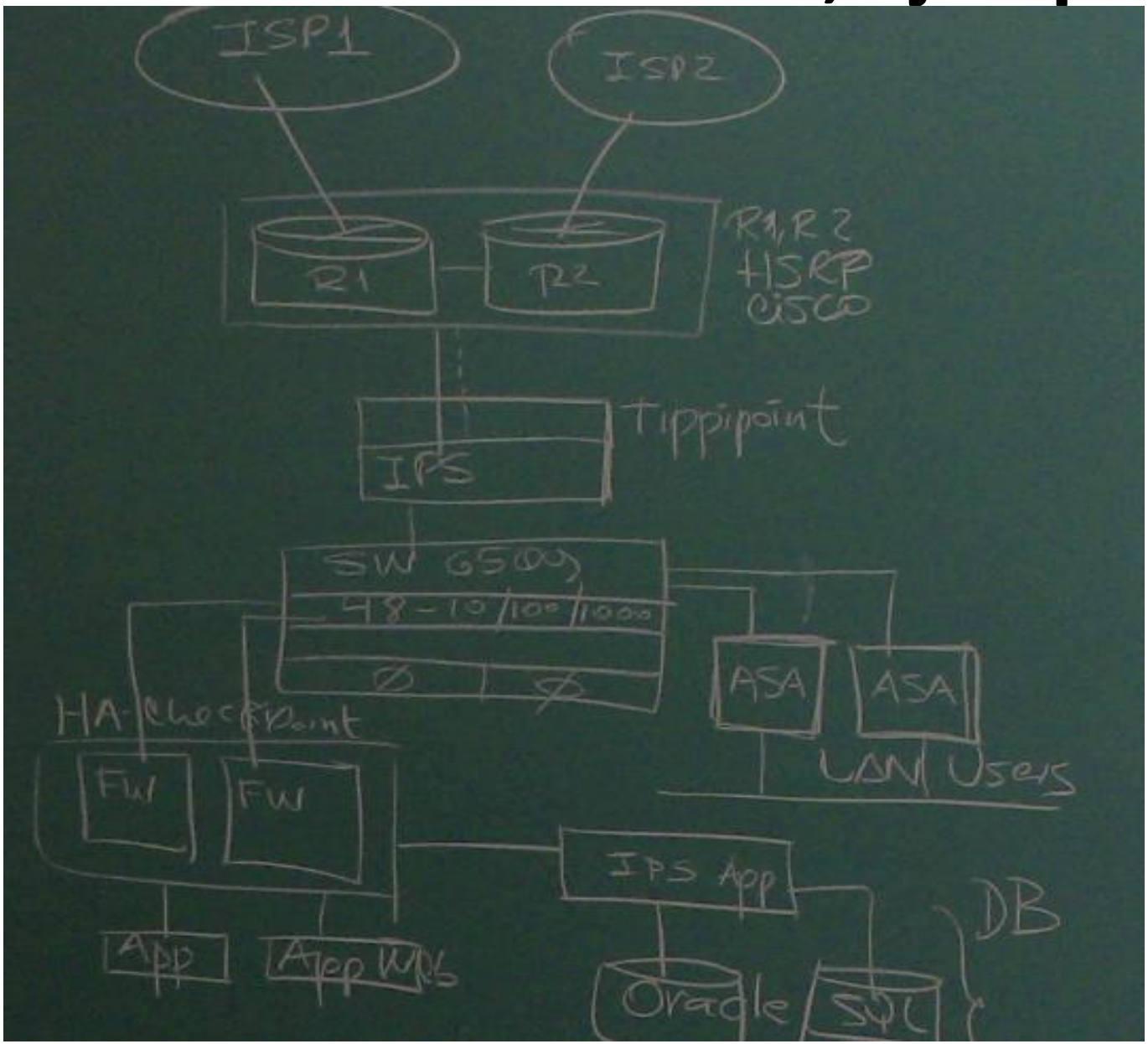
Ataques DDoS

cesar.farro@gmail.com
@cesarfarro
SANS Institute/GIAC Firewall Analyst y GIAC System Network Auditor
Lima, Perú 2014

DOS, puede ser un simple paquete de datos que confunde al host destino.*

* Fuente: Official CEH Certified Ethical Hacker for version 7.1

Características Red LAN, Ejemplo:



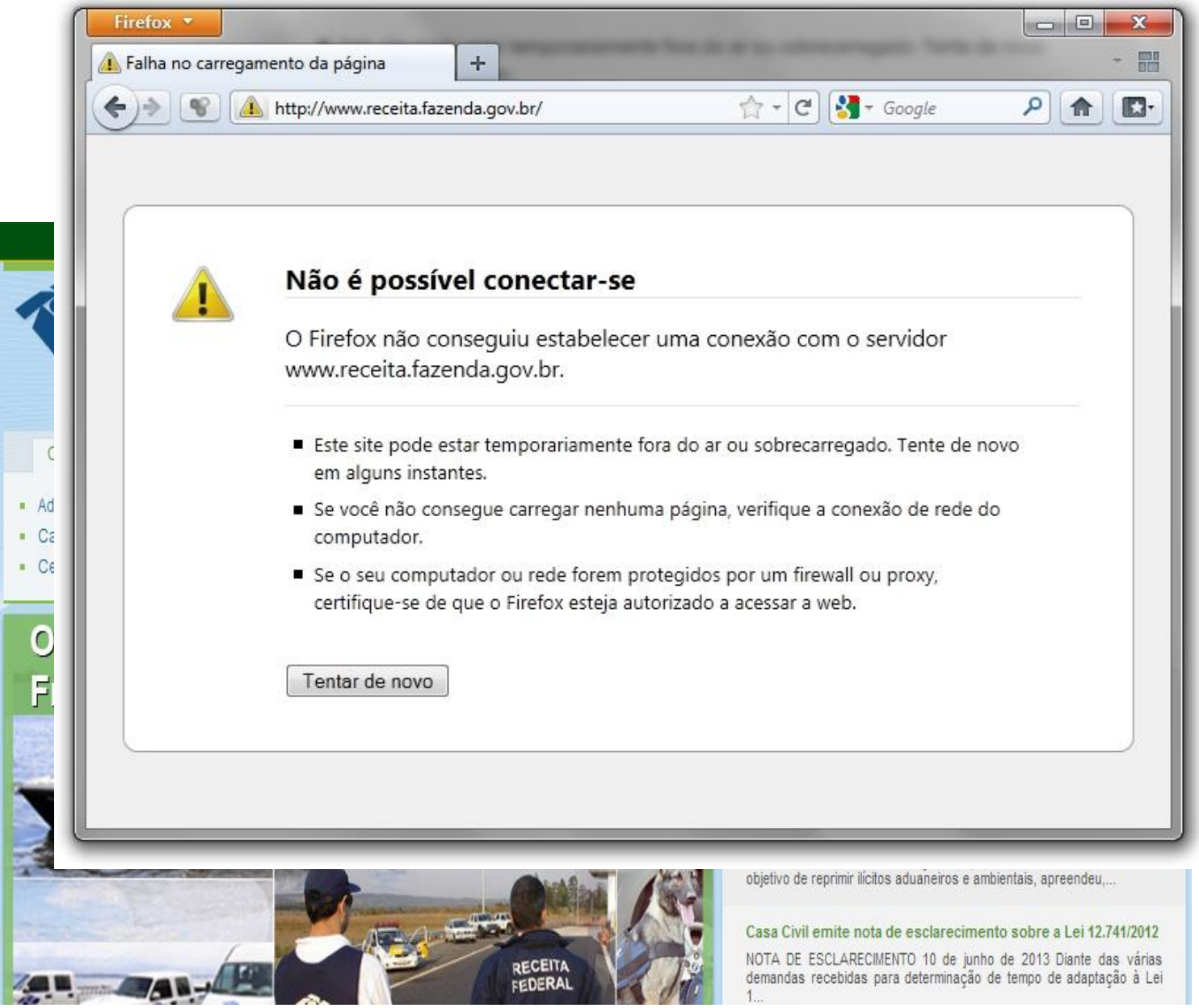
I. Introducción de Conceptos

- ¿ Qué es un Ataque DoS (Denial of Service)?
  - Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Provoca la **perdida** de:
    - Conectividad, por el consumo del ancho de banda.
    - Sobre Carga los recursos computacionales (CPU, Memoria, Firewall).
- ¿ Qué es un Ataque DDoS (Distributed Denial of Service)?
  - Es un ataque Distribuido que usa diferentes fuentes de ataque : Nacional e Internacional para atacar un objetivo.

Brute Force-DDoS:

Direcciones origen hacia tú servicio web?

