

INTERNET BACKGROUND RADIATION

John Graham-Cumming
Virus Bulletin Conference 2012



MALTRAFFIC

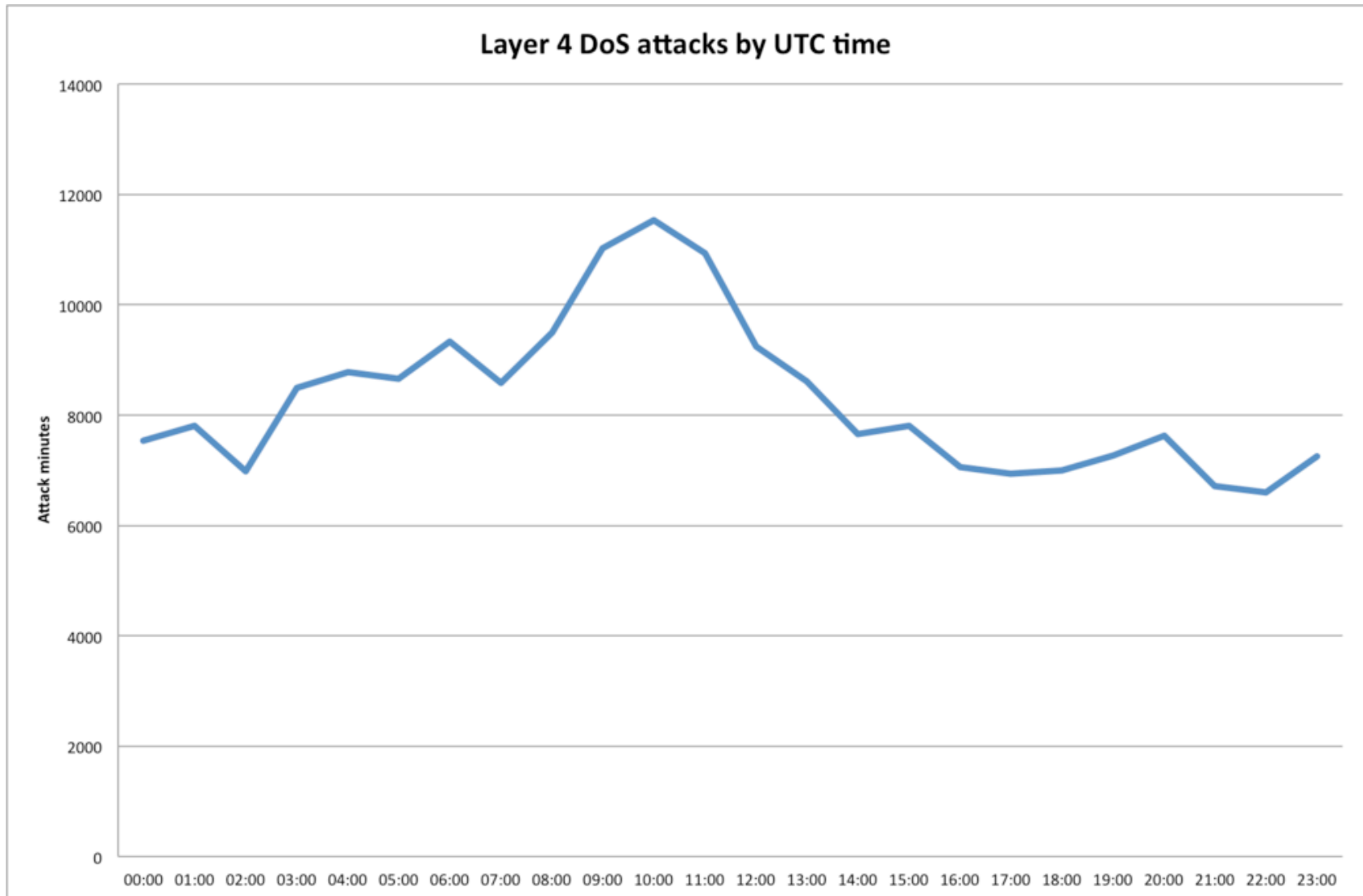
Quick CloudFlare Background



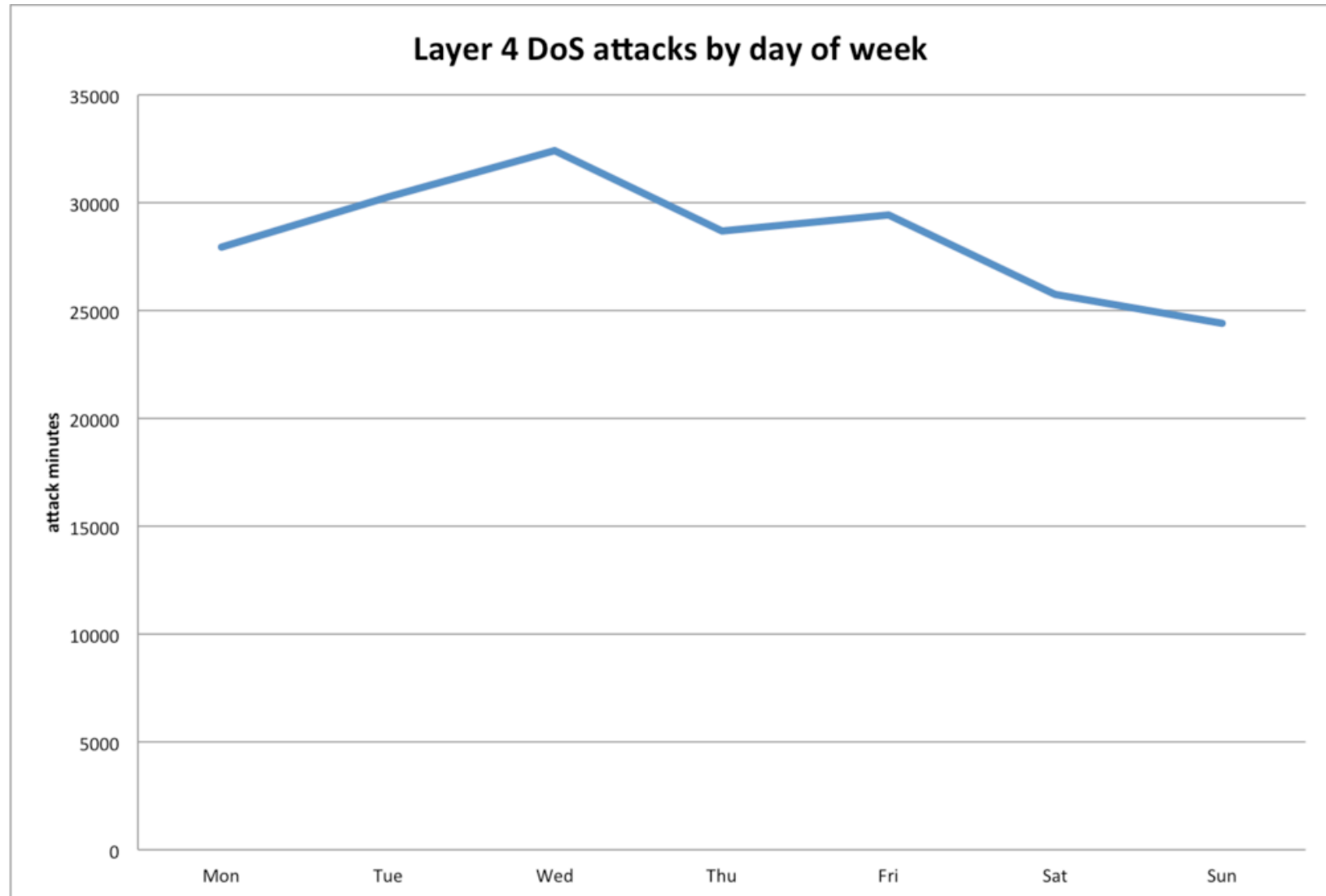
Overview

- 64 billion page views per month
- 40% of the time we see a layer 4 DDoS attack
- 95.5% of the time we see a layer 7 DDoS attack
- Largest DDoS attack we've seen was 65Gbps
- Overall trend in layer 4 DDoS is slightly down
- Overall trend in layer 7 DDoS is up (overall 10%; large: 21%)
- Layer 7 attacks from from 0.05% of connecting IPs
- Data drawn from monitoring between January 2012 to July 2012

