Soluciones prácticas para los ataques de amplificación

Damian Menscher, Google

$ whoami

Ingeniero de fiabilidad de la

seguridad centrado en

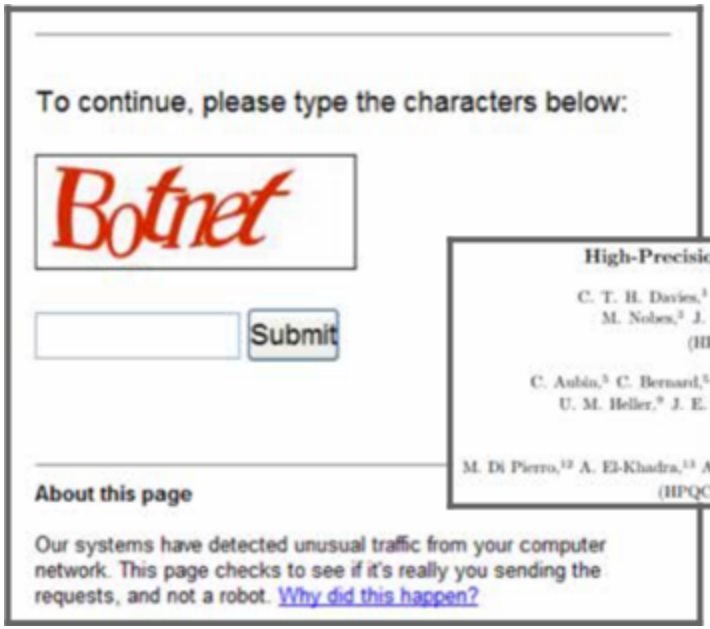
DDoS durante más de 10

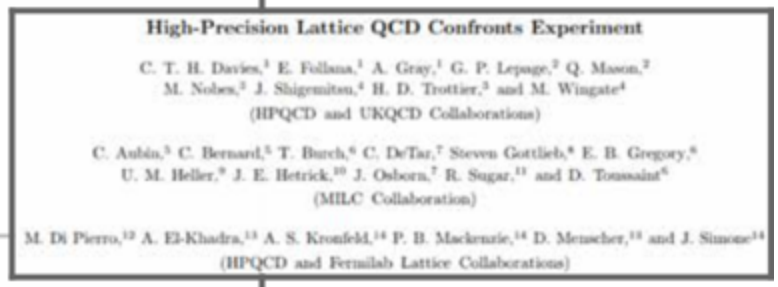
años

- autor de esa molesta página

captcha Fondo científico

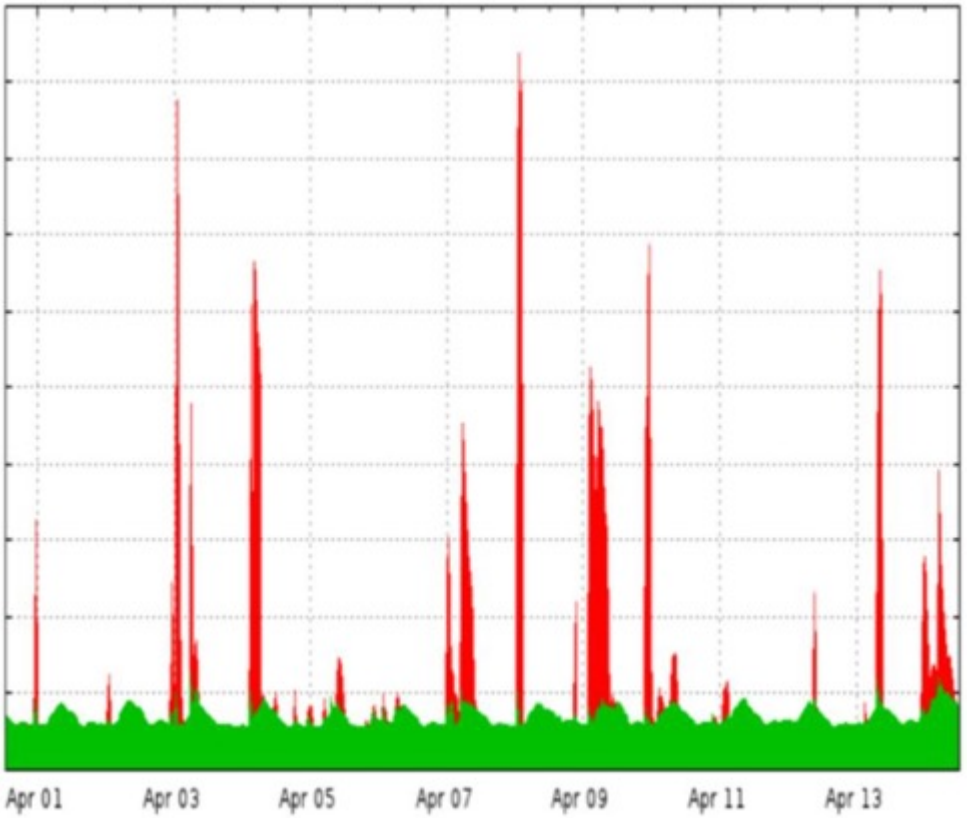
NO es un ingeniero de redes.





Agenda

2 Revisión de los ataques DDoS
3 Enfoques fallidos
4 Diseñar una solución



La creciente amenaza de los DDoS

Biggest DDoS attack in history slows Internet, breaks record at 300 Gbps

GitHub hit with the largest DDoS attack ever seen

DDoS attackers have found a new way of magnifying their attacks, with experts warning that bigger attacks are likely.