1.168.128.18 1.168.133.232 1.171.106.21 1.226.84.109 2.229.114.95 24.172.71.54 31.193.199.11 41.41.157.67 42.96.186.119 42.96.188.254 46.166.179.121 46.191.253.31 60.8.151.41 61.129.79.156 61.177.119.232
62.90.169.167 62.99.69.102 62.131.32.107 62.162.122.197 64.31.41.108 64.216.87.201 66.18.189.200 69.28.57.85 72.215.205.84 76.72.165.98 78.186.125.49 78.187.137.186 79.5.31.209 79.13.8.107 81.12.40.210
82.127.123.186 83.110.242.198 85.105.87.79 85.111.29.6 85.173.221.29 87.102.63.186 87.106.9.136 87.110.46.24 87.240.199.89 88.163.52.153 89.97.101.81 91.183.60.216 93.174.94.79 94.37.34.122 94.43.71.137
94.43.245.253 94.43.250.199 94.45.65.63 94.103.140.151 94.129.251.152 94.229.39.170 94.230.68.36 94.233.114.164 94.240.224.101 94.240.239.112 94.241.197.67 94.241.212.162 94.241.216.11 94.241.251.221 94.242.21.183
94.242.190.126 94.243.14.87 94.243.130.99 94.245.163.189 94.249.60.238 95.70.31.230 95.97.235.138 95.243.93.141 96.228.20.131 103.10.222.2 108.171.193.112 108.176.117.45 109.105.4.43 110.143.40.163 111.74.239.61
111.146.13.72 111.248.18.243 112.65.240.228 112.170.76.34 113.160.112.224 114.43.5.23 115.200.222.244 115.239.229.231 116.228.88.134 117.25.173.18 117.223.17.192 118.0.188.90 118.122.176.42 118.175.16.2
118.175.16.4 121.15.255.50 122.16.163.82 122.228.242.85 123.63.3.34 124.232.137.184 128.73.243.47 151.49.58.76 151.240.54.42 173.54.24.3 174.141.36.41 175.139.187.57 177.99.172.63 178.91.252.106 180.211.213.4
182.52.33.134 183.82.53.233 187.62.211.66 188.94.210.154 189.15.218.69 190.5.121.71 190.85.212.11 193.77.147.194 194.231.246.114 194.244.248.42 195.110.151.130 198.64.251.8 198.175.124.18 200.27.66.70
200.212.47.72 201.27.46.239 201.77.5.78 202.9.104.183 202.112.31.17 203.39.158.1 203.220.78.66 209.205.72.199 211.138.127.214 211.158.255.9 212.106.59.98 213.96.144.92 213.126.23.106 213.139.19.30 216.107.155.37
218.23.4.77 218.75.77.174 220.246.71.243 221.12.60.184 221.123.163.106 222.186.57.37 159.253.46.234 198.96.93.159 216.157.93.224 61.158.162.167 83.110.224.195 71.190.247.28 61.12.10.86 112.175.63.45 115.28.40.214
139.228.138.90 74.86.194.8 82.221.99.231 85.214.41.33 91.183.225.194 85.214.148.36 2.229.114.95 85.214.45.152 200.204.155.97 115.28.40.211 200.20.1.8 108.21.72.98 218.29.134.138 125.212.36.116 78.93.43.58
113.10.238.168 61.147.103.81 199.182.233.143 202.105.183.89 207.82.97.4 208.110.82.178 218.23.49.154 220.135.97.12 79.113.41.61 168.63.209.246 105.236.214.137 202.71.238.230 24.85.86.184 88.191.97.61 218.56.38.228
62.38.217.240 109.230.244.207 98.126.49.98 115.28.40.226 115.239.229.231 65.111.165.108 77.68.236.114 67.199.160.150 92.55.23.24 71.177.42.136 58.241.40.74 38.96.153.52 216.197.160.38 109.230.217.21 131.107.86.236
68.178.128.111 85.110.59.115 61.177.119.227 71.167.115.208 108.62.170.178 114.43.24.187 122.226.95.38 82.165.197.46 61.160.195.43 195.19.246.190 85.214.80.6 103.15.61.222 124.232.150.47 202.155.212.70 92.27.52.214
124.207.235.2 142.4.109.199 182.237.2.90 188.138.24.230 198.96.93.141 211.95.79.53 64.216.87.201 87.106.1.184 61.146.235.118 94.233.114.164 222.186.59.231 174.142.34.249 79.113.36.119 125.210.185.133 188.40.244.53
213.88.21.212 122.89.30.208 173.22.119.157 46.191.221.126 66.182.253.103 210.56.63.149 79.48.104.152 111.85.65.78 115.236.79.211 115.30.227.159 202.109.145.3 221.133.245.213 61.183.11.163 211.142.19.249
111.68.96.83 183.46.184.247 202.30.46.96 41.160.216.82 79.181.178.150 94.127.53.48 188.231.1.3 115.28.41.123 116.52.250.210 122.10.131.215 123.161.157.11 163.43.48.5 190.5.216.7 190.85.212.11 202.104.137.173
202.176.90.148 212.119.89.11 212.69.54.74 60.55.8.10 60.55.8.11 60.55.8.12 60.55.8.13 60.55.8.14 62.233.76.80 69.197.189.48 69.64.65.141 71.6.147.158 80.141.177.11 88.191.237.207 115.28.41.12 220.180.190.118
113.105.185.130 200.232.176.75 208.115.38.125 42.96.194.20 42.96.197.80 88.191.237.207 95.133.2.14 113.105.185.130 200.232.176.75 208.115.38.125 42.96.194.20 42.96.197.80 88.191.237.207 95.133.2.14 115.28.41.124
60.8.151.41 61.161.187.18 61.191.55.182 41.0.114.212 80.92.188.253 95.66.103.194 187.45.247.156 77.72.140.226 187.45.247.156 173.55.116.154 178.216.126.86 115.28.41.118 198.100.114.85 117.135.138.150 81.174.58.210
64.143.229.76 75.149.199.153 103.30.43.57 115.28.41.128 118.32.247.83 122.224.9.198 163.20.242.75 221.12.60.184 62.103.69.67 64.247.170.12 95.211.58.234 109.230.222.219 112.65.240.228 115.28.41.13 115.28.41.132
116.255.227.144 134.75.217.67 137.116.211.162 165.228.127.81 175.194.101.207 176.40.104.119 177.135.247.140 190.12.31.162 194.1.154.161 198.46.103.165 200.35.74.75 202.9.104.185 203.115.125.2 208.115.38.125
210.209.72.66 211.75.195.128 212.55.161.59 213.8.110.249 218.50.191.165 218.60.25.130 221.120.19.29 41.41.233.172 61.177.119.232 61.177.119.233 63.131.77.78 66.76.242.28 68.62.200.2 70.62.237.233 72.77.202.79
79.39.88.28 81.241.64.234 85.102.236.87 89.207.78.174 89.33.78.189 92.45.199.54 94.127.53.48 95.9.176.208 99.58.27.156 176.42.7.249 218.50.191.165 23.19.75.26 41.220.115.59 93.92.147.98 94.132.159.7 94.59.167.34
95.31.213.156 50.78.218.163 41.131.50.234 1.234.89.223 111.74.238.32 119.92.180.165 173.201.18.225 176.109.227.66 192.74.238.106 199.21.69.95 201.217.32.8 217.11.189.242 68.16.111.201 71.188.25.51 184.75.36.69
59.108.67.188 61.191.55.39 89.151.119.14 118.175.16.2 12.217.136.132 187.188.94.178 192.116.96.22 195.26.77.175 198.100.124.87 203.45.140.117 208.105.149.74 209.42.77.17 216.104.144.42 218.75.155.6 61.164.116.80
68.124.228.238 77.87.132.21 78.93.242.82 83.170.96.6 84.22.180.243 88.26.180.66 90.176.237.145 91.123.18.112 112.134.198.154 119.2.3.88 187.216.131.243 187.216.131.254 192.198.94.98 42.96.140.141 94.177.148.67
94.229.74.195 99.179.97.169 112.134.198.154 119.2.3.88 187.216.131.243 187.216.131.254 192.198.94.98 42.96.140.141 94.177.148.67 94.229.74.195 99.179.97.169 168.62.200.183 184.173.136.244 216.164.45.201
218.28.172.7 84.235.5.222 85.105.48.251 218.65.30.26 175.139.158.77 189.115.193.76 190.44.249.126 193.93.122.60 2.50.185.145 221.131.92.21 222.186.25.148 37.105.222.199 41.32.28.23 60.13.231.10 64.166.137.83
81.213.156.39 82.221.99.231 91.225.83.237 92.115.144.251 95.225.218.147 1.215.230.162 111.93.159.69 115.28.39.140 12.217.136.131 121.199.6.185 140.114.71.222 141.8.244.238 144.76.4.74 188.169.176.238
189.41.217.139 189.76.69.148 190.191.55.199 202.77.177.186 203.223.93.43 218.17.158.115 219.235.1.74 222.134.50.106 222.186.30.244 31.210.68.34 42.96.196.209 61.129.79.130 61.177.119.228 62.219.133.45
65.90.114.138 70.148.51.112 77.73.8.125 77.94.122.183 78.186.178.9 88.248.250.67 199.119.201.79 115.28.42.208 175.139.187.57 183.63.190.50 184.105.171.8 203.109.197.8 85.110.154.50 110.191.41.145 112.136.142.180
115.91.92.222 116.247.97.134 12.199.11.146 120.105.97.72 125.88.8.30 142.46.18.34 168.63.101.188 168.63.42.113 175.102.0.8 184.82.53.204 187.40.69.54 188.138.89.100 190.120.237.4 192.34.65.165 193.227.46.18
201.223.57.67 203.92.34.85 210.56.63.39 218.63.105.146 222.42.62.99 35.8.219.233 5.134.200.202 63.131.80.201 64.64.201.135 66.2.52.130 78.47.248.101 80.99.9.157 82.137.243.57 88.247.33.129 91.187.93.5 189.73.155.167
93.108.250.117 95.229.237.153 115.28.33.136 121.234.31.190 185.12.45.55 218.75.153.138 58.248.185.20 131.107.86.236 61.147.103.81 108.62.206.86 114.100.213.253 115.28.42.178 119.254.22.2 186.3.54.50 196.221.147.45
211.20.146.95 216.198.12.32 216.198.13.182 216.45.55.123 80.55.100.226 82.221.99.235 1.34.184.8 107.21.151.138 109.162.129.212 115.28.35.4 115.28.42.206 117.79.80.82 118.97.39.29 119.139.193.236 137.214.10.20
142.54.188.249 180.186.16.142 184.82.179.148 187.95.188.145 202.142.23.162 211.142.154.94 218.27.198.244 221.203.138.9 24.37.2.218 31.13.163.110 50.73.201.241 60.166.5.152 62.105.48.78 62.219.142.191 67.32.61.230
70.184.3.211 74.115.92.254 78.129.252.159 82.79.52.171 86.122.180.160 87.205.8.201 98.100.75.219 123.85.182.15 212.86.255.31 62.215.162.23 93.107.163.235 116.11.185.10 118.35.209.136 124.193.127.94 180.140.190.54
187.60.224.2 192.80.188.204 203.199.32.242 58.240.163.98 61.183.129.254 62.33.136.220 66.155.5.4 182.18.21.11 180.150.249.19 220.123.31.85 188.254.155.134 115.28.39.63 116.55.226.206 117.3.173.146 118.70.197.53
119.57.35.253 174.136.39.54 176.28.30.128 177.135.246.81 198.27.85.95 208.53.157.171 216.176.33.88 218.108.17.25 50.197.19.99 58.108.193.88 64.16.185.50 87.106.39.171 87.106.7.23 94.143.52.151 98.158.148.210
116.55.226.206 117.3.173.146 118.70.197.53 119.57.35.253 174.136.39.54 176.28.30.128 177.135.246.81 198.27.85.95 208.53.157.171 216.176.33.88 218.108.17.25 50.197.19.99 58.108.193.88 64.16.185.50 87.106.39.171
87.106.7.23 94.143.52.151 98.158.148.210 200.52.73.150 103.31.242.13 109.238.179.82 110.84.239.135 113.92.45.206 121.127.226.104 121.15.226.210 121.199.53.254 121.9.150.156 122.113.39.199 189.164.106.132
189.187.127.15 189.203.101.217 192.69.219.228 201.229.251.178 211.138.108.115 212.77.221.180 217.45.134.65 218.23.4.77 5.135.204.25 61.189.48.158 61.191.114.33 62.63.152.10 77.240.95.35 78.167.111.6 79.116.138.192
85.33.208.212 96.56.83.156 98.102.118.18 115.28.35.225 115.28.42.65 122.143.10.14 122.224.142.114 134.91.218.180 14.119.93.219 157.56.163.195 174.129.201.182 177.3.250.74 188.130.40.6 198.23.64.182 201.217.215.66
218.29.188.230 222.240.176.131 59.48.44.154 78.189.222.27 85.214.148.126 91.183.59.228 110.76.47.89 113.118.190.96 123.30.211.166 173.203.49.42 183.14.54.110 183.15.56.22 183.203.34.203 183.49.82.49 203.158.166.3
213.126.23.106 218.23.178.250 220.167.52.144 112.170.76.67 189.111.145.183 217.91.172.52 81.26.89.239 178.77.69.108 186.215.126.236 187.115.149.90 203.117.199.117 203.29.67.133 218.89.201.169 41.160.177.114
54.250.152.198 60.190.190.8 67.50.227.26 72.167.49.159 113.242.114.227