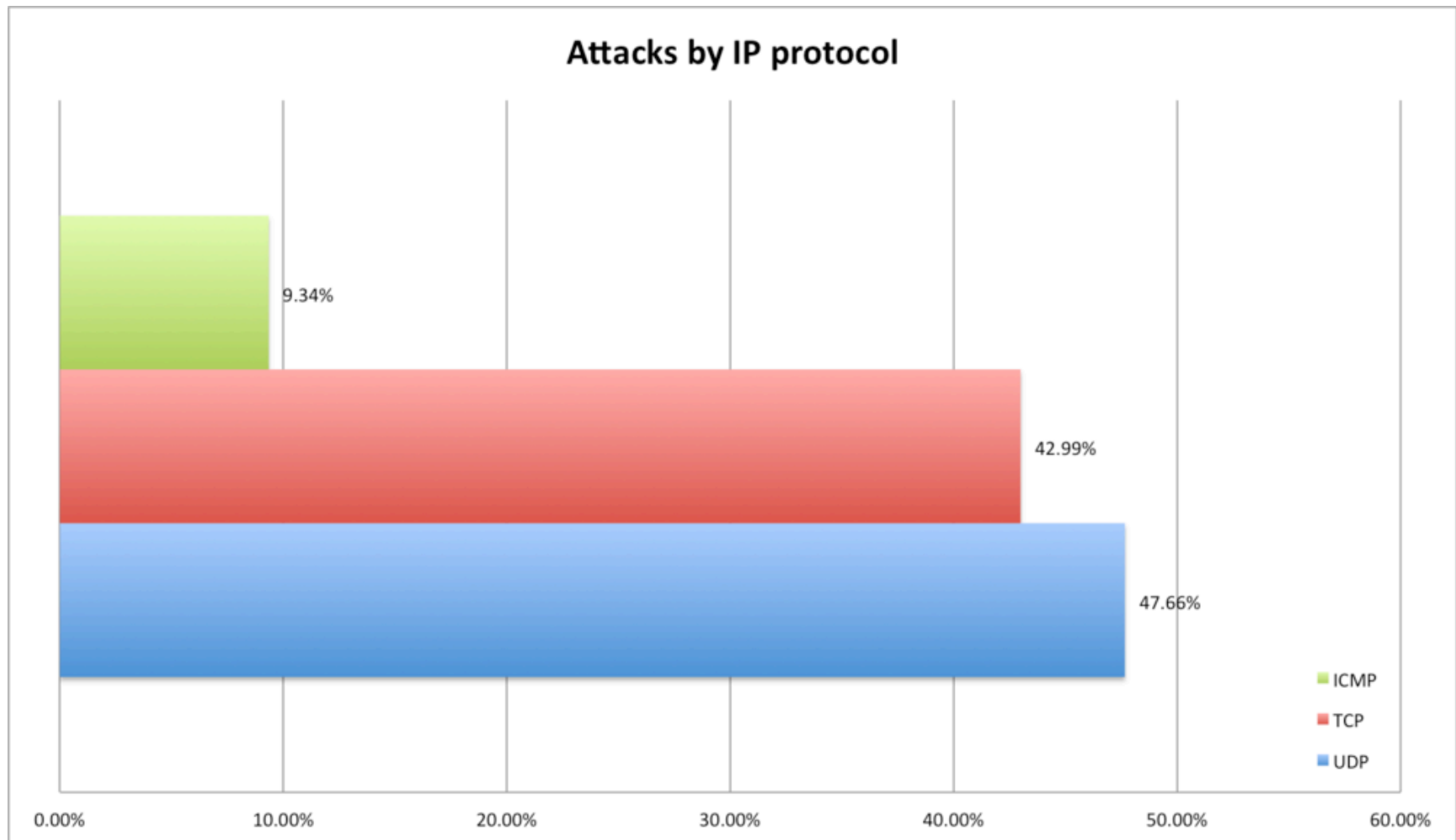
Layer 4 DoS by UTC time



Layer 4 DoS by day of week



Layer 4 Protocol Breakdown



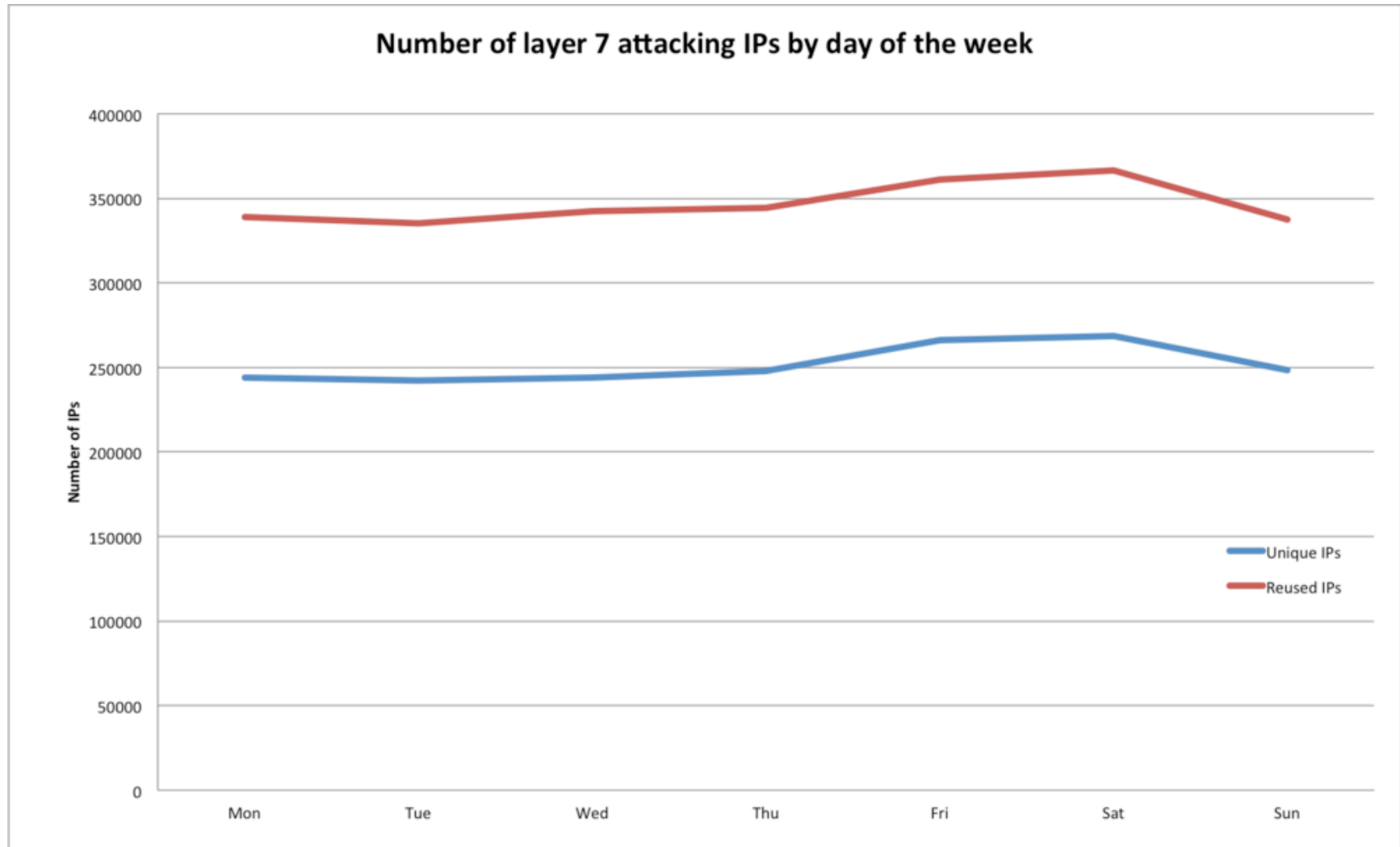
Layer 4 Port Data

- TCP
 - 92% against port 80
 - SYN flooding
- UDP
 - 97% against DNS
 - Reflection/amplification attacks
- Other significant attack ports
 - TCP port 53 (DNS)
 - UDP port 514 (syslog)

