DDOS

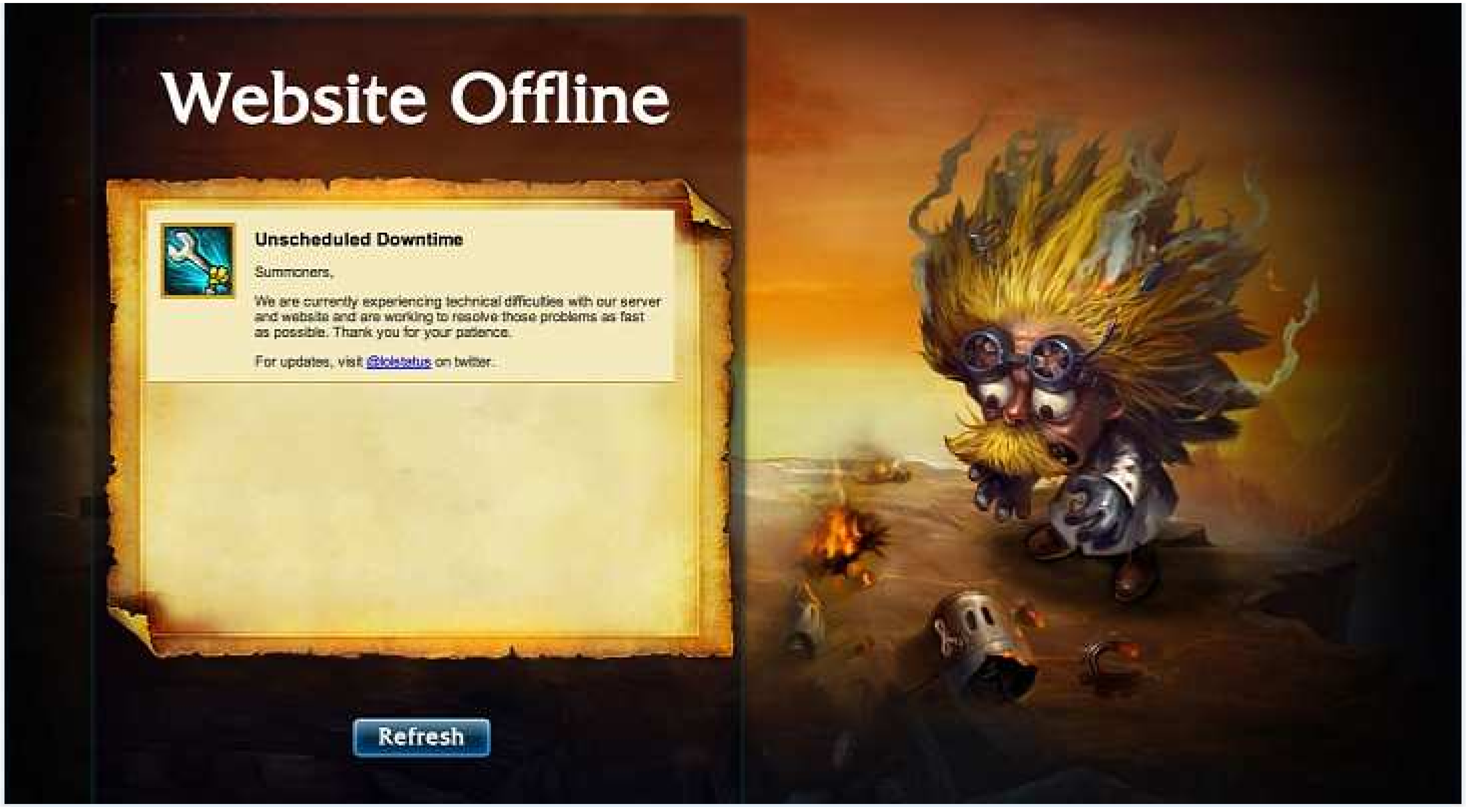
Marc Lampo - Principal Security Consultant

Telenet for Business

December 31st, 2013, 06:52 GMT · By Andrei Dobra

BLOG

Hackers Take Down Battle.net, EA, League of Legends, and World of Tanks in DDoS Attacks



