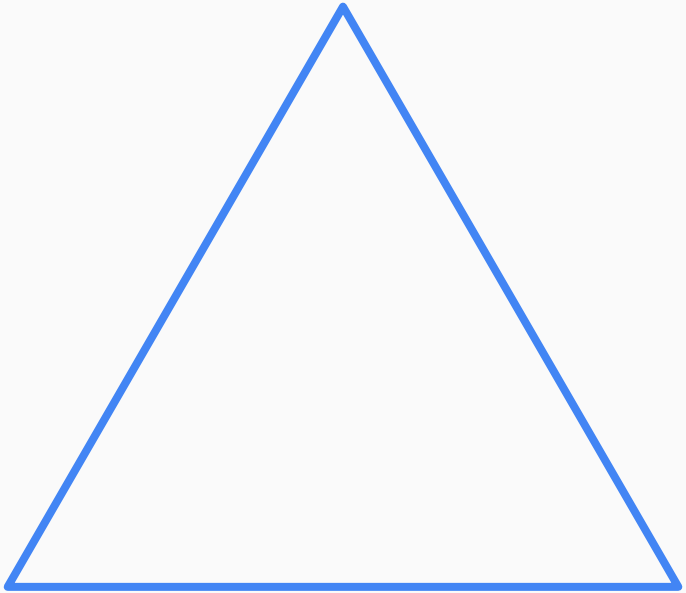
Drawing the Foul

Operation of a DDoS Honeypot

Damian Menscher, Google

Confidentiality



Integrity

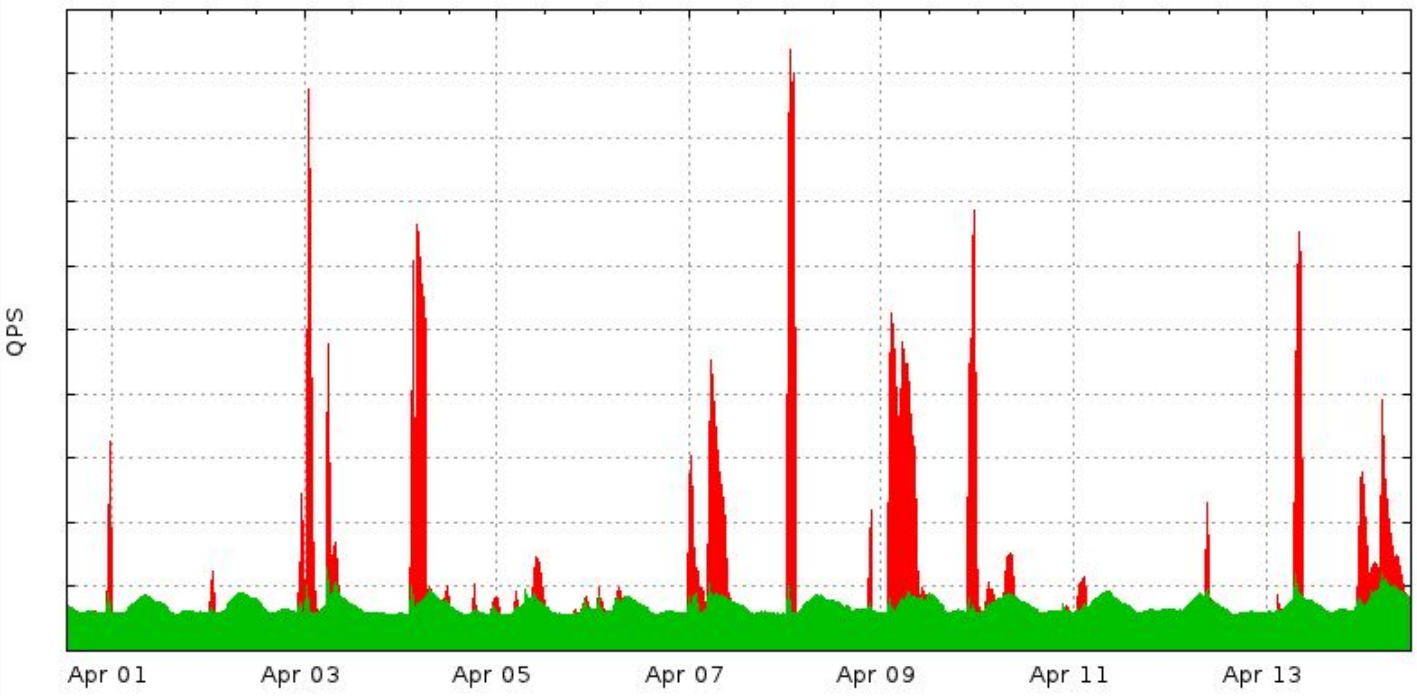
Availability

Information Security Triad

Where's the love?



Site Reliability Engineers

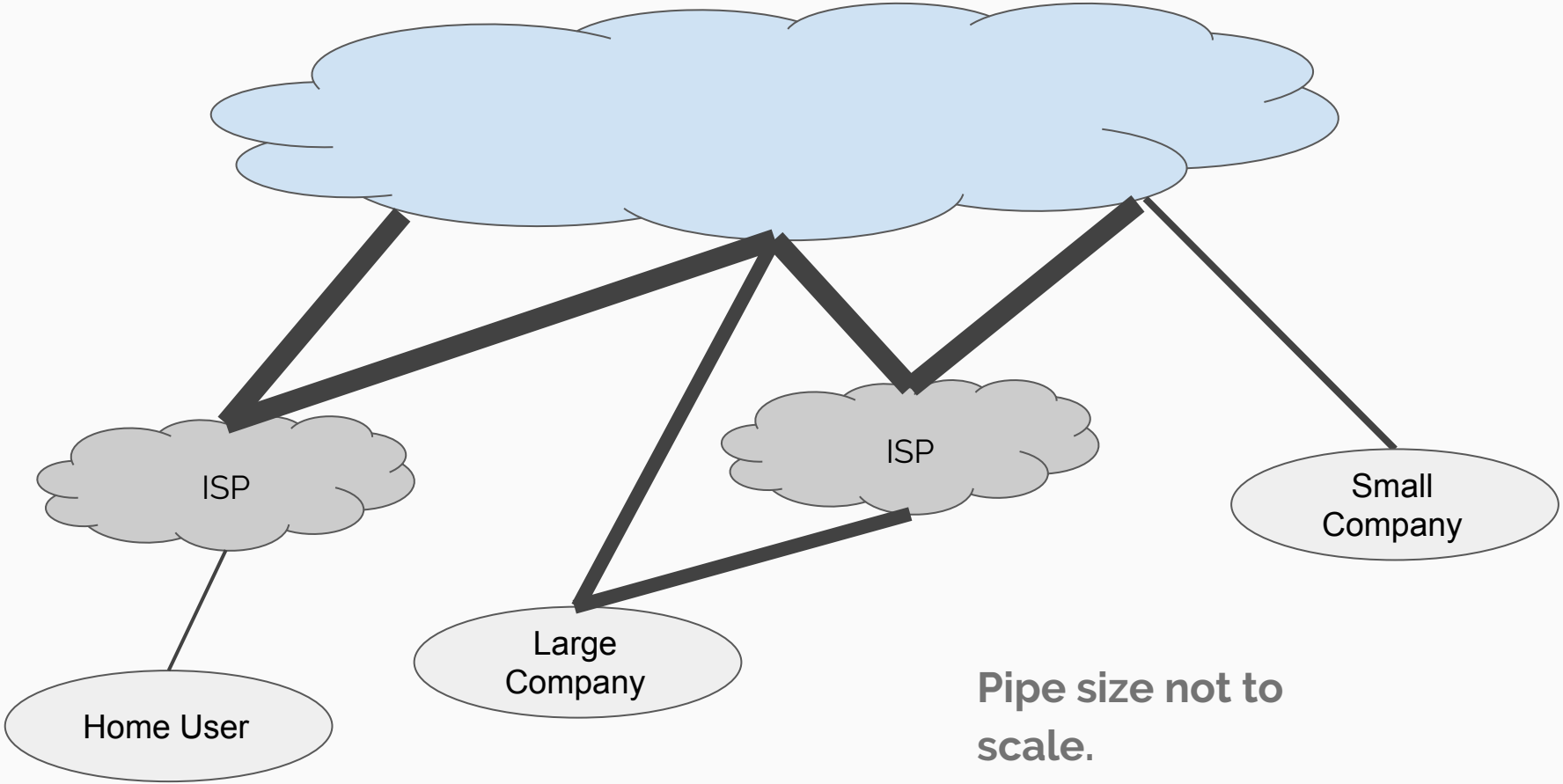


Look! Graphs!

Look! Spikes!