Ataque cuyo objetivo es saturar los recursos de un sistema, produciendo indisponibilidad de los usuários.

Fuente: Receita Fazenda, Sistema y Administración Tributaria de Brasil

Escenario

Herramientas para ataques DDoS

Name	Type
Itsoknoproblembro	TCP Flood
	UDP Flood
	HTTP Get Flood
	HTTP Post Flood
Kamikaze	HTTP Get Flood
Amos	HTTP Post Flood

Revisión de Estadísticas

cert.br 15 ANOS
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013

Tabela: Totais Mensais e Trimestral Classificados por Tipo de Ataque.

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**36067**	2217	6	15	0	2149	5	1305	3	18954	52	6247	17	5180	14
fev	**26471**	1523	5	6	0	1206	4	1364	5	12664	47	5573	21	4135	15
mar	**28090**	1771	6	6	0	1686	6	1113	3	13913	49	5259	18	4342	15
abr	**29943**	2084	6	14	0	1511	5	1479	4	13465	44	6615	22	4775	15
mai	**23409**	1638	7	6	0	972	4	1349	5	10378	44	5338	22	3728	15
jun	**29713**	2580	8	15	0	592	1	2177	7	15664	52	5061	17	3624	12
jul	**30874**	2932	9	123	0	509	1	1710	5	13769	44	7530	24	4301	13
ago	**28531**	2090	7	24	0	542	1	1942	6	12336	43	8145	28	3452	12
set	**31482**	2365	7	86	0	419	1	1573	5	15911	50	8538	27	2590	8
out	**28842**	2847	9	34	0	741	2	1066	3	13231	45	8239	28	2684	9
nov	**30213**	2843	9	28	0	363	1	2247	7	13263	43	8876	29	2593	8
dez	**29290**	3089	10	673	2	517	1	1396	4	11848	40	10254	35	1513	5
Total	**352925**	27979	7	1030	0	11207	3	18721	5	165396	46	85675	24	42917	12

Fuente: CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira
http://www.cert.br/stats/incidentes/2013-jan-mar/total.html

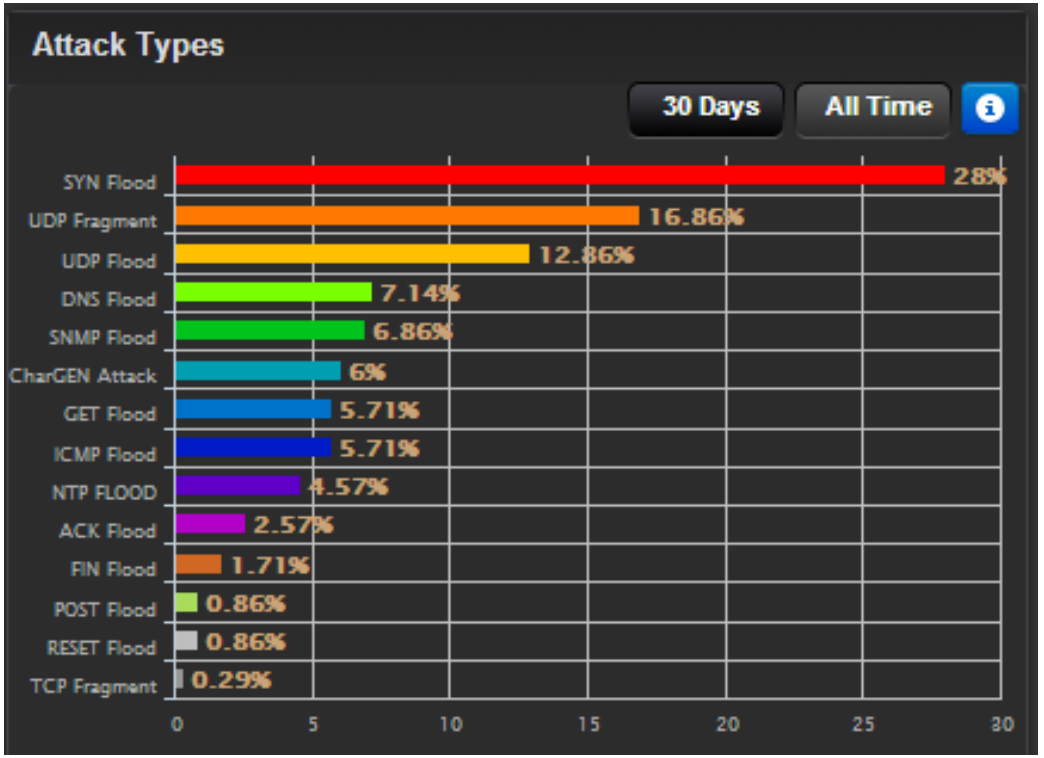
SOURCES (PAST 24 HOURS)

BY COUNTRY

COUNTRY	ATTACKS	PERCENTAGE
US (United States)	474	13.1%
CN (China)	186	5.1%
DE (Germany)	142	3.9%
BR (Brazil)	104	2.9%
GB (Great Britain)	69	1.9%
RU (Russian Federation)	54	1.5%

ATTACK SUBCLASS	NUMBER OF ATTACKS	PERCENTAGE
UDP	731	28.1%
Total Traffic	699	26.9%
DNS	564	21.7%
IP Fragment	222	8.5%
TCP SYN	185	7.1%