Website Offline

Unscheduled Downtime

Summoners,

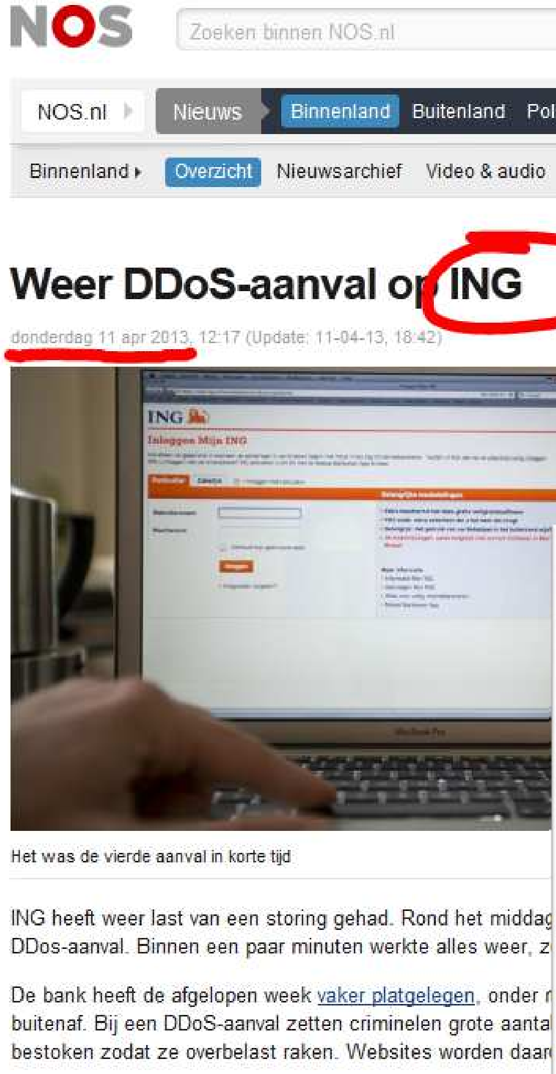
We are currently experiencing technical difficulties with our server and website and are working to resolve those problems as fast as possible. Thank you for your patience.

For updates, visit @lolstatus on twitter.

ENLARGE - *League of Legends was offline for a period*

A new hacker group called DERP has just taken down a variety of gaming targets, from Blizzard's Battle.net online services, to the Electronic Arts website, the World of Tanks one, or League of Legends in massive DDoS attacks apparently aimed at a single user.

200% increase of DDOS attacks in 1 year!



NOS

Zoeken binnen NOS.nl

NOS.nl | Nieuws | Binnenland | Buitenland | Politiek | Economie | Opmerkelijk | Sp

Binnenland | Overzicht | Nieuwsarchief | Video & audio | Journaal 24 | Politiek 24 | Dossiers

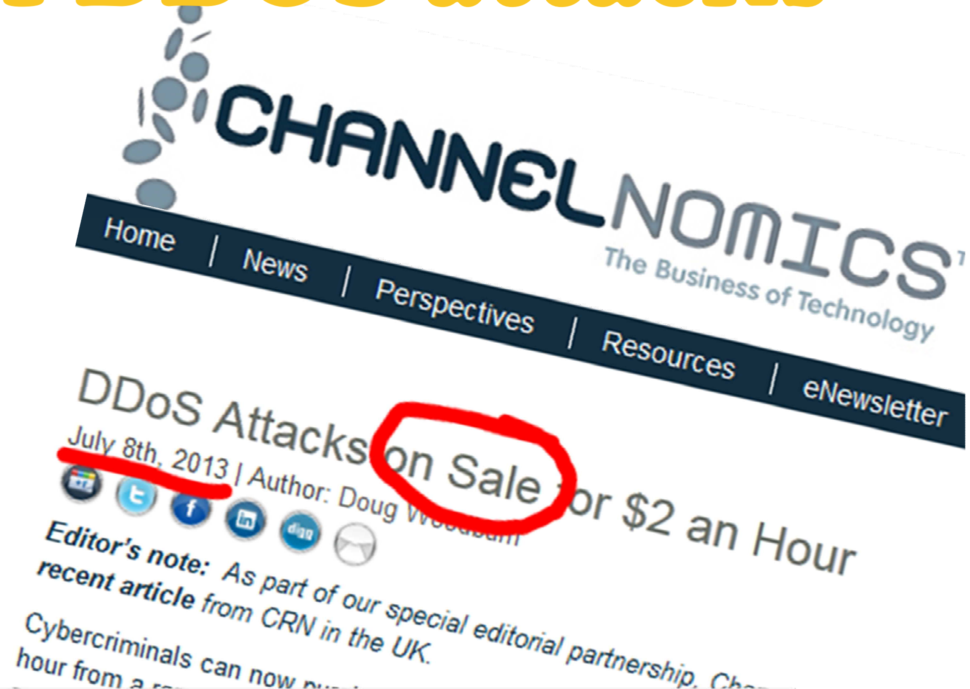
Weer DDoS-aanval op ING

donderdag 11 apr 2013, 12:17 (Update: 11-04-13, 18:42)

