VeriSign®

Recent DNS Reflector Attacks

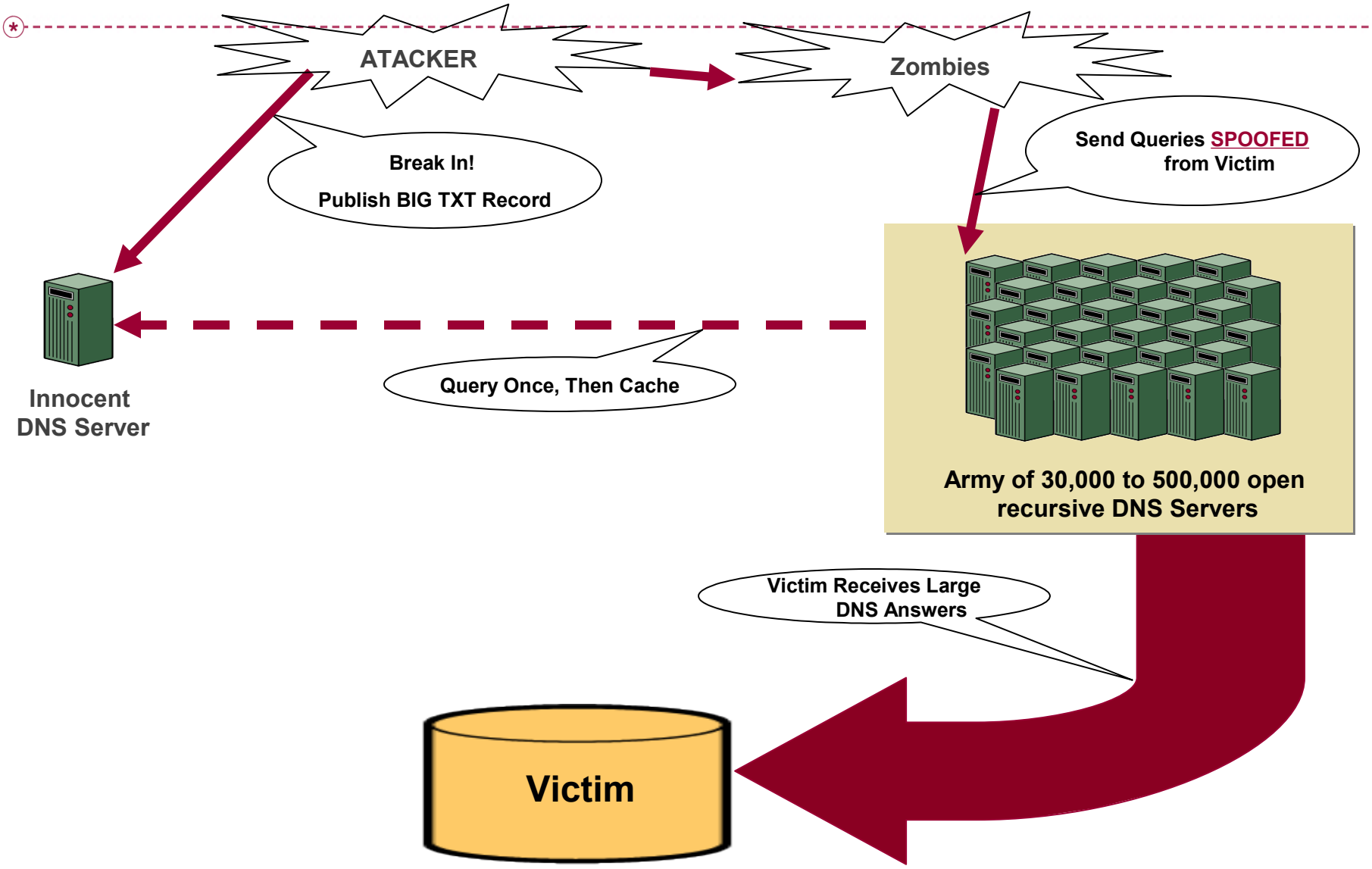
From the Victim and the Reflector POV

Name of Presenter: Frank Scalzo

Date: June 2, 2006

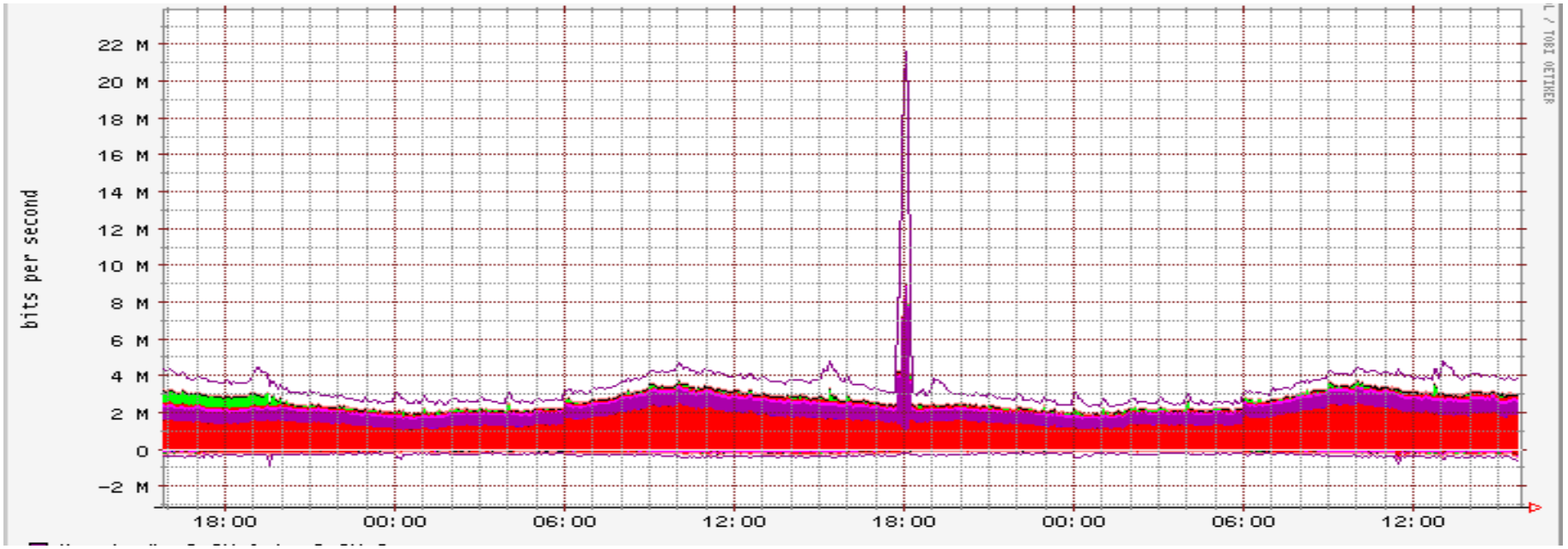
Where it all comes together.™

The Attack


ATACKER
Zombies
Break In!
Publish BIG TXT Record
Send Queries SPOOFED from Victim
Innocent DNS Server
Query Once, Then Cache
Army of 30,000 to 500,000 open recursive DNS Servers
Victim Receives Large DNS Answers
Victim