Fuente:https://atlas.arbor.net/summary/dos#summary



Fuente: http://www.prolexic.com/plxpatrol/index.html

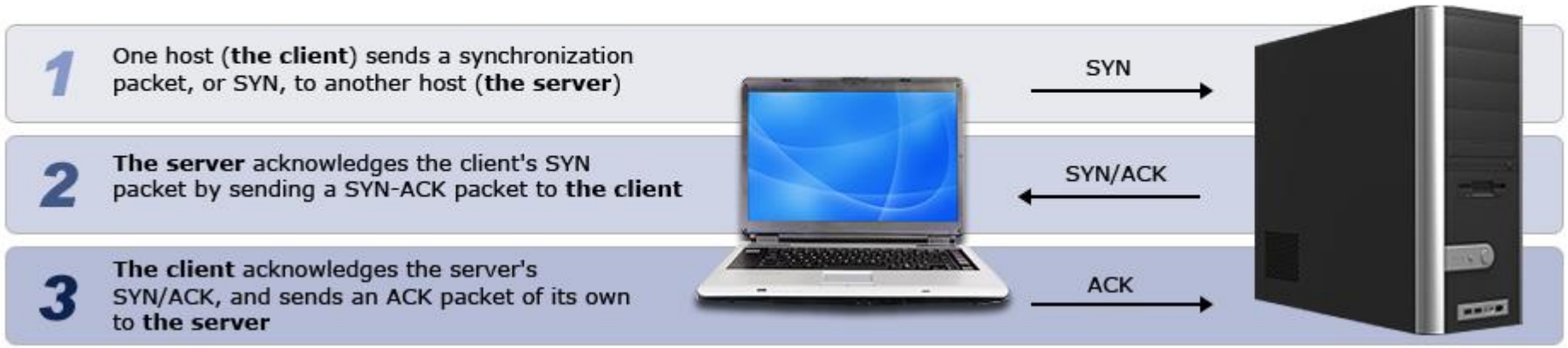
TARGETS (PAST 24 HOURS)

BY COUNTRY

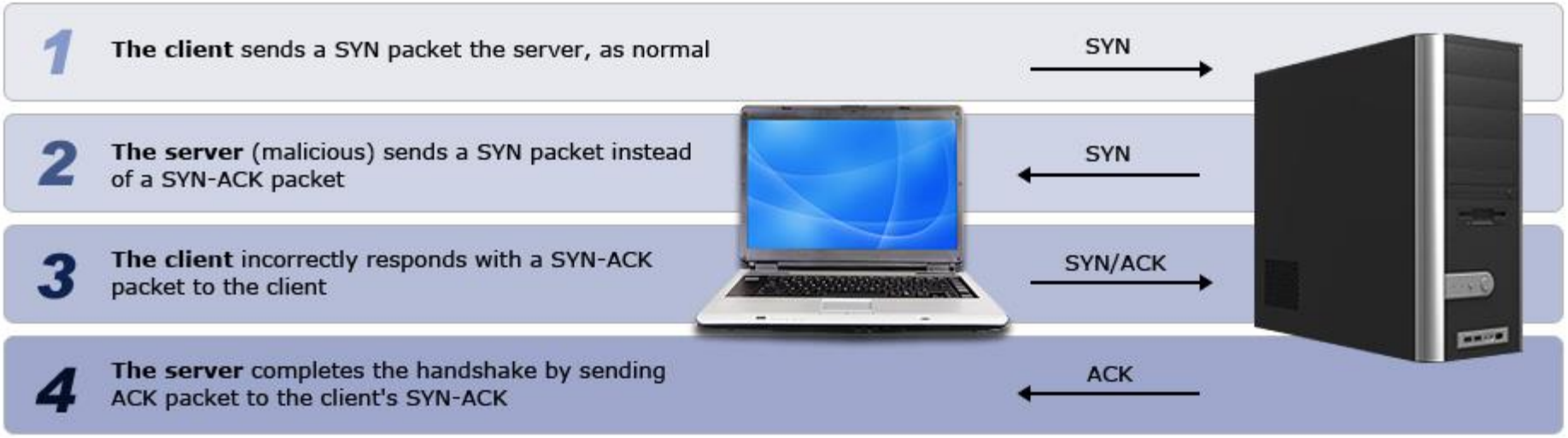
COUNTRY	ATTACKS	PERCENTAGE
US (United States)	1285	26.5%
CN (China)	425	8.8%
PE (Peru)	195	4.0%
SE (Sweden)	133	2.7%

What is a TCP Handshake?

The **Transport Control Protocol (TCP)** controls most Internet connections between computers and data traffic between them. All TCP connections begin with a 3-step **"TCP handshake"**:



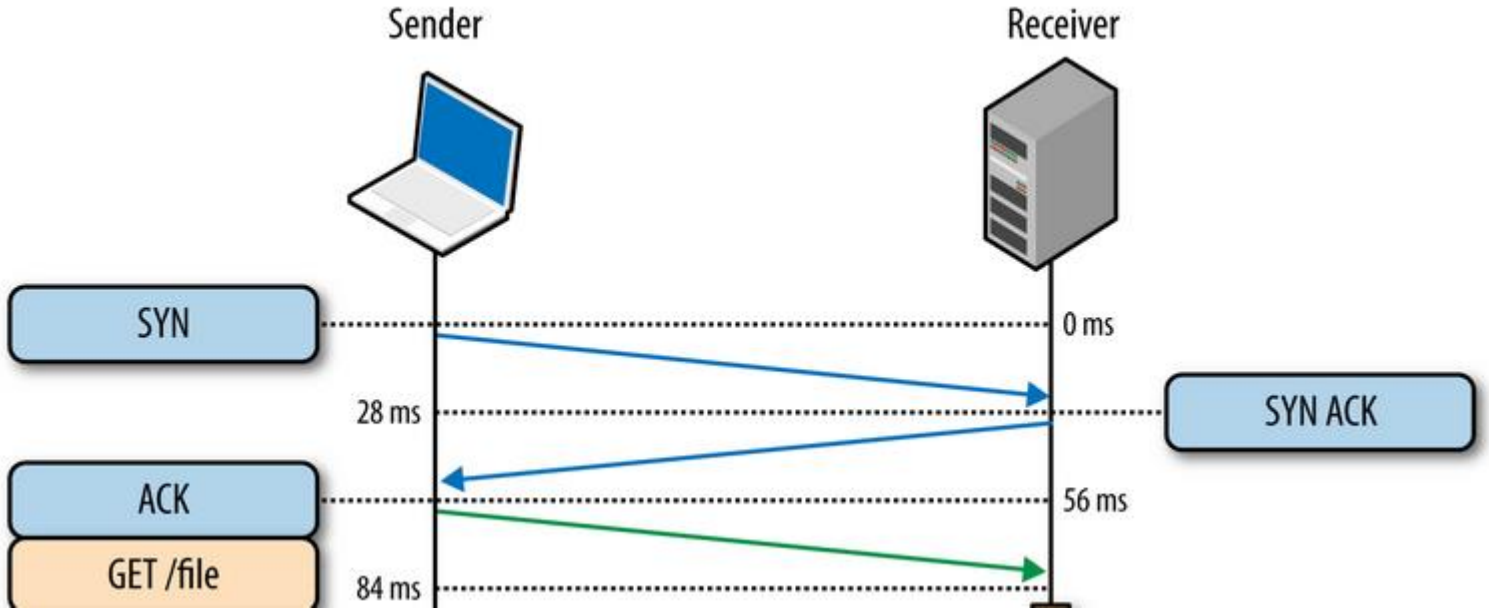
A **TCP Split Handshake** causes inconsistent behavior by reversing the connection direction flow by the end of handshake as follows:



TCP:

What is a TCP Handshake?

The **Transport Control Protocol (TCP)** controls most Internet connections between computers and data traffic between them. All TCP connections begin with a 3-step **"TCP handshake"**:

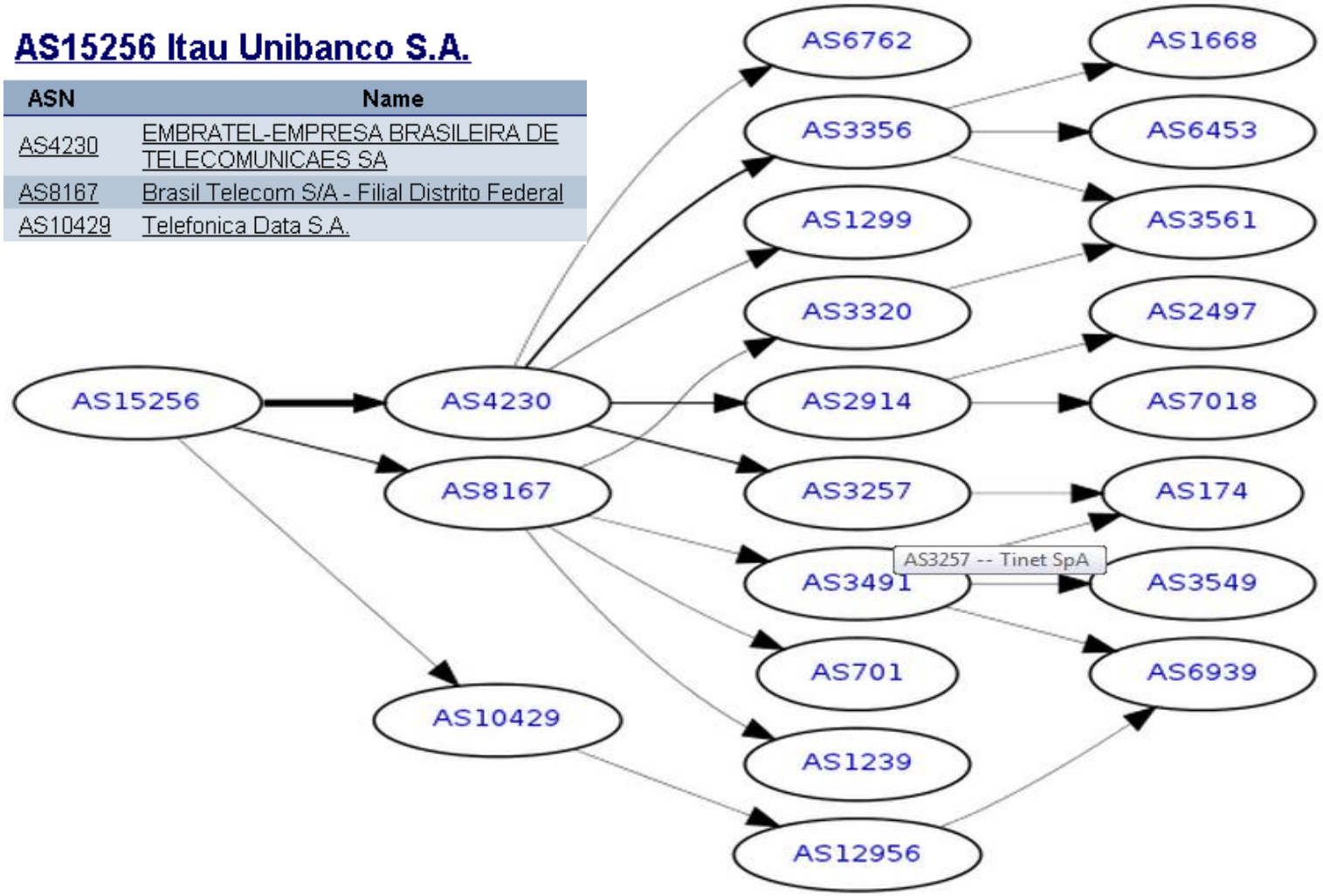


¿ Cómo salgo a Internet?

AS15256 IPv4 Route Propagation

AS15256 Itau Unibanco S.A.

ASN	Name
AS4230	EMBRATEL-EMPRESA BRASILEIRA DE TELECOMUNICAES SA
AS8167	Brasil Telecom S/A - Filial Distrito Federal
AS10429	Telefonica Data S.A.

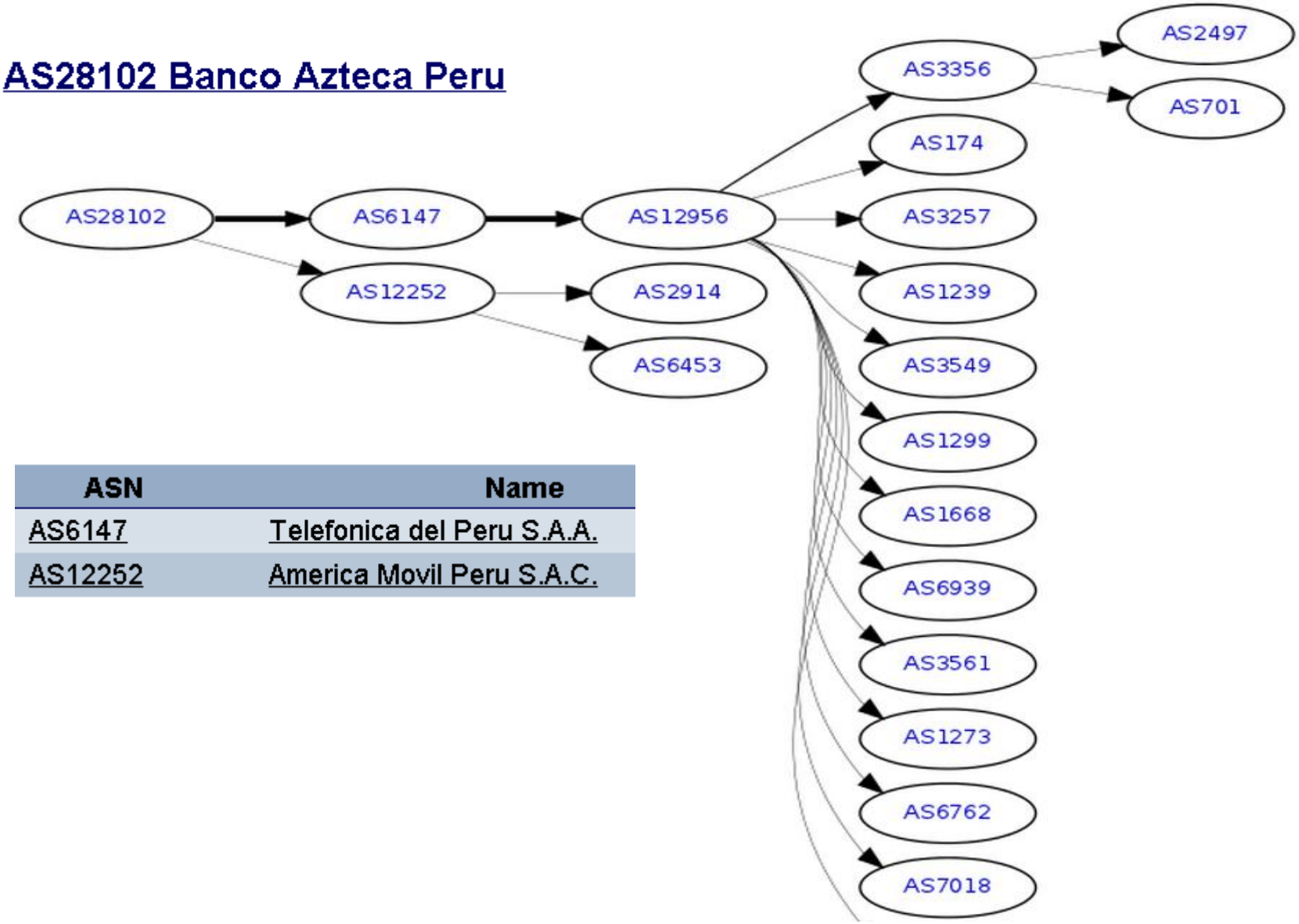


Fuente:http://bgp.he.net/AS15256#_graph4

¿ Cómo salgo a Internet?

AS28102 IPv4 Route Propagation

AS28102 Banco Azteca Peru



ASN	Name
AS6147	Telefonica del Peru S.A.A.
AS12252	America Movil Peru S.A.C.

Fuente:http://bgp.he.net/AS28102#_asinfo

¿ Cómo se crea una botnet?

Ejemplos de una botnet

Date created	Date dismantled	Name	Estimated no. of bots	Spam capacity	Aliases
2009 (May)	2010-Oct (partial)	BredoLab	30,000,000[13]	3.6 billion/day	Oficla
2008 (around)	2009-Dec	Mariposa	12,000,000[14]	?	
2008 (November)		Conficker	10,500,000+[15]	10 billion/day	DownUp, DownAndUp, DownAdUp, Kido
2010 (around)		TDL4	4,500,000[16]	?	TDSS, Alureon
?		Zeus	3,600,000 (US only)[17]	n/a	Zbot, PRG, Wsnpoem, Gorhax, Kneber
2007 (Around)		Cutwail	1,500,000[18]	74 billion/day	Pandex, Mutant (related to: Wigon, Pushdo)
2008 (Around)		Sality	1,000,000[19]	?	Sector, Kuku
2009 (Around)	2012-07-19	Grum	560,000[20]	39.9 billion/day	Tedroo
?		Mega-D	509,000[21]	10 billion/day	Ozdok
?		Kraken	495,000[22]	9 billion/day	Kracken
2007 (March)	2008 (November)	Srizbi	450,000[23]	60 billion/day	Cbeplay, Exchanger
?		Lethic	260,000[24]	2 billion/day	none
2004 (Early)		Bagle	230,000[24]	5.7 billion/day	Beagle, Mitglieder, Lodeight
?		Bobax	185,000[24]	9 billion/day	Bobic, Oderoor, Cotmonger, Hacktool.Spammer, Kraken
?		Torpig	180,000[25]	n/a	Sinowal, Anserin
?		Storm	160,000[26]	3 billion/day	Nuwar, Peacomm, Zhelatin
2006 (Around)	2011 (March)	Rustock	150,000[27]	30 billion/day	RKRustok, Costrat

Fuente: http://www.enigmasoftware.com/top-10-botnet-threats-in-the-united-states/
Top 10 Botnet Threats in the United States,
http://user-agent-string.info/list-of-ua/bots

Top ten ZeuS hosting ISPs (by number of ZeuS C&Cs)