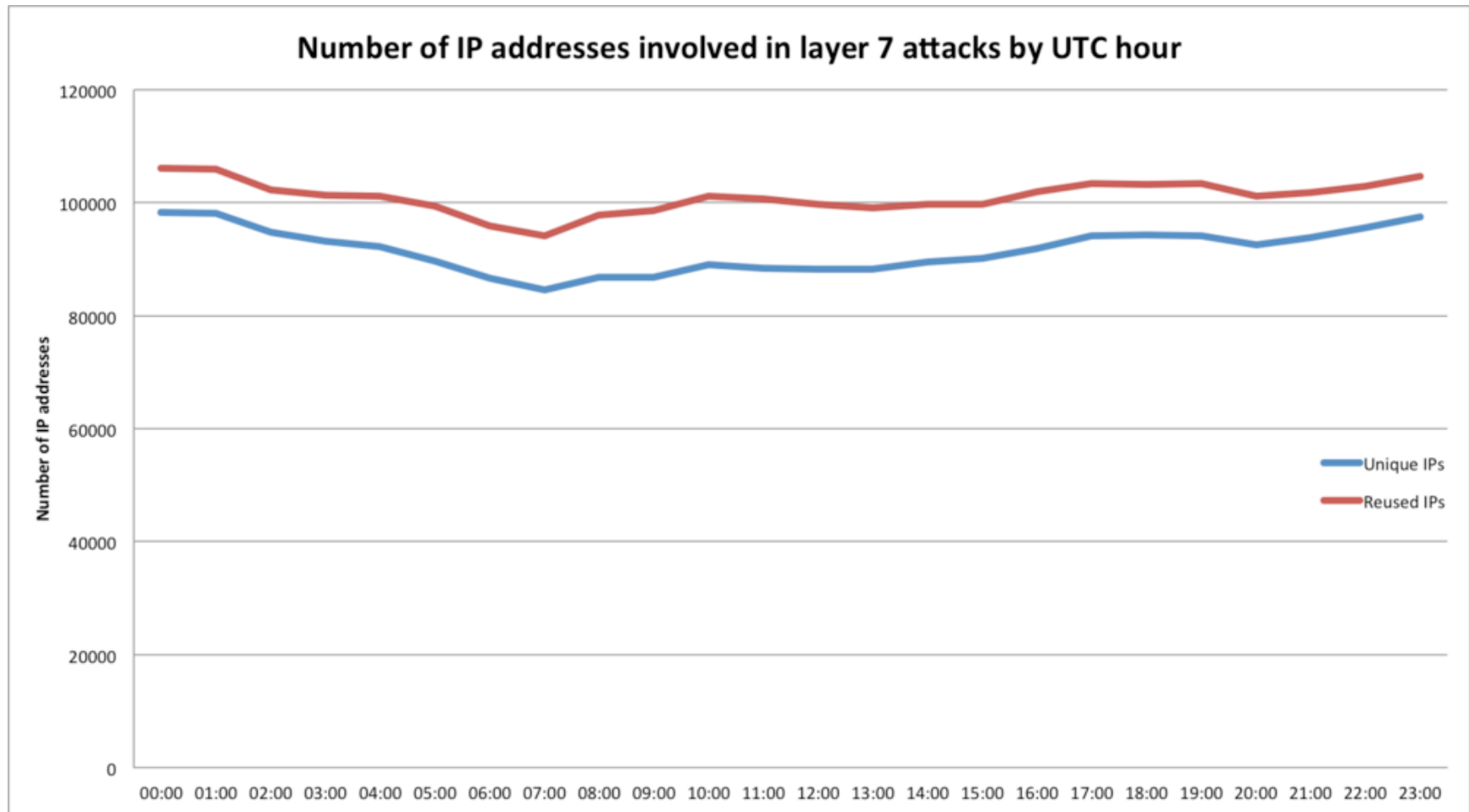
Layer 4 Source Network Data

- Addresses are spoofed:
 - 23% from Martian addresses
 - 3.45% from China Telecom
 - 2.14% from China Unicom
 - 1.74% from Comcast
 - 1.45% from Dreamhost
 - 1.36% from WEBNX.
- 37,284 different networks around the world. With a total of 41,838 networks, we've apparently been attacked during July by 89% of the networks.