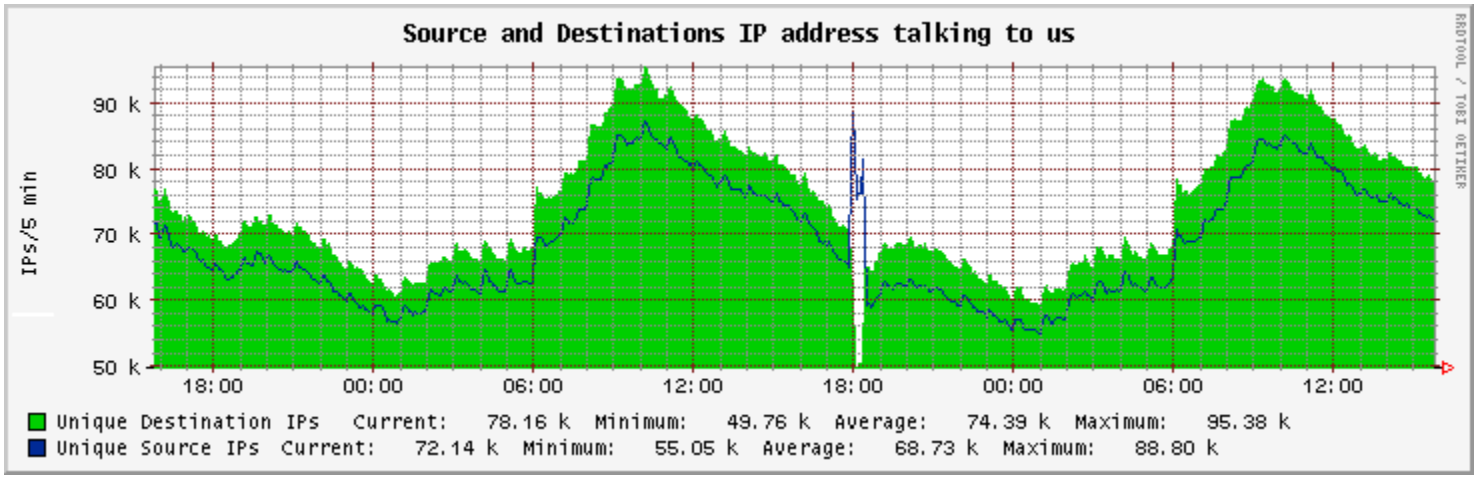
What Does The Victim See?

+ Traffic! Lots and Lots of Traffic!
  - 1 % Netflow sample shows us 22 Mbps, which is 2.2 Gbps
  - 3 Gbps never made it in. > 5Gbps total



What Does The Victim See?

+ What does the Traffic Look Like?
  - DNS Answers for E.TN.CO.ZA
  - 4028 byte answer, the result of a 64 byte query yields 63:1 amplification
  - 34,688 Reflectors



  - TTL histogram on a random sampling shows traffic is not spoofed
  - Analysis of the list of reflectors shows very sequential IP addresses, very likely generated by a sequential scan
  - Random sampling shows the reflectors were open recursive DNS servers

What Does The Victim See?

- 5 Gbps of traffic from 34,688 reflectors is an avg. of 144,142 bps per reflector, which is approximately 13.5 packets per second, and 4.5 DNS answers per second.
- Factoring in 63:1 amplification the avg. reflector was receiving 2,287 bps
- 2 Kbps inbound and 144 Kbps outbound at the reflector is very unlikely to be noticed by the operator of the reflector
- Looking at a capture file during the attack, the top talker of the reflectors was only sending 8.5 DNS responses per second, indicating small standard deviation from the mean

What Does The Victim See?

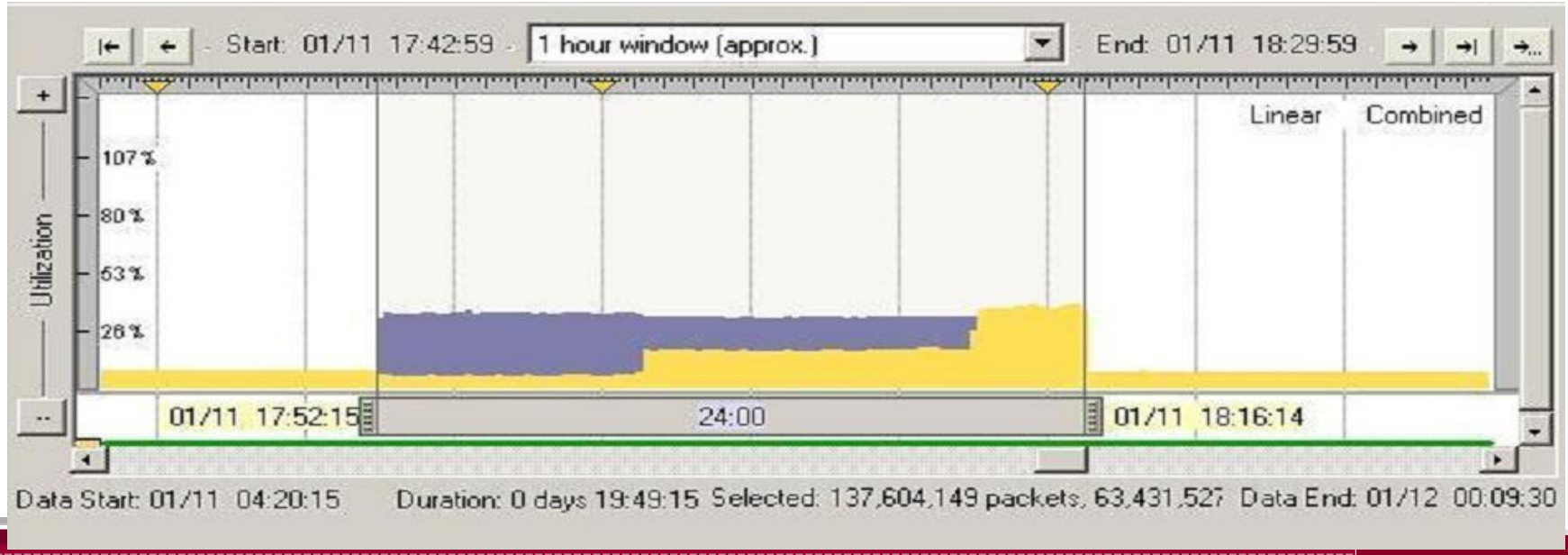
- As a reflected attack there is no visibility into the attacker, but knowing the amplification, and total attack traffic, we estimate that the attacker traffic to the reflectors was only about 79 Mbps