Considerations

Saturate Links - Gbps



Overwhelm Routers: Mpps

```
05:47:26.545075 IP bot.ip.117.169.30974 > victim.53: Flags [S], seq 4216826094, win 0, options [mss 1403,sackOK,TS val 4077582479 ecr 0,nop,wscale 6], length 0
05:47:26.545075 IP bot.ip.50.172.57359 > victim.53: Flags [S], seq 2977898070, win 0, options [mss 1402,sackOK,TS val 4064444216 ecr 0,nop,wscale 6], length 0
05:47:26.545076 IP bot.ip.239.42.7585 > victim.53: Flags [S], seq 856292681, win 0, options [mss 1413,sackOK,TS val 2939637319 ecr 0,nop,wscale 6], length 0
05:47:26.545103 IP bot.ip.47.65.48129 > victim.53: Flags [S], seq 1042074479, win 0, options [mss 1413,sackOK,TS val 288877622 ecr 0,nop,wscale 6], length 0
05:47:26.545104 IP bot.ip.108.229.64199 > victim.53: Flags [S], seq 4068648250, win 0, options [mss 1411,sackOK,TS val 2281532953 ecr 0,nop,wscale 6], length 0
05:47:26.545104 IP bot.ip.206.12.11462 > victim.53: Flags [S], seq 339821198, win 0, options [mss 1410,sackOK,TS val 2895301571 ecr 0,nop,wscale 6], length 0
05:47:26.545105 IP bot.ip.100.134.28043 > victim.53: Flags [S], seq 3626573737, win 0, options [mss 1400,sackOK,TS val 1751093807 ecr 0,nop,wscale 6], length 0
05:47:26.545105 IP bot.ip.206.150.26160 > victim.53: Flags [S], seq 3404229375, win 0, options [mss 1414,sackOK,TS val 1511549060 ecr 0,nop,wscale 6], length 0
05:47:26.545106 IP bot.ip.157.190.44558 > victim.53: Flags [S], seq 1069343643, win 0, options [mss 1404,sackOK,TS val 792848825 ecr 0,nop,wscale 6], length 0
05:47:26.545106 IP bot.ip.66.63.34848 > victim.53: Flags [S], seq 2026406947, win 0, options [mss 1413,sackOK,TS val 1711030813 ecr 0,nop,wscale 6], length 0
05:47:26.545106 IP bot.ip.14.207.36802 > victim.53: Flags [S], seq 988690396, win 0, options [mss 1412,sackOK,TS val 162558170 ecr 0,nop,wscale 6], length 0
05:47:26.545107 IP bot.ip.47.65.22819 > victim.53: Flags [S], seq 2016377686, win 0, options [mss 1413,sackOK,TS val 288877622 ecr 0,nop,wscale 6], length 0
05:47:26.545108 IP bot.ip.76.208.25730 > victim.53: Flags [S], seq 1138759984, win 0, options [mss 1400,sackOK,TS val 1730861437 ecr 0,nop,wscale 6], length 0
05:47:26.545108 IP bot.ip.166.158.1226 > victim.53: Flags [S], seq 2728234819, win 0, options [mss 1409,sackOK,TS val 3366055157 ecr 0,nop,wscale 6], length 0
05:47:26.545109 IP bot.ip.163.255.4269 > victim.53: Flags [S], seq 4197704920, win 0, options [mss 1408,sackOK,TS val 2324195277 ecr 0,nop,wscale 6], length 0
05:47:26.545109 IP bot.ip.116.14.56887 > victim.53: Flags [S], seq 1069188328, win 0, options [mss 1404,sackOK,TS val 1773000954 ecr 0,nop,wscale 6], length 0
05:47:26.545110 IP bot.ip.83.192.27229 > victim.53: Flags [S], seq 381313653, win 0, options [mss 1409,sackOK,TS val 3896409249 ecr 0,nop,wscale 6], length 0
05:47:26.545110 IP bot.ip.187.203.11563 > victim.53: Flags [S], seq 696618361, win 0, options [mss 1412,sackOK,TS val 327368824 ecr 0,nop,wscale 6], length 0
05:47:26.545111 IP bot.ip.105.234.9058 > victim.53: Flags [S], seq 3171504314, win 0, options [mss 1411,sackOK,TS val 3724302273 ecr 0,nop,wscale 6], length 0
05:47:26.545111 IP bot.ip.108.229.53950 > victim.53: Flags [S], seq 3844211368, win 0, options [mss 1411,sackOK,TS val 2281532953 ecr 0,nop,wscale 6], length 0
05:47:26.545112 IP bot.ip.206.12.42721 > victim.53: Flags [S], seq 4217520655, win 0, options [mss 1410,sackOK,TS val 2895301571 ecr 0,nop,wscale 6], length 0
05:47:26.545112 IP bot.ip.145.164.3136 > victim.53: Flags [S], seq 2871563388, win 0, options [mss 1400,sackOK,TS val 2747220493 ecr 0,nop,wscale 6], length 0
05:47:26.545113 IP bot.ip.145.164.30748 > victim.53: Flags [S], seq 802009603, win 0, options [mss 1400,sackOK,TS val 2747220493 ecr 0,nop,wscale 6], length 0
05:47:26.545113 IP bot.ip.112.8.30971 > victim.53: Flags [S], seq 1249343228, win 0, options [mss 1407,sackOK,TS val 4187963713 ecr 0,nop,wscale 6], length 0
05:47:26.545114 IP bot.ip.177.209.39313 > victim.53: Flags [S], seq 2085003906, win 0, options [mss 1402,sackOK,TS val 546225852 ecr 0,nop,wscale 6], length 0
05:47:26.545115 IP bot.ip.233.170.20947 > victim.53: Flags [S], seq 2905223702, win 0, options [mss 1411,sackOK,TS val 2399533981 ecr 0,nop,wscale 6], length 0
05:47:26.545115 IP bot.ip.47.86.37697 > victim.53: Flags [S], seq 2620063750, win 0, options [mss 1411,sackOK,TS val 1033949236 ecr 0,nop,wscale 6], length 0
05:47:26.545115 IP bot.ip.0.167.47639 > victim.53: Flags [S], seq 2302138845, win 0, options [mss 1402,sackOK,TS val 3171135266 ecr 0,nop,wscale 6], length 0
05:47:26.545116 IP bot.ip.177.209.36016 > victim.53: Flags [S], seq 1907967281, win 0, options [mss 1402,sackOK,TS val 546225852 ecr 0,nop,wscale 6], length 0
05:47:26.545117 IP bot.ip.190.17.9552 > victim.53: Flags [S], seq 2928268719, win 0, options [mss 1412,sackOK,TS val 1716994567 ecr 0,nop,wscale 6], length 0
05:47:26.545117 IP bot.ip.16.156.26698 > victim.53: Flags [S], seq 618175648, win 0, options [mss 1403,sackOK,TS val 2341433627 ecr 0,nop,wscale 6], length 0
05:47:26.545118 IP bot.ip.169.214.39398 > victim.53: Flags [S], seq 117628387, win 0, options [mss 1401,sackOK,TS val 1333774479 ecr 0,nop,wscale 6], length 0
05:47:26.545119 IP bot.ip.202.6.55383 > victim.53: Flags [S], seq 4261198633, win 0, options [mss 1407,sackOK,TS val 2209910493 ecr 0,nop,wscale 6], length 0
05:47:26.545119 IP bot.ip.233.170.20825 > victim.53: Flags [S], seq 1773488662, win 0, options [mss 1411,sackOK,TS val 2399533981 ecr 0,nop,wscale 6], length 0
05:47:26.545119 IP bot.ip.60.4.4358 > victim.53: Flags [S], seq 3514783804, win 0, options [mss 1400,sackOK,TS val 1975182005 ecr 0,nop,wscale 6], length 0
05:47:26.545120 IP bot.ip.46.104.51597 > victim.53: Flags [S], seq 1144915436, win 0, options [mss 1414,sackOK,TS val 2338192922 ecr 0,nop,wscale 6], length 0
05:47:26.545120 IP bot.ip.208.207.60880 > victim.53: Flags [S], seq 3909313286, win 0, options [mss 1406,sackOK,TS val 3415352270 ecr 0,nop,wscale 6], length 0
05:47:26.545121 IP bot.ip.111.239.33065 > victim.53: Flags [S], seq 2823809286, win 0, options [mss 1405,sackOK,TS val 3042854054 ecr 0,nop,wscale 6], length 0
05:47:26.545121 IP bot.ip.194.176.14406 > victim.53: Flags [S], seq 2623079499, win 0, options [mss 1408,sackOK,TS val 1599832793 ecr 0,nop,wscale 6], length 0
05:47:26.545122 IP bot.ip.177.225.23854 > victim.53: Flags [S], seq 4208441923, win 0, options [mss 1409,sackOK,TS val 3746502324 ecr 0,nop,wscale 6], length 0
```

