



Registrarseminar 2013

Oslo, NO

wed, december 4th, 2013

Marco Davids

“The accidental hacker”

DNS Amplification

Norid registrar seminar 2013



Pleased to meet you!

Personalia:

- Marco Davids
- Technical Advisor @ SIDN



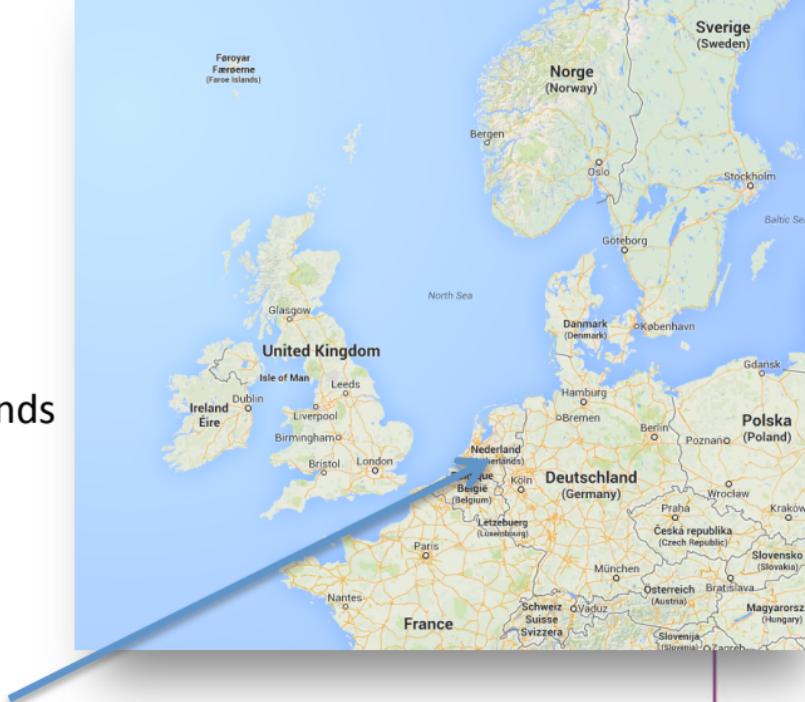
: @marcodavids





SIDN

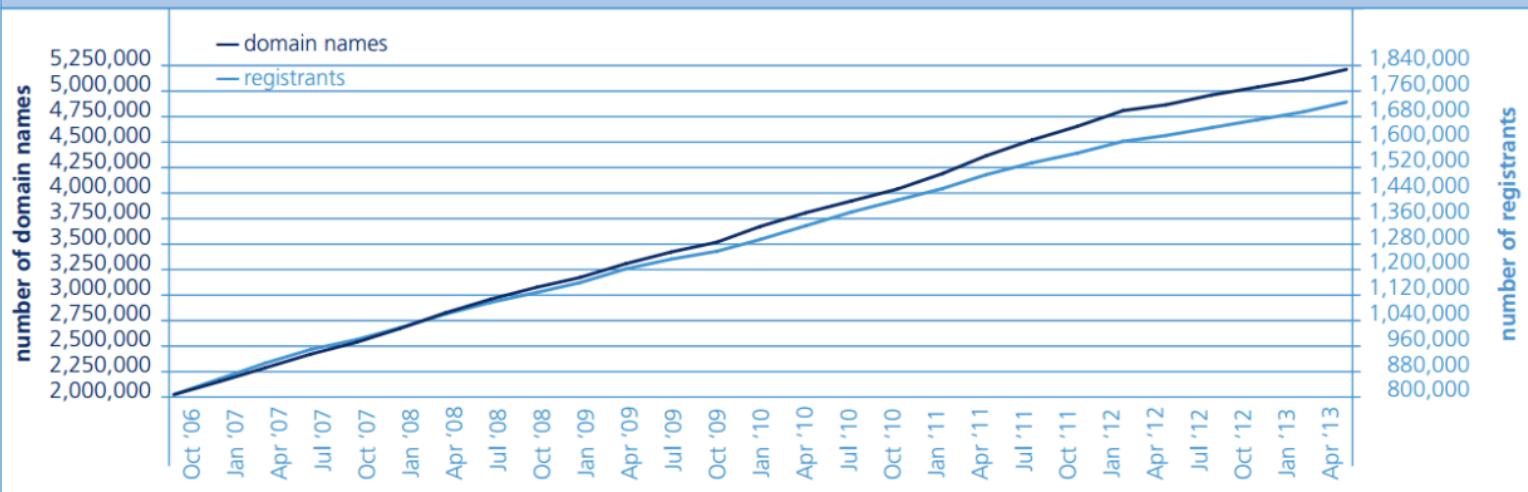
- Registry for .nl ccTLD
- Based in Arnhem, the Netherlands



SIDN labs
Internet Research & Innovation

SIDN

Number of .nl domain names and registrants



Early December 2013: **5.377.690** domain names (**1.673.979** DNSSEC, >30%)
 ~30 domain names per 100 inhabitants
 7th TLD, after .com, .de, .net, .uk, .org and .info

- Introduction
- Case study (just an example)
- Modus operandi of DNS amplification
- Countermeasures

Introduction

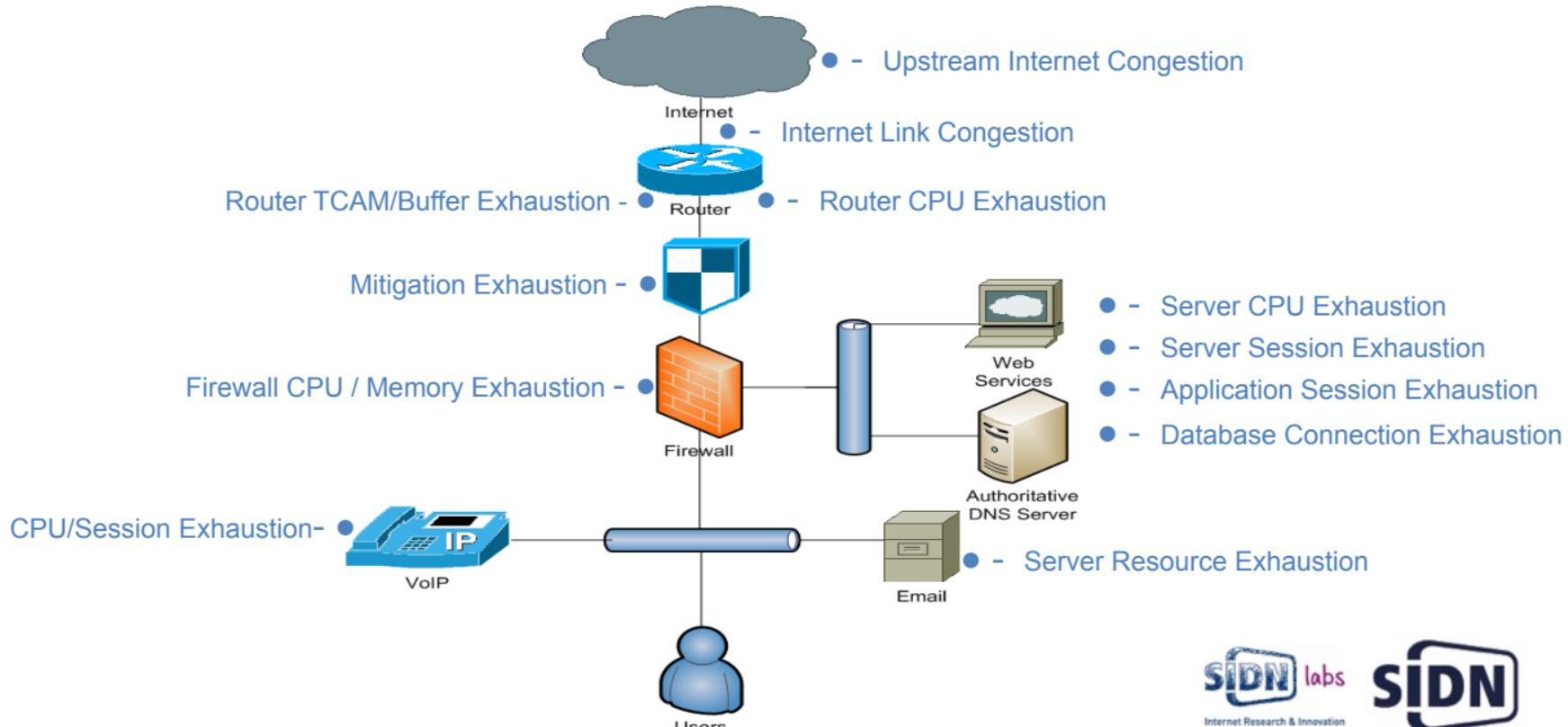
There are many attack types:

PROTOCOL	TYPE	DESCRIPTION
DNS	DNS Reflection/ Amplification	Spoofing DNS queries from the target of the attack towards DNS providers, to generate large responses that overwhelm the bandwidth of the attack target.
TCP	Connect	This flood involves a client repeatedly creating a full TCP session.
	SYN	This flood involves a client sending "synchronize" packets and does not create a full TCP session; therefore, SYN floods are candidates for source IP spoofing.
UDP	UDP Flood	This flood involves a client sending UDP packets of data. UDP is connectionless and does not require a session, which makes this type of flood a perfect candidate for spoofing.
ICMP	ICMP Flood	This flood involves ICMP packets that contain data; because ICMP does not require a session, this flood type is a good candidate for spoofing.
HTTP	HTTP Flood	These floods inundate a target with HTTP requests (typically GET and POST requests).
	Slowloris	By slowly sending HTTP requests, this attack type attempts to exploit a weakness in Web servers that waits for the completion of an HTTP request.
SSL	SSL Renegotiation	This attack type involves a client repeatedly performing an SSL handshake on an established SSL connection to consume a server's resources.