- Working with the appropriate Registry, ISP, and eventually the owner of the DNS server, it was confirmed this DNS server was compromised, and had the TXT record maliciously installed

- The domain had two authoritative DNS servers but only one had been compromised. Looking at the attack traffic 65% of the packets were large DNS answers, 35% were Name Error (NXDomain) responses

What Does The Victim See?

- Because the answer is bigger then the standard Ethernet MTU of 1500 bytes, the answer comes in 3 fragments
- Attacker can set the destination port of the attack by setting the source port of the query sent to the reflectors
- Attack was 24 minutes in duration in three distinct phases - Phase 1: destination port 666, Phase 2: split between ports 666 and 53, Phase 3: all port 53
- Attack is very well controlled; near vertical start, and shift of destination ports, indicating tight command and control



What Can the Victim Do?

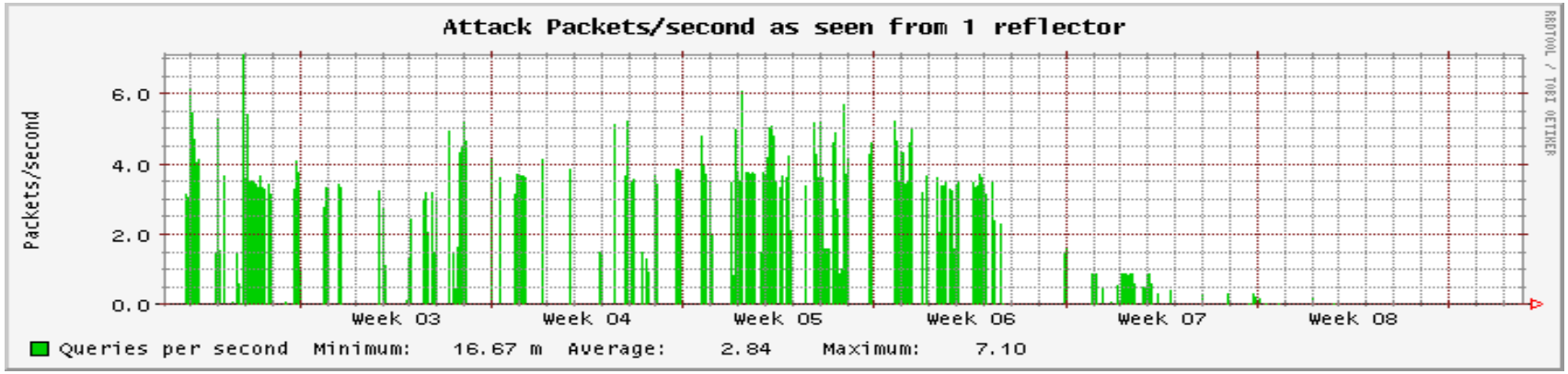
+ Many filtering techniques have been discussed
  - Filter out open Recursive DNS Servers: ACL would be way too big to put on a router, too big to even have a blackhole route-server, and would break 500,000+ DNS servers
  - Limit DNS packet size to 512 bytes, breaks many things!
  - Stop transiting port 53 traffic across the core of the Internet, breaks DNS!
  - Drop fragments toward the victim

What Can the Victim Do?

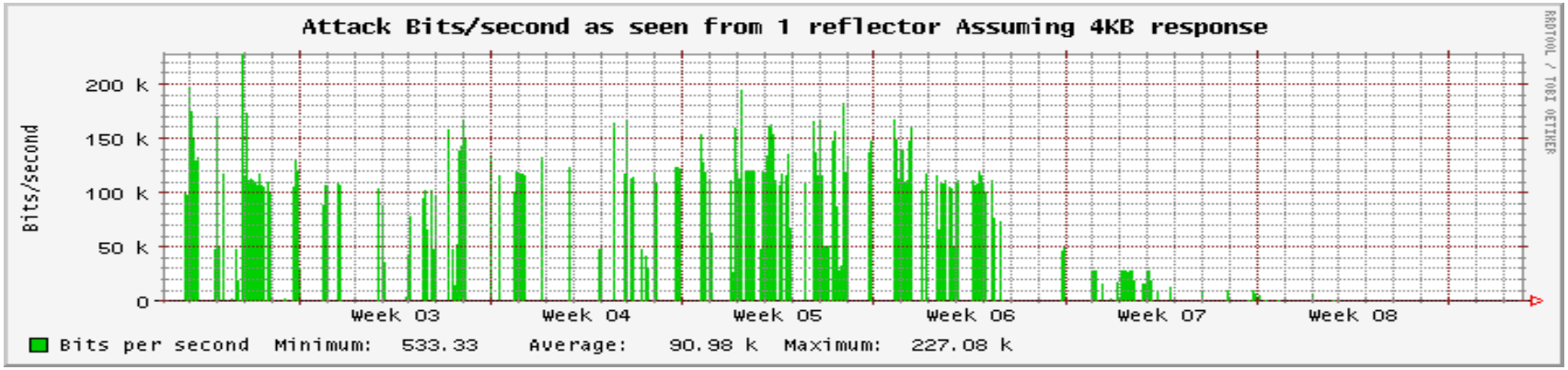
+ Many filtering techniques have been discussed (Continued)
  - Whatever the technique, the ISP has to implement it
  - ISP hardware doesn't always have good filtering features
  - Some ISPs will not filter if they do not see live attack packets, which by the time they are on the phone it is already over
  - Some ISPs will not leave filters in place for long periods of time
  - If the ISP does leave it in place, there is NO visibility into what is happening

What does the reflector see?