ZeuS C&C count	AS number	AS name
21	47583	HOSTING-MEDIA Aurimas Rapalis tradi
19	51852	PLI-AS Private Layer INC
15	36351	SOFTLAYER - SoftLayer Technologies
12	198310	PALLADA-AS Pallada Web Service LLC
10	24940	HETZNER-AS Hetzner Online AG RZ
9	7162	Itanet - Itamarati On-Line Ltda.
9	16276	OVH OVH
9	32475	SINGLEHOP-INC - SingleHop
9	40676	PSYCHZ - Psychz Networks
8	6301	HP-CLOUD-SERVICES - Hewlett-Packard

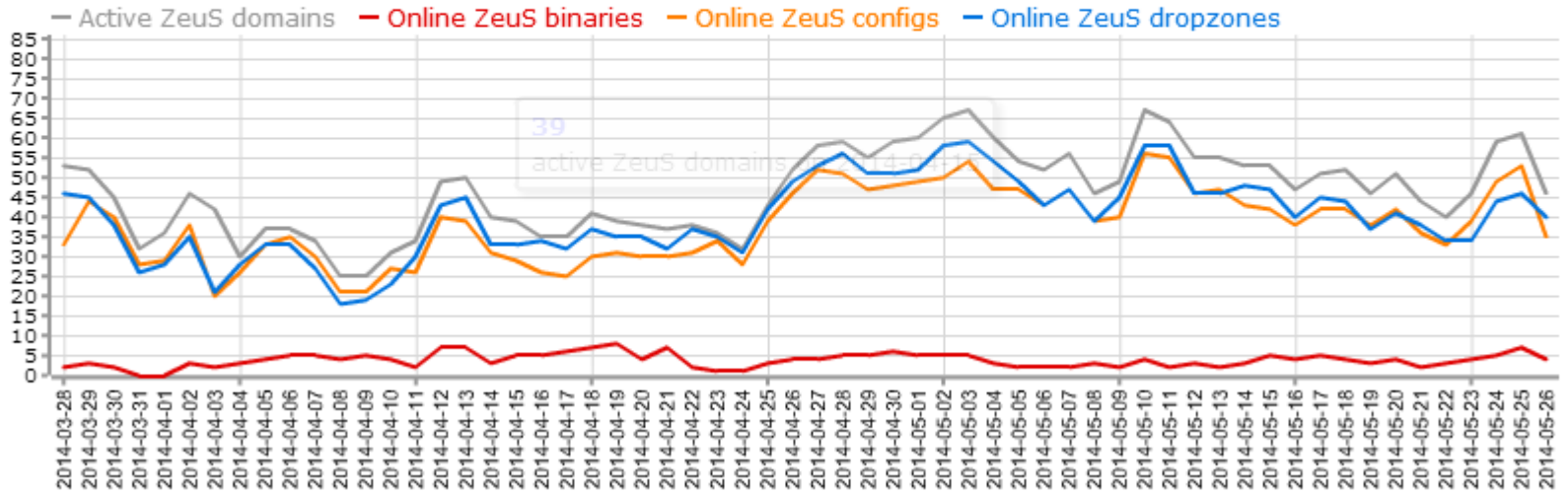
Top ten ZeuS hosting countries (by ZeuS hosts)

ZeuS C&C count	country
201	United States (US)
56	Russian Federation (RU)
30	Netherlands (NL)
30	Turkey (TR)
30	Germany (DE)
22	United Kingdom (GB)
21	Brazil (BR)
20	Ukraine (UA)
18	Canada (CA)
17	Switzerland (CH)

ZeuS Tracker :: Statistic

Here are some statistics about the ZeuS crimeware. Note: You need th

# of active ZeuS files (last 60 days)



Fuente: https://zeustracker.abuse.ch/statistic.php

Índice:

• DDoS Service

- Foros: shopworld.biz
- Precio: $150 -$1000

CONTACTOS:
Número de ICQ 803077 (Online)
JABBER legal.d @ jabber.ru

Attackers enter the targets within the grey box, sets the threads and timeout. A difference between Pandora and Dirt Jumper is that there is no "Stop" button. Attackers must stop attacks by setting the threads to 0.

Fuente: David Barroso T. Digital (España), http://www.lostinsecurity.com/, https://twitter.com/lostinsecurity
Fuente: http://shopworld.biz/showthread.php?t=1908

Índice:

III. Acontecimientos en Brasil:

Histórico, ataques DDoS 2012:

#OPWeeksPayment

06/01 — 10/01 — 19/01 — 25/01 — 29/01 — 04/02 — 15/02

Interrupción de sites Gobierno

Cierra/MegaUpload USA

30/01 Itaú

31/01 Bradesco

01/02 Banco de Brasil

02/02 HSBC

03/02 Citibank, Panamericano, BMG, Febraban, Cielo, Redecard

Interrupción de los sites: TAM y GOL

En Junio, durante #OPRio+20, Anonymous ataco diversos sites:

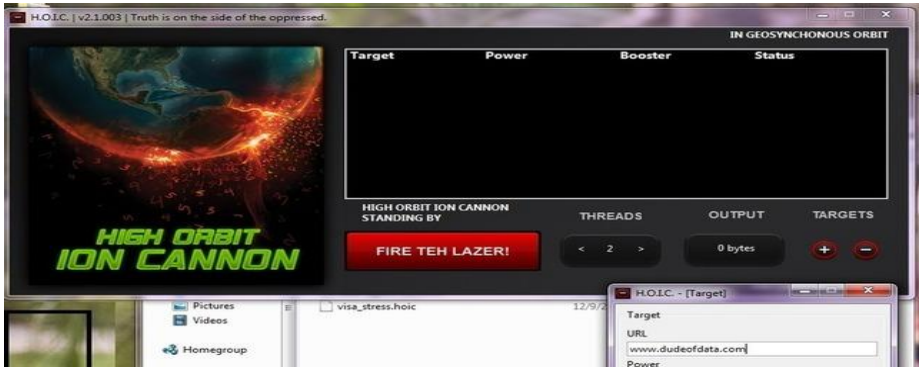
- **ONU.br,**
- **Camara de Diputados,**
- **Senado Federal.**

Escenario

Herramientas para ataques DDoS

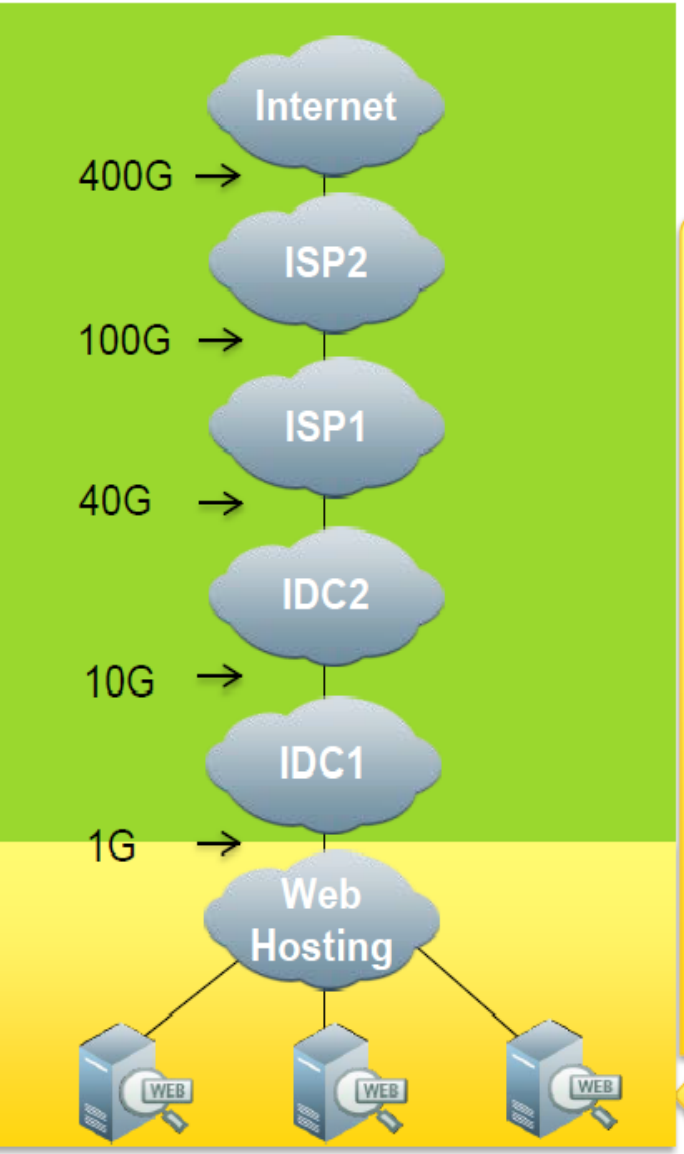
- Existen muchas herramientas específicas para lanzar ataques DDoS.
  - Packet flooding tools
  - Specialized application ddos tools
  - DDos specialized botnets
  - **DDoS comercial services**

- Ataques “**multi-vector**”:
  - Ataque volumétrico + ataque de aplicación



Índice:

Web Attack Mitigation



On the other hand, Web attack, e.g. SQL Injection, is not large in volume, but its payload goes up to data level. Data Center usually provides Web attack mitigation as a dedicated service to Web Hosting customer.