Ejemplos de titulares

#	Method Name	Method Type	Target Type	Target Syntax
1	GET-HTTP	Layer 7	Websites. WebServers. etc .	URL: http://target.com
2	HEAD-HTTP	Layer 7	Websites. WebServers. etc .	URL: http://target.com
3	POST-HTTP	Layer 7	Websites. WebServers. etc .	URL: http://target.com
4	JSBYPASS-HTTP	Layer 7	Websites. WebServers. etc .	URL: http://target.com
5	JOOMLA	Layer 7	Websites. WebServers. etc .	URL: http://target.com
6	SNMP	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
7	SSDP	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
8	DNS	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
9	CHARGEN	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
10	NTP	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
11	TS3	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
12	SSYN	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
13	DOMINATE	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
14	ACK	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
15	NGSSYN	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
16	OVX	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
17	TCPACK	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
18	TCPSYN	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
19	TCPRST	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
20	TCPURG	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
21	TCPPUSH	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
22	TCPECE	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
23	TCPCWR	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
24	ICMP	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
25	MUDP	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
26	VSE	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337
27	ATCP	Layer 4	Home / Peoples. Servers. Custom IPs. etc .	IP:1337

PRICING PACKAGES / perfect price

MONTHLY BRONZE	MONTHLY SILVER	MONTHLY DIAMOND
19.99$	24.99$	29.99$
XyZ Public Network	XyZ Public Network	XyZ Public Network
150-200Gbps Network Capacity	150-200Gbps Network Capacity	150-200Gbps Network Capacity
26 Attack Methods	26 Attack Methods	26 Attack Methods
1800(s) Stress Time	2400(s) Stress Time	3600(s) Stress Time
1 Months Membership	1 Months Membership	1 Months Membership
1 Parallel attacks	1 Parallel attacks	1 Parallel attacks
REGISTER	REGISTER	REGISTER