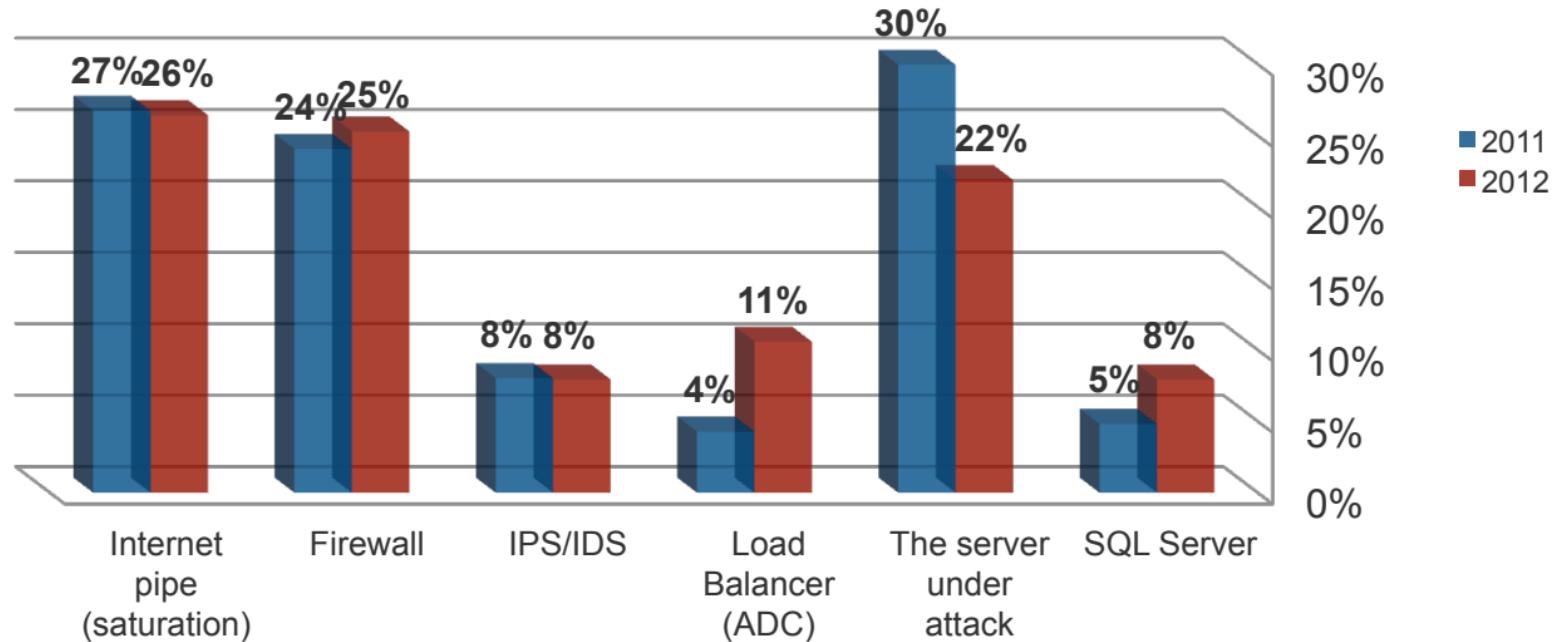
(source: Verisign DDoS malware whitepaper)



Attack vectors



Attack vectors (2)



Who, for what?



Gepubliceerd: 19 april 2013 17:26
Laatste update: 19 april 2013 20:21

DDoS-aanval oorzaak van storing KLM

De internetstoring waar KLM vrijdag mee kampt is het gevolg van een cyberaanval. Dat heeft een woordvoerster van de luchtvaartmaatschappij vrijdag gezegd.

De internetservice van KLM was vrijdagochtend niet bereikbaar. De reizigers die dat vroeg werden verteld dat er een storing was. De woordvoerster van KLM, Linda van der Veen, zei dat de storing veroorzaakt werd door een DDoS-aanval. De storing duurde tot in de middag.

GitHub Status
@githubstatus

We are recovering from a major service outage as we work to mitigate another DDoS attack.

Vertaling weergeven

Beantwoorden Retweeten Toevoegen aan favorieten Meer

23 RETWEETS 2 FAVORIETEN

3 oktober 13 om 11:43 's ochtends

<https://www.facebook.com/klmnl>

de Gelderland

Abonneren E-Paper Webwinkel

HOME & REGIO ALGEMEEN

Algemeen Binnenland Lesse

Lessen op ROC W cybercrime

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.

In the 21st century it's not just about tanks and artillery," one spokesman James Appathurai told BBC News. "We have sent one of our experts at the request of the Estonian authorities to help them in their defence."

SEE ALSO

- The cyber pirates hitting Estonia 17 May 07 | Europe
- Views diverge on Estonia's history 27 Apr 07 | Europe
- Russia accused of 'attack on EU' 02 May 07 | Europe
- Estonia uncovers Soviet war dead 30 Apr 07 | Europe
- Tallinn tense after deadly riots 28 Apr 07 | Europe
- In pictures: Estonia clashes 27 Apr 07 | In Pictures
- Country profile: Estonia 30 Apr 07 | Country profiles
- Hi-tech crime: A glossary 05 Oct 06 | UK

RELATED INTERNET LINKS

- Estonian foreign ministry
- Russian government
- The BBC is not responsible for the content of external internet sites

TOP EUROPE STORIES

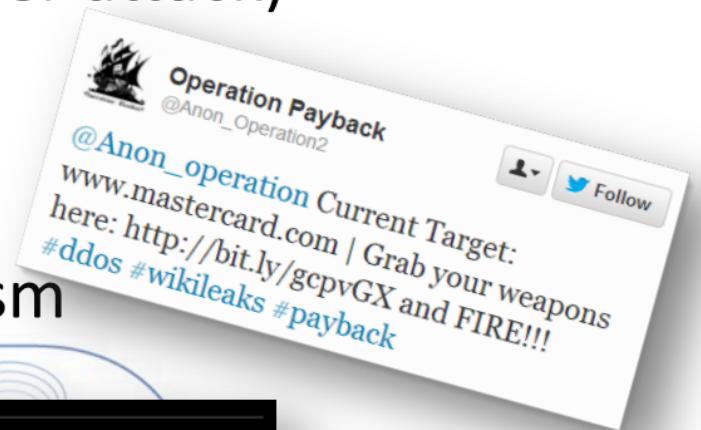
- Credit Suisse offices are raided
- French row over Bastille parade
- EU gives backing to BA alliance

Internet Research & Innovation

DN

Who, for what?

- Kiddies
- Distraction (from another attack)
- Blackmail
- Hacktivism
- Cyber warfare / terrorism



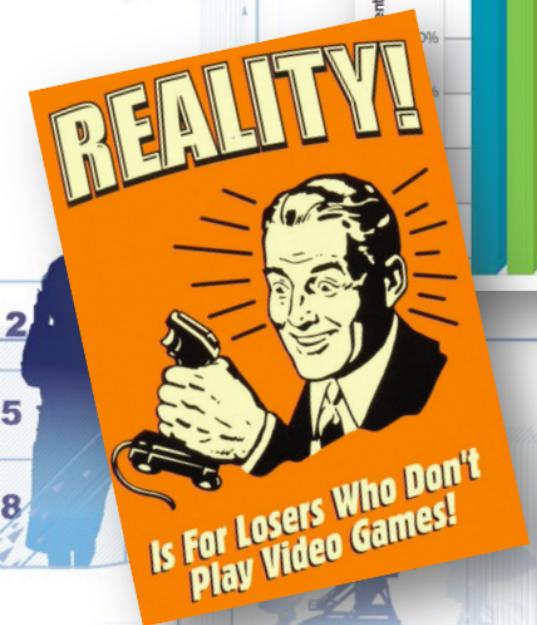
■ Zackipedia Member Posts: 458 Gamertag: GrIM MagiK

◆ Re: How to prevent host booting/ip flooding?
« Reply #8 on: 08:28 AM - 04/29/13 »

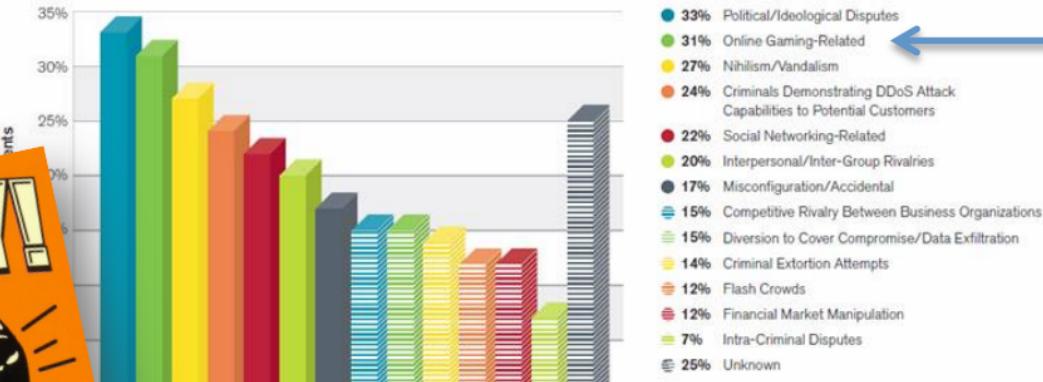
Fight fire with fire. Get a program similar to the Low Orbit Ion Cannon, get a bunch of your friend's computers together and flood your enemies connection faster than they flood yours, hence putting a stop to their floodiness... that's a word now.. Floodiness...

Logged

Who, for what?

