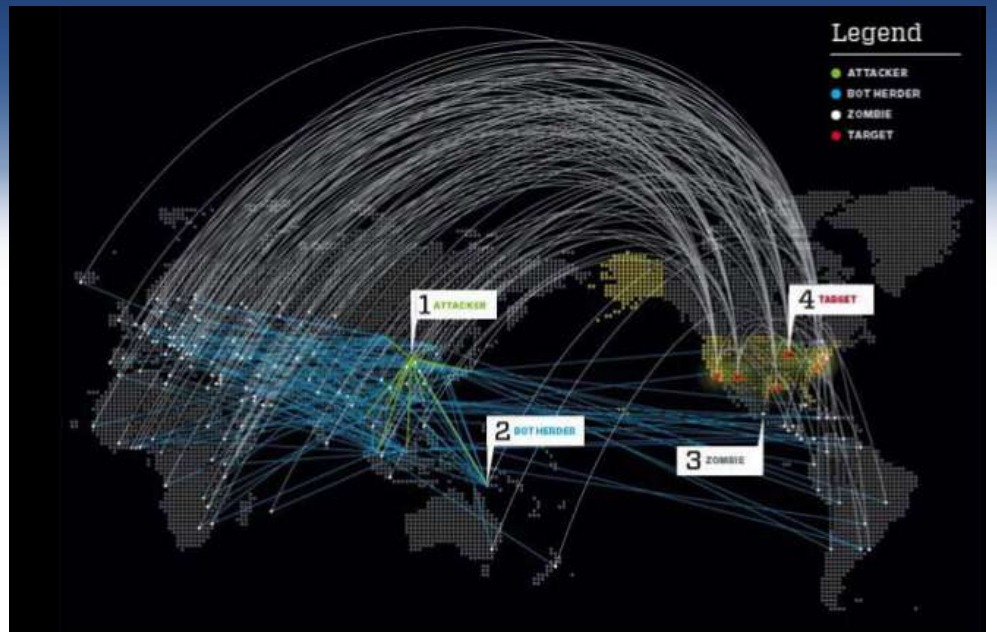
NBS System

"Grow your business safely"



DrDOS, reloaded

OSSIR

Managed Hosting & Security

www.nbs-system.com

Qui ?

- Philippe Humeau, D.G de NBS System
- Sécurité et tests d'intrusion depuis 1999
- Infogérance de serveurs depuis 2005
- 1000+ sites
- 600+ serveurs

Comment ?

- DRDOS = Distributed Reflection Denial Of Service
- Concept décrit en Juillet 2002 par Tom Vogt
- Une faille du protocole Quake 3 permet d'envoyer à une cible 3 fois de paquets que ce que l'on "investit"
- Reflection car l'attaque repose sur un protocole UDP spoofable
- A l'époque, en 2002, on compte ~15 000 serveurs de jeu public
- Jamais réellement exploité à cause du faible effet de levier

- L'attaquant est, pour ainsi dire, indétectable, sauf si l'on a le concours des administrateurs des serveurs de jeu utilisés

À partir de 1 Gb/s, nous parlons déjà un gros problème

Pourquoi ?

- Du 7 au 10 octobre, RIM (blackberry) est probablement victime d'une DrDOS
- Le 11 octobre 2011, NBS System est victime d'une attaque de DrDOS (7 Gb/s)
- Le 12 octobre 2011, NBS System publie un article sur la DrDOS après analyse
- Mi octobre Gandi connait une DrDOS (50 Gb/s)
- Mi octobre, plusieurs sites clefs, dont certains étatiques, sont visés
- Depuis, les sites et hébergeurs ayants gouté aux joies de la DRDOS sont nombreux, Facebook, Nerim, Typhon, etc.

- Les attaques ont varié en débit de 6 Gb/s à plus de 50 Gb/s…

À partir de 1 Gb/s, nous parlons déjà d'un gros problème

Comment ?