Ejemplo de servicio de arranque/estresado

Evitar las limitaciones de recursos

Coste asimétrico

Utilizar el cálculo de otros

Utilizar el ancho de banda de otros

DNS

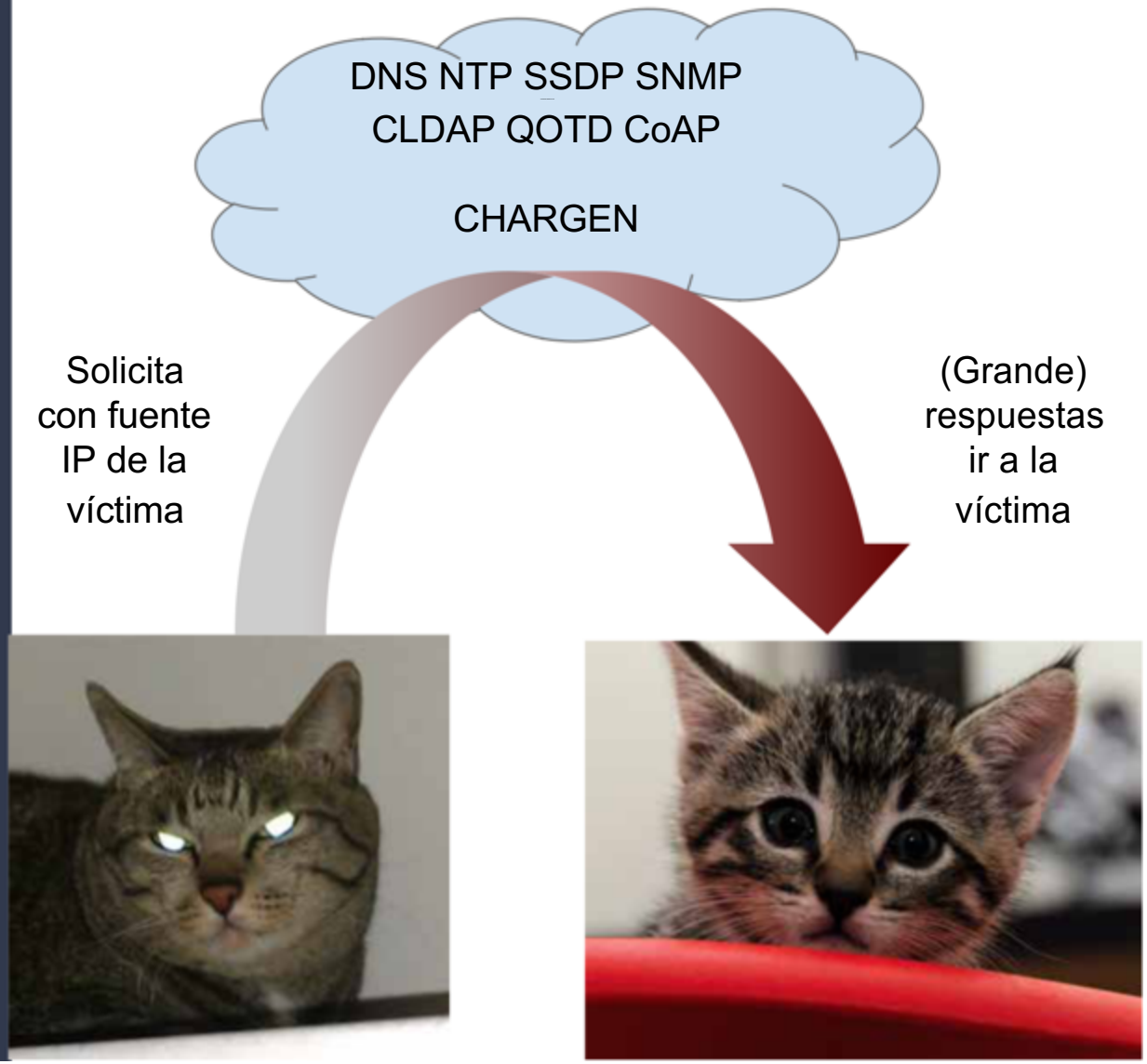
? cpsc.gov./ANY

```
cpsc.gov.	15880	EN	MX	0 hormel.cpsc.gov.
cpsc.gov.	15880	EN	RRSIG	MX 8 2 21600 20190515095424 20190512085424 35763 cpsc.gov. Pw8uxFtJ6bFXqCKhh+C4EQvzMoAfY6HydLyy9Oog/nFpfvopqGqfGUwV olQDf0Ixz6bPhxpZtOAfCZWQlDMUgk/CAXac82Ol2sV6PTydl20jA7lg YgUy8/06U8LmaU7M/E2kRt5Va+qdgXJ84sSENY8Ji4OkOc44QXmQ7ujv Ekw=
cpsc.gov.	1480	EN	DNSKEY	25638 AwEAAdpTN+Q/AWyqJuGr9cNbFLIVB2NLeIbMIb3HbOdZBnJr/2GiZPoX OUbRpLd7xvlitj9gsOjY7SuqcX3KF2YUq2UuPsEVUREi0BtZmhd5nRbK KCHzsPgyjBCkZyhy2j4BCHN9xlWT5isx0S322HXlxhOVTm/GWat59BW7 ey5IkkBX
cpsc.gov.	1480	EN	DNSKEY	25638 AwEAAeFVM04Xf7Y2etYKzgWua0rwLgsndqpac3qo2UMcIH3m87mCvpPw IHajpTEA6CEiGOq2thrxqDgpZqa81RgtXU2NAXaAX+cuCTDrDZrJ+AUs ID1vpVwDYKlBy59M+Q0B7KgWLNEX3uSrHXo56wAUuFDloGOsxobz2BGC NX1VbKDL
cpsc.gov.	1480	EN	DNSKEY	25738 AwEAAdRzvqE80pdmC3yXSdhUIuHHdLBjpaGOB4ZGQ6xVH+S5x7R+QHUp QQ13hLlWj1PFb1lahZH4jDiPV3KJFJSi/3FZE33wUg+kF/hdR5UqHel lRgvucNjnSpehc7CRNvBNEnraSqpvmHRp3qSJ85pIGpqexUPtee2BbN 7mFgvtPX0M9lQCxA5cLA8xFQdjSe7+WmeM3uEHcybTNgyjFV9lEeLikS rx5TTXtCacRZIXG0ib+hLMUFzItHw4YyRbmsoO0w0eNRhOZOg80tG+Zq QXe+zKhJn7ZVJ3DosJ4CY5iPuebZPyPe7AHjpZkrJS7co8+zE5AcohzV J4RiFxR85rU=
cpsc.gov.	1480	EN	RRSIG	DNSKEY 8 2 7200 20190515095424 20190512085424 40399 cpsc.gov. oTRqoVkzDAQV4obh9Fa+Qm1BW0sJpr16zwpHDlmdlwOyTNJtnwcv/nXl 6Zlr2SUPf0bsB6Z+65z3x2bJqcX1NArckdLWTwEjAWJ1W7dPcDPePZ51 TPGZ+bi13E3hrsmZhe9fUSg77jLOV2qERx4kPSSvyKPnTsi1R5K/OMZG gCOB8guNjRT7D3jNUPyy1R2lBzMmq1fEdbrlkSJ5gpaLYllzfMoM0yMz 4xdU8rLDG0rfE/ASGH3yB26xLgmtNdhLVsK176dOso6bJGUyDB5mVjby eQ46c5Zswya+CWkx46SsrBXF9f5VNx652lGSoJGss7dUbk5uIXX74EW3 +Metwg==
cpsc.gov.	15880	EN	NS	a1-85.akam.net.
cpsc.gov.	15880	EN	NS	a13-64.akam.net.
cpsc.gov.	15880	EN	NS	a3-67.akam.net.
cpsc.gov.	15880	EN	NS	a20-65.akam.net.
cpsc.gov.	15880	EN	NS	a4-64.akam.net.
cpsc.gov.	15880	EN	NS	a28-66.akam.net.
cpsc.gov.	15880	EN	RRSIG	NS 8 2 21600 20190515095424 20190512085424 35763 cpsc.gov. i8UkkKujiJiySKg+j59Mu9vl3qujIzHpAUzdRdPhSfZ1vpmWqv+F/7Yy NPLDDrtajHVMKpjEBCvW4rLTa/1/otM6OjPXY6n5nP9CbnFXfrtpIW1K 8rJZ9bbMQ44HeOTU0+OaMfMKQxwZ4Es4FLTGpIHCI9II0nTdOzgDDSk6 oyM=
cpsc.gov.	15880	EN	TXT	"da5eeb81385047fcb72043e2fcb34ac8"
cpsc.gov.	15880	EN	TXT	"v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.25 ip4:63.74.109.20 mx a:list.cpsc.gov -all"
cpsc.gov.	15880	EN	TXT	"2y97jj9vwr9ctt9v1yqdy88nyh39vmrk"
cpsc.gov.	15880	EN	TXT	"MS=ms34764123"
cpsc.gov.	15880	EN	RRSIG	TXT 8 2 21600 20190515095424 20190512085424 35763 cpsc.gov. xQsbL3stF/Wk8TBo3zXvbjOOfvkEWWSClYYgonTb0gxEYEzmqV34ioBV w44Xw9tCrQA2/MUnfTUkYUsVfRyU8ZqEu6BN/W8L1miX67cCiO7XO+3c YL/9eWnhKMwFQXTPExpPnQStGgBQVlxDFpTf0Hxsc9T8BwF7XLDI YFA=
cpsc.gov.	15880	EN	NSEC3PARAM	1 0 1 A14CB8E2EAF3B5A2
cpsc.gov.	15880	EN	RRSIG	NSEC3PARAM 8 2 21600 20190515095424 20190512085424 35763 cpsc.gov. Q7TA+3SJw/l1GHH/cuRB7sUMwQ6LjKcZ7TtLKdsBN4sCSkVV39bT3yda evn6d3izOdTdoSE4EX8NSqtq8PrbVmV/OzqeGS4Bu9zhqnnsuVeBld7t mtmPBw1H0cgonkRz1qUqmKZyMksmclDJ1kvHe4p8qV5rs/diYZ66Q0Va otQ=
cpsc.gov.	15880	EN	SOA	a1-85.akam.net. hostmaster.akamai.net. 1554486850 21600 3600 1728000 21600
cpsc.gov.	15880	EN	RRSIG	SOA 8 2 21600 20190515095424 20190512085424 35763 cpsc.gov. eSJ0Dt/U4lpuNhIV7bXyW9ZUrLA9pPfBaIF2tdw01pKycbY0glagHNy qyC+uKCkMV1M2ahQGUuiqfH56TpQ72llKbtoxwAl2aEGloSPlwrPzFiA 0LGlRWHh7GbIaGwfWEYw8O8cWok12UMsuDZYTKOWQUKFlbGY9VPfTqA asM=
cpsc.gov.	15880	EN	A	63.74.109.48
cpsc.gov.	15880	EN	RRSIG	A 8 2 21600 20190515095424 20190512085424 35763 cpsc.gov. owQZV2pTlCpYQg7VjoKlwHYWVR9KvXRI70lbk8E/eBFpY2Ml0mKfSJsA YO8kj54NZYOabaz6P/zRWW/nXxRqU/cw43DwlWVtvtIFe3DPk6Uv1Ix SXiG5r2R9J9Il/zYrw7NDIT/N9KaVYkHgHg0QRWvaXlWtfW8a7gqX2 j6w=
cpsc.gov.	15880	EN	AAAA	2600:803:240::2
cpsc.gov.	15880	EN	RRSIG	AAAA 8 2 21600
```