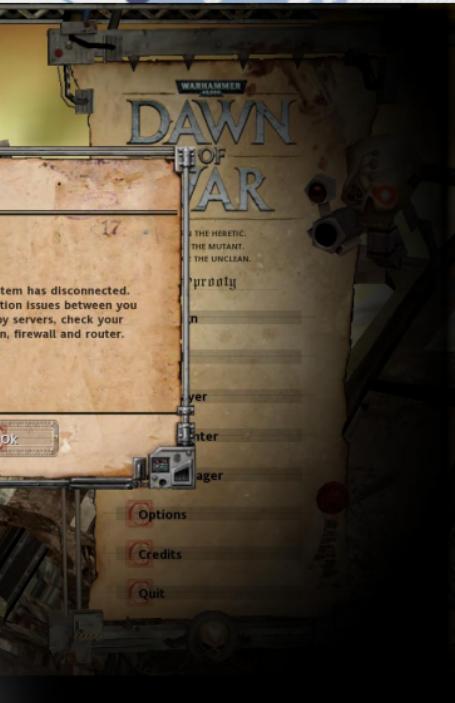
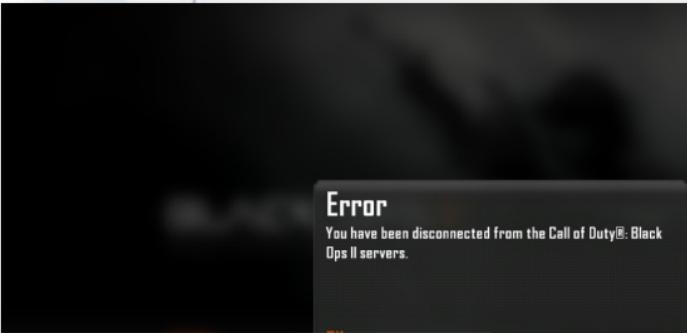


Most Common Motivations Behind DDoS Attacks



(source: Carbon60)

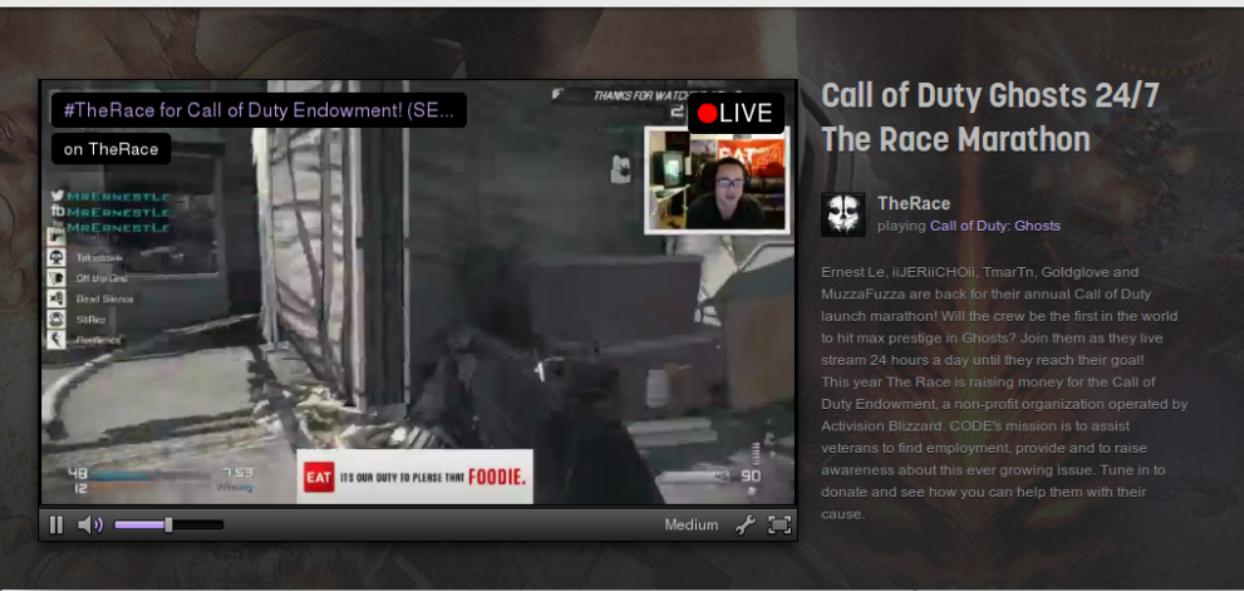
What?! Gamers??



Gaming, gaming, gaming...

twitch

Browse Go Turbo Log In Sign Up



(source: <http://www.twitch.tv>)

SIDN labs
Internet Research & Innovation

SIDN

Gaming sometimes is big \$\$\$

Top 100 Highest Overall Earnings						
ID	Name	Total (Overall)	Highest Paying Game	Total (Game)	% of Total	
1.	Jaedong	Lee, Jae Dong	\$489,384.83	<i>StarCraft: Brood War</i>	\$375,712.95	76.77%
2.	Fatal1ty	Johnathan Wendel	\$454,544.98	<i>Painkiller</i>	\$240,550.00	52.92%
3.	Flash	Lee, Young Ho	\$446,371.91	<i>StarCraft: Brood War</i>	\$410,243.17	91.91%
4.	MC	Jang, Min Chul	\$414,302.11	<i>StarCraft II</i>	\$414,221.84	99.98%
5.	Dendi	Danil Ishutin	\$410,314.28	<i>Dota 2</i>	\$407,697.79	99.36%
6.	XBOCT	Oleksandr Dashkevych	\$408,010.19	<i>Dota 2</i>	\$407,697.79	99.92%
7.	Puppey	Clement Ivanov	\$406,410.19	<i>Dota 2</i>	\$406,097.79	99.92%
8.	Mvp	Jung, Jong Hyun	\$388,916.38	<i>StarCraft II</i>	\$384,290.06	98.81%
9.	Moon	Jang, Jae Ho	\$335,634.08	<i>WarCraft III</i>	\$309,021.95	92.07%
10.	Loda	Jonathan Berg	\$325,521.37	<i>Dota 2</i>	\$322,778.16	99.16%

(source: <http://www.esportsearnings.com/players>)

Gaming sometimes is big\$\$\$\$\$

1. Johnathan "Fatal1ty" Wendel - \$454,544.98 From 35 Tournaments

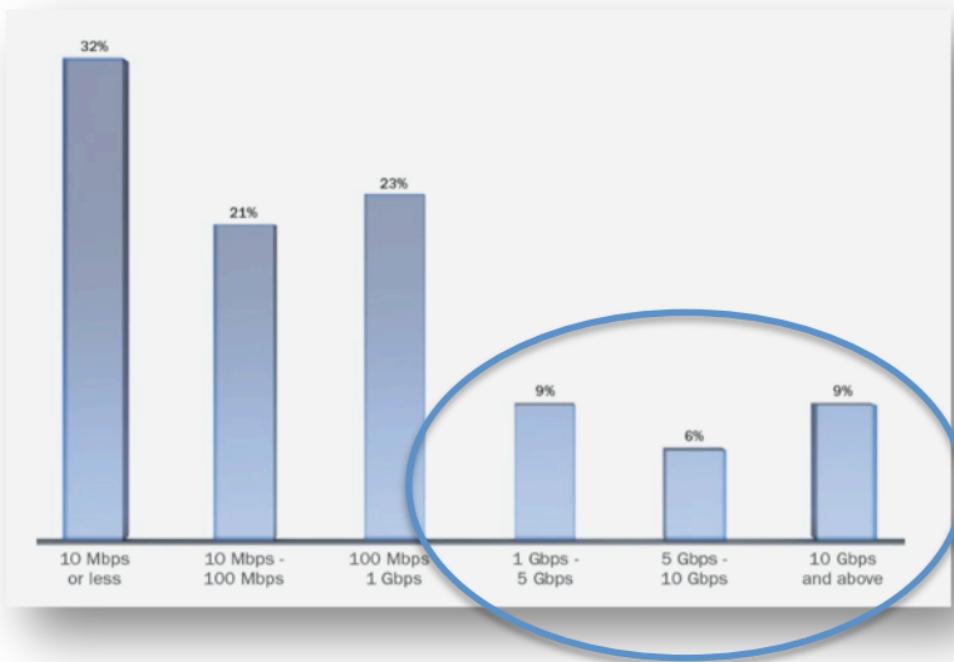
The world's first prominent professional gamer, America's Johnathan Wendel success playing first-person shooters **earned him massive cash prizes** and sponsorship deals with **major computer hardware companies**.