Real Data, Anonymized

Application Layer: kqps



Overwhelm Defenses: kIPs

112.223.190.109 120.118.89.154 180.201.130.48 61.241.8.31 110.44.19.151 58.54.142.76 22.191.233.5 173.251.91.63 196.252.108.95 92.179.73.139 9.42.64.113 181.67.69.244 104.254.126.185
50.243.189.63 146.61.169.217 119.13.72.175 213.51.1.143 92.208.7.40 218.174.220.191 82.146.126.113 123.234.252.147 69.60.242.234 29.2.93.164 58.15.207.181 38.12.221.19 180.80.249.65
29.125.68.140 161.209.60.188 98.215.215.17 162.81.24.184 213.193.133.214 44.79.251.52 192.80.69.35 156.133.129.111 69.214.173.23 73.217.245.21 106.214.217.84 94.210.82.234 13.239.217.226
5.57.56.81 184.107.112.142 160.21.8.179 143.14.143.31 189.95.147.158 38.225.228.248 217.9.254.148 205.161.97.145 65.238.77.31 180.214.139.186 127.135.220.65 58.7.67.8 24.38.104.203
53.191.188.149 25.155.189.190 178.167.245.156 82.63.219.67 70.133.72.218 3.206.241.134 144.82.64.235 112.24.78.250 127.87.79.120 145.56.237.244 159.162.39.106 63.76.127.21 22.160.25.168
132.13.206.82 168.45.141.38 216.217.198.191 221.14.219.131 167.43.62.61 108.217.207.53 123.107.38.229 6.34.82.187 5.140.196.177 187.239.2.116 44.34.71.53 11.85.164.138 64.236.23.251
16.123.97.236 186.218.114.161 197.115.32.208 117.48.142.150 74.87.178.186 132.247.75.7 108.191.207.10 40.47.24.114 183.211.88.123 155.34.229.14 156.120.144.24 81.43.48.134 155.57.7.250
92.91.5.59 163.111.121.4 15.84.90.93 36.221.14.224 29.11.163.233 135.33.160.59 130.72.189.155 80.180.213.7 155.95.135.246 197.145.23.49 198.204.91.180 124.147.213.219 6.0.34.233 82.4.49.67
3.185.99.145 143.120.178.29 169.121.127.63 24.61.131.76 104.194.82.88 144.23.215.102 134.14.234.105 110.16.211.34 20.140.78.237 79.181.43.156 105.224.88.173 19.92.185.70 142.52.245.146
31.143.225.124 131.72.222.168 86.223.219.110 69.107.129.106 195.129.195.193 223.237.136.182 89.138.187.196 151.49.40.22 190.46.63.241 90.83.6.63 57.236.134.207 90.87.239.164 52.191.33.26
74.215.96.20 111.44.96.142 30.147.161.23 1.82.29.3 94.88.144.40 124.160.243.77 208.151.11.64 149.134.150.115 188.226.1.173 101.2.58.67 170.32.249.13 130.253.48.158 94.15.205.234
29.155.216.107 104.212.54.39 119.233.85.223 169.147.181.164 109.10.231.49 219.13.165.219 10.251.223.65 211.242.72.172 161.15.99.195 177.66.246.106 101.228.148.146 90.120.169.96 23.44.182.31
179.162.187.22 151.86.71.234 8.86.75.247 115.5.29.117 213.244.85.111 119.0.132.240 77.25.198.4 66.113.215.240 74.75.242.45 66.219.79.63 151.174.162.89 97.186.5.234 106.57.165.97
209.184.32.217 1.17.171.149 137.19.169.73 148.72.25.119 93.174.233.143 131.180.90.244 183.41.85.243 206.232.165.155 192.145.210.86 189.177.186.20 166.118.79.29 172.237.29.181 42.9.38.130
56.211.233.68 53.91.215.235 179.118.102.232 204.155.141.66 221.206.101.185 74.87.35.30 186.157.245.3 31.155.160.63 212.154.96.142 196.179.157.136 210.181.115.52 45.17.2.5 47.91.212.61
129.155.251.195 140.119.136.254 173.182.44.43 2.37.52.132 12.59.215.128 21.172.154.83 171.35.161.220 176.73.60.195 55.238.218.228 12.69.115.161 192.94.1.103 94.242.93.123 50.190.249.35
200.248.186.77 25.9.198.203 177.99.201.110 63.231.37.58 182.65.222.70 24.71.230.148 148.14.182.84 164.132.1.72 182.179.142.21 47.200.41.38 188.184.197.89 20.104.240.35 97.225.35.131
165.2.152.252 11.72.1.189 142.155.183.33 193.23.158.126 179.164.172.215 107.175.115.8 194.201.0.66 89.249.14.70 27.13.172.217 65.253.64.178 74.25.50.41 67.56.16.5 142.252.130.47 129.79.96.252
87.48.3.202 20.136.79.103 214.83.7.85 61.96.158.177 83.15.119.26 132.175.59.121 212.214.132.12 144.30.191.67 202.206.32.135 83.219.52.158 155.249.160.167 209.69.117.143 210.195.4.5
96.123.248.98 125.233.99.90 12.85.82.175 201.175.84.218 74.120.69.4 106.101.50.90 97.192.244.89 15.117.67.171 211.68.216.163 82.138.126.142 130.165.245.200 117.43.184.229 156.225.60.239
163.128.232.46 15.48.69.198 5.97.46.107 153.114.20.38 152.57.213.107 161.194.14.16 93.171.120.122 189.2.86.246 26.18.223.22 198.180.192.140 204.112.165.139 121.103.114.17 12.15.171.33
58.44.151.119 204.69.60.238 87.72.127.19 114.68.213.235 41.10.38.9 158.54.224.31 179.99.24.209 115.67.229.197 103.167.244.161 188.196.178.70 35.75.193.45 84.236.106.253 153.183.22.232
186.176.158.45 106.168.19.156 153.45.43.177 195.245.46.145 57.158.158.43 12.26.121.223 31.19.146.104 168.61.142.228 53.50.218.210 216.195.161.53 11.197.143.108 198.95.45.38 11.100.237.157
54.61.96.193 159.73.237.159 152.184.189.52 105.208.126.33 5.63.131.60 97.215.237.239 172.34.158.89 100.108.70.17 0.165.90.169 74.217.251.99 93.97.168.155 51.221.19.196 151.69.246.141
121.198.9.145 36.86.150.128 75.208.204.125 129.94.122.117 193.181.35.62 94.38.134.234 177.57.204.8 161.27.184.134 56.48.76.50 109.218.174.37 221.77.71.93 181.170.14.248 100.53.154.224
117.113.110.106 17.162.107.77 178.124.153.210 120.127.12.165 182.157.211.108 219.140.67.82 85.238.152.130 141.101.139.78 27.233.138.157 80.226.183.145 9.39.154.24 113.51.234.84 126.36.84.111
212.0.7.134 65.229.145.126 79.239.139.42 37.87.222.40 3.132.140.164 27.160.87.16 42.234.214.102 109.247.111.147 77.209.231.76 131.98.214.22 140.235.135.117 139.136.55.75 115.15.99.123
76.134.67.247 34.104.194.174 51.51.242.128 92.206.97.157 117.135.197.53 104.141.139.86 62.44.55.143 54.60.165.25 183.113.157.9 163.226.96.11 30.41.48.198 198.3.89.186 208.154.232.28
156.26.191.117 3.17.33.50 150.34.105.4 178.192.165.88 171.63.99.178 17.32.13.22 167.7.184.164 33.173.60.236 196.138.67.144 56.81.17.235 43.226.143.245 40.47.128.222 99.30.5.156 74.243.80.150
187.211.108.96 165.136.99.160 187.215.44.60 122.117.231.115 201.118.201.205 62.95.49.248 168.132.236.183 33.177.200.229 102.101.169.170 152.246.1.18 202.50.133.144 154.100.118.185 85.99.133.7
63.164.158.206 31.85.127.133 12.5.26.141 11.51.181.50 106.131.13.212 1.17.222.249 170.41.135.226 107.220.228.64 154.135.125.44 43.162.175.15 187.20.244.197 204.205.98.206 80.13.244.246
51.101.179.34 158.174.15.218 184.10.70.151 68.158.42.65 81.148.201.115 102.41.160.236 53.128.98.189 67.56.236.34 130.147.8.176 48.95.145.170 189.186.9.4 156.41.112.167 184.167.17.240
109.212.14.105 176.102.83.84 124.98.252.34 16.59.140.102 200.119.17.221 139.67.154.164 105.184.232.50 101.97.194.54 63.22.48.198 106.253.204.191 18.191.135.197 121.231.47.175 156.173.210.214
126.106.234.90 218.71.154.240 45.172.141.24 105.243.45.82 120.246.118.80 117.121.99.195 154.49.145.36 205.46.208.143 202.120.117.108 43.203.55.108 68.41.53.191 12.72.64.3 70.229.184.114
82.84.236.121 18.249.106.246 210.60.132.68 51.60.107.125 87.169.157.51 214.182.225.8 178.218.139.120 77.124.87.120 162.220.105.247 96.74.8.17 201.170.29.42 175.210.114.143 108.179.125.40
43.42.246.82 27.64.169.248 35.180.73.195 54.175.137.40 136.199.141.53 12.199.60.93 156.85.221.133 125.3.236.205 21.251.41.147 122.34.159.16 52.40.180.186 138.249.15.253 194.116.191.51
199.195.168.156 13.195.158.244 143.215.148.253 23.114.201.175 148.209.195.62 38.22.34.82 122.250.155.193 125.140.13.110 38.170.94.185 106.116.225.107 205.187.91.233 10.77.56.42 82.206.212.29
177.186.104.4 189.103.95.216 88.250.213.253 139.241.195.253 200.170.241.243 35.228.149.68 87.188.248.189 19.155.41.21 36.55.249.124 160.115.15.64 83.91.86.26 46.125.166.182 147.150.37.66
107.104.191.221 11.142.154.155 187.70.243.88 38.125.82.162 217.163.0.161 195.98.39.45 60.214.137.97 7.146.127.62 117.81.54.135 157.235.217.31 48.88.80.61 127.232.202.230 111.157.109.166
63.196.6.221 97.148.128.234 213.186.144.103 183.199.135.28 70.35.82.216 222.207.108.145 120.53.83.20 56.25.196.7 74.189.131.79 84.125.29.73 179.222.125.16 99.31.177.22 26.119.37.203
116.73.54.130 164.113.102.192 66.19.129.141 15.180.97.1 60.113.113.182 131.230.35.5 140.234.2.221 109.247.160.119 104.245.41.151 209.109.1.217 156.4.244.24 197.68.121.237 25.51.126.154
57.80.8.23 13.1.173.182 13.155.179.9 99.228.126.7 34.180.249.41 52.168.111.44 126.82.53.244 32.136.126.228 6.23.148.175 33.222.232.72 210.41.74.26 38.144.70.111 50.35.122.205 52.238.44.190
210.75.202.133 46.191.74.51 125.202.18.222 4.173.59.115 222.219.174.85 75.221.213.79 161.116.20.18 46.151.119.80 198.78.151.111 110.225.197.243 97.61.131.221 28.140.131.196 38.99.215.106
163.169.215.6 220.128.68.144 117.52.153.58 81.45.62.28 8.83.245.30 65.19[illegible]155 71.142.177.[illegible]84.217.134.86 181.107.241.249 47.218.244.26 203.70.53.90 192.110.171.89 151.192.228.231
123.126.235.172 215.17.99.76 185.247.132.207 42.81.35.104 3.190.147.38 2[illegible]58.[illegible]93.52.[illegible]245 61.164.47.228 80.166.8.122 169.60.30.120 160.93.192.218 101.137.60.95
216.92.156.40 168.215.172.121 115.24.43.45 35.75.193.45 84.236.106.253 153.[illegible]98.5.28 53.114.20.38 152.57.213.107 161.194.14.16 93.171.120.12 52.224.88.173

Fake Data

Attack Trends

Russo-Georgian War Anniversary

(600 kqps)

botnet 08/2009

c|net

Twitter crippled by denial-of-service attack

Microblogging service says it's recovering but still defending itself against the attack. Facebook has also confirmed it was targeted by a DoS attack.

theguardian

Georgian blogger Cyxymu blames Russia for cyber attack

Blogger claims attack on Twitter, Facebook and LiveJournal was part of plot to silence his criticism of the Kremlin

BBC NEWS

Web attack 'aimed at one blogger'

A "massively co-ordinated" attack on websites including Google, Facebook and Twitter was directed at one individual, it has been confirmed.

