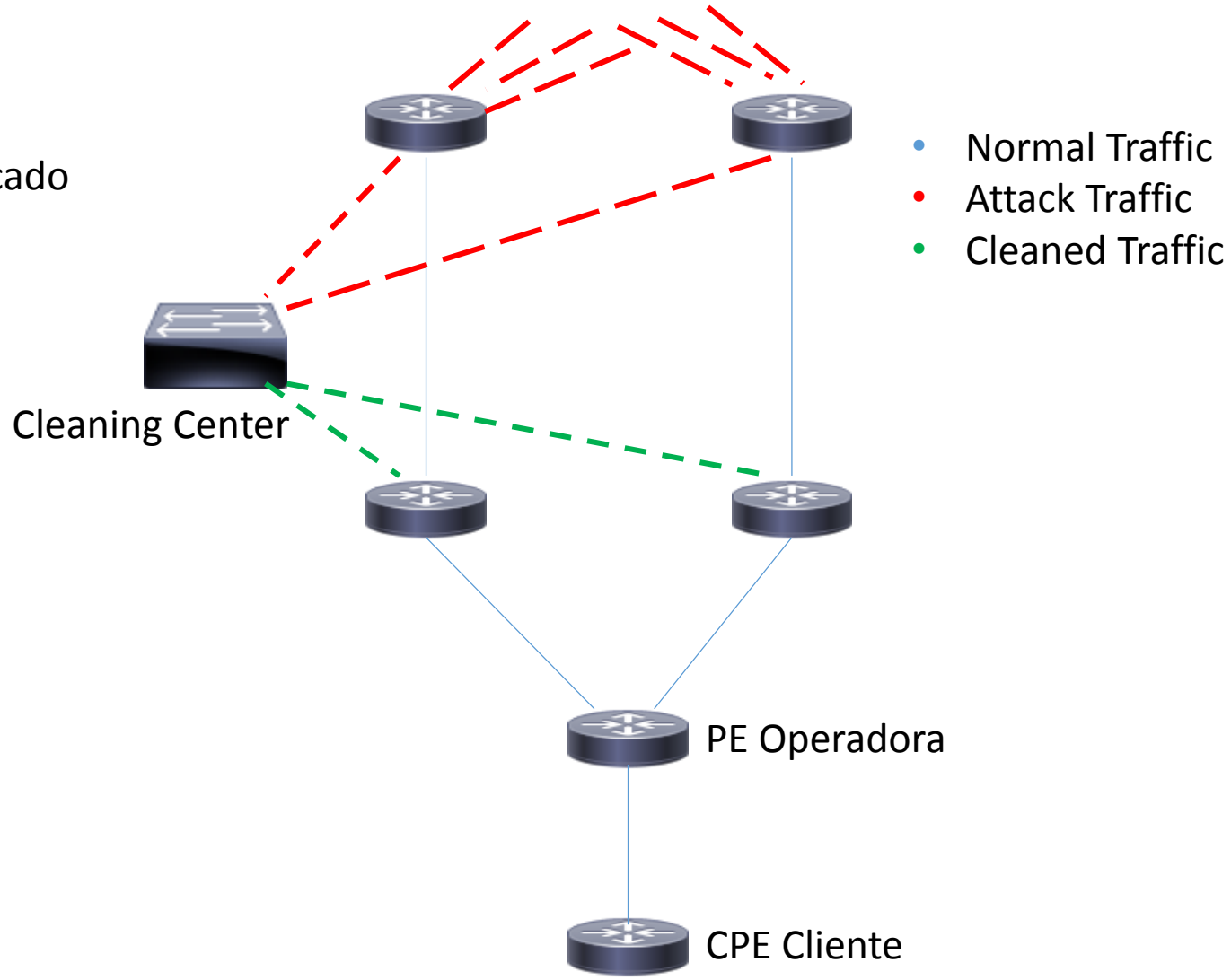
- Provedores de acesso para usuário doméstico
  Usuário(s) fica(m) sem acesso e o provedor salva sua rede

Talvez Recomendado...

- ISPs, Provedores de conteúdo e aplicações web
  Efetiva ao DoS - Serviço inacessível (news home, e-commerce basket, bakline page)

Mitigação – *Clean Pipe* IP Transit Providers

- Detecção do ataque via Netflow
- Anúncio mais específico via BGP do ip/prefixo atacado
- “Limpeza” do tráfego
  - Syn cookies
  - Filtros estáticos: drop udp src port 1900
    drop udp src port 123
  - Rate Limit per src/dst prefix and ports
  - Protocol Authentication
  - Payload regular expressions
  - TCP connection limit
  - Rate limit using GeoIP