Gia To

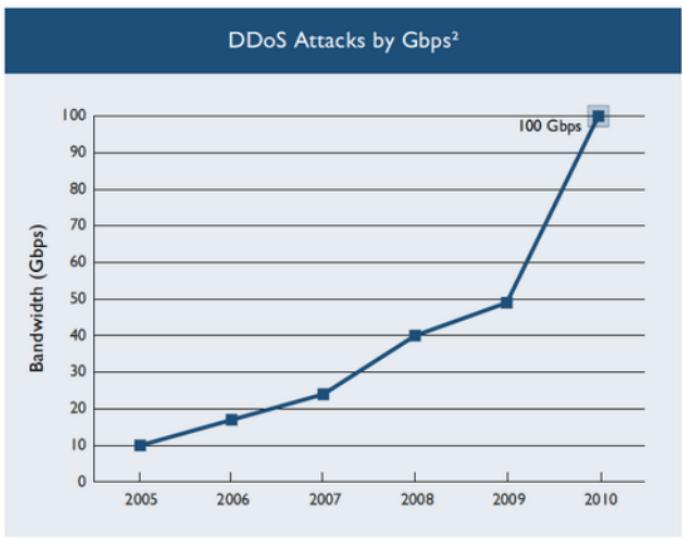
(source: <http://www.businessinsider.com>)

Trend

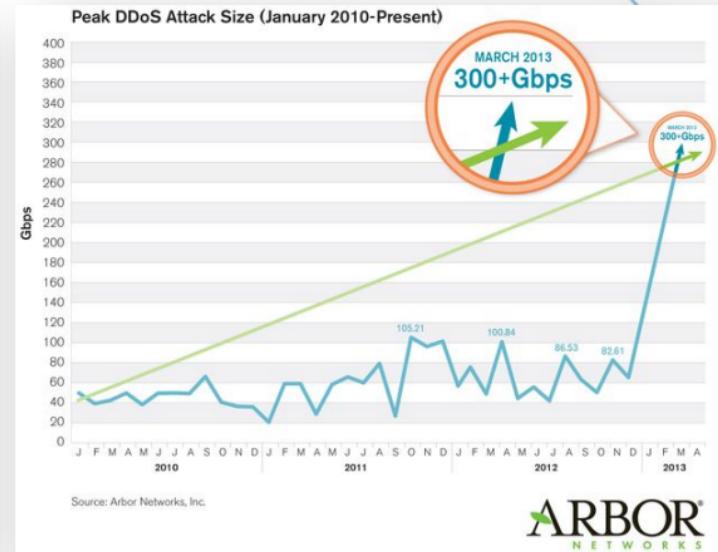


(source: Radware)

Trend



(source: Arbor)



DDoS means business



DELTA INITIATIVE INTELLIGENCE NETWORK

LATEST NEWS TOOLBOX TUTORIALS MARKETPLACE

DDOSING SERVICE

[Return to board index](#)

You are not logged in. [Log in](#) | [Sign up](#)

-- ExploitBay posted 30 days 22 hours ago:

I will DDoS any person or server that you want me to.
0.01 BTC per 5 minutes.
My Torchcat:
6bviasif62kyoknq5
I can provide proof if you need it.

--★ Scorz99 posted 29 days 6 hours ago:

How many attackers does this service provide?

--● operations posted 24 days 7 hours ago:

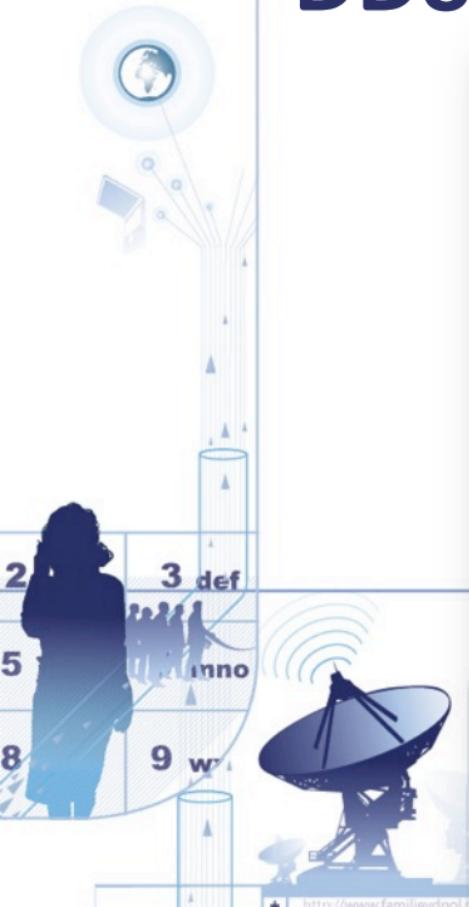
Checked and verified

--kiki posted 18 days 21 hours ago:

Can modify the database on the server to?
Than I would be interested in your services !

-- ExploitBay posted 6 days 21 hours ago:

No, sorry.
Just DDoSing.
I'm back after a week~ hiatus.



DDoS means business

```
mib_Oydffp> hey
<mib_Oydffp> come in pm
<Al-Majourhi> hello
<Al-Majourhi> can you help me
<mib_Oydffp> sure
<mib_Oydffp> how much is the pay and who is the target?
<mib_Oydffp> goodbye
<Al-Majourhi> are you here
== No such nick/channel: mib_Oydffp
<Al-Majourhi> Hey back
<mib_Oydffp> Sorry had to handle a dog.
<Al-Majourhi> Thats okay. I have been polishing my RPG (kidding)
<Al-Majourhi> So I know you helped qassam last few days with your PPM DDos thing. (Multiboot.me)
<mib_Oydffp> Who?
<mib_Oydffp> Qassam against US bank?
<mib_Oydffp> A fine piece of work.
<Al-Majourhi> We are affiliated with the same group. Have funds but your prices are much.
<Al-Majourhi> If I can get it for $200 for 1000 hours - I can fund the whole 10000 hours, thats $2000 now.
<Al-Majourhi> And you want to use Multiboot slots, at 10GB/s right? Answer carefully.
<mib_Oydffp> We can do that. how can you pay/
<mib_Oydffp> Do you have 'name' of someone I dealt with recently so we can expedite this process.
<Al-Majourhi> Op Operation Kudab
<Al-Majourhi> Same guys.
<mib_Oydffp> got that, good.
<mib_Oydffp> contact me on agbimrwy@sharklasers.com - and we can talk more.
<mib_Oydffp> I have to gtfo now.
<mib_Oydffp> You have payment means available now - I can do $200 for 1K hours, any target.
<mib_Oydffp> Make the contact we can deal.
== mib_Oydffp [webirc@AN-143.4vr.fmlari.IP] has quit [Quit: ]
```

DDoS means business



Welcome back, . You last visited: Today, 01:53 AM ([User CP](#) — Log Out)

[View New Posts](#) | [View Today's Posts](#) | [Your Threads](#) | [Your Posts](#) | [Private Messages](#) (Unread 0, Total 431)

Current time: 08-14-2012, 01:53 PM
[Open Buddy List](#)

Hack Forums / Marketplace / Premium Sellers Section / **Server Stress Testing**

Important Stress Testing Rules

1. No posting requests for DDOS attacking sites.
2. Section is for server, firewall, and network stress testing.
3. No discussions on attacking websites.
4. No take down proof posts allowed.
5. No asking for vouch or free copies.
6. No cross-posting. If you create a thread here do not make it anywhere else.

Pages (2): [1](#) [2](#) [Next »](#) [New Thread](#) [Mark this forum read](#)

Thread / Author	Replies	Last Post [asc]
◆ ◆ Elite Stresser ◆ PP/LR/Bots ◆ SSYN/SUDP ◆ Skype Resolve ◆ Web Based ◆ Autobuy ◆ (Pages: 1 2 3) 1337B345T3R	140	Today 11:28 AM Last Post: drpanda15
► ★ Versatile Stresser★ 4 Gbps ★ 3000 second max boot-time ★ Custom Source ★ Cyber	49	Today 05:54 AM Last Post: Omniscent
► absoBoot - Unlimited Boot Time - [RUDY UDP SSYN HTTP Get Head Slowloris] (Pages: 1 2 3 4 ... 7) BV1 ✓	302	Today 04:53 AM Last Post: derekm22098
► Meep AIM Booter Attacks sent via AIM 6+gbps peak with proof Rooted Servers 2 hour (Pages: 1 2 3) BluntMayne	123	Today 02:44 AM Last Post: Im Coco
↳ Stresser++ ↳ AutoBuy ◆ Powerful ◆ Private Servers ◆ Skype Resolver ◆ 1 Hour+ Hit (Pages: 1 2 3 4 5) TyrantElf	229	08-12-2012 12:56 AM Last Post: TyrantElf

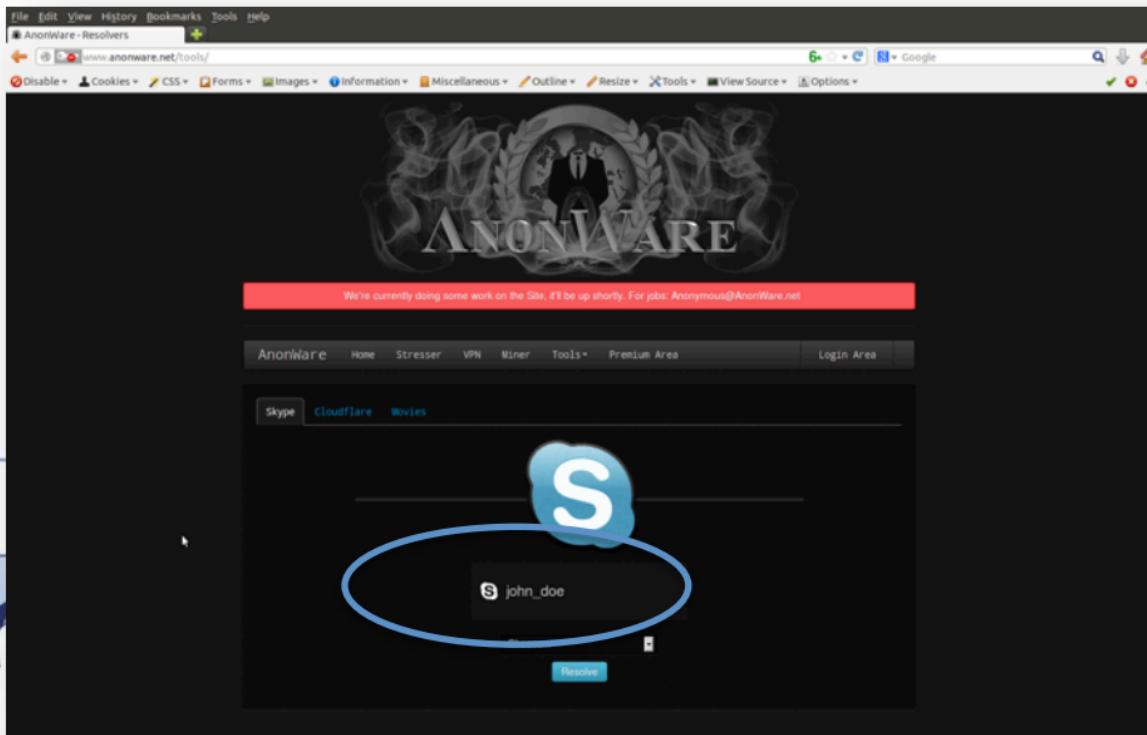


Case study (just an example)

Possible scenario:
John Doe is a target...