Russo-Georgian War Anniversary

(600 kqps)

FOX BUSINESS

Capital One Targeted Again in Cyber Attack Spree

REUTERS

Customers reporting BofA website problems

botnet 08/2009

servers 09/2012

BroBot Attacks US Banks

(125 Gbps)

BB&T

October 17, 2012 ·

BBT.com is experiencing intermittent delays and outages. We apologize for the inconvenience and assure you that your accounts and personal information remain secure. Please know that we are working diligently to restore service as soon as possible.

Russo-Georgian War Anniversary

(600 kqps)

Spamhaus Attack

(300 Gbps)

LINX — Est. 1994 —

botnet 08/2009

servers 09/2012

DNS amp 03/2013

BroBot Attacks US Banks

(125 Gbps)

CLOUDFLARE

The DDoS That Almost Broke the Internet

27 Mar 2013 by Matthew Prince.

Russo-Georgian War Anniversary

(600 kqps)

Spamhaus Attack

(300 Gbps)



Google says Chinese Great Cannon shows need to encrypt web

The large DDoS attack on GitHub and Greatfire that occurred over March and April would not have been possible with encrypted web traffic, Google has said.

botnet 08/2009

servers 09/2012

DNS amp 03/2013

javascript 04/2015

BroBot Attacks US Banks

(125 Gbps)

China's Great Cannon vs. GitHub

(400k IPs)



Russo-Georgian War Anniversary

(600 kqps)

Spamhaus Attack

(300 Gbps)

botnet 08/2009

servers 09/2012

DNS amp 03/2013

javascript 04/2015

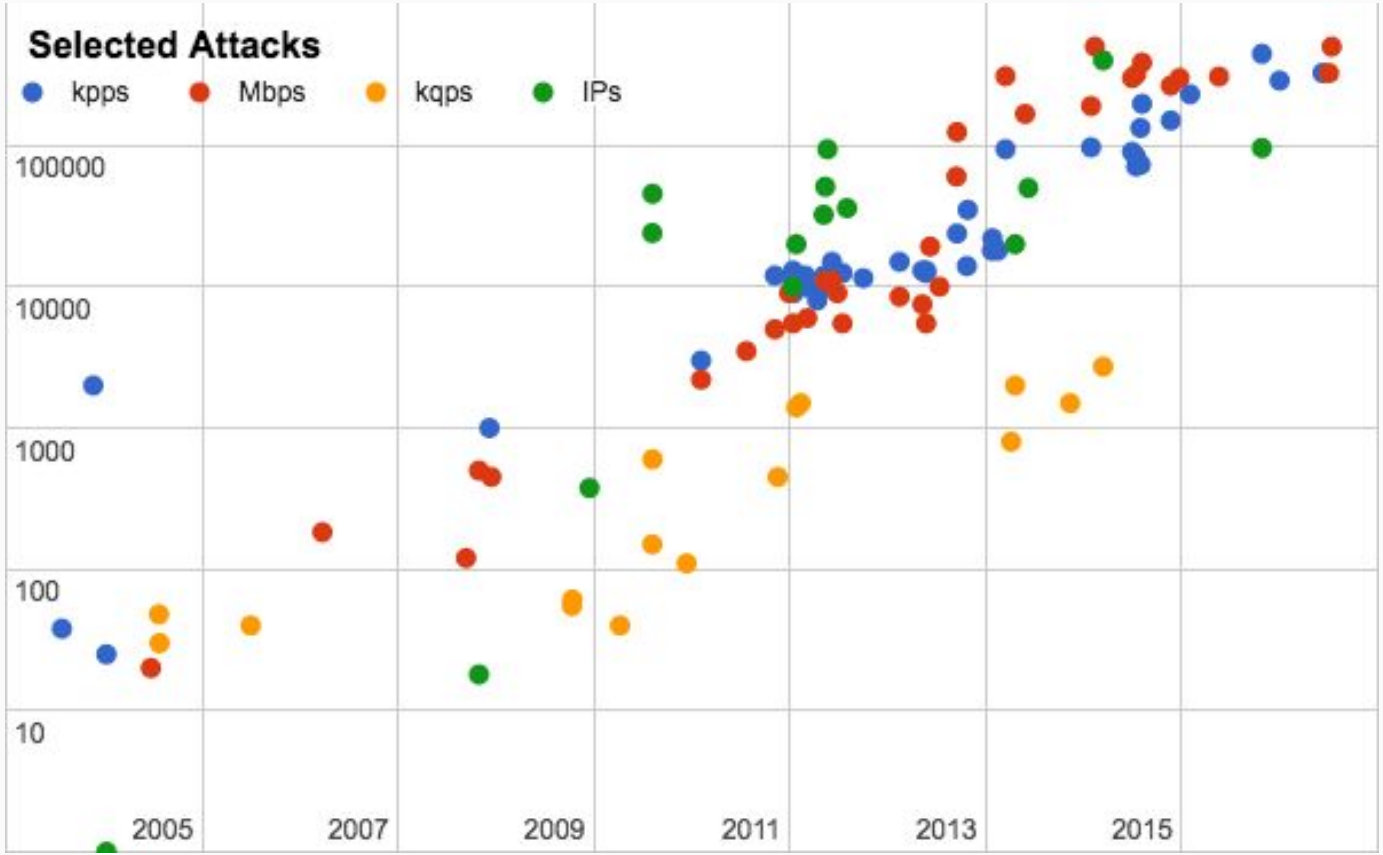
IoT 08/2016

BroBot Attacks US Banks

(125 Gbps)

China's Great Cannon vs. GitHub

(400k IPs)