- Attack Queries/Second consistent with avg reflector qps #’s

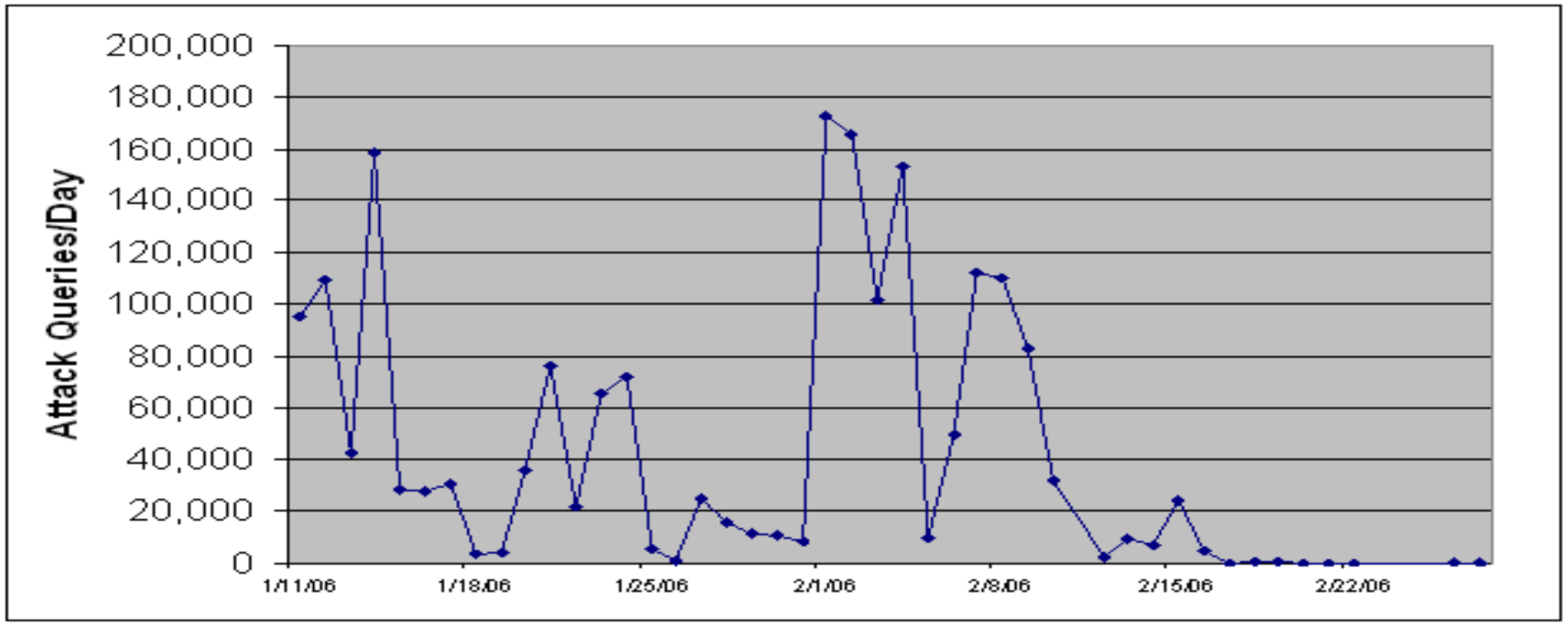


- Assuming 4 KB TXT record we can extrapolate the bandwidth from the reflector, again consistent with avg reflector bps



What does the reflector see?

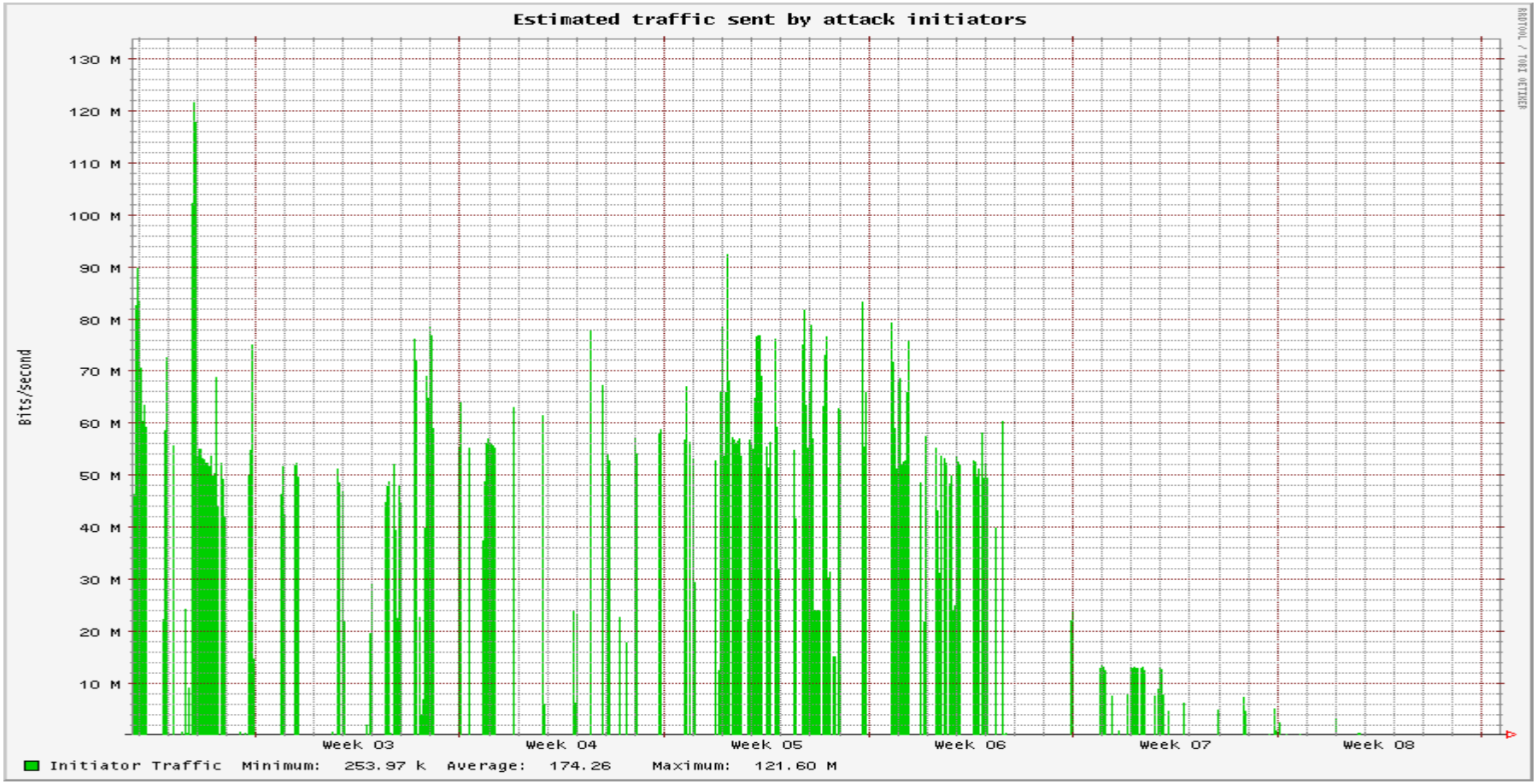
+ Studied a query log off of a reflector from 1/11/2006 – 2/27/2006
  - During that time the reflector sent 1.9 million DNS answers out to 1,593 victims, using 605 different queries to generate answers!