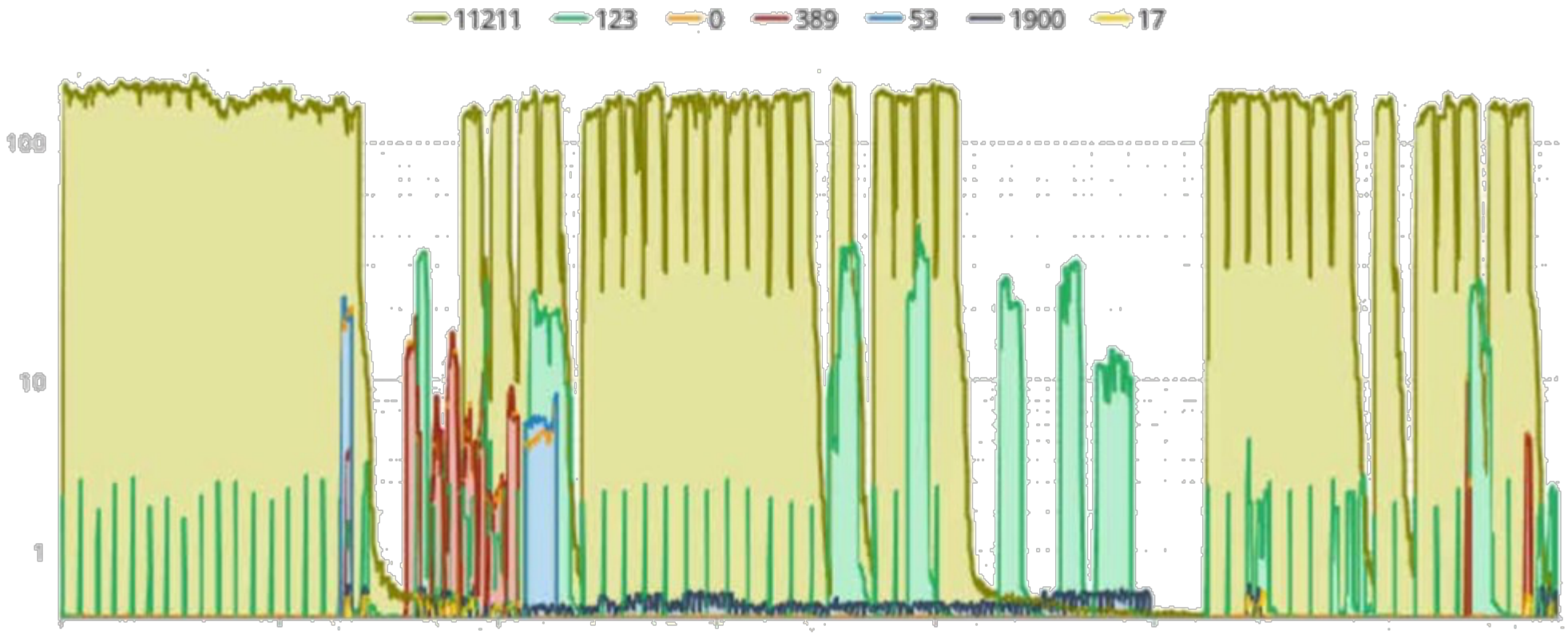
Reflexión / Amplificación Ataques

Amplificación de

5 ancho de banda
6 paquetes



Vista de la víctima de una serie de ataques de amplificación de DNS en agosto de 2017



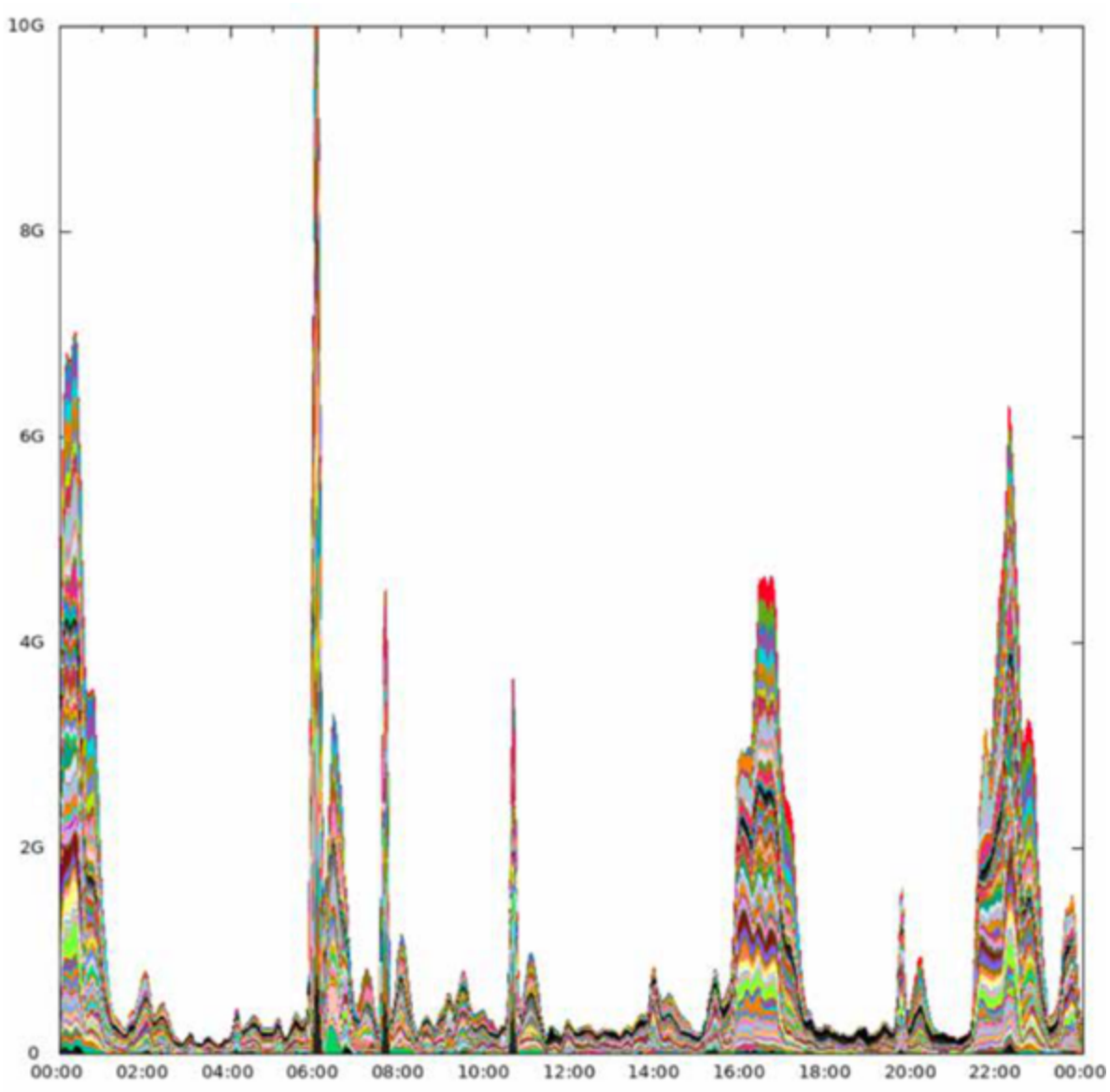
Opinión de una víctima de una mezcla de ataques de amplificación en abril de 2019