Het was de vierde aanval in korte tijd

ING heeft weer last van een storing gehad. Rond het middag
DDos-aanval. Binnen een paar minuten werkte alles weer, z

De bank heeft de afgelopen week vaker platgelegen, onder r
buitenaf. Bij een DDoS-aanval zetten criminelen grote aanta
bestoken zodat ze overbelast raken. Websites worden daar



CHANNELNOMICS
The Business of Technology

Home | News | Perspectives | Resources | eNewsletter

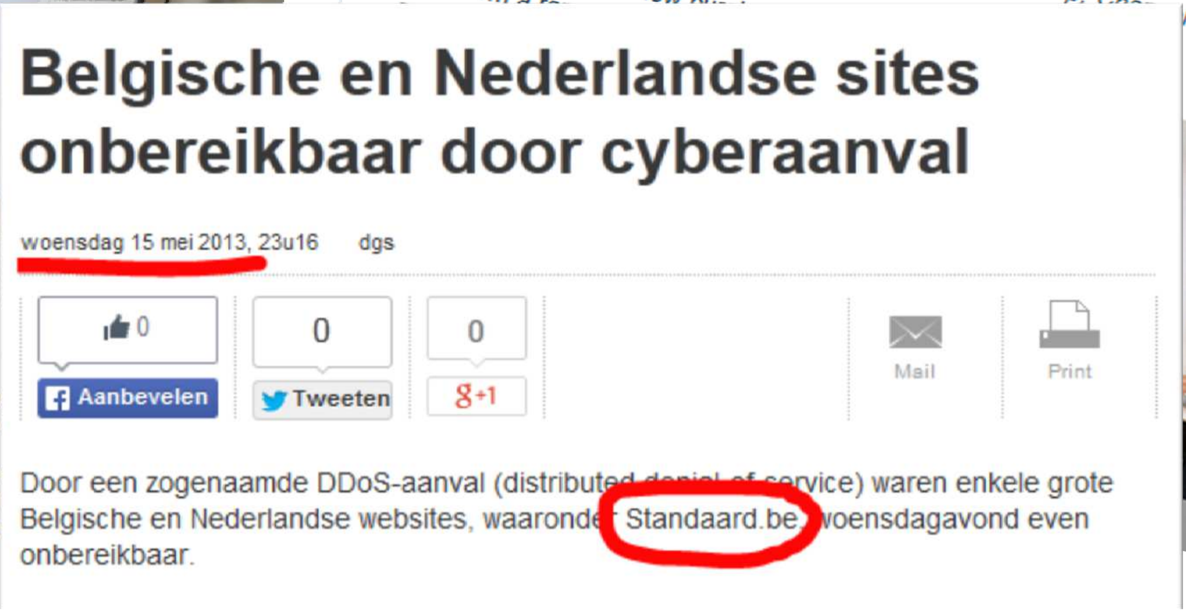
DDoS Attacks on Sale for $2 an Hour

July 8th, 2013 | Author: Doug Woodburn

Editor's note: As part of our special editorial partnership, Cha… **recent article** from CRN in the UK.

Cybercriminals can now pu…
hour from a …

…nomics is publ…



Belgische en Nederlandse sites onbereikbaar door cyberaanval

woensdag 15 mei 2013, 23u16 dgs

Door een zogenaamde DDoS-aanval (distributed denial of service) waren enkele grote Belgische en Nederlandse websites, waaronder Standaard.be, woensdagavond even onbereikbaar.

DDOS what?