- DRDOS v2 :
  - 2011 : plusieurs dizaine de milliers de serveurs de jeu, plus proche de 100 000 que de 15 000
  - L'attaque permet maintenant un ratio de 50 à **70:1** selon le protocole
  - Plusieurs jeux sont disponibles : COD4, Q3, Valve, Halflife, Gamespy
  - Un attaquant avec une liaison **ADSL de particulier** peut aligner un flux de **70 Mb/s**
  - Un serveur **OVH à 30 €** par mois permet d'envoyer **5 à 7 Gb/s** de flux

<u>La magnitude est incomparable et les dégâts colossaux :</u>

- A partir de 1 Gb/s, des problèmes d'infrastructure se pose à toute société et petit hébergeur
- A partir de 5 Gb/s, des problèmes d'infrastructure se posent à des hébergeurs moyen (Nerim, NBS, Typhon, etc.)
- A partir de 10 Gb/s, les grands sont susceptibles de tomber (Gandi)
- A partir de 50 Gb/s, les opérateurs Tiers 1 sont dans le rouge vif, au mieux
- A partir de 150 Gb/s, certains points clefs d'Internet, comme les DNS, peuvent être balayés de la carte

NBS System
"Grow your business safely"

Comment ?

Proof of concept

Pour le cas de Quake 3, il est très simple de faire une démonstration :

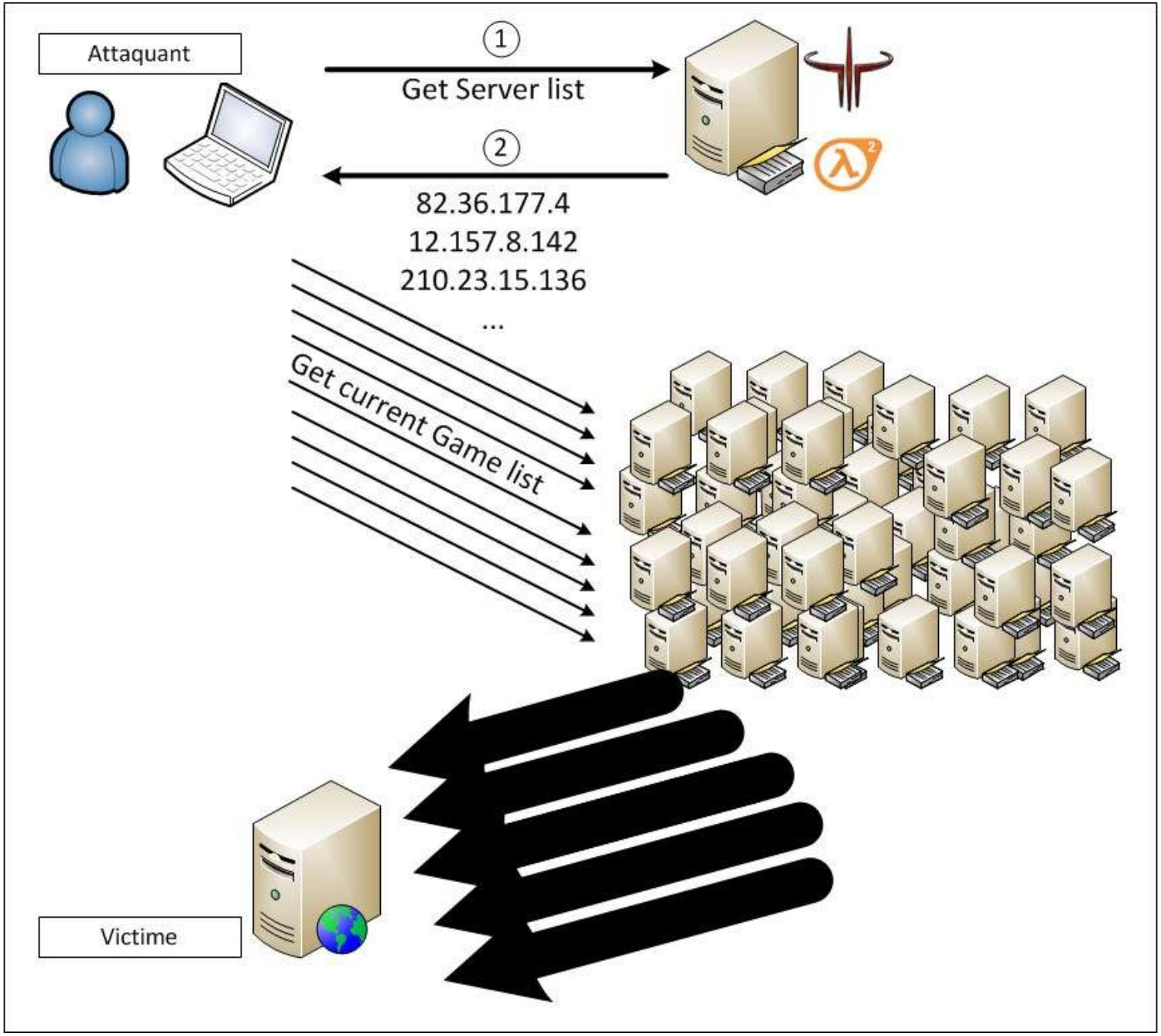
echo 'FF FF FF FF 67 65 74 73 74 61 74 75 73 0A' | xxd -r -p - > ./q3payload