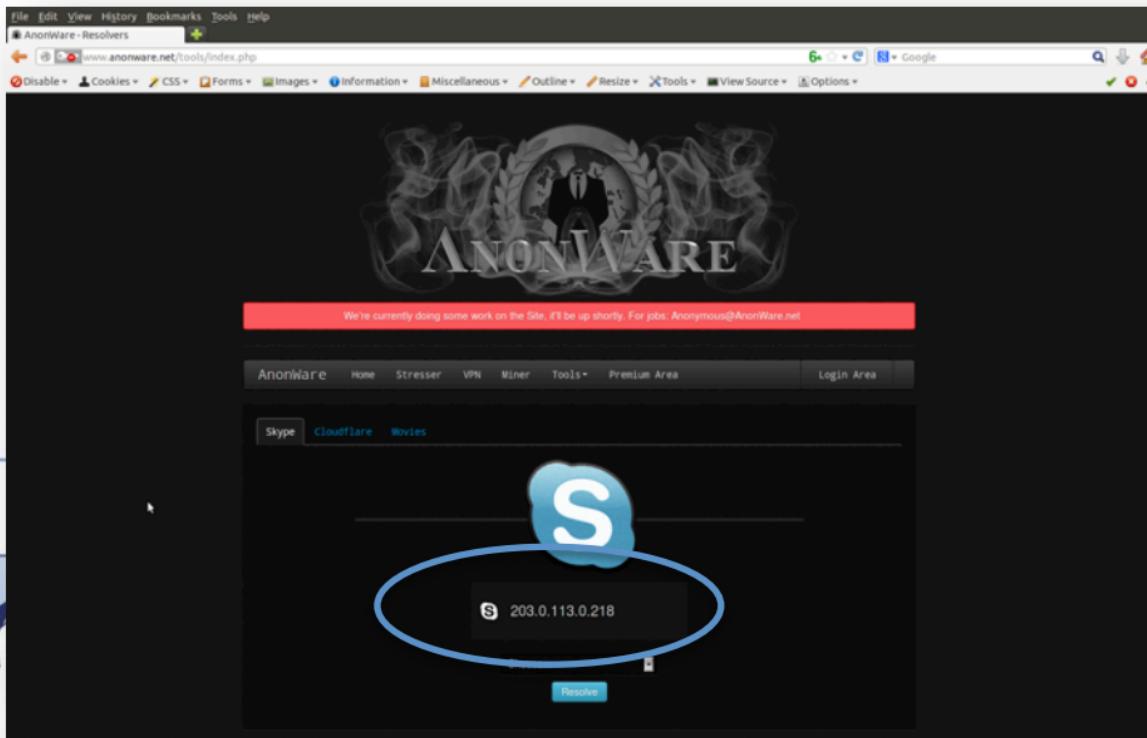
Step 1: find his IP address

John has Skype, so let's use a 'Skype Resolver'...



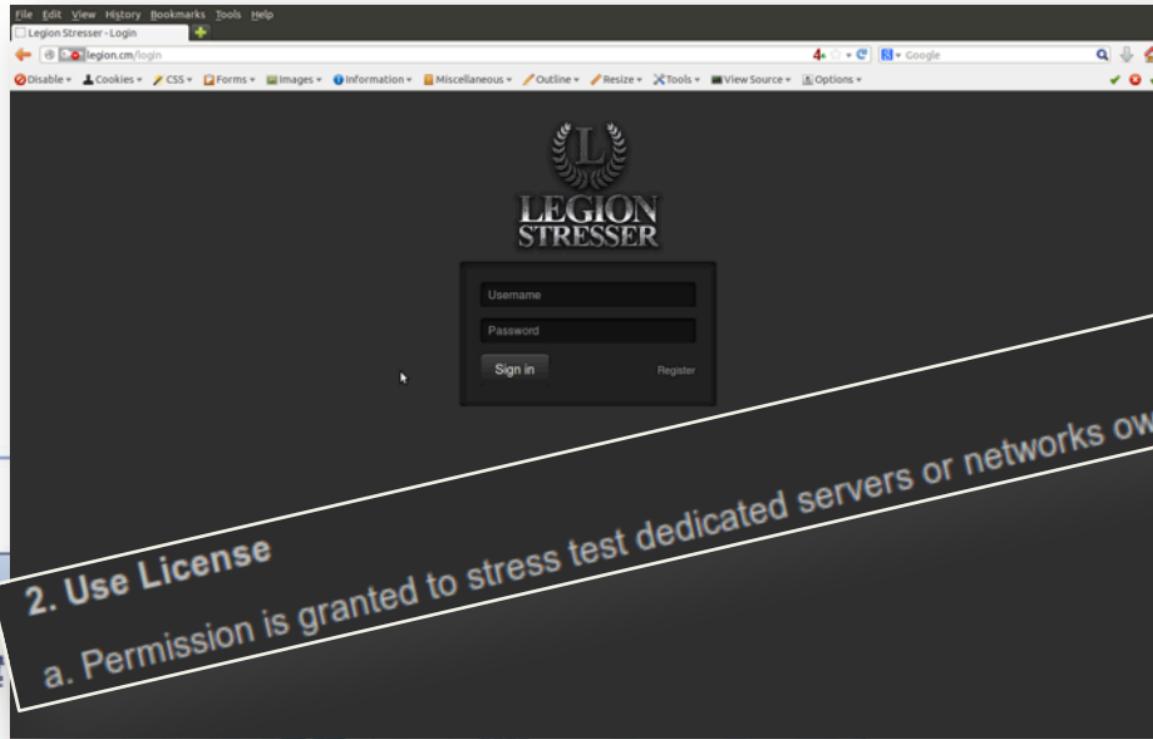
Step 2: IP address found

That wasn't too hard now, was it?



Step 3: Initiate a DDoS...

My cool DDoS-stresser, I mean stressTESTer ;-)



Step 3: Initiate a DDoS...



Here's another example (of the many out there)

The image displays two side-by-side browser windows. The left window shows the 'iSkyperesolve.com' website, which has a 'Skype Resolver' feature where users can enter a Skype username to find their current IP address. The right window shows the 'Power Stresser' website, which features a login form with fields for 'Username' and 'Password', and buttons for 'Login' and 'Register'. Both sites have a dark theme and are framed by decorative silhouettes of people and mountains.

iSkyperesolve.com

Power Stresser

Skype Resolver

Skype Username:

Resolve

Skype: johndoe
Current IP: 168.62.23.92:40031
Recent IP's: 168.62.23.92[172.31.255.249|213.146.168.254]

There are 5 users online!

PowerStresser 60GB/s Starting a

Brought to you by,
Power Stresser
SafeSkyHacks

Donate Bitcoins

powerstresser.com

PowerStress

Login

Username:

Password:

Login Register

By logging in you agree to our [Terms of Service](#) & [Privacy Policy](#)

Forgot credentials?

Live Support

DDoS means business



Google
booter stresser

Web Images Maps Shopping Videos More ▾ Search tools

About 18,200 results (0.25 seconds)

DESTRESS Booter Home

destressbooter.com/ ▾

THE BEST Booter ... Protected. Destress Booter is powered by quick, strong, and DDoS protected servers to guarantee uptime and stability. With the ...

Rage Booter

ragebooter.net/ ▾

We are a professional and reputable stress testing service that has been ... that persons gone thanks and I hope its stays this way cause RAGE Booter is #1!

Quantum Booter - Stress Testing Service

quantumstresser.net/ ▾

We are a professional and reputable stress testing service that has been online for almost two years now. We maintain a large and dedicated network of servers. You visited this page on 9/3/13.

Agony Booter / Stresser

agonystresser.com/ ▾

Agony Booter V.2! Available Now! Please visit our client panel to purchase and receive support! HackForums Thread · DMCA.com.

Top 10 DDosers's (Booters/Stressers) - SafeSkyHacks

www.safeskylhacks.com/Forums/showthread.php?...%28Booters-Stressers%29 ▾

Mar 28, 2013 - Top 10 Booters. #1: iDDos Stresser - <http://iddos.net>(So Powerful ... (Instant)(3 working Skype resolvers)(Cheap)(Steam Resolver)(Chargen ...

XR Shellbooter

xrshebooter.com/ ▾

Login. Username: Password: By Logging in you agree to all Terms of service.

Opaque Booter - Home

opaquebooter.weebly.com/ ▾

Create a free website with Weebly. Quantum Booter. Affordable and professional stress testing service. Main · Stress Test · User CP · Forums · Tools · Logout ...

RAGE Booter

HOME ABOUT US PLANS & PRICING FEATURES OUR AFFILIATES MEMBER AREA

PLANS & PRICING

Rage Bronze Monthly

\$5.00 /mo

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

300 Second Boot time

RageBooster Client

BUY NOW

Rage Silver Monthly

\$10.00 /mo

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

600 Second Boot time

RageBooster Client

BUY NOW

Rage Gold Monthly

\$15.00 /mo

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

900 Second Boot time

RageBooster Client

Rage Platinum Monthly

\$50.00 /mo

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

3000 Second Boot time

RageBooster Client

RAGE ULTIMATE MONTHLY

\$125.00 /mo

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

5000 Second Boot time

RageBooster Client

RAGE OMEGA MONTHLY

\$150.00 /mo

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

9000 Second Boot time

RageBooster Client

RAGE BRONZE LIFETIME

\$20.00

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

300 Second Boot time

RageBooster Client

RAGE SILVER LIFETIME

\$30.00

Skype Resolver

Cloudflare Resolver

Geo Ip Locator

600 Second Boot time

RageBooster Client

DDoS means business



TOP- DDOS Service (Support)

Order a ddos attack! Removable poster competition!