Defensa

Tubos de grasa

Peering global

ACLs del router para *estrangular los* paquetes UDP *de gran tamaño* procedentes de puertos de amplificación *conocidos*

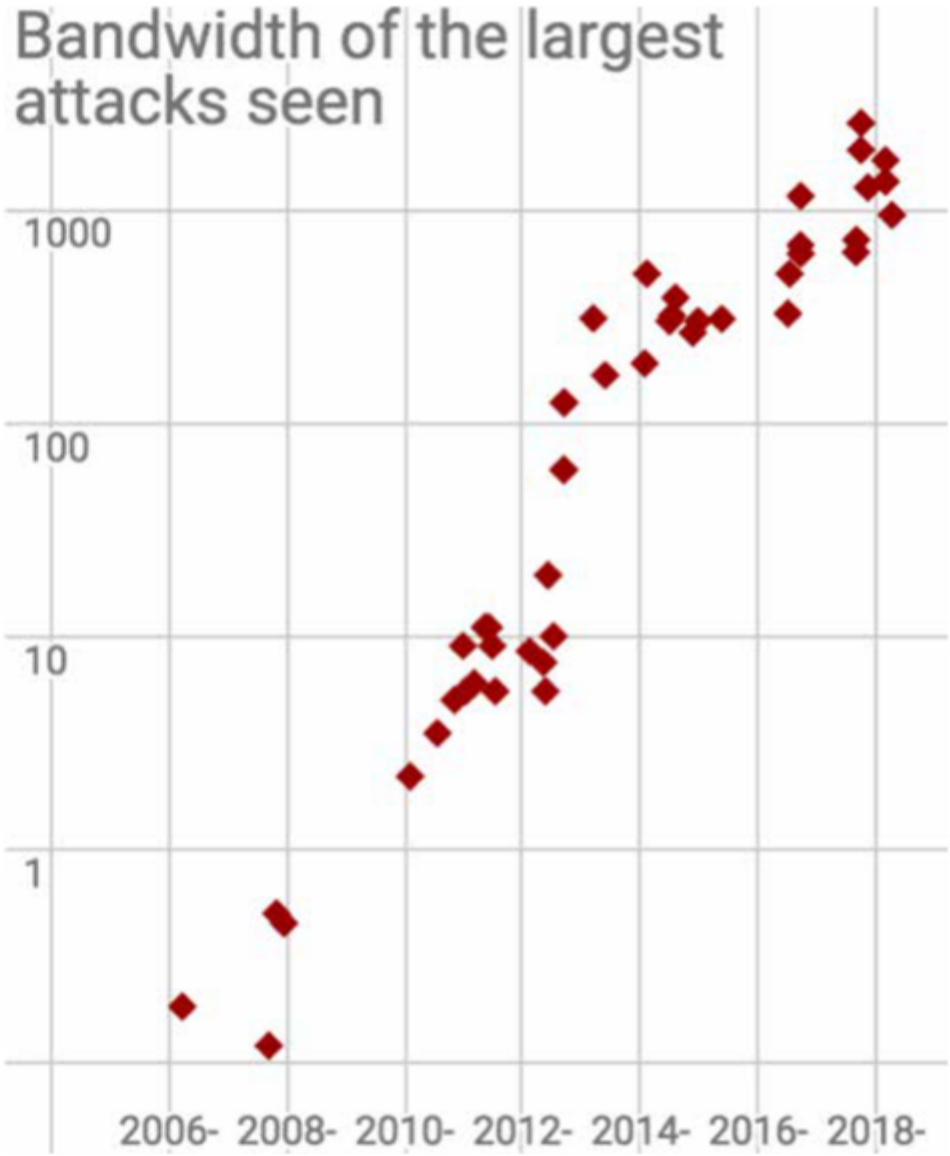


Crecimiento exponencial

Ley de Moore

Más dispositivos

- 5 Tbps de ataques este año



Enfoques fallidos

Bloquear / Acelerar UDP

Perjudica los protocolos existentes

¿Qué pasa con los DNS, QUIC, juegos?

¿Ampliación TCP?

Limpiar los amplificadores

Requiere demasiados

participantes Tasa de éxito del

99,9% → Fracaso

BCP 38

Ningún incentivo

Ayuda a los demás, no a uno mismo
→ ¿prioridad?