1. Network Access Control	2. TCP Flood Protection	3. HTTP Termination
6. HTTP Flood Protection	5. Data Normalization	4. SSL Decryption
7. HTTP Validation	8. HTTP Access Control	9. Web Server and Plug-in Protection

12. Customized Protection Mechanism

- White List
- Smart Patch
- Custom Security
- Exception Policy

11. Behavior-Based Protection

- Illegal File Upload
- Illegal Download
- Information Disclosure
- Leech
- CSRF
- Scanning
- Cookie Hijacking

10. Rule-Based Protection

- Crawler
- XSS
- SQL Injection
- LDAP Injection
- SSI Command Injection
- XPath Injection
- Command Line Injection
- Path Traverse
- Remote File Inclusion

Fuente: RSA Conference ASIA Pacifico 2013 – Congyu Li NS Focus,
http://www.rsaconference.com/writable/presentations/file_upload/das-t01_final_copy1.pdf

Fin

cesar.farro@gmail.com
@cesarfarro
Lima, Perú Mayo 2014

SOCIETE GENERALE CERT SOCIETE GENERALE

Incident Response Methodology

Public Safety Canada Sécurité publique Canada

Canada

IRM #4

DDoS incident response

Guidelines to handle Distributed Denial of Service incidents

IRM Author: CERT SG / Vincent Ferran-Lacome
IRM version: 1.3

E-Mail: cert.sg@socgen.com
Web: http://cert.societegenerale.com
Twitter: @CertSG

1.-Preparación

Establecer los sistemas críticos, contactos, definir procedimientos.
ISP, Inventario, Red.

2.-Identificación

Detecta el Incidente, determina el objetivo y comunica las partes involucradas.

3.- Contención

Mitiga los efectos del ataque en el sistema afectado.

4.- Remediación

Tomar acciones para parar el ataque DDoS.

5.- Retornar

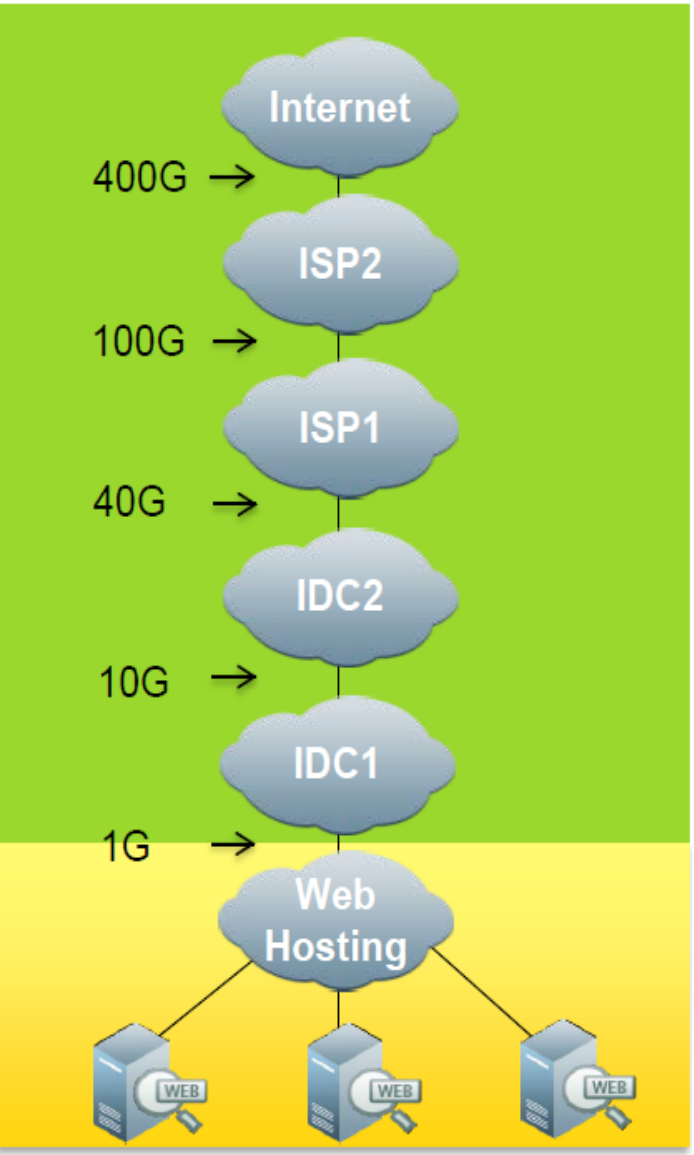
Retorna al estado original.

6.- Documentar

Documentación y reajusta el nuevo procedimiento de respuesta.

Fuente: http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

DDoS Attack Mitigation



1. IP address Verification
- Source/destination IP address check/verification

2. Access Control List
- Layer 4 ACL
- Conn-Exhaustion ACL
- URL ACL

3. Reputation List
- White/Black List
- Dynamic Prioritizing

4. Protocol Analysis
- Protocol Validation by RFC check

5. Layer 4 Flood Mitigation
- Source/destination IP address check/verification
- Various mitigation algorithms

6. Layer 7 Flood Mitigation
- Various mitigation algorithms
- Pattern Matching

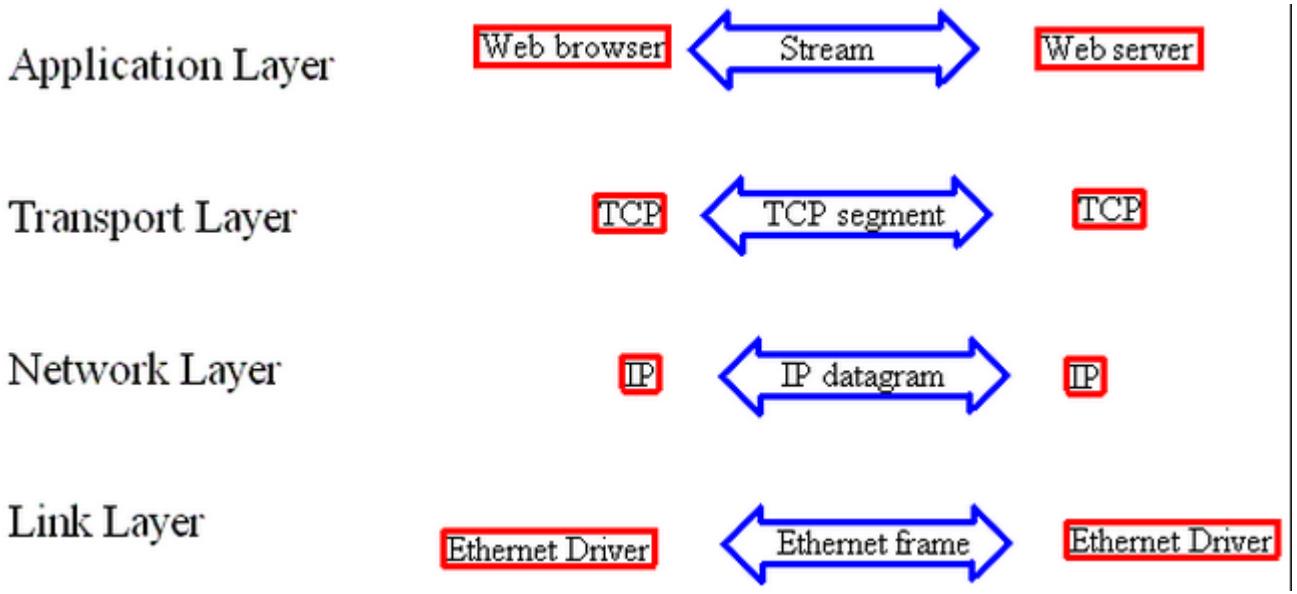
7: Rate Limit
- Restricts traffic and ensures the critical business.

It has been consensus in Data Center industry that the best place to stop DDoS attack, e.g. SYN flood, is in backbone network, since the attack traffic volume can be large, e.g. 10Gbps. Data Center usually provides DDoS attack mitigation as a part of its infrastructure service.

Fuente: RSA Conference ASIA Pacifico 2013 – Congyu Li NS Focus,
http://www.rsaconference.com/writable/presentations/file_upload/das-t01_final_copy1.pdf

I. Introducción de Conceptos

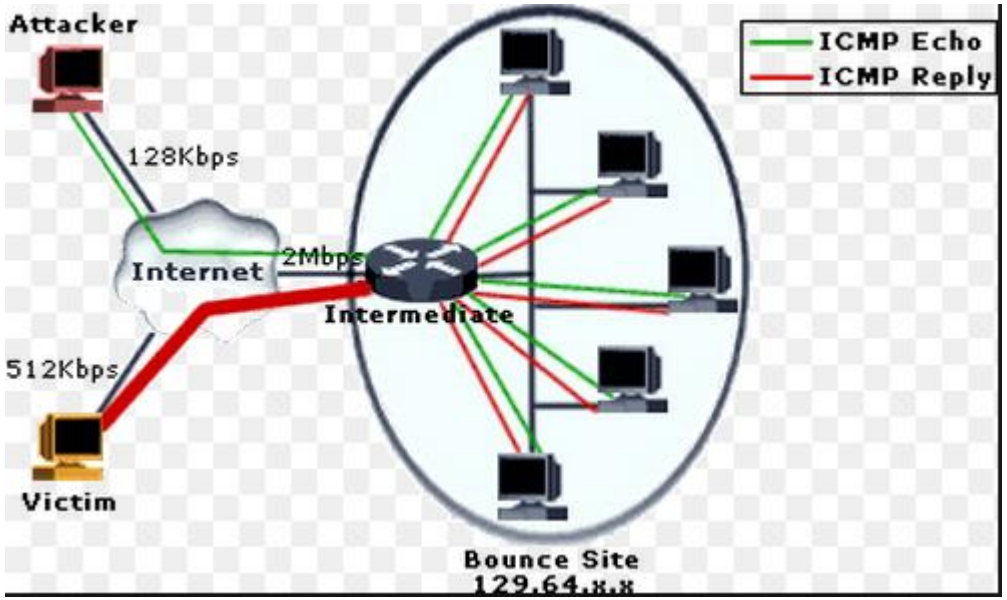
- ¿ Cuales son los tipos de ataques DDoS?
  1. Volumétrico: Saturar el Ancho de Banda de la Victima.
  2. Protocolo: Saturar el servidor, consuma recursos .
  3. Aplicación: Ej: Envía multiples Http-request a la victima para intentar bajar el servidor Web, afectandose IIS/Apache.