MENU

Home

Reviews

Rates

Methods of payment

Contacts

Top-d

It seems
recently
company
control d

Ddos-att
prevent
resource
not all pr
the card
trying to
besides,
sites of y

Type c

- ✓ HTTP
- ✓ DOW
- ✓ ICMP
- ✓ UDP
- ✓ SYN

Our se



TOP- DDOS Service (Support)

Order a ddos attack! Removable poster competition!

MENU

Home

Reviews

Rates

Methods of payment

Contacts



Rates

- ✓ 1:00, \$ 5
- ✓ 24-from \$ 40
- ✓ 1 week - from \$ 260
- ✓ 1 month - from \$ 900
- ✓ This is the minimum price. Prices depend on the line of targets.

Discounts:

- ✓ 1 week - 5%
- ✓ 2 weeks - 7%
- ✓ 3 weeks - 10%
- ✓ 1 month or more - 15%
- ✓ Also, when ordering from two sites also discounts.

[Order a ddos attack](#), 2011-2012. All rights reserved.

[Order a ddos attack](#), 2011-2012. All rights reserved.



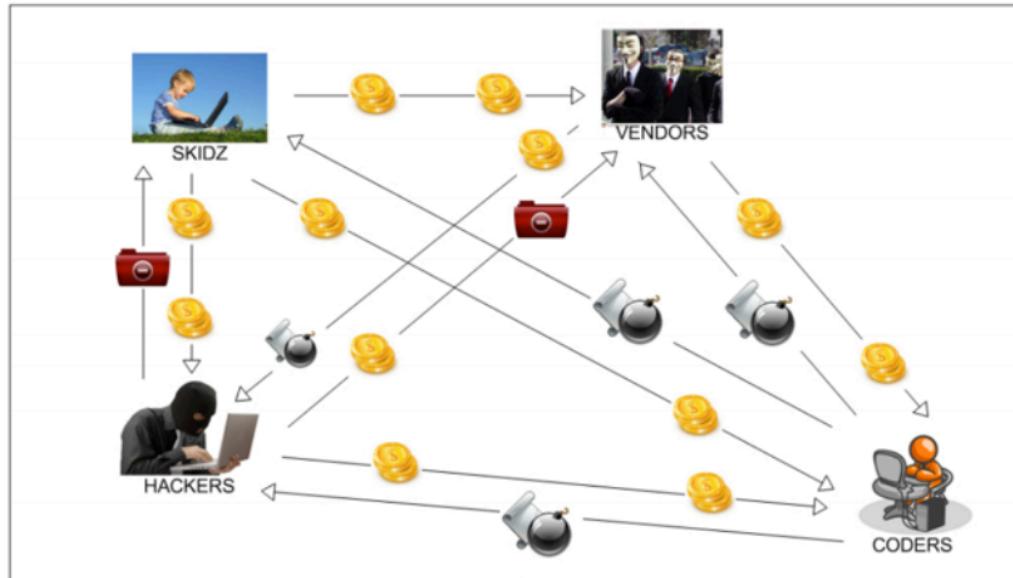
DDoS means business

The screenshot shows a web-based interface for launching DDoS attacks. At the top, there's a search bar with a red 'GO!' button and a dropdown menu showing attack types: dns amplification, spoofed syn, spoofed udp, and http. Below the search bar is a navigation bar with tabs: Главная (Home), Команды (Commands) - which is selected and highlighted in red, Сервера (Servers), Листы (Lists), and Выход (Logout). A welcome message 'Добро пожаловать!' (Welcome!) is displayed above a 'Список атак' (Attack List) table. The table has columns: Сервер (Server), Цель (Target), Осталось (Remaining), and Тип атаки (Attack Type). To the right of the table is an 'Информация' (Information) box containing a warning about the purpose of the script and contact details. Below the table is a 'Послать команду' (Send Command) form with fields for Параметр (Parameter), Значение (Value), and a dropdown for Тип атаки (Attack Type) set to 'DNS Amplification'. Other fields include 'Цель' (Target IP), 'Порт' (Port), 'Сервера для атаки' (Attack servers), and a text area for 'Сообщение' (Message).

DDoS means business



HACKFORUMS DDoS Booter Ecosystem



- MONEY
- TOOLS
- PRIVATE LISTS

(source: Prolexic)

Modus operandi of DNS amplification

- Open recursive resolvers
- Authoritative name servers

DNS Amplification/reflection

```
; <>> DIG 9.8.1-P1 <>> +dnssec +multi ANY isc.org @199.6.1.30
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<< opcode: QUERY, status: NOERROR, id: 58517
;; flags: qr aa rd; QUERY: 1, ANSWER: 26, AUTHORITY: 0, ADDITIONAL: 15
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;isc.org.           IN ANY

;; ANSWER SECTION:
isc.org.        7200 IN  RRSIG SPF 5 2 7200 20131002233248 (
                           20130902233248 50012 isc.org.
                           enxTfXMywtZw9rmSzE20svQnla3whFcblQ2mpqjtT
                           3BxuqpGcvlbCwjLxNhn89xY2//pkN1EPVgwz2y7lI
                           BoLV9X/VnGCH/sB1NaRtcckB2SE75cuh2L7jkR1d6JChC
                           wLNQhp1HbYeLmW2n18yifj33TorU7HwUrhaN0-
)
isc.org.        7200 IN  SPF "v=spf1 a mx ip4:204.152.184.0/21 ip4:149.20.0.0/16 ip6:2001:04F8::/48 ip6:2001:500:6::/48 ~all"
isc.org.        7200 IN  RRSIG DNSKEY 5 2 7200 20131002230127 (
                           20130902230127 12892 isc.org.
                           ioxDVytff4voAHCVxdz6U/fuQah2f2XVUExExeo4855
                           vLVNrse5ckG1Wyn/4FeWLOUVWm5HElL/hk2QEResp0c
                           sAwTnllU7w8FM65aS7p109JZQMNVkPxQjsTYzEP1P2GA
                           8NVGRUhz17RMLLSFgAJJS9aEl7xK0fMsds9u4Az+B9J8x
                           Vz5GGM68FStEXMyauE9r825g4zzR2Uv619LYH+Uha5
                           QuFq1cVVvtot+QL1dwNV4Kt3fp3m6KveBaiIiOrFSjod
                           40Ffwzd3Cq4GqVicseyA15bKN1hvgtFRhl8MqGexvbP
                           vu49RkekeJ1hf7pzFM6nlo5+XqvjWB+EQ=="
)
isc.org.        7200 IN  RRSIG DNSKEY 5 2 7200 20131002230127 (
                           20130902230127 50012 isc.org.
                           HfC6EpppKBDieqnYccCLEMP3uhCFENhY9pwbcqwYh9f
                           VOMMeElm/Xsyq1k9FsVGZnxw25gc946gsXntTkldaoawi
                           boZLq2oJ0uGbsF2+4SreLixn6Vejh1nSxfQch7DcfT
                           uMSBUMBmleJ1OfPC12zTzFetu2qgnM4hCovp3vA= )
isc.org.        7200 IN  DNSKEY 256 3 5 (
                           BQEAAAOhHQDBrhQbtphgg2wQUpEQ5t4DtUHxoMFVu2hW
                           LDmwoOMRkJGrhCeFvAzih7yJhf82GFW6h3d8XG/xyl
                           YC06Krbpdjojwx8YMXL5A/kAu50N1L8Zr1R6KTbsYVm
                           /Qx5RinNbPclv+vt+8eXEmo20jIS1uLggy347cbBlzM
                           nnz/4LjpA0da9Cbkj3A254T515sNIMcwB8/2+2E63/z
                           zrqZkjj0Brn9Bexpjks3jRhzatEsxn3dTy47R09UiX
                           5WcJt+xzq27+yssLKOoed3927SDmsn2eAFKtQpwa6L
                           XeG2w+)*xmw3cA81VUgkf/rzeC/bByBns07uAETd
                           );
key id = 50012
)
isc.org.        7200 IN  DNSKEY 257 3 5 (
                           BEAAAAOOhHQDBrhQbtphgg2wQUpEQ5t4DtUHxoMFVu2hW
                           LDmwoOMRkJGrhCeFvAzih7yJhf82GFW6h3d8XG/xyl
                           YC06Krbpdjojwx8YMXL5A/kAu50N1L8Zr1R6KTbsYVm
                           /Qx5RinNbPclv+vt+8eXEmo20jIS1uLggy347cbBlzM
                           nnz/4LjpA0da9Cbkj3A254T515sNIMcwB8/2+2E63/z
                           zrqZkjj0Brn9Bexpjks3jRhzatEsxn3dTy47R09UiX
                           5WcJt+xzq27+yssLKOoed3927SDmsn2eAFKtQpwa6L
                           XeG2w+)*xmw3cA81VUgkf/rzeC/bByBns07uAETd
                           );
key id = 12892
)
isc.org.        3600 IN  RRSIG NSEC 5 2 3600 20131002233248 (
                           20130902233248 50012 isc.org.
                           K3/RL0nn54FRkvPmaeccG263jJQVCZLlg41zB02YssxzN
                           K/71r0M4od4K8r0N1d4w54MwvVtu0m4idwalcotavv0
```

- DNS response far greater than original question
- 78 bytes ANY query may easily result in ~4K bytes reply
- Amplification factor 50-100 times is possible.
- Example: ‘ANY isc.org’ (factor 53x amplification)