  - After 2/15 massive ramp down, Further study required

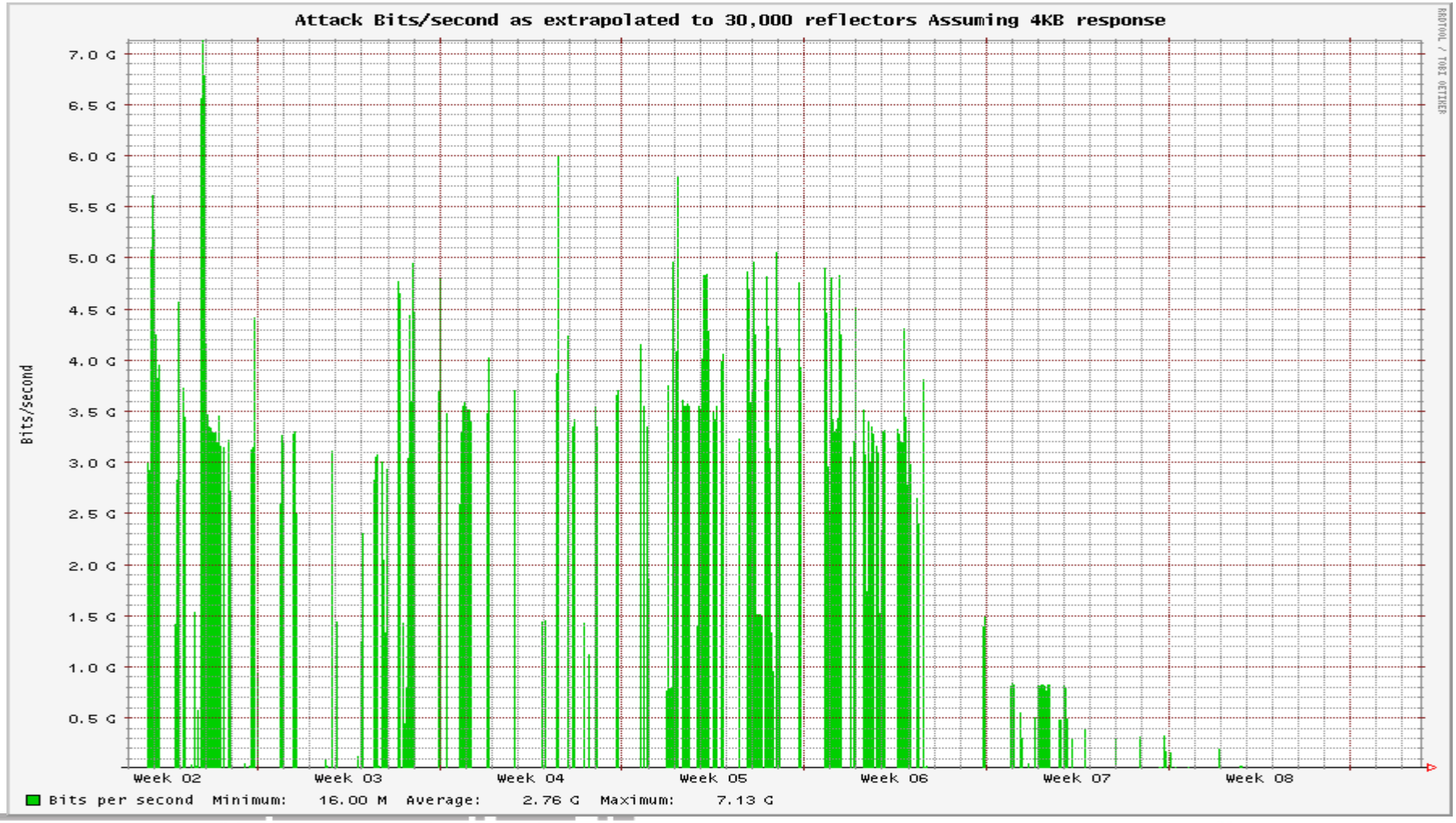
What did the attack initiators send?