14 octets

hping3 -2 -E ./q3payload -d 14 -c 1 --destport 27960 -a <IP victime> <Q3 server>

et l'on constate que la réponse du serveur fait de ~700 à **~1000 octets**.

Don't do this at home !


Attaquant
1
Get Server list
2
82.36.177.4
12.157.8.142
210.23.15.136
...
Get current Game list
Victime

Que faire ?

Temporairement :

- Mettre une Null route sur l'IP attaquée (efficace mais coupe le système ciblé)
- Demander à l'ISP des réseaux où sont hébergés les serveurs de jeux les plus agressifs de les couper (long et peu efficace)

Définitivement :

- Demander aux éditeurs de jeux vidéo de patcher leur protocoles de handshake
  - Peu crédible, tout particulièrement pour les jeux qui ne sont plus supportés (ex : Quake 3)
- Demander aux hébergeurs de serveurs de jeux de limiter les requêtes par seconde à destination d'une IP avec Iptables –m limit par exemple
  - Complexe à imposer, trop technique pour la plupart
  - Soucis des cybercafé et IP de Nat

Que faire ?

La seule vraie solution

- Extrêmement technique & complexe

  permit ip <%MY_CIDR_BLOCKS%> any
  deny ip any any

- Les ACL sont traité en INGRESS par préfix (pas de traitements L4-L7)

- Ça ne verra jamais le jour car
  - C'est trop complexe techniquement ☺
  - Surtout, les Tiers 1 facturent le transit montant et n'ont pas intérêt à l'arrêter donc !

Ce qui va se passer (probablement)

- La DrDOS sera toujours possible pendant plusieurs mois
- Tant qu'un gros évent de sécurité n'aura pas eu lieu
- Ou tant que la nuisance ne sera pas assez « lourde » pour imposer le changement

- Rien ne laisse penser que le phénomène s'endiguera de lui-même sans l'un ou les deux facteurs précédents, Null router une IP est tellement plus simple…

- La DrDOS va s'installer durablement dans le paysage, « expect shit storm »

Un scénario d'apocalypse le DDrDOS

- Une DrDOS distribuée à travers un outil de type LOIC
- Utilisant plusieurs milliers de connexions sources
- Plusieurs milliers de serveurs cibles
- Un trafic entrant sur les serveurs agrégé ainsi peut atteindre plusieurs Gb/s
- La réflexions atteindra sont maximum, à travers 30 000 serveurs par exemple
- Qui renverrons chacun plusieurs dizaines de mégabits par seconde, au minimum
- Soit plus d'un térabit par seconde…
- Si les IP ciblées changent assez vite, toute les 5 minutes par exemple, l'attaque ne peut être arrêtée par un nul routage

- Aucune infrastructure ne peut tenir cela dans le monde. Si un tel trafic doit être routé, les routeurs BGP de tête vont tout simplement flancher et le trafic global d'Internet avec.

(les plus grosses DDOS clearance facility annoncent pouvoir traiter de 70 à 120 Gb/s)

Webographie

Attaque originale :

http://www.lemuria.org/security/application-drdos.html

Attaque publiée :

http://pastebin.com/SpiDgR0n

Principe de fond :

http://palisade.plynt.com/issues/2006Apr/ddos-reflection/

Merci pour votre attention !

www.nbs-system.com
Telephone : +33.1.58.56.60.86
Mail : phu@nbs-system.com

Nous hébergeons
De manière optimisée
De manière sécurisé

Nous testons
De manière professionnelle
En boite noire, grise, blanche