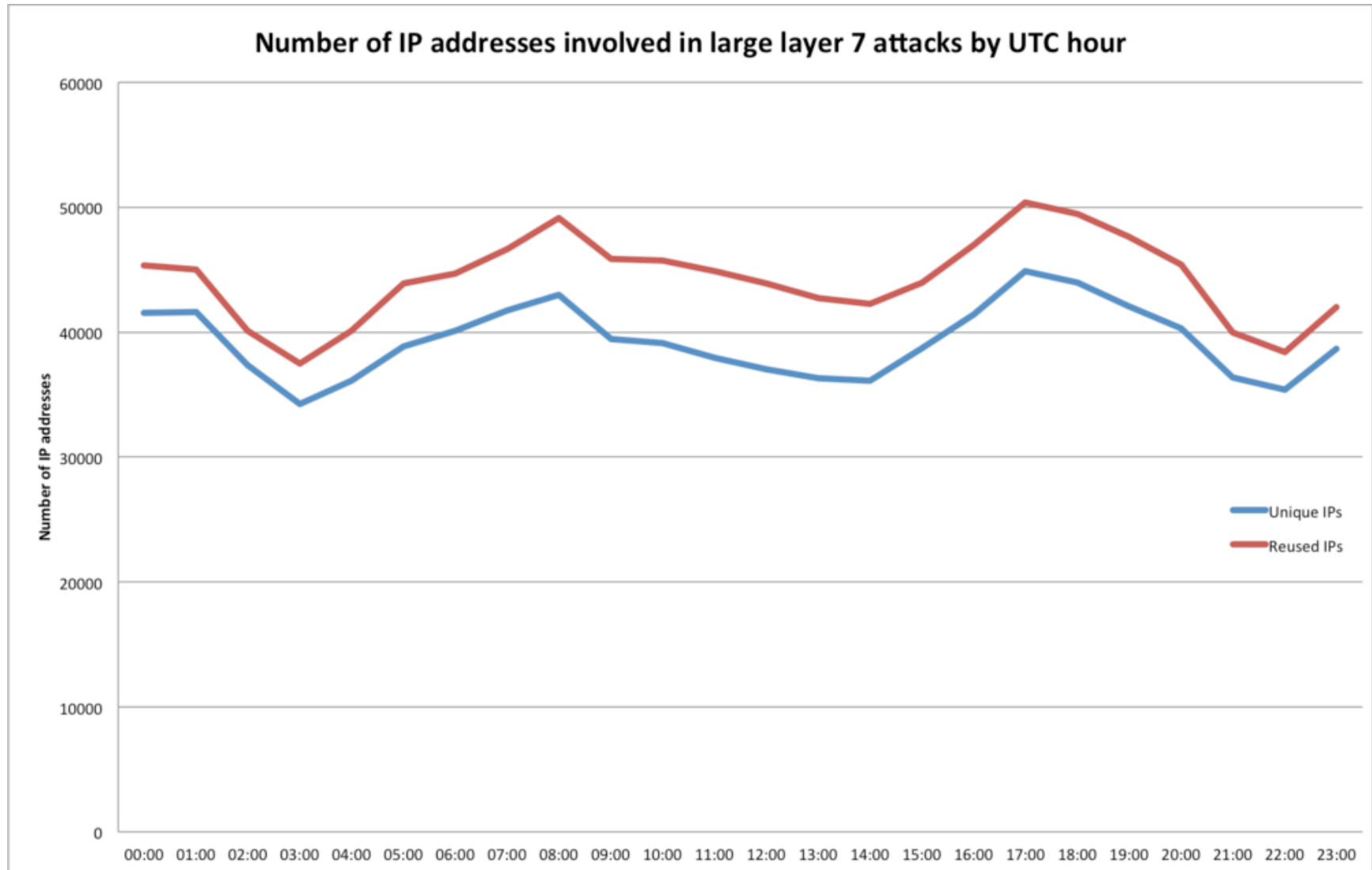
Layer 7 Number of IPs by day of week



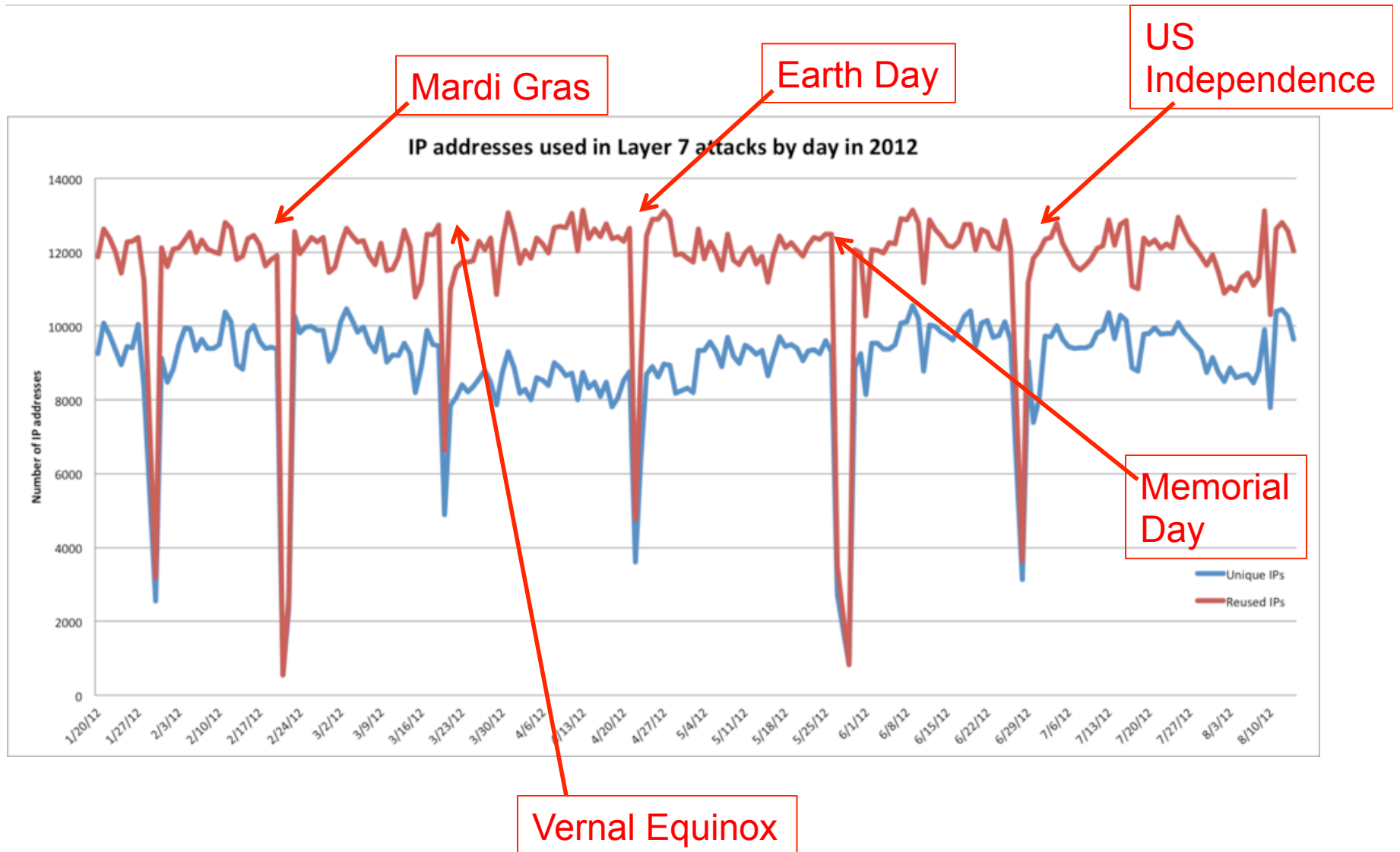
Layer 7 IPs by UTC Hour



Layer 7 IPs in large attacks by UTC Hour



Layer 7 IPs by day



Top countries performing Layer 7 attacks

- 18.34% from US
- 11.47% from China
- 7.88% Turkey
- 6.96% Brazil
- 6.55% Thailand

Not just about botnets

- We don't do a good job of tracking this (yet)
- Four types of attacking forces:
 - Botnets
 - Legitimate servers participating in reflection attack
 - Supporters of campaigns using tools like LOIC
 - Booter web sites

Reflection Attacks

- UDP-based protocols are prone to source IP spoofing
- Use genuine UDP servers on Internet to attack by reflection
 - Send spoofed UDP query to legitimate server indicating source address as the target