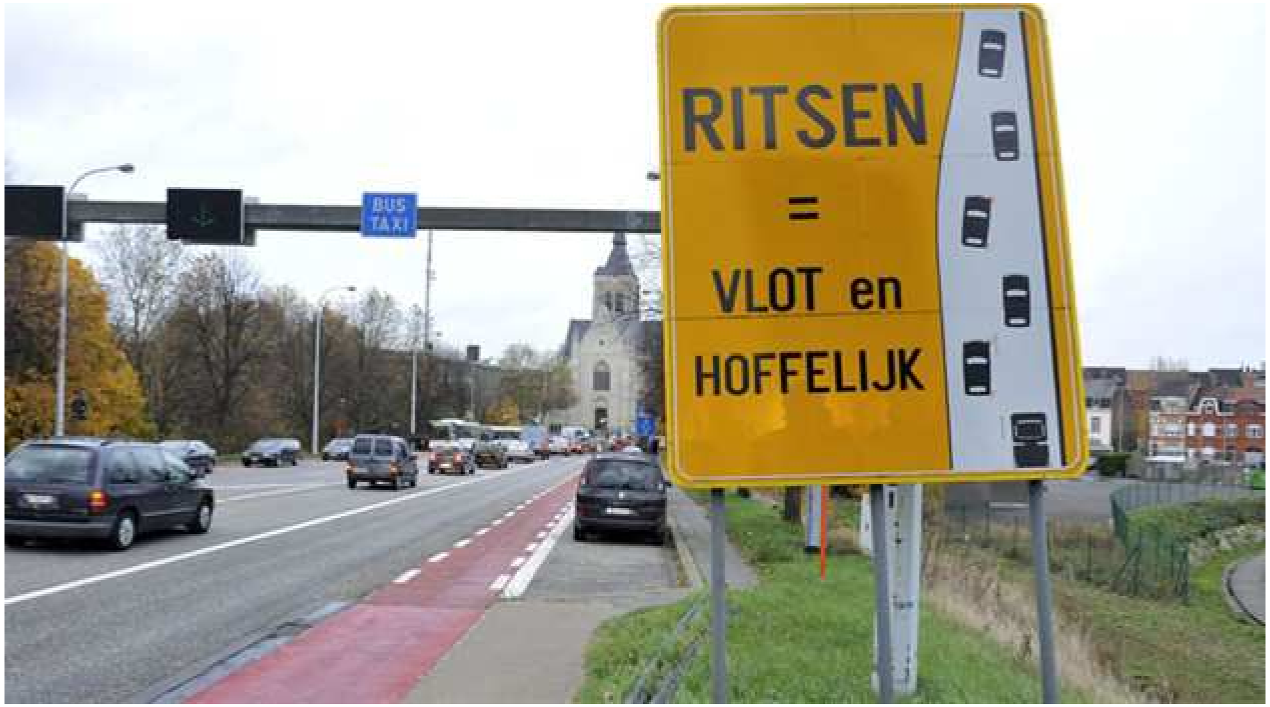
“A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.”

(Source: wikipedia)

Agenda

- Desired traffic (or too much of it)
- Undesired traffic (or too much of it)
- Traffic with protocol errors
- Conclusion

Desired traffic



Too much desired traffic

- Examples
  - HTTP GET (flood) for a big page
    in Q4 2013 : ~20% of DDOS attacks
    (source : Prolexic Q4 2013 DDOS attack report)
  - HTTP POST (flood) to attack
    the servers processing capabilities
  - (too frequent) SSL Key renegotiations

Too much desired traffic

- The organisation offers a number of services to Internet users
  - The firewall allows the traffic
  - The service is ready for clients
  - A load balancer for redundancy

  But the attacker generates
  a lot more than expected/normal
  amount of queries to those services

Too much desired traffic

- Attacks :
  - Firewalls : CPU / connection table
  - Server load balancers
  - Servers : CPU / backend
  - (Outgoing) bandwidth

Too much desired traffic

- Mitigation :
  - Grab control – do not believe the client
    - Impose limits in the application
    - Let the load balancer exercise control
    - Deny access based on geo-location