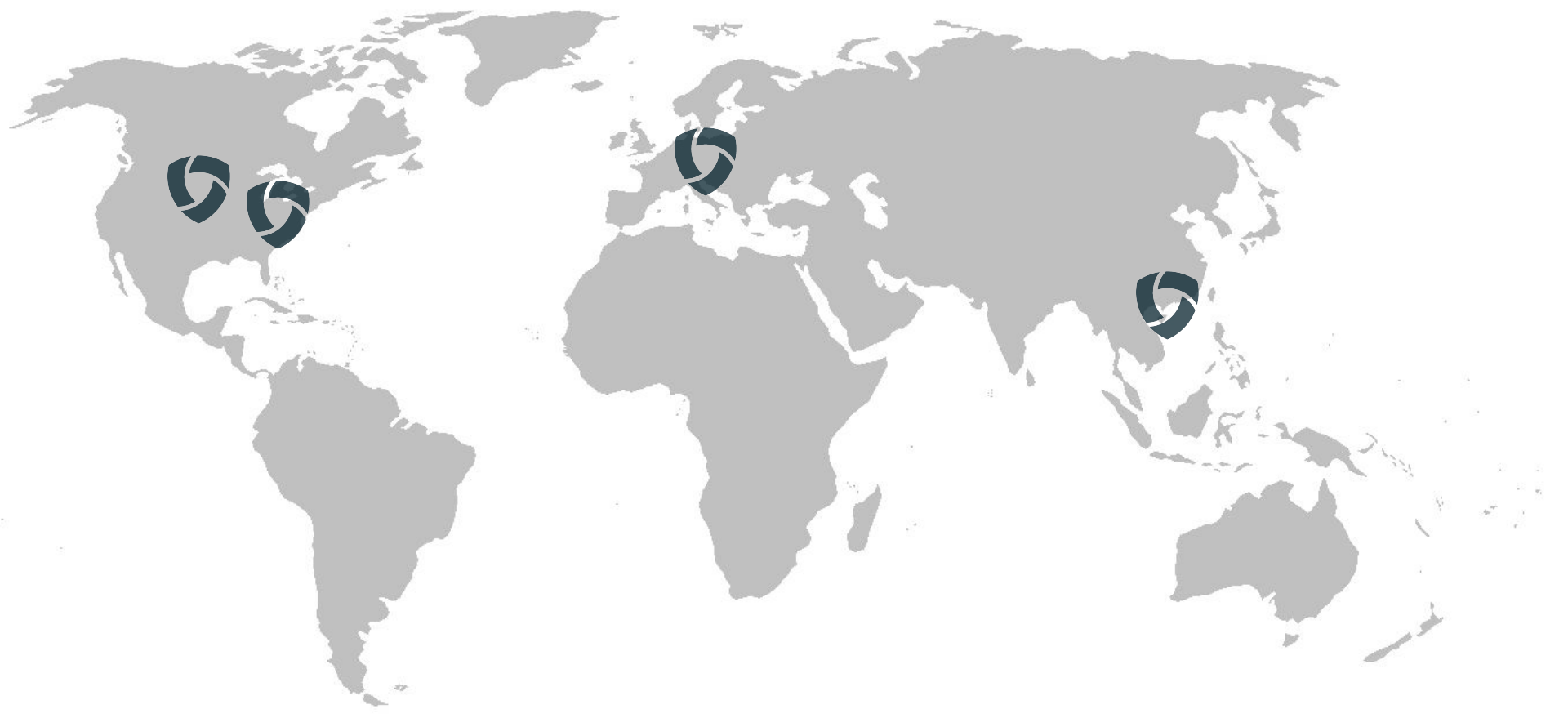
Moore's Law: Up and to the right

Defense

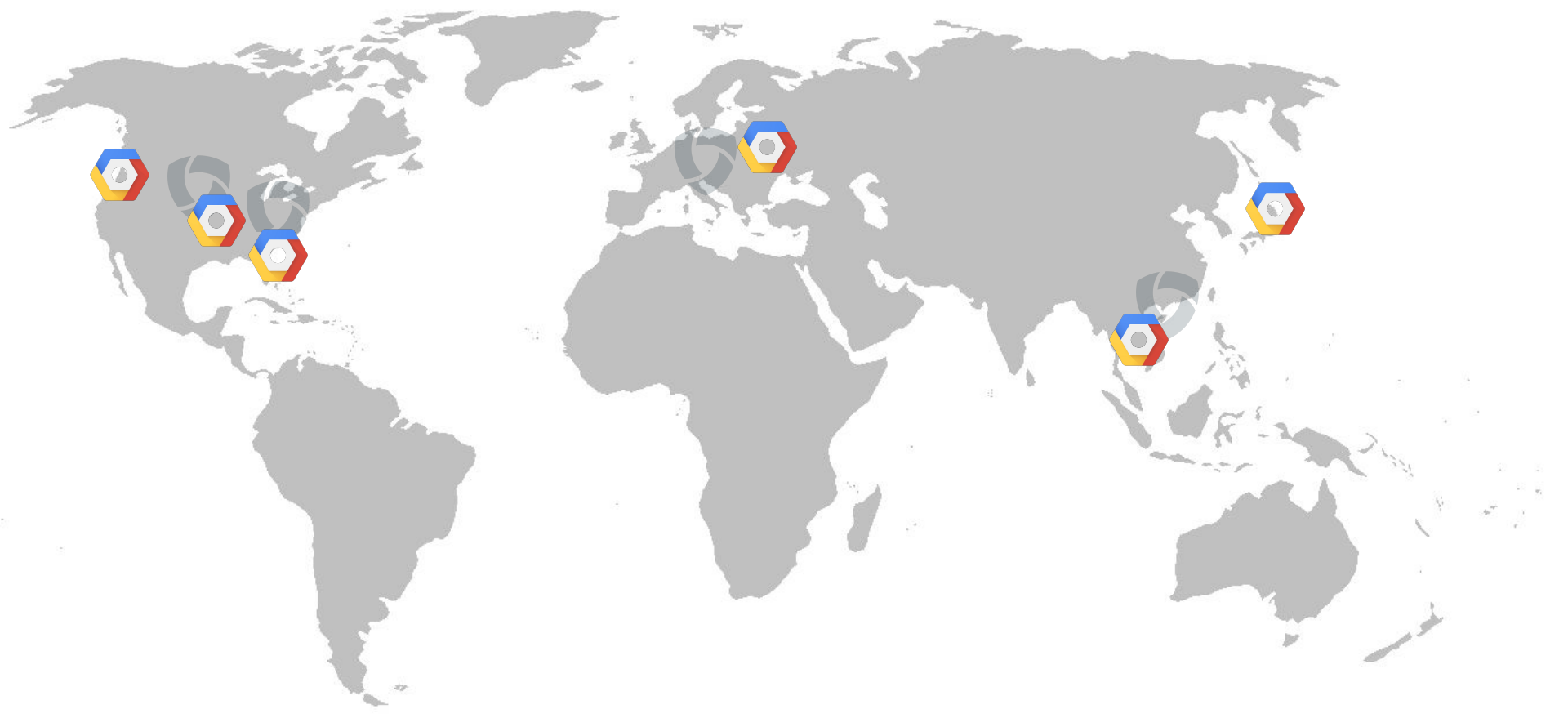

Google


Jigsaw

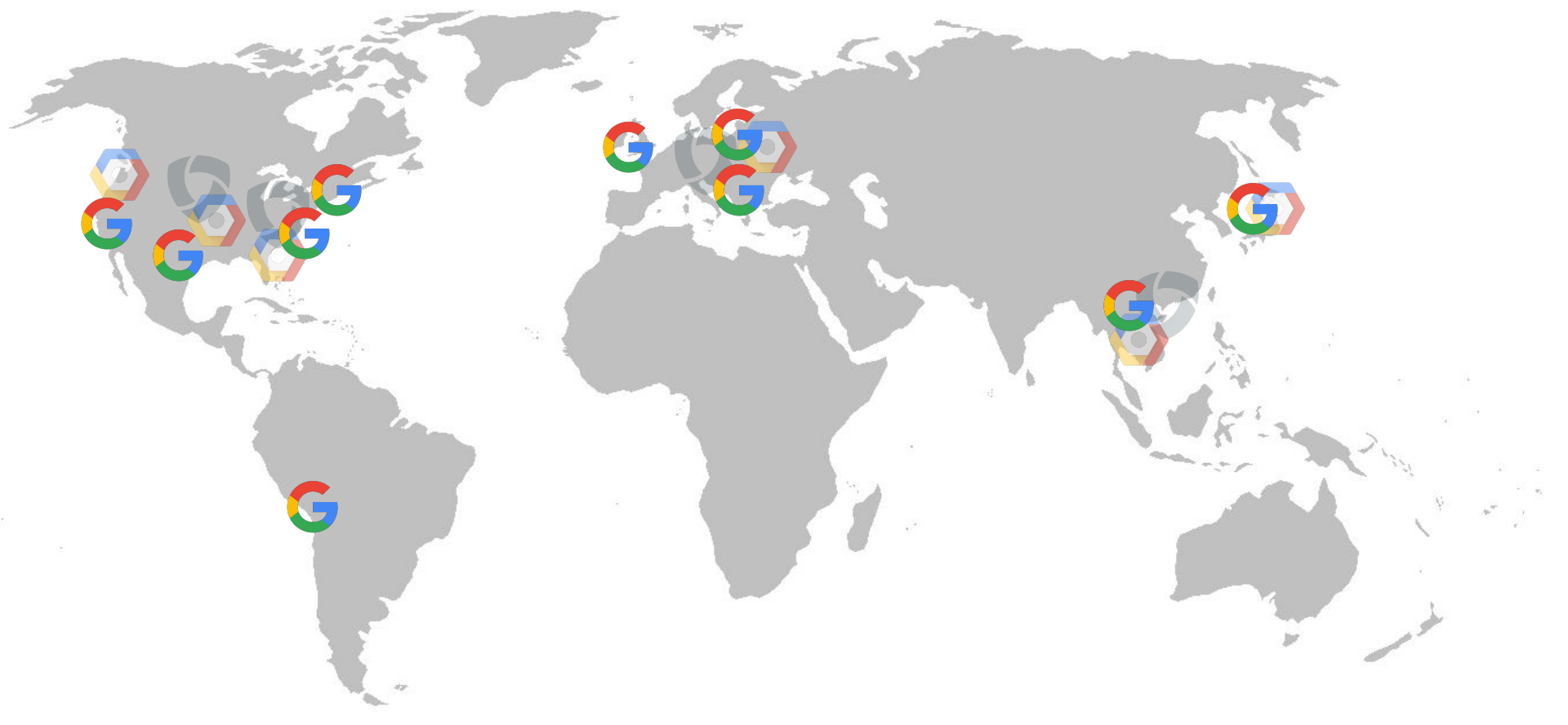

Project Shield



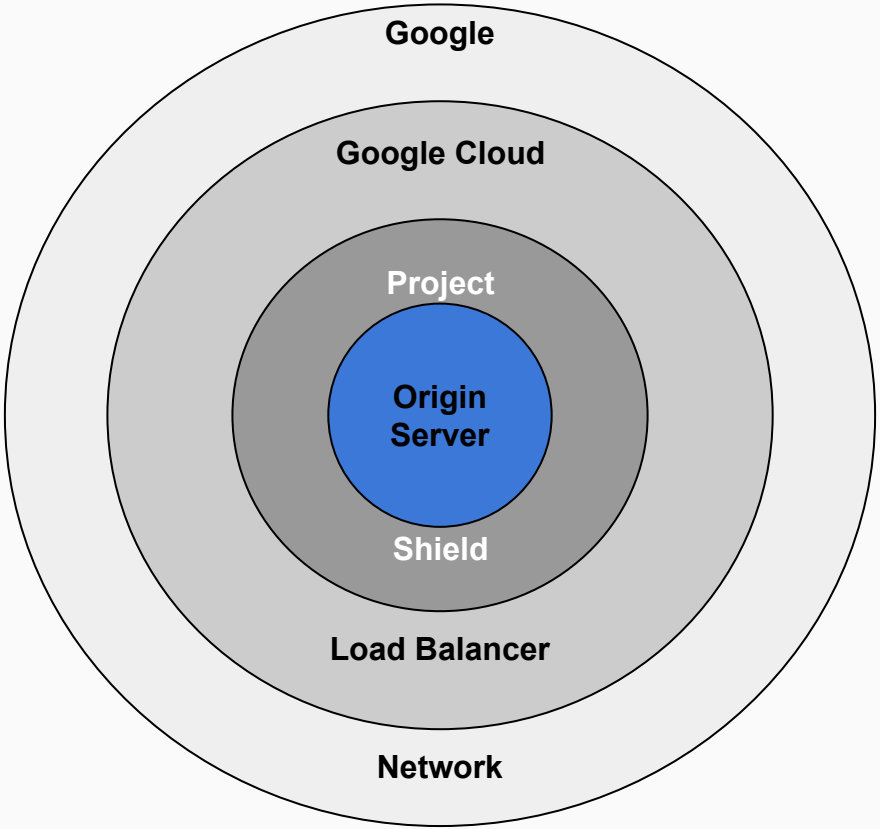
Shield servers protect the origin



Google Cloud HTTP(S) Load Balancing protects Shield



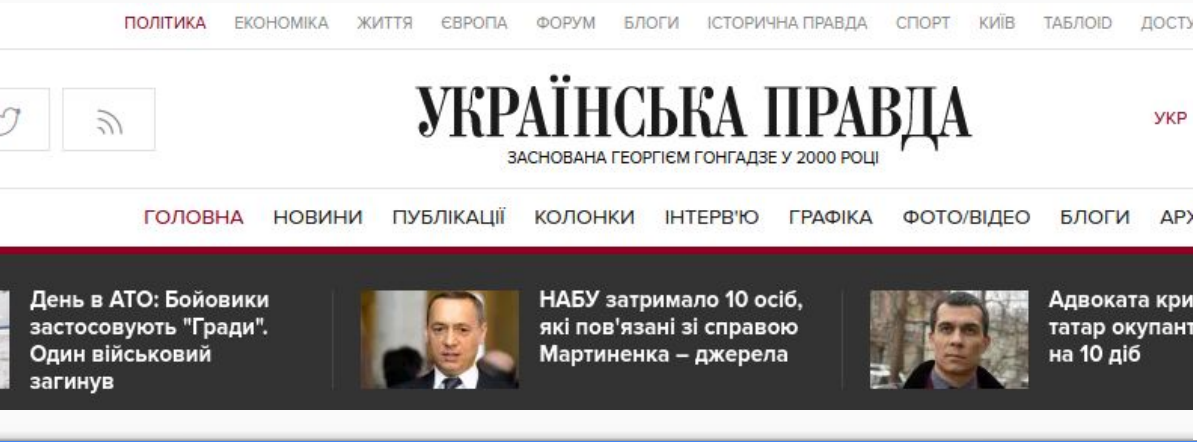
Google frontends protect GCP

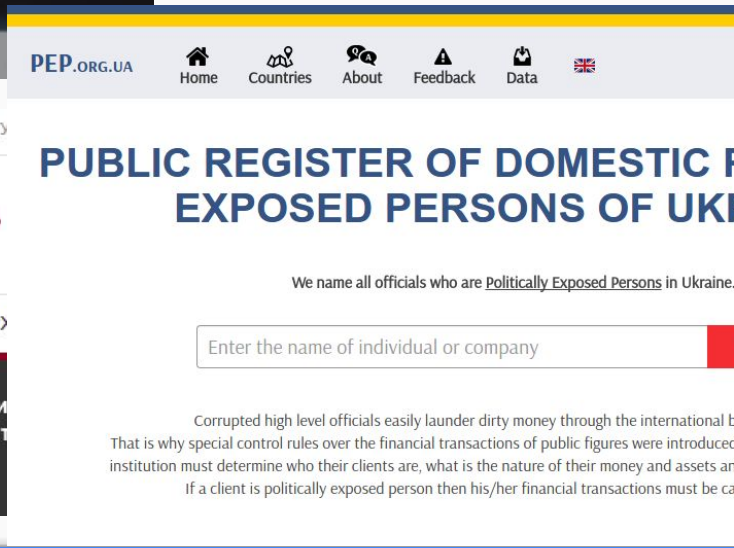


Project Shield Architecture









Hosted Sites

Assembling the pieces ...

Meet Brian Krebs



25 MAY 13 **Reports: Liberty Reserve Founder Arrested, Site Shuttered**

18 DEC 13 **Sources: Target Investigating Data Breach**

29 MAY 14 **True Goodbye: 'Using TrueCrypt Is Not Secure'**

19 JUL 15 **Online Cheating Site AshleyMadison Hacked**

Brian Krebs vs. Mirai Botnet

08 SEP 16 **Israeli Online Attack Service 'vDOS' Earned $600,000 in Two Years**

10 SEP 16 **Alleged vDOS Proprietors Arrested in Israel**

20 SEP 16 **DDoS Mitigation Firm Has History of Hijacks**

21 SEP 16 **KrebsOnSecurity Hit With Record DDoS**



briankrebs @briankrebs · Sep 22

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