Network Working Group
Request for Comments: 2827
Obsoletes: 2267
BCP: 38
Category: Best Current Practice

P. Ferguson
Cisco Systems, Inc.
D. Senie
Amaranth Networks Inc.

May 2000

**Network Ingress Filtering:
Defeating Denial of Service Attacks which employ
IP Source Address Spoofing**

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Abstract

Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

Table of Contents

1. Introduction 2
2. Background 3
3. Restricting forged traffic 5
4. Further capabilities for networking equipment. 6
5. Liabilities. 6
6. Summary. 7
7. Security Considerations. 8
8. Acknowledgments 8
9. References 8
10. Authors' Addresses 9
11. Full Copyright Statement 10

Solución por diseño

$$PSuccess = \frac{Incentivo}{Participantes}$$

Identificación de las ASN problemáticas

Servidores de cebo

El atacante necesita miles de servidores de amplificación

Algunos están en su red

Contadores del router

Control sencillo en tiempo real

Busque puertos UDP a amperios

conocidos Más fácil a medida que

se acerca a la fuente

Considere la posibilidad de repetir para los paquetes SYN para atrapar los synfloods suplantados

```
término potencial_udp_amp {
  de {
    protocolo udp;
    puerto-destino [ 17
                     19
                     53
                     69
                     111
                     123
                     137-139
                     161
                     389
                     1900
                     3702
                   ] 11211
  } entonces {
} } count potential_udp_amp;
```

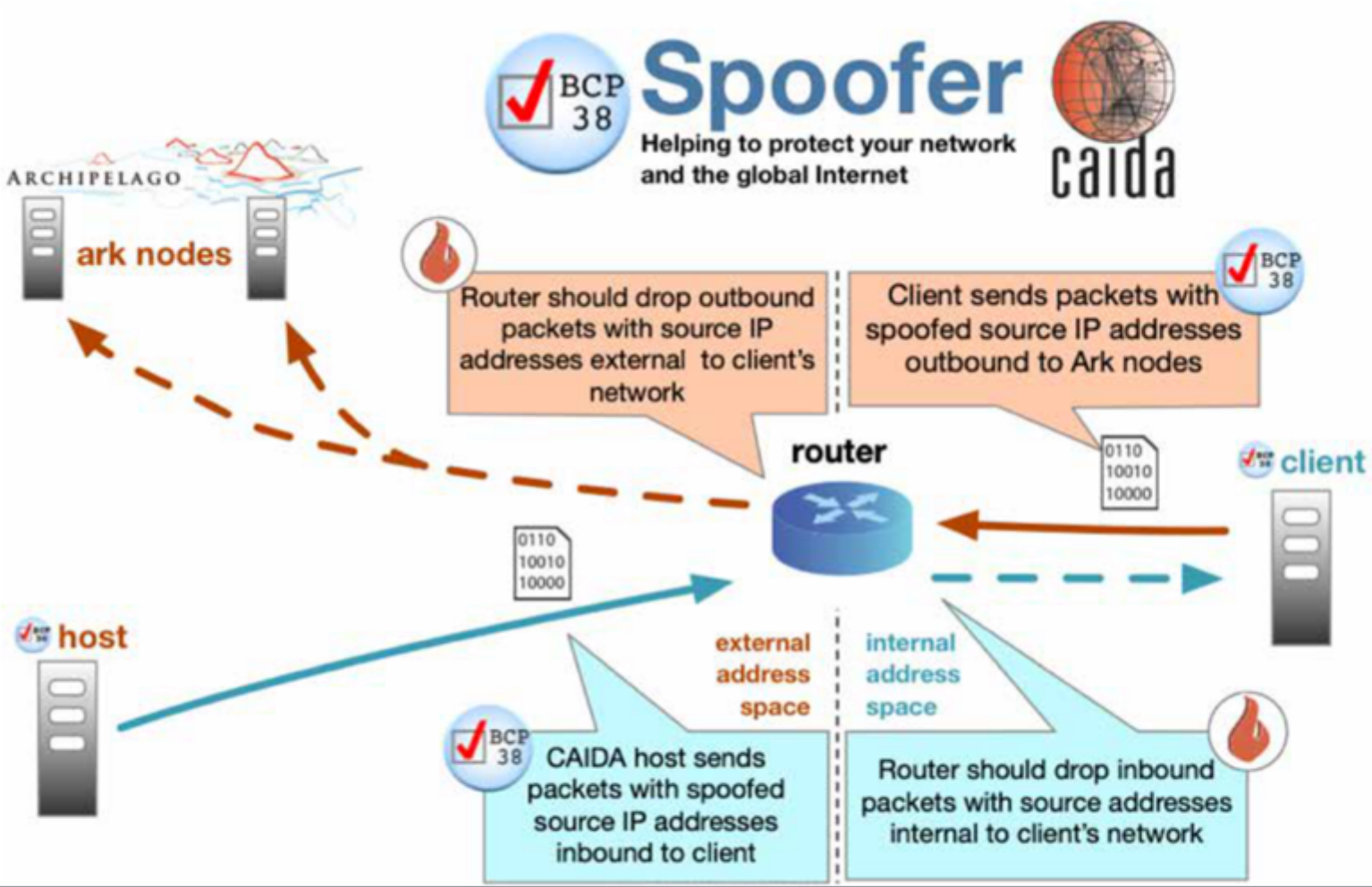
Netflow / Sflow

Busque muchos ASN que entren
en un solo enlace

Preocupaciones comunes

- Tamaño: 1:64k frecuencia de muestreo
- Privacidad: retención de 2 semanas
- Análisis: Base de datos SQL

```
dremel> select count(distinct source_ASN),
                iface from netflow;
+------- +-------+--------------------
                 | Descripción del
| ASNs   | metro enlace
+------- +-------+--------------------
| 44235 | ams    | Asteroide
| 32423 | lga    NYIIX
| 16585 | lax    AS 3491
| 15054 | fra    | InterLan
| 12814 | mil    AS 3257
|   8730 | fra    DE-CIX
|   8654 | lis    GIGAPIX
|   8269 hkg      AS 4134
|   7032 | maa    AS 55410
|   7026 | lax    AS 3356
|   6204 | orden AS 6453
|   5905 | svo    AS 12389
|   5828 | mil    AS 6453
|   5828 | svo    AS 12389
|   5739 | lax    AS 3356
|   5693 | svo    AS 12389
|   5336 | orden AS 6453
|   5036 | gru    PTT.BR
|   4915 | mct    AS 8529
|   4557 hkg      AS 4134
```