- Estimated > 7 Gbps of attack traffic, > 220 Kpps fits with public comments by other organizations; generated with < 130 Mbps



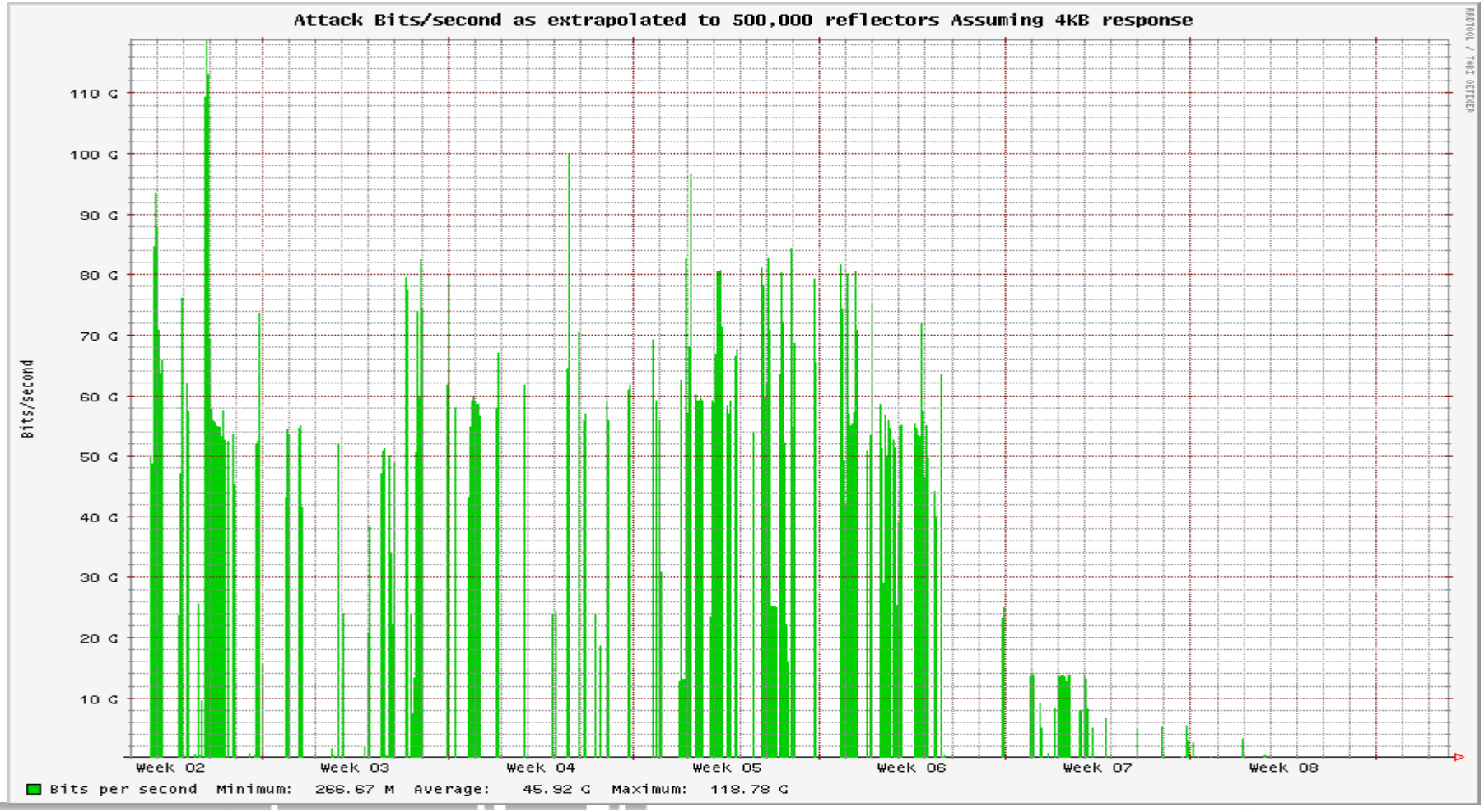
What did the victims see?

- Extrapolate out to 30,000 reflectors we can estimate total attack traffic



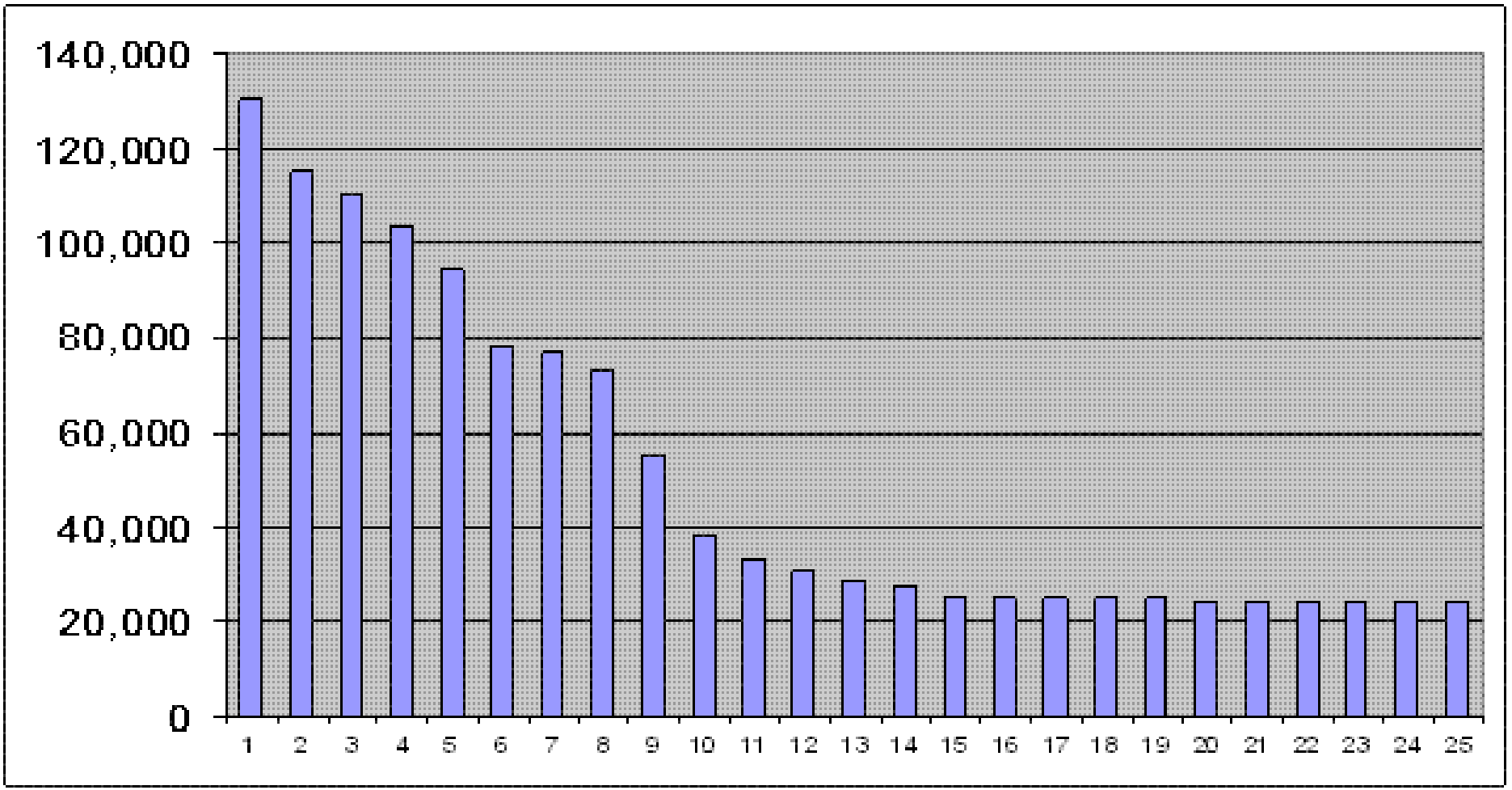
What is the worst that could happen?