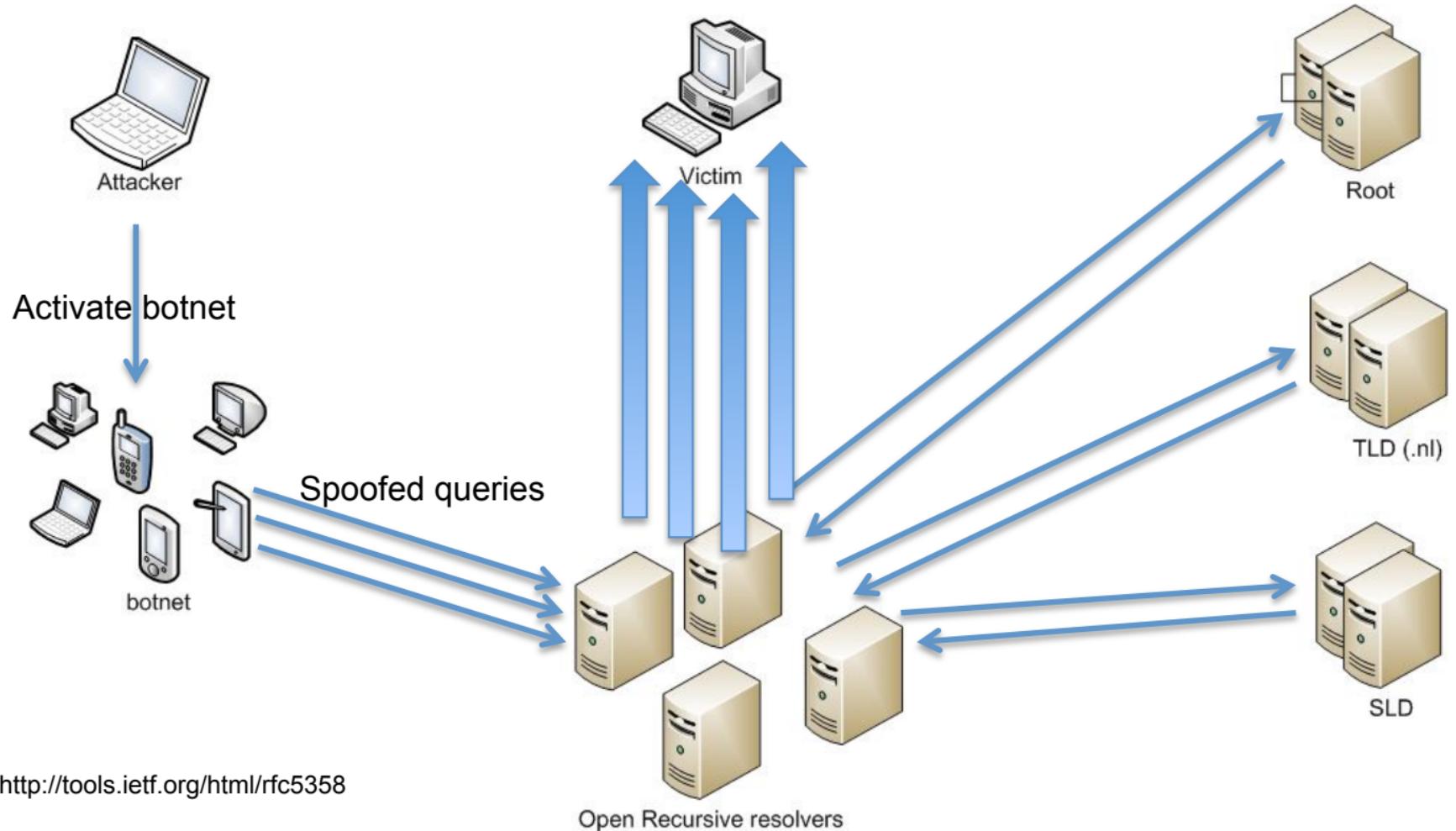
DNS Amplification/reflection

Specially crafted RR's

```
; Truncated, retrying in TCP mode.  
;  
; <>> DiG 9.8.4-rpz2+r1005.12-P1 <>> ANY ddostheinter.net  
; global options: +cmd  
;; Got answer:  
;; ->>HEADER<< opcode: QUERY, status: NOERROR, id: 8510  
;; flags: qr rd ra; QUERY: 1, ANSWER: 513, AUTHORITY: 2, ADDITIONAL: 2  
  
;; QUESTION SECTION:  
;ddostheinter.net. IN ANY  
  
;; ANSWER SECTION:  
ddostheinter.net. 17 IN SOA ns1.ddostheinter.net.  
root.ddostheinter.net. 2012291001 28800 30 330000 86400  
ddostheinter.net. 17 IN A 172.33.43.83  
ddostheinter.net. 17 IN A 172.33.43.84  
ddostheinter.net. 17 IN A 172.33.43.85  
ddostheinter.net. 17 IN A 172.33.43.86  
ddostheinter.net. 17 IN A 172.33.43.87  
ddostheinter.net. 17 IN A 172.33.43.88  
ddostheinter.net. 17 IN A 172.33.43.89  
ddostheinter.net. 17 IN A 172.33.43.90  
ddostheinter.net. 17 IN A 172.33.43.91  
ddostheinter.net. 17 IN A 172.33.43.92  
ddostheinter.net. 17 IN A 172.33.43.93  
ddostheinter.net. 17 IN A 172.33.43.94  
ddostheinter.net. 17 IN A 172.33.43.95  
ddostheinter.net. 17 IN A 172.33.43.96  
ddostheinter.net. 17 IN A 172.33.43.97  
ddostheinter.net. 17 IN A 172.33.43.98  
ddostheinter.net. 17 IN A 172.33.43.99  
ddostheinter.net. 17 IN A 172.33.43.100  
ddostheinter.net. 17 IN A 172.33.43.101  
ddostheinter.net. 17 IN A 172.33.43.102  
ddostheinter.net. 17 IN A 172.33.43.103  
ddostheinter.net. 17 IN A 172.33.43.104  
ddostheinter.net. 17 IN A 172.33.43.105  
ddostheinter.net. 17 IN A 172.33.43.106  
ddostheinter.net. 17 IN A 172.33.43.107  
ddostheinter.net. 17 IN A 172.33.43.108  
ddostheinter.net. 17 IN A 172.33.43.109  
ddostheinter.net. 17 IN A 172.33.43.110  
ddostheinter.net. 17 IN A 172.33.43.111  
ddostheinter.net. 17 IN A 172.33.43.112  
ddostheinter.net. 17 IN A 172.33.43.113  
ddostheinter.net. 17 IN A 172.33.43.114  
ddostheinter.net. 17 IN A 172.33.43.115  
ddostheinter.net. 17 IN A 172.33.43.116  
ddostheinter.net. 17 IN A 172.33.43.117  
ddostheinter.net. 17 IN A 172.33.43.118  
ddostheinter.net. 17 IN A 172.33.43.119  
ddostheinter.net. 17 IN A 172.33.43.120  
ddostheinter.net. 17 IN A 172.33.43.121  
ddostheinter.net. 17 IN A 172.33.43.122  
ddostheinter.net. 17 IN A 172.33.43.123  
ddostheinter.net. 17 IN A 172.33.43.124  
ddostheinter.net. 17 IN A 172.33.43.125
```

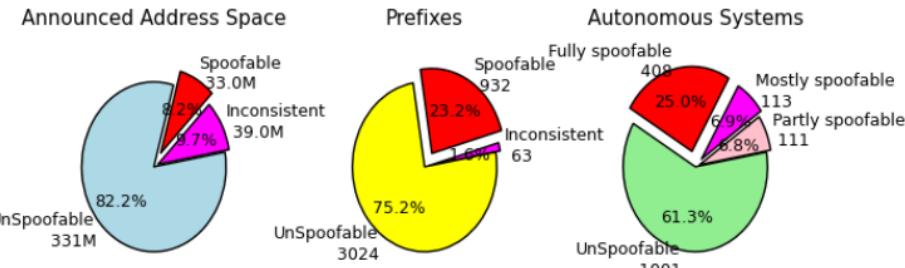
- Domain names are registered or even hijacked
- Sometimes they have 'funny' names, such as 'dd0s.asia', 'ddos.cat', bitstress.com or 'ddostheinter.net'
- Look at it...
- Now respect it...
- 8K... (100x amplification)
- Botnet == 100 PC's (each 1 Mbit/s)
- X 100...
- DDoS == 10 Gbit/s !!





Problem 1: Spoofing is (still) rather easy

- BCP38 / SAC004/ uRPF / Ingress filters
- RFC3704
- <http://www.bcp38.info>



(source: <https://spoofier.cmnd.org/>)



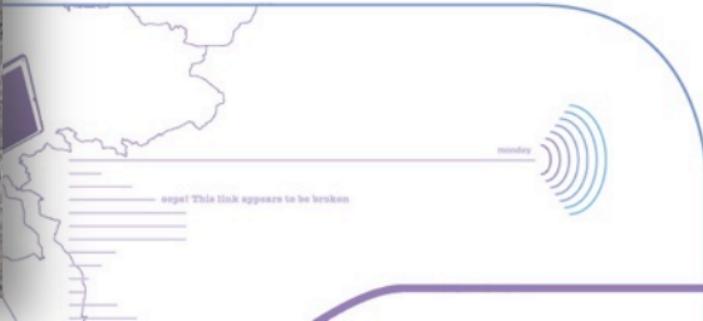
Problem 2: many (!) open resolvers

- Roughly 30.000.000 worldwide
- ~180.000 in the Netherlands
- ~32.000 in Norway



Problem 2: many (!) open resolvers

- ~180.000 in the Netherlands
- ~120.000 in AS5390...
- Huawei HG655d
- New firmware is available!