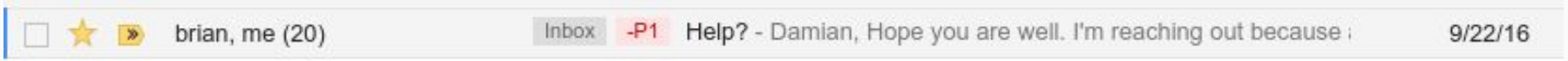
Brian Krebs vs. Mirai Botnet

❝I spoke with multiple DDoS mitigation firms. One offered to host KrebsOnSecurity for two weeks at no charge, but after that they said the same kind of protection I had under Akamai would cost between $150,000 and $200,000 per year.

A number of other providers offered to help, but it was clear that they did not have the muscle to be able to withstand such massive attacks.❞

Brian Krebs
The Democratization of Censorship

Brian Krebs vs. Mirai Botnet - Addressing the Tradeoffs



Unknown threat to primary business

Unknown Attack Volumes

Can others help

How can we help

Public Relations concerns

Opportunity to find out

Opportunity to measure

Most are afraid of the risks

Existing product offering

Nothing to lose (no expectations)

Brian Krebs vs. Mirai Botnet - Migrating the Website

```
Domain Name: KREBSONSECURITY.COM
...
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
...
...
Name Server: NS-CLOUD-D1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D4.GOOGLEDOMAINS.COM
```

Brian Krebs vs. Mirai Botnet

Come at me, bro.