- Nightmare potential using 500,000 reflectors, would only require 2 Gbps of initiating traffic to create a 120 Gbps dDos



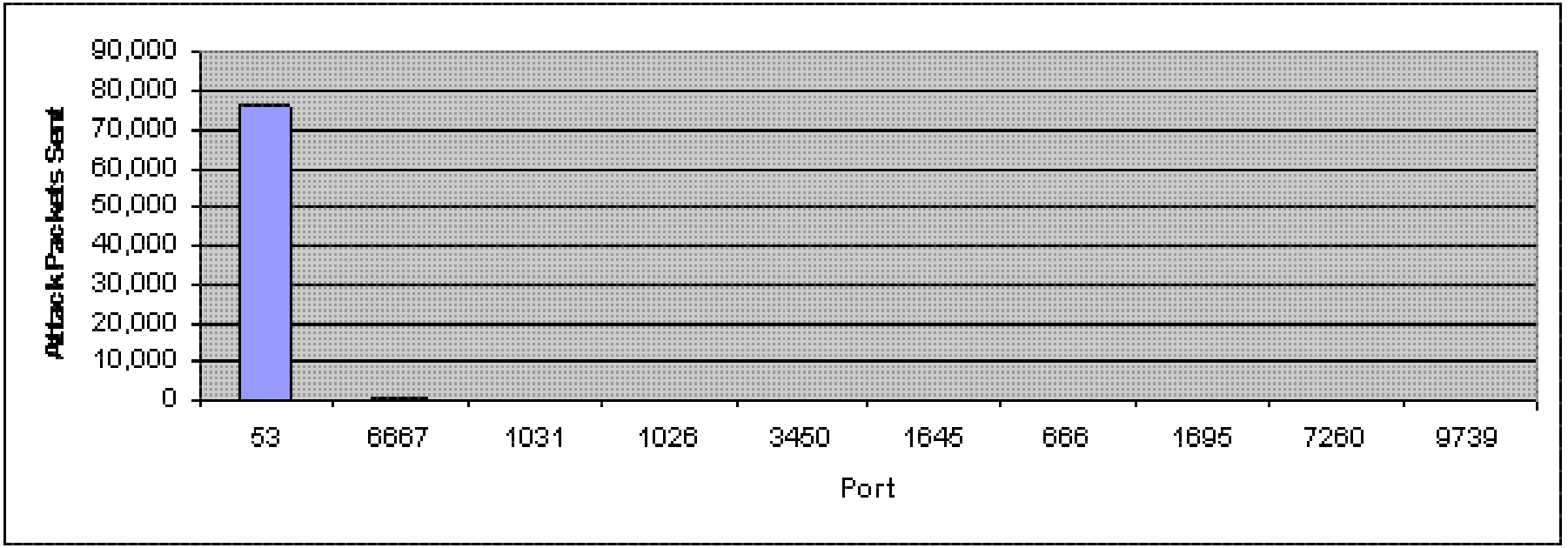
What does the reflector see?

- Queries over the duration to the top 25 Victims



What does the reflector see?

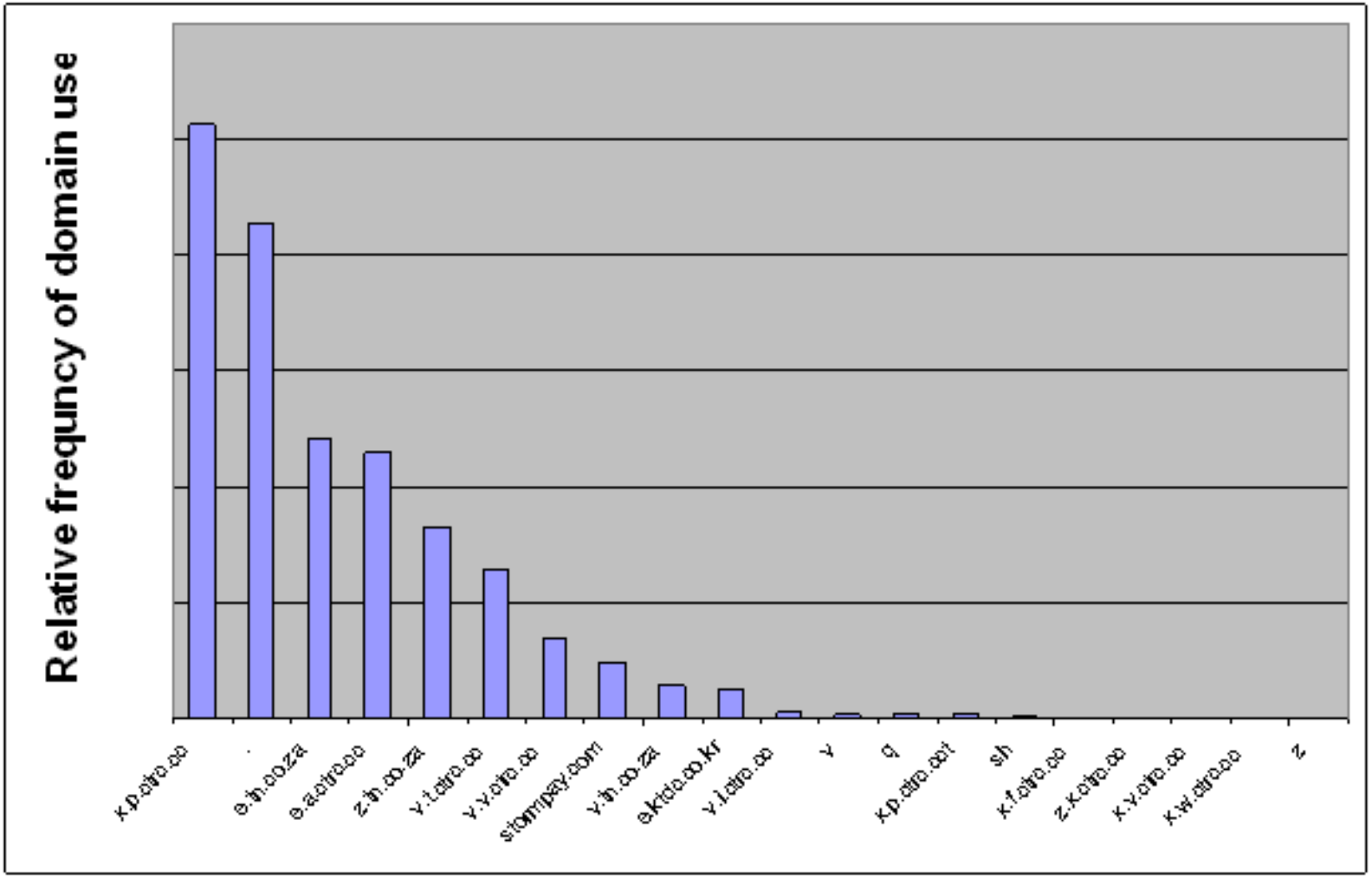
- Top 10 source ports used in the attacks