Undesired traffic

Too much undesired traffic

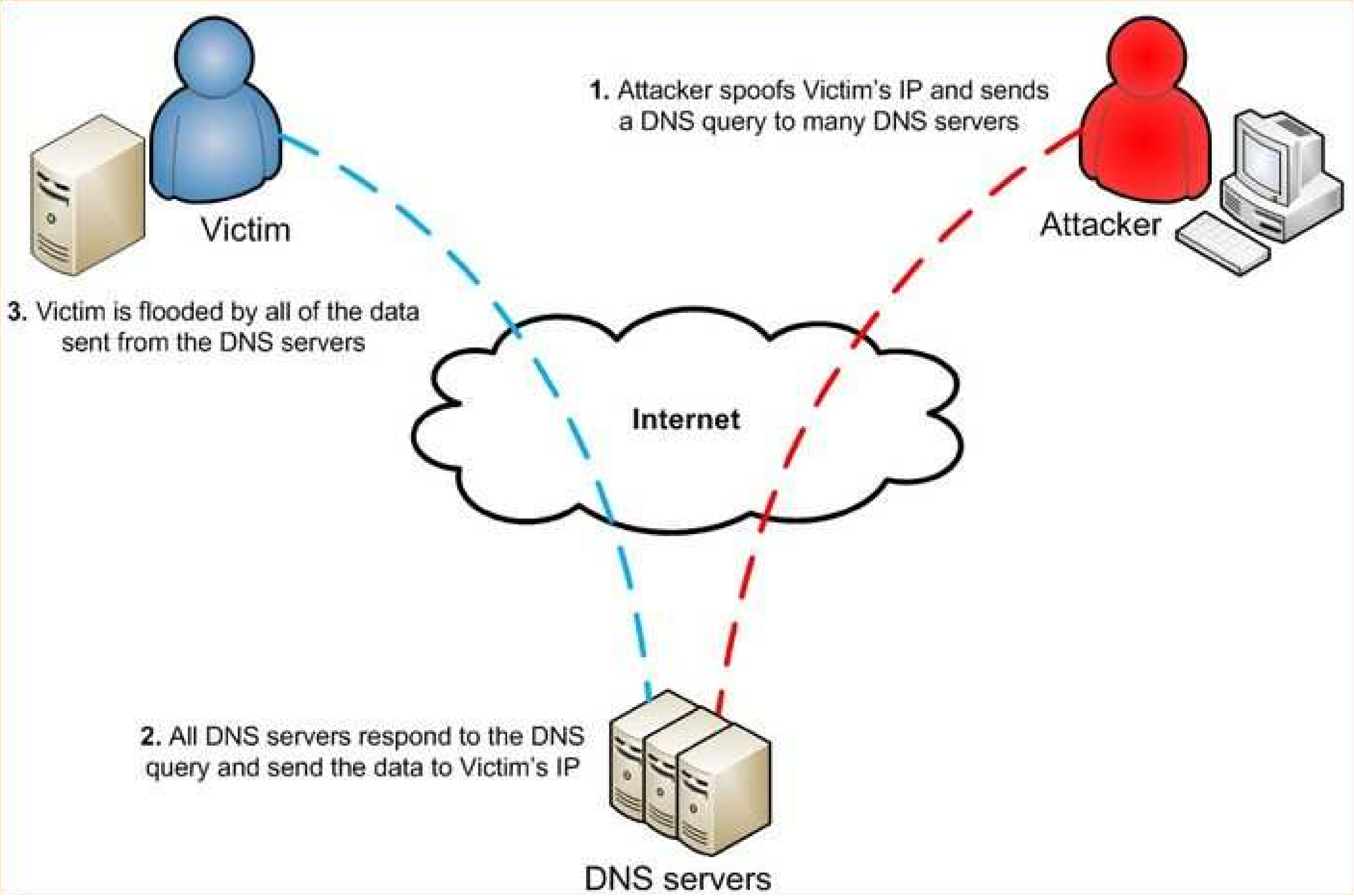
- The attacker generates a **lot** of traffic towards an organisation

- Traffic that is
  - not expected
  - nor desired
  - nor allowed

Too much undesired traffic

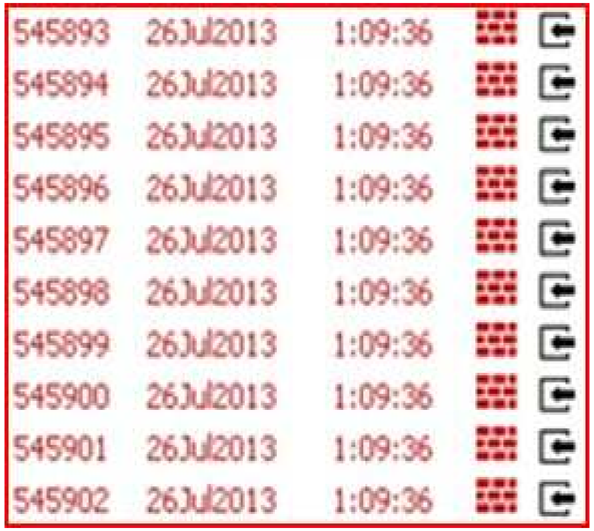
- Examples
  - DNS amplification attack
    - The most popular in this category
    - Can achieve a multiplification factor of 50 :
      - ~80 bytes input → ~4100 bytes output
      - 100 infected PC's sending 1Mbps each → 5Gbps for the victim
    - Responsible for largest volumetric attacks detected so far
  - Others : chargen and (lately) NTP