Mitigação – Cloud DDoS Mitigation Service Providers

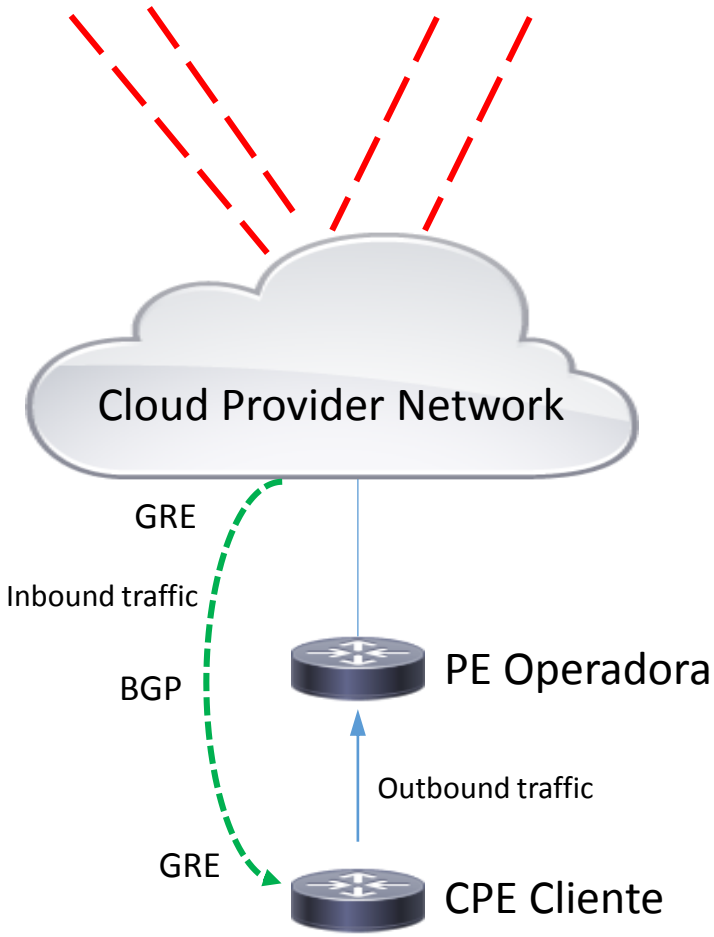
- Túnel GRE com a rede do Cloud Provider
- Sessão BGP estabelecida
- Detecção do ataque via Netflow
- Anúncio do bloco atacado via BGP
- Cloud Provider divulga o anúncio para seus upstreams
- Bloqueio de ataques de camada 3 e 4
- Serviço de Proxy / WAF HTTP/HTTPS

Prós

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

Contras

- Latência
- 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**

  - Rate limit IP/URL/URI

  - Análise header HTTP

    Check de User Agent
    Check de Referer

  - Inserção de cookies

  - Inserção de js

  - Inserção de captcha

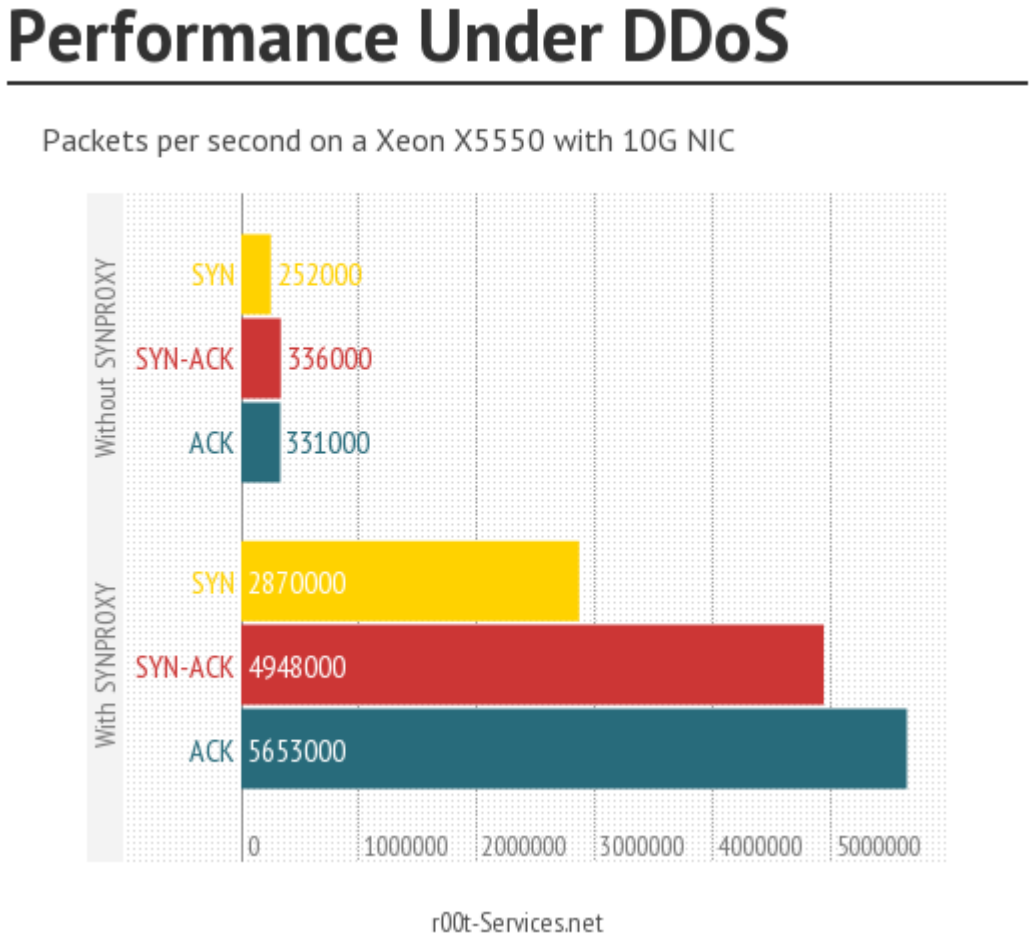
Mitigação – Home Made

- **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 Gerais

- **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

- **Configure Control Plane Policy. Filtre tráfego com destino ao control plane dos equipamentos**

- **Separe prefixos ip de infraestrutura de prefixos ip de serviços e clientes**

- **Facilite a mitigação – Separe ips/servidores para cada tipo de serviço – http(s), dns, smtp...**

- **Bom e velho Anycast**

- **Fuja de controles statefull na borda**

Referências

- CERT.BR - Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS) http://www.cert.br/docs/whitepapers/ddos/
- 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/
- UTRS - https://www.cymru.com/jtk/misc/utrs.html
- Google Project Shield - https://projectshield.withgoogle.com/public