- 65,461 ports used, Top port is less then 5% of the traffic

What does the reflector see?

- Top 20 domains used to generate traffic



Fundamental Challenges

+ UDP
  - UDP lacks 3 way handshake
  - DNS is a good target because there are so many unsecured DNS servers
  - Other UDP protocols need to be evaluated for small query, large response pairs
    - SIP, NFS, SNMP, Radius, TFTP, NTP, IRIS, RTP
  - Are there really enough reflectors for any of these protocols to be used?

Fundamental Challenges

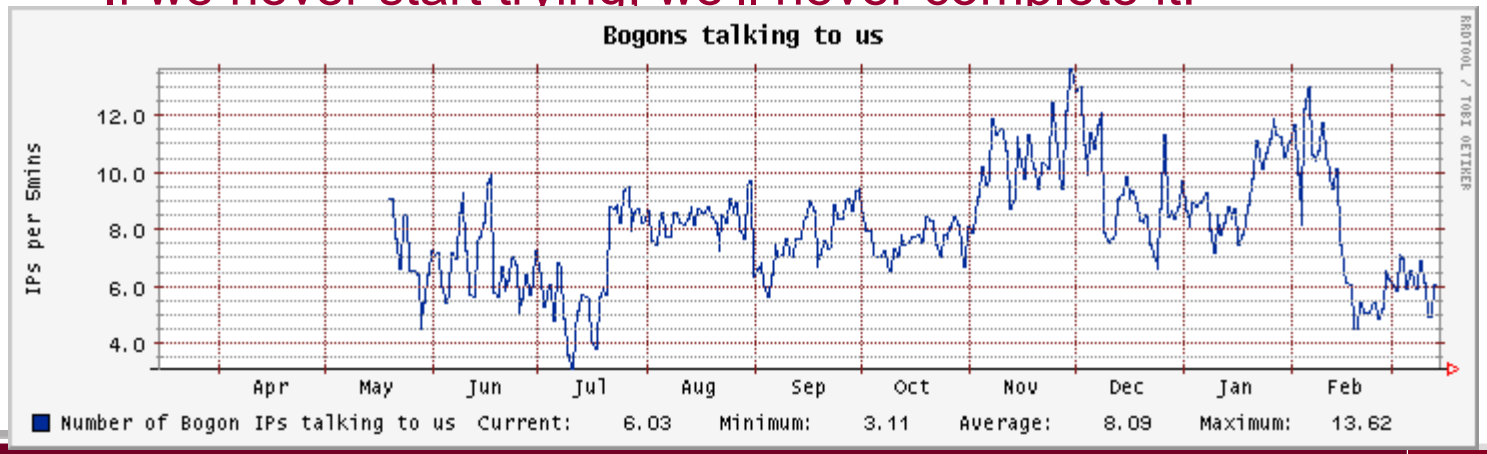
- DNS
  - Estimated >500,000 open recursive DNS servers
  - Poor separation between authoritative and recursive DNS servers
  - Allow-recursion ACL does not prevent server from responding with an already cached record
    - Large commonly cached record could still be used
      - .com/SOA, aol.com/MX, _domainkeys.yahoo.com/TXT
  - DNS servers that allow recursion should not even accept queries from outside (eg. BIND's allow-query ACLs)
  - Some of these are bad code on SOHO routers with DNS proxies
  - More and more we depend on larger records in the public DNS tree
    - RFID, DNSSEC, IPv6, ENUM, Domain Keys, and SPF

Fundamental Challenges

- Beyond Open Recursive DNS servers
  - The root domain (“.”) was used
  - Most authoritative name servers will answer with an upward referral
    - Doesn’t actually include IPs which makes it better, but number of reflectors becomes astronomical and they have to be open

Fundamental Challenges

+ Source Validation
  - IETF BCP 38
  - How do you manage 70,000+ ACL's on 500 routers?
  - What about people who are multi-homed with static routes?
  - What about legacy stuff that has been working that shouldn't?
  - Strict RPF has issues with traffic asymmetry , Loose RPF doesn't help
  - ISPs see the problem as long, hard, and expensive to overcome, and they are right!
  - If we never start trying, we'll never complete it!



Recommended Actions

+ Close Open Recursive DNS Servers
+ DNS Software Vendors should include filtering
+ SOHO Routers With Better DNS Proxy Code
+ BCP 38

VeriSign®

Questions?

Where it all comes together.™