130Mpps SYN flood +
60Mpps of RSTs

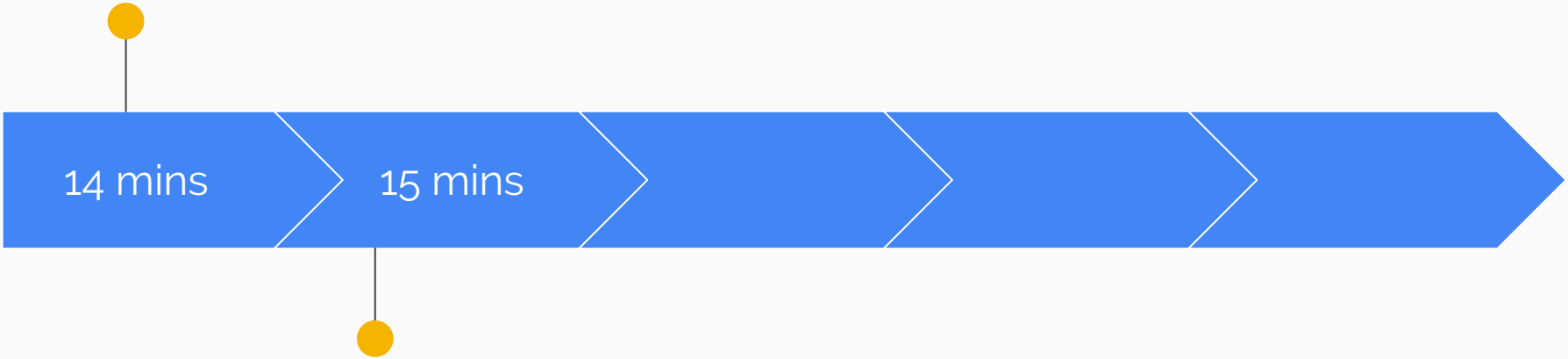




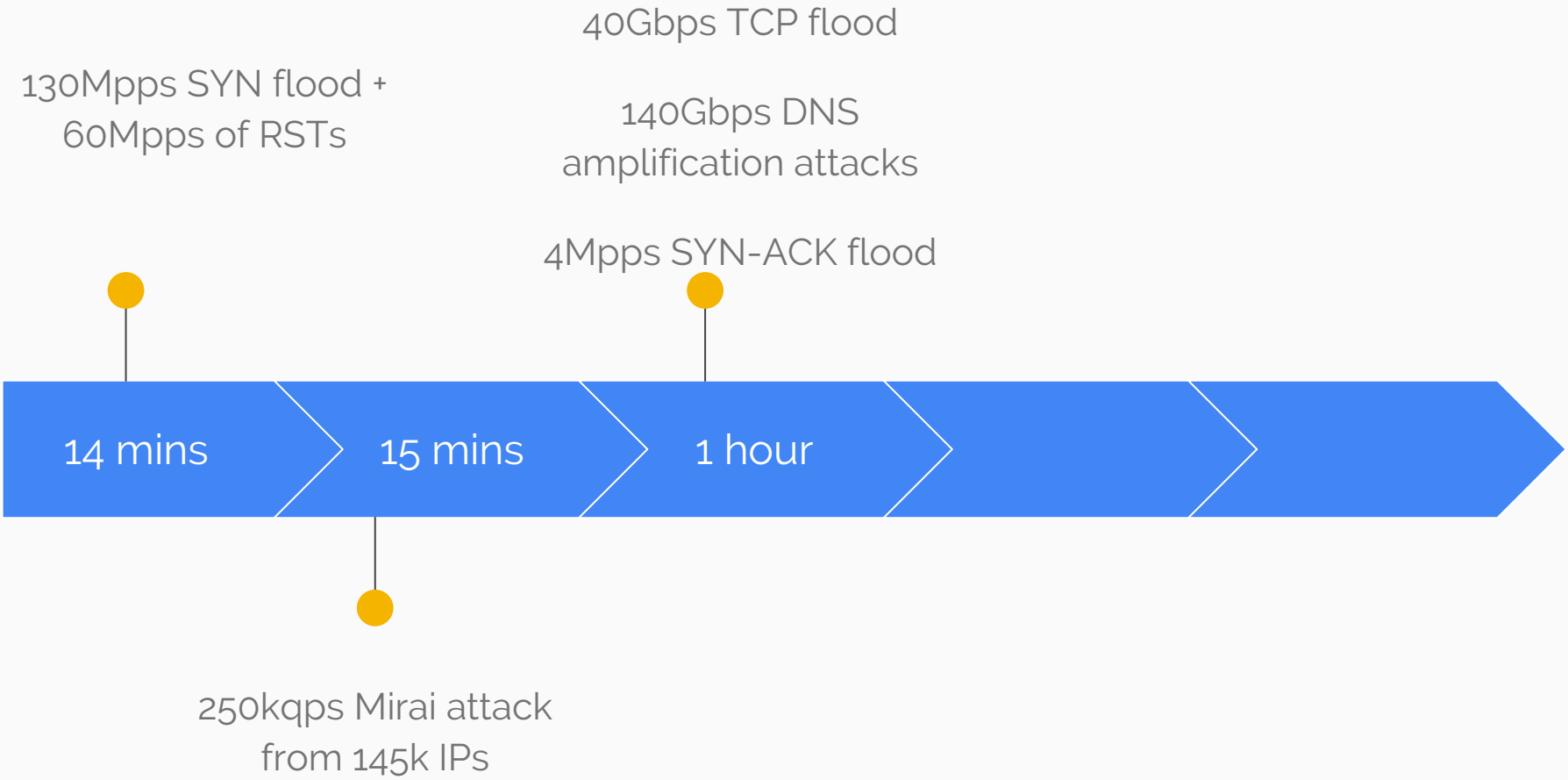
briankrebs @briankrebs · Sep 24

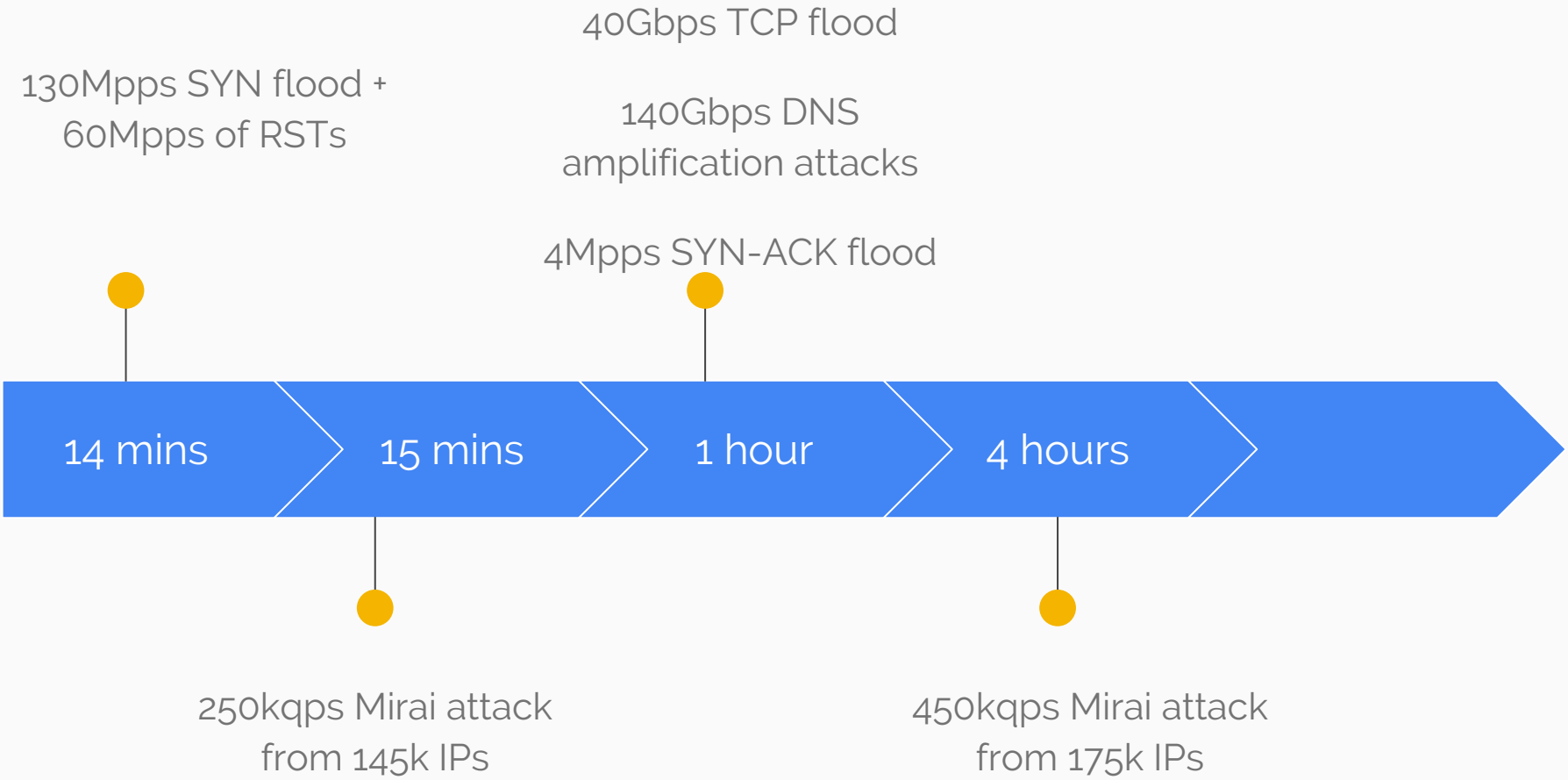
KrebsOnSecurity.com should be coming back up gradually now and over the next 48 hours.

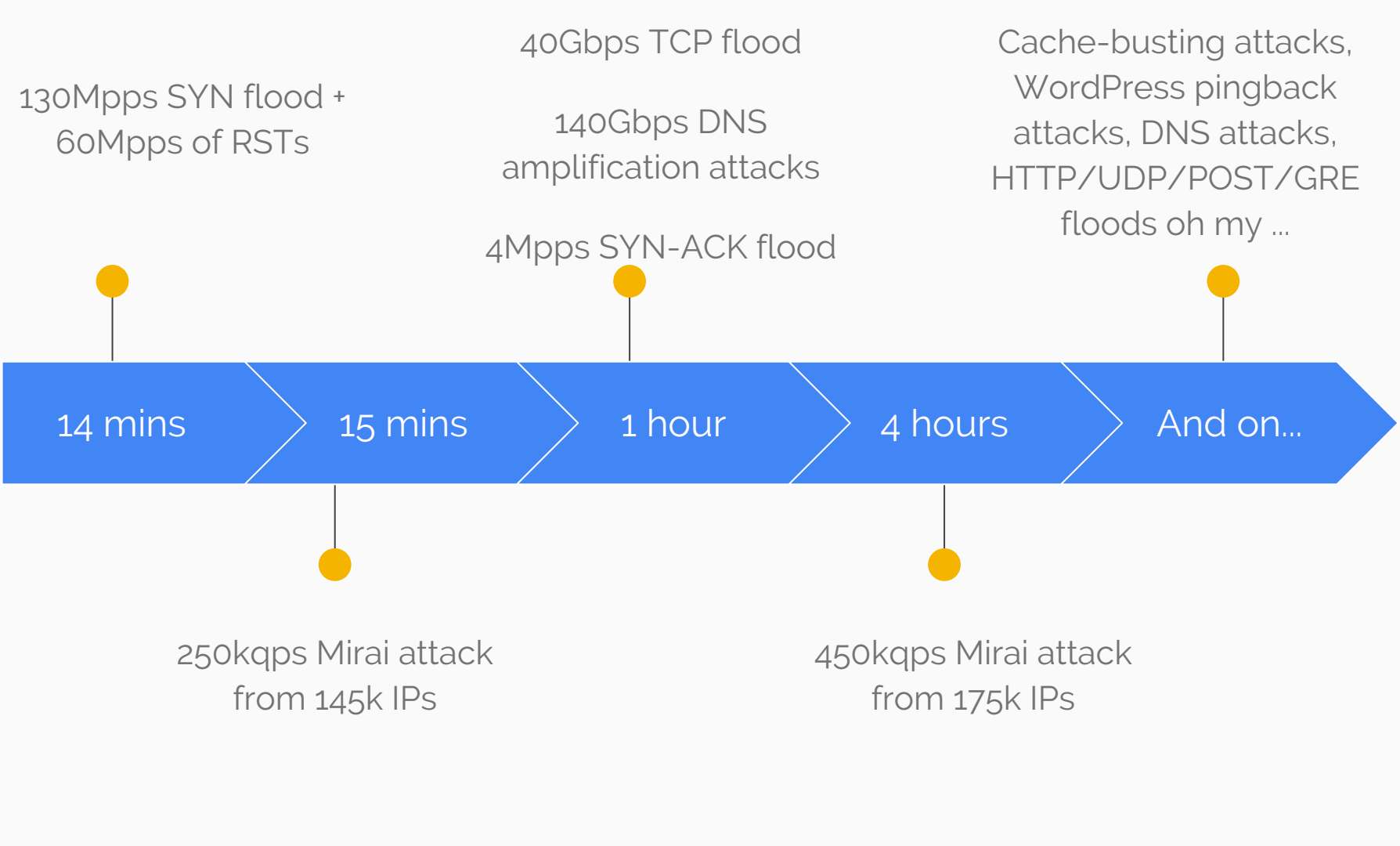
130Mpps SYN flood +
60Mpps of RSTs



250kqps Mirai attack
from 145k IPs


40Gbps TCP flood
130Mpps SYN flood +
60Mpps of RSTs
140Gbps DNS
amplification attacks
4Mpps SYN-ACK flood
14 mins
15 mins
1 hour
250kqps Mirai attack
from 145k IPs


40Gbps TCP flood
130Mpps SYN flood +
60Mpps of RSTs
140Gbps DNS
amplification attacks
4Mpps SYN-ACK flood
14 mins
15 mins
1 hour
4 hours
250kqps Mirai attack
from 145k IPs
450kqps Mirai attack
from 175k IPs

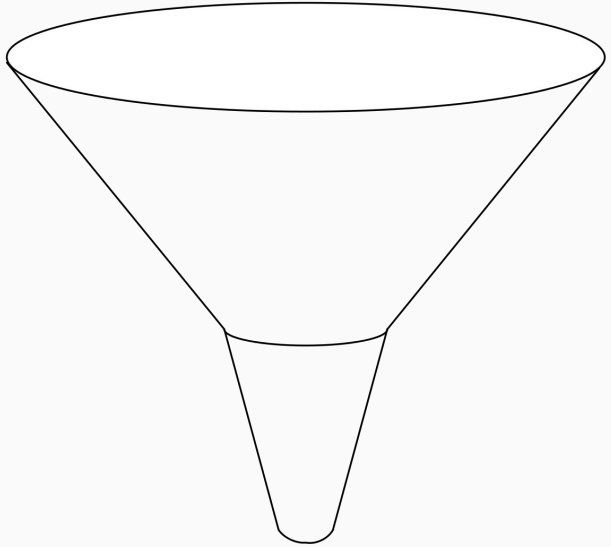

130Mpps SYN flood + 60Mpps of RSTs
40Gbps TCP flood
140Gbps DNS amplification attacks
4Mpps SYN-ACK flood
Cache-busting attacks, WordPress pingback attacks, DNS attacks, HTTP/UDP/POST/GRE floods oh my ...
14 mins
15 mins
1 hour
4 hours
And on...
250kqps Mirai attack from 145k IPs
450kqps Mirai attack from 175k IPs

Lessons

Defending a small site ...