Proyecto Spoofer de CAIDA

Fuente: https://www.caida.org/projects/spoofer/

AMS-IX	EXTREME IX DELHI	SWISSIX	ASNs:
AMS-IX HONG KONG	FRANCEIX	TIE-ATLANTA	
CUALQUIER2	Giganet	TORIX RS2	209 701 1239 1273 1299 2711 2914 3255
BBIX SINGAPUR	HKIX	UA-IX	3257 3267 3320 3356 3491 3741 3786 4134
BIX-BG	HORYZONT	W-IX	4230 4657 4755 4761 4766 4788 4826 4837
Dataline-IX	InterLan		5391 5650 6128 6453 6461 6762 7385 7418
DE-CIX	IXPN		7497 7552 7922 8100 8151 8251 8473 8595
DECIX	JPNAP TOKYO 1		8717 8881 8928 8966 9050 9121 9198 9299
DE-CIX Hamburgo	LONAP		9304 9318 9381 9416 9498 9658 9829 10026
ECIX-Hamburgo	MEGAPUERTO LOS ANGELES		10429 11014 12389 12552 12578 12670
EQUINIX	MEGAPUERTO DE SINGAPUR		12714 12876 12956 13489 14259 16637
Equinix Ashburn	MIX		16735 17451 17547 17557 17639 17917
EQUINIX DALLAS	MSK-IX		17922 18101 18207 18229 18403 18734
EQUINIX HONG KONG	MUMBAI-IX		18747 21859 23520 23930 24203 24961
EQUINIX LOS ANGELES	PEERING.CZ-ROUTE-SERVERS		26613 27552 29049 29091 31133 33480
EQUINIX PARÍS	PTT.BR		33576 34772 34867 36351 36884 36944
EQUINIX SAN JOSE	RoNIX		38193 40676 41798 44217 45194 45769
EQUINIX SINGAPUR	SGIX		45899 45903 52320 55352 55410 55818
EQUINIX SYDNEY	SEIS		58453 58587 58601 58717 60294 132602
Equinix Zúrich	SPB-IX		132876 133840 134009 135834

Compañeros que envían tráfico suplantado a Google en un ataque de botnet el 30-05-2018

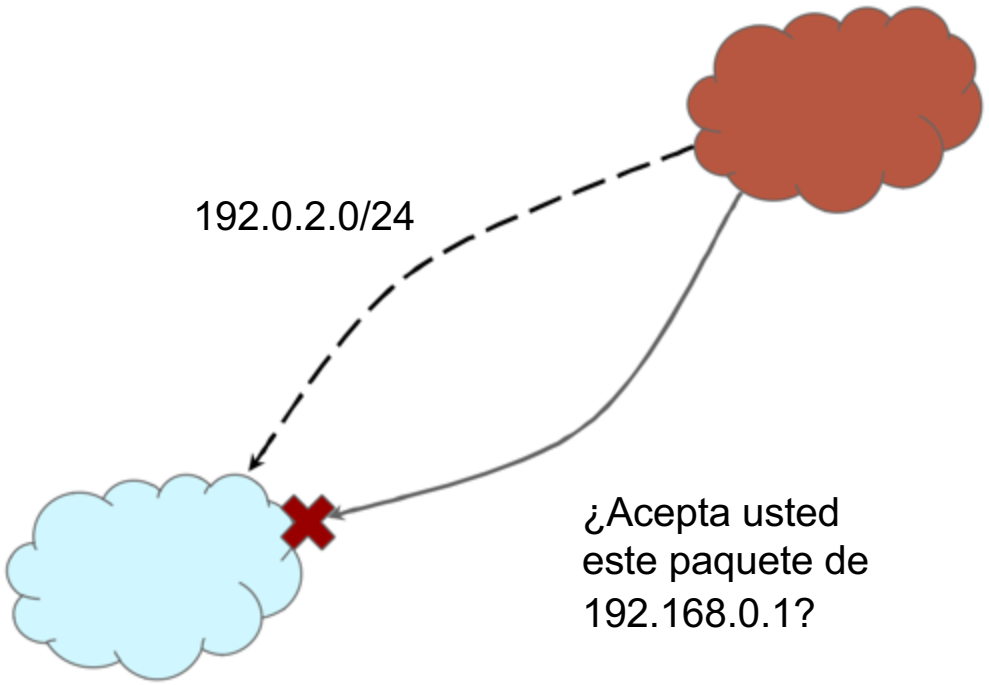
(Des)cooperación
Remediación
de las ASN problemáticas

uRPF

¿Suelto o estricto?

¿Ruta asimétrica?

¿El doble de búsquedas de rutas?