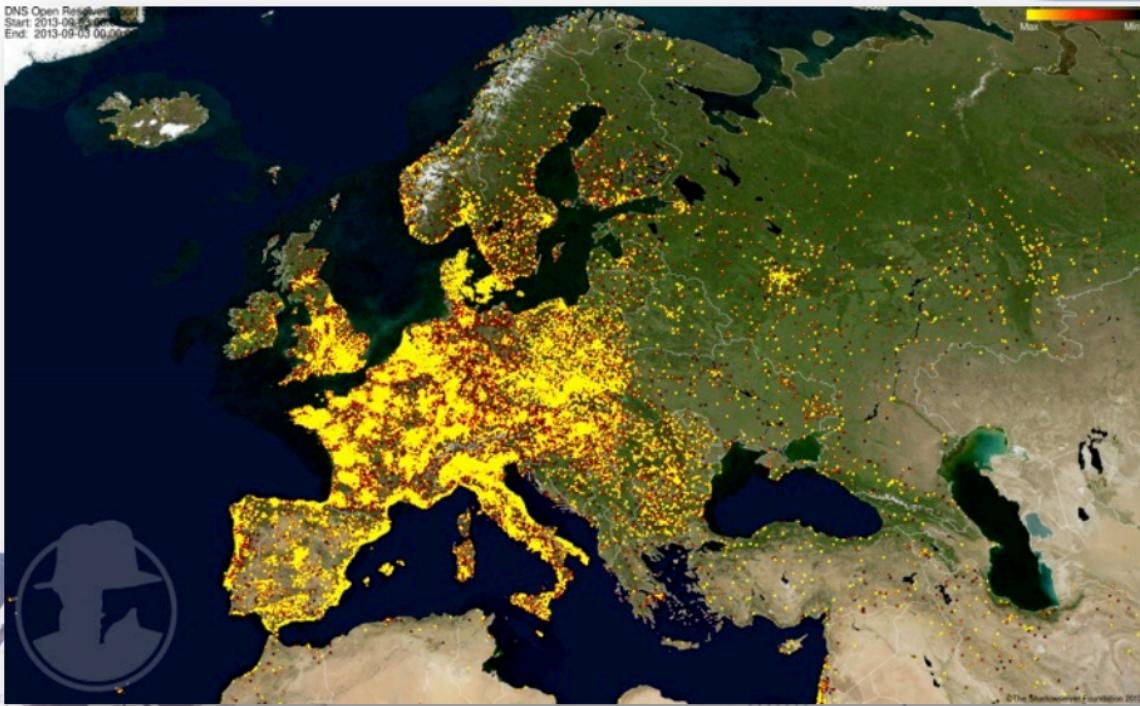
Problem 2: many (!) open resolvers

- ~32.000 in Norway
 - Telenor Norge, Direct Connect, GET Norway
 - Broadnet, Hafslund Telekom Nettjenester
 - Loqal, NEXTGENTEL, Altibox
 - Eidsiva bredband and others..

- Sometimes weird ADSL-modems
- Sometimes wrong defaults

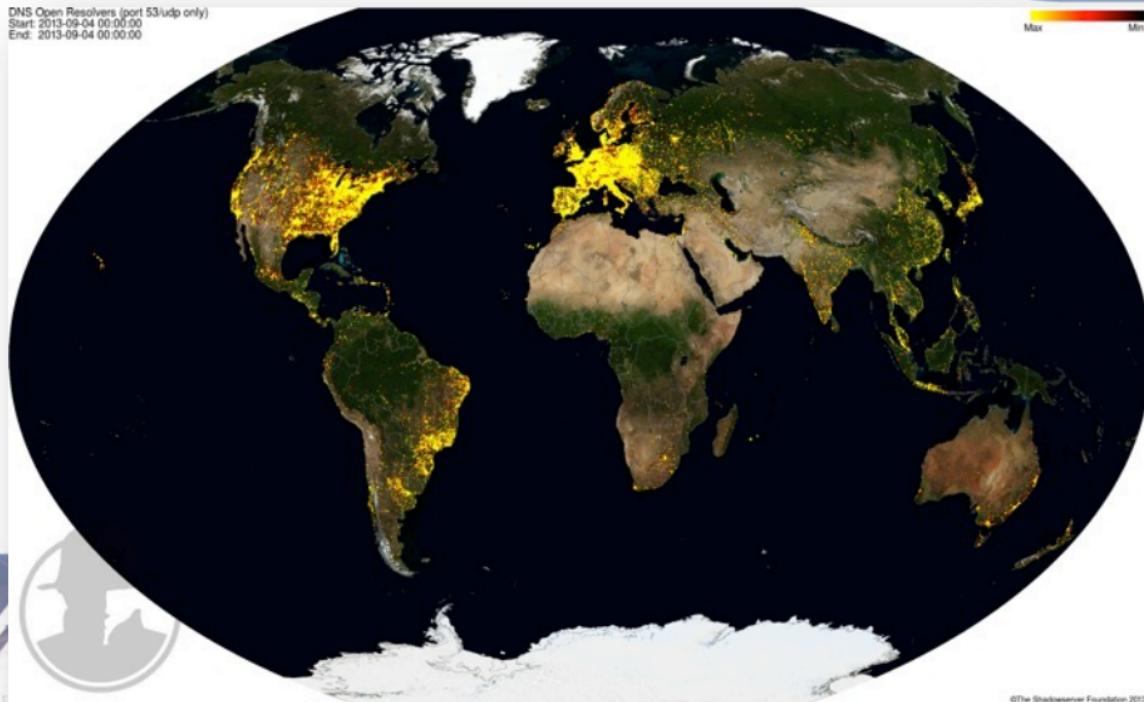


Problem 2: many (!) open resolvers



(source: <https://dnsscans.shadowserver.org/>)

Problem 2: many (!) open resolvers

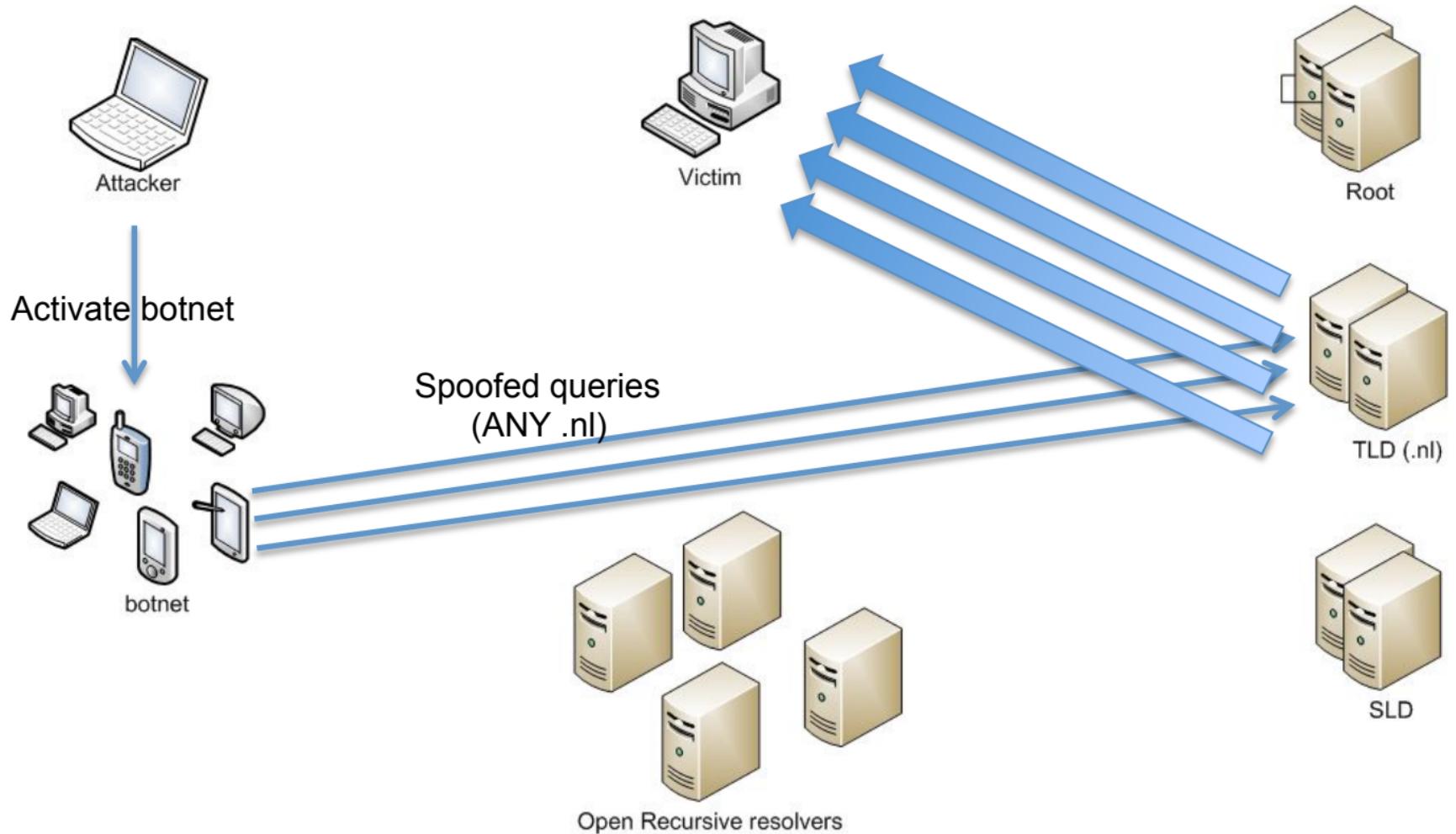


(source: <https://dnsscan.shadowserver.org/>)