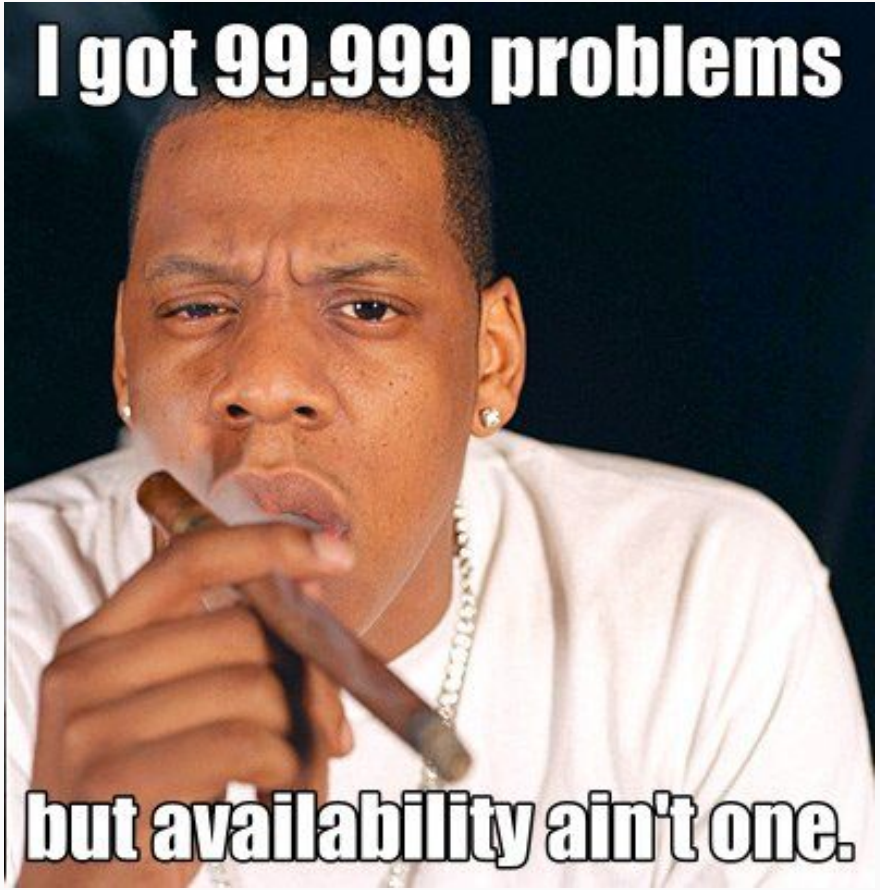
Is hard.

450,000 qps



20 qps

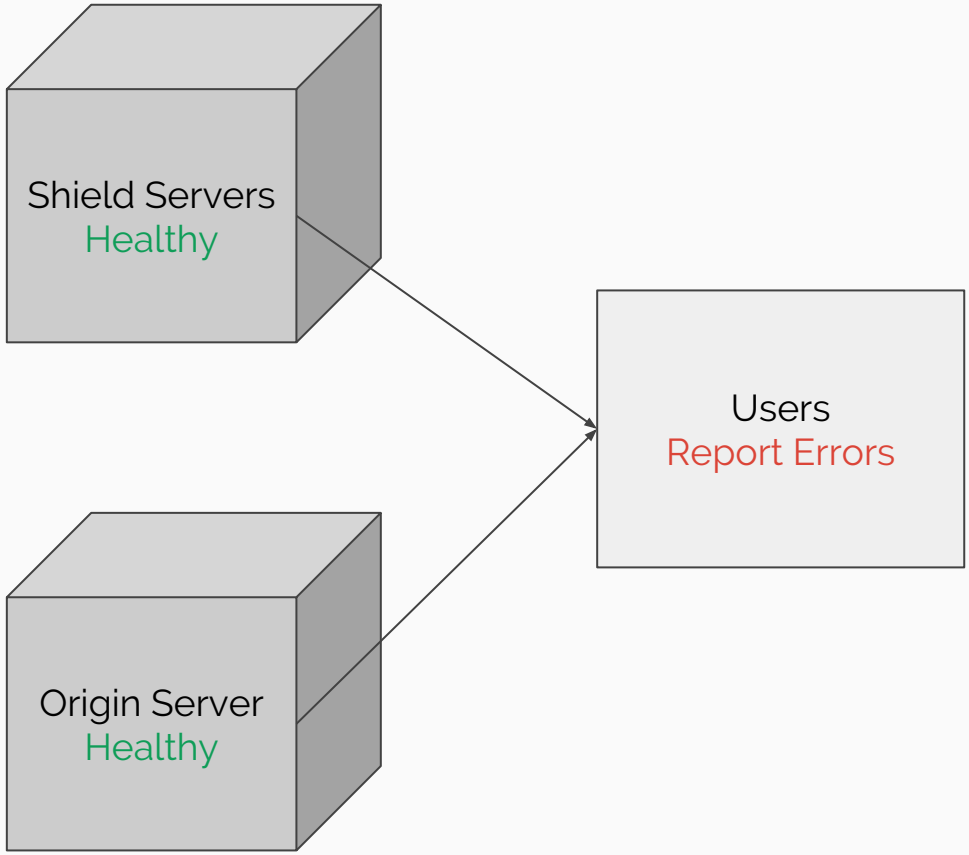
Good Enough Defense



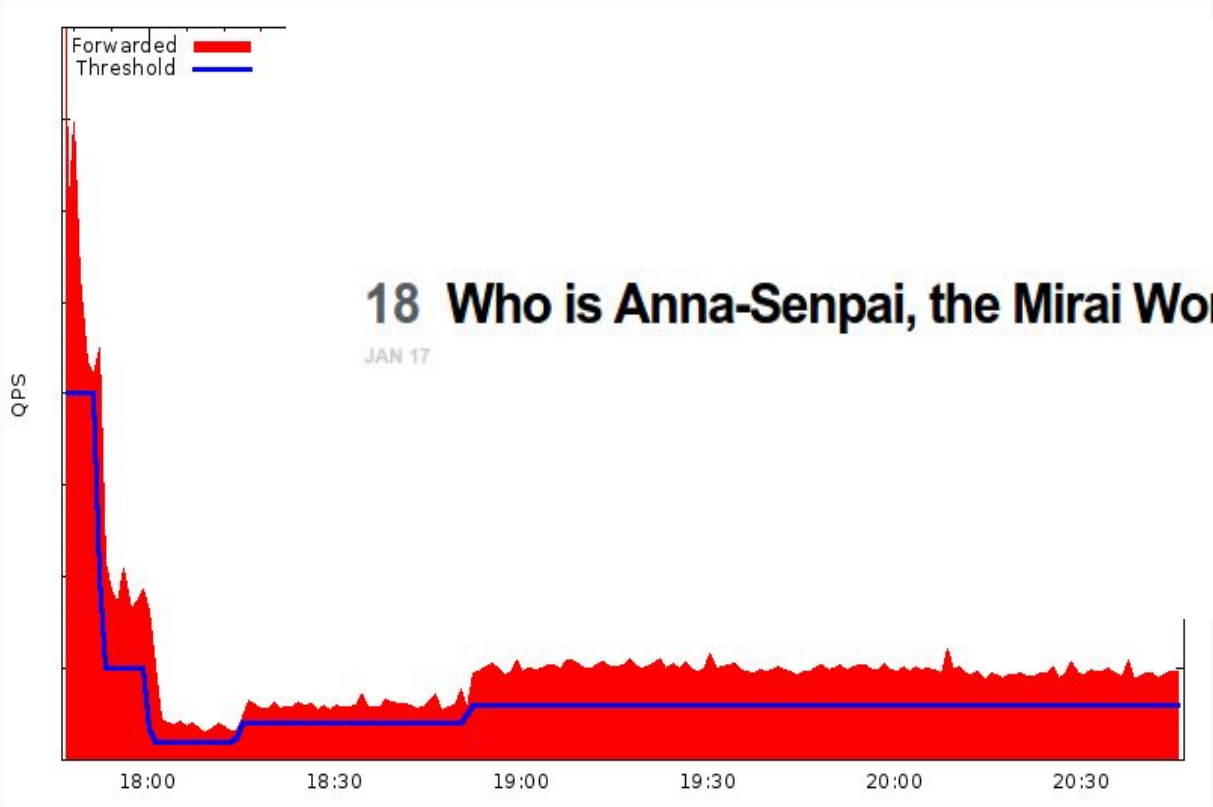
Shared debugging

...

Is hard.



Brian Krebs vs. Mirai Botnet - Benefits



18 Who is Anna-Senpai, the Mirai Worm Author?

JAN 17

Questions?