ACLs

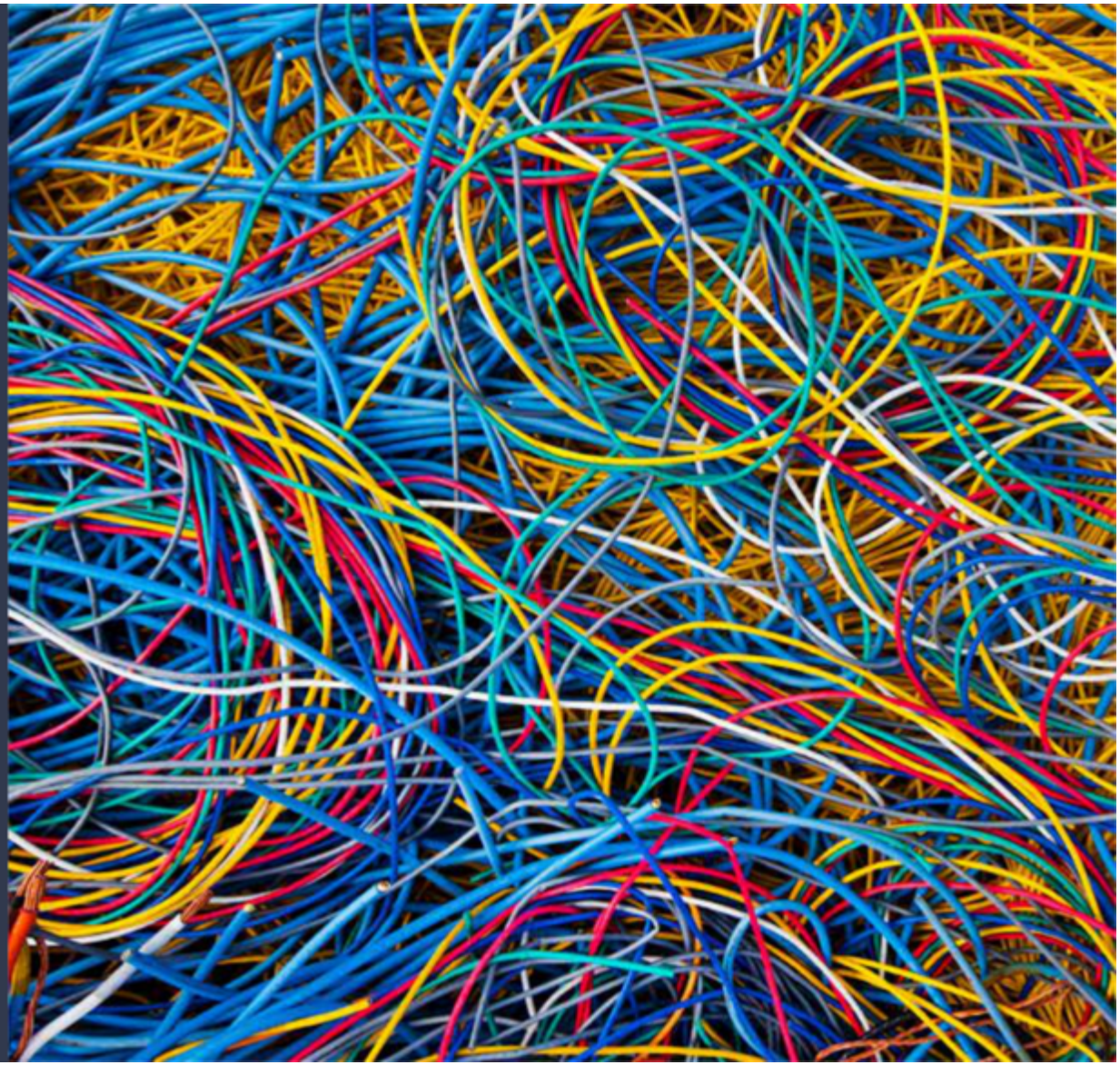
Útil para los clientes con

problemas Automatización

para mantenerse al día

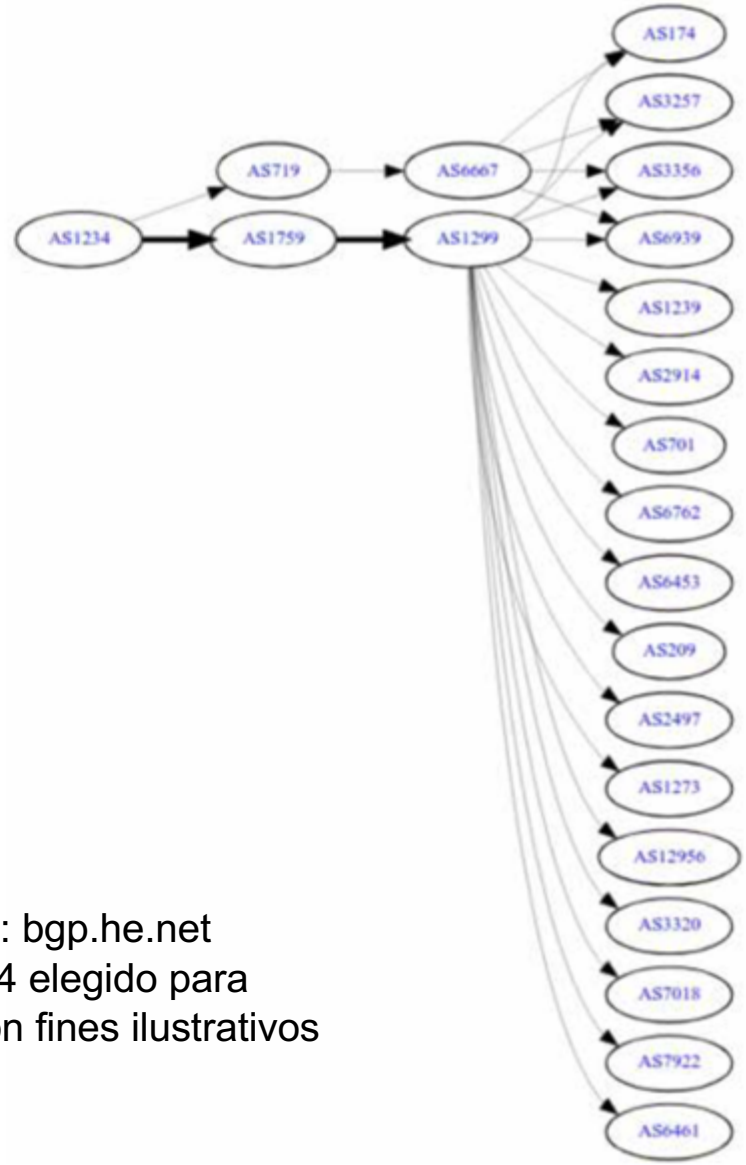
Sin embargo, ¿el router sólo puede soportar 10k prefijos?

- 15169: 500
- 16509: 3,500
- 4134: 14,500 → 470



Puntos de aplicación

Atacante → Tránsito → Amplificador



Fuente: bgp.he.net
AS1234 elegido para
sólo con fines ilustrativos

¿Incentivos para los proveedores de transporte?

Los proveedores de tránsito están en condiciones de eliminar todos los ataques de amplificación de UDP (y los synfloods de fuente falsa).

¿Cómo podemos animarlos?

Proactivo: mejorar la estabilidad de Internet

Reactiva: respuesta a las denuncias de abusos

Legal: solicitudes de rastreo de ataques por parte de las fuerzas de seguridad

11. evitar la carga de responder filtrando el tráfico de ataque falsificado

Económico: los clientes prefieren a los proveedores de tránsito que filtran los paquetes falsos

Regulación: (amenazas de) mandatos gubernamentales ¿Otros?

Llamada a la acción

Proveedores de software:

9 DEBE minimizar la amplificación a fuentes no verificadas

Proveedores de la red:

- están OBLIGADOS a filtrar el tráfico de salida para evitar la suplantación de identidad
- PUEDEN solicitar a sus proveedores de tránsito que rastreen el origen de los ataques de falsificación

Proveedores de transporte:

- DEBERÍA utilizar los contadores de netflow o de los routers para identificar las fuentes de tráfico falsificado
- DEBE aplicar ACLs a los clientes que no cooperan