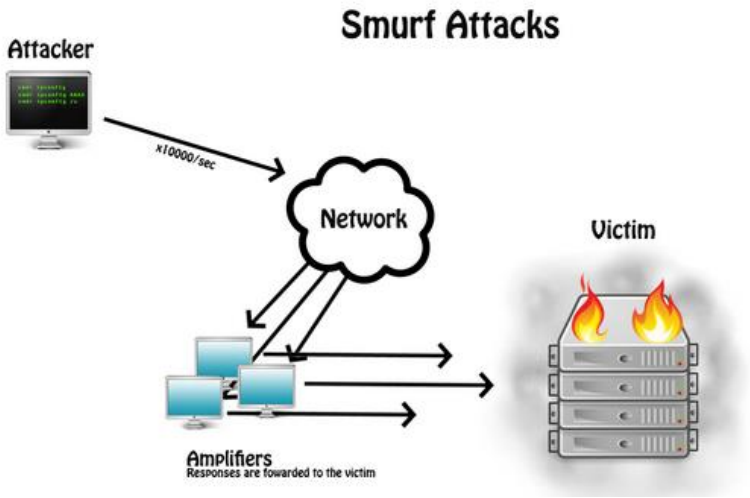


Fuente: http://blog.infranetworking.com/los-ataques-ddos/

I. Introducción de Conceptos

- Smurf Attack:
  - Utilizar mensajes ICMP echo request to the brodcast, con Spoofing para inundar (flood) un objetivo.

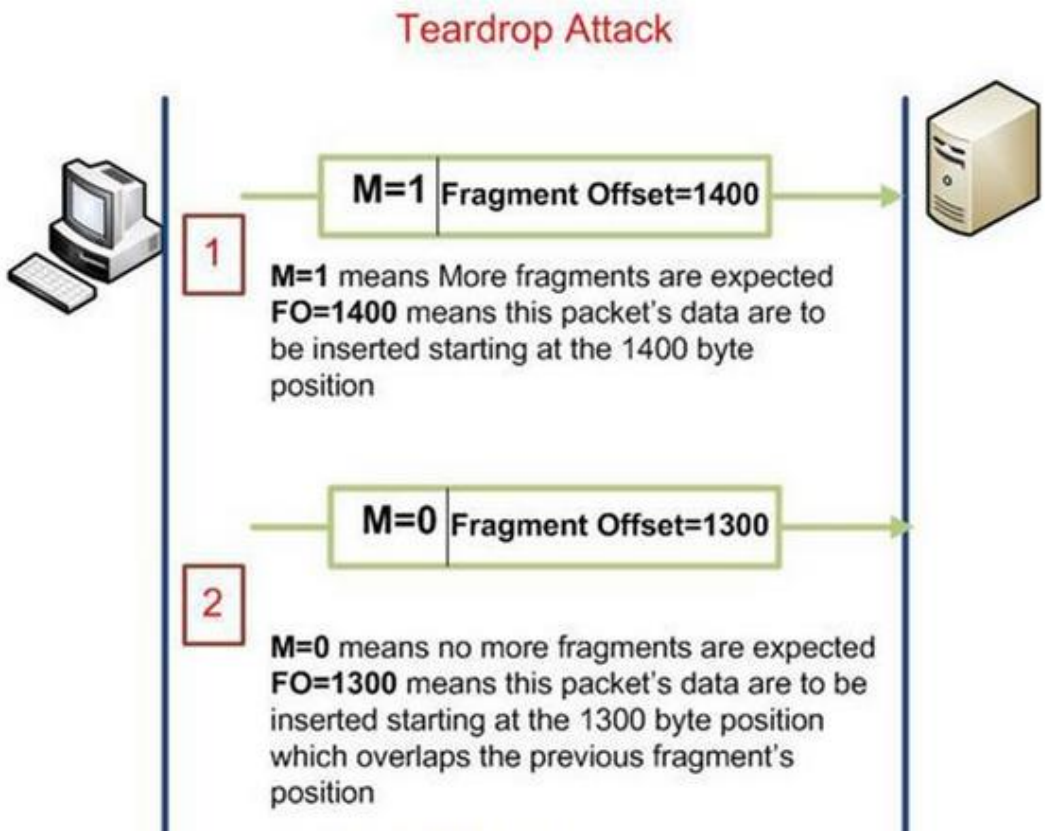




Fuente: http://es.wikipedia.org/wiki/Ataque_smurf

I. Introducción de Conceptos

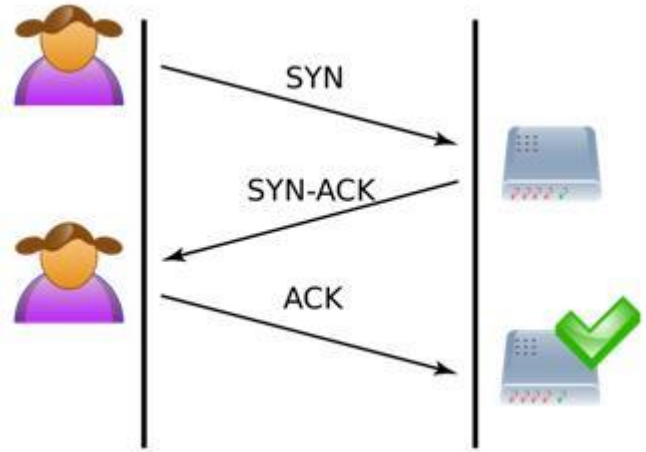
- Teardrop
  - El ataque consistía en enviar dos tramas IP fragmentadas a ensamblar en el destino, en el cual en el segundo fragmento enviado se establece un valor en el campo de desplazamiento del fragmento que cae dentro del bloque anterior.

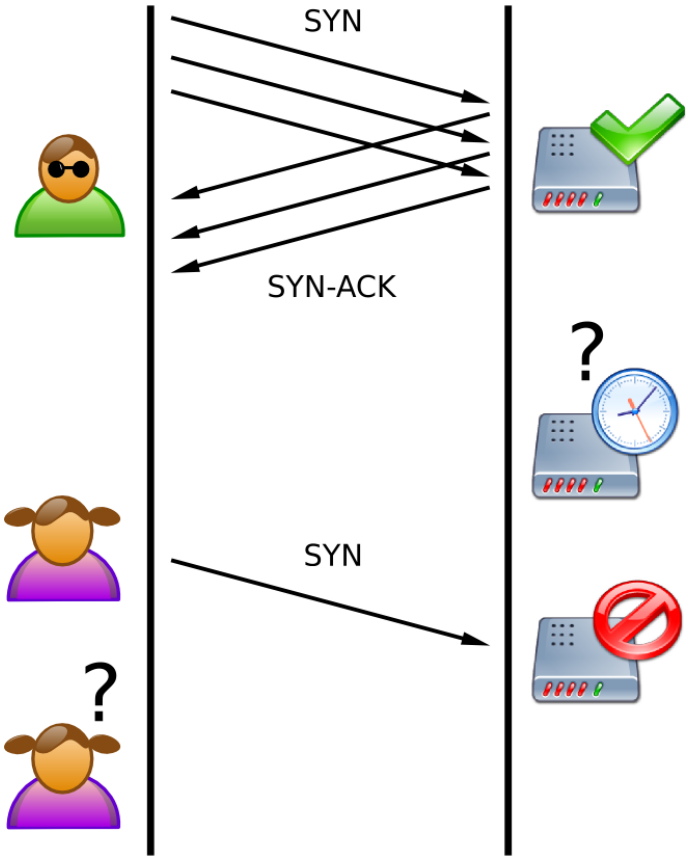


Fuente: http://www.ac.usc.es/docencia/ASRII/Tema_3html/node16.html

I. Introducción de Conceptos

- SYN Flood:
  - La inundación SYN envía un flujo de paquetes TCP/SYN (varias peticiones con Flags SYN en la cabecera), muchas veces con la dirección de origen falsificada. Esperando el paquete de respuesta TCP/ACK (Parte del proceso de establecimiento de conexión TCP de 3 vías).





Fuente: Unicorn College, DDoS Milan Petrasek
Fuente: http://www.ac.usc.es/docencia/ASRII/Tema_3html/node16.html