Too much undesired traffic

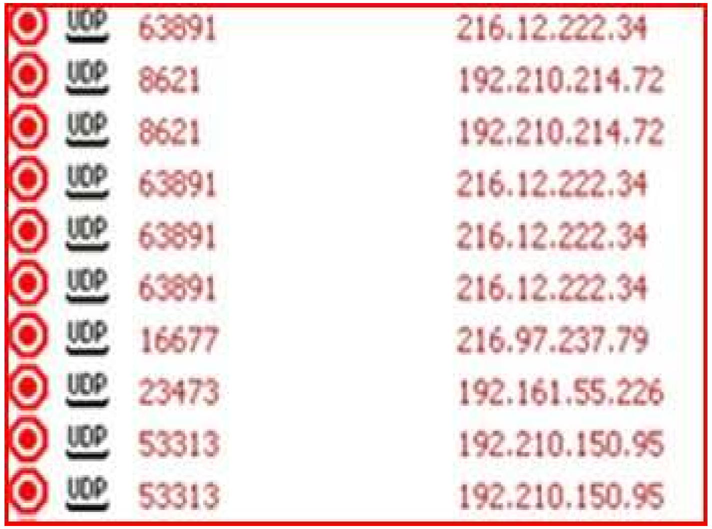


Victim
1. Attacker spoofs Victim's IP and sends a DNS query to many DNS servers
Attacker
3. Victim is flooded by all of the data sent from the DNS servers
Internet
2. All DNS servers respond to the DNS query and send the data to Victim's IP
DNS servers

The result ...



```
545893   26Jul2013   1:09:36
545894   26Jul2013   1:09:36
545895   26Jul2013   1:09:36
545896   26Jul2013   1:09:36
545897   26Jul2013   1:09:36
545898   26Jul2013   1:09:36
545899   26Jul2013   1:09:36
545900   26Jul2013   1:09:36
545901   26Jul2013   1:09:36
545902   26Jul2013   1:09:36
```



```
UDP   63891          216.12.222.34
UDP   8621           192.210.214.72
UDP   8621           192.210.214.72
UDP   63891          216.12.222.34
UDP   63891          216.12.222.34
UDP   63891          216.12.222.34
UDP   16677          216.97.237.79
UDP   23473          192.161.55.226
UDP   53313          192.210.150.95
UDP   53313          192.210.150.95
```

During 25 minutes,
exclusively red lines in the log (+2M),
no business traffic possible!

Too much undesired traffic

- Attacks :
  - Incoming bandwidth
    - Destination IP does not matter !
  - Firewalls : CPU
    - DNS amplification results in a lot of fragments

Too much undesired traffic

- Popularity (Prolexic) :
  - DNS : 9,58%
    - UDP fragment : 17,11%
    - So, DNS amplification : ~25% ?
  - Chargen : 6,39%
  - NTP : 0,26%
- Volumetric attacks are
  the most frequent types of DDOS

Too much undesired traffic

- Mitigation :
  - Prevent undesired traffic from being sent over your Internet connection
    - Talk to your ISP :
      - Have a plan for assistance
    - Mitigate *in the cloud* :
      - Prolexic can announce your addresses and receive all traffic.
        Then clean it and send only clean traffic.

Protocol errors

Traffic with protocol errors

- Examples
  - Slowloris
    - TCP based
    - Unexpected behaviour
    - Sends valid request, but **s…l…o…w…l…y…**
  - Optimistic ACK (Prolexic : 2,81%)
    - TCP based
    - Protocol error
    - Attacker sends ACK for data not yet received

Traffic with protocol errors

- The attacker generates traffic - need not even be : high volume - that contains
  - unexpected behaviour
  - low level protocol errors
- Abuses the fact that partners in a TCP communication have too much trust : **TCP != secure**

Traffic with protocol errors

- Mitigation :
  - Firewall should prevent protocol errors
    - At what effort ? (CPU cycles ...)
  - Internal IDS/IPS can detect/prevent
    - More focussed (traffic already allowed)
  - Anti-DDOS appliance in front of firewall
    - Focuses on abnormal behaviour
    - Dynamically adjusts filters
    - Takes stress away from the firewall layer

Conclusion

Globally three flavours of DDOS

- Too much desired traffic
- Too much undesired traffic
- Traffic with protocol errors

But you are not without defences !

hp

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

paloalto
NETWORKS
the network security company™

telenet

Barracuda

MobileIron®

VASCO®
THE AUTHENTICATION COMPANY

PROLEXIC
DDoS Attacks End Here.

TREND MICRO
Silver Accredited Partner

f5®