 - Legitimate server replies to the query hitting the target
- Works well for DNS and SNMP
 - Saw a 25Gbps SNMP reflection attack from Comcast modems
- Has secondary effect
 - The legitimate servers think the target is attacking them!

Amplification

- A corollary to reflection attacks
- Exploit asymmetry between query and response sizes
- Send small query to many servers that returns a large response
- Can turn small outbound bandwidth into a large attack
- Examples:
 - DNS: Take 64 byte query and return 512 bytes response (8x increase in bandwidth)
 - DNSSEC/EDNS0 makes situation worse because of large response sizes
 - SNMP: Take 100 byte query and return up to the UDP datagram size (theoretically 65k bytes)

Booter Web Sites

- Originally used to 'boot' users off chat and online games
- Repurposed to knock web sites off line
- Buy access on hacker forums
- Usually simple PHP web sites
- The booter uses multiple VPS or other accounts to perform small DDoS attacks

Carpet Bombing

- Attacks come in waves
 - TCP SYN flood against target web server's IP addresses
 - TCP SYN flood against the DNS server for the attacked site
 - DNS reflection attack against the same DNS server
 - Repeat for the rest of the /24

Attack Reasons

- Political/Economic
 - EuroVision Song Contest 2012
 - “Anonymous”
 - Mexican and Russian Elections
 - Government Web Sites
- Extortion
 - Typically against ‘sinful’ business types
 - Gambling Sites
 - Prostitution
- Feuds

An Appeal

- We have lots of data
- We have smart people who can write filters to capture more data
- What should we be doing?
- We need your help

jgc@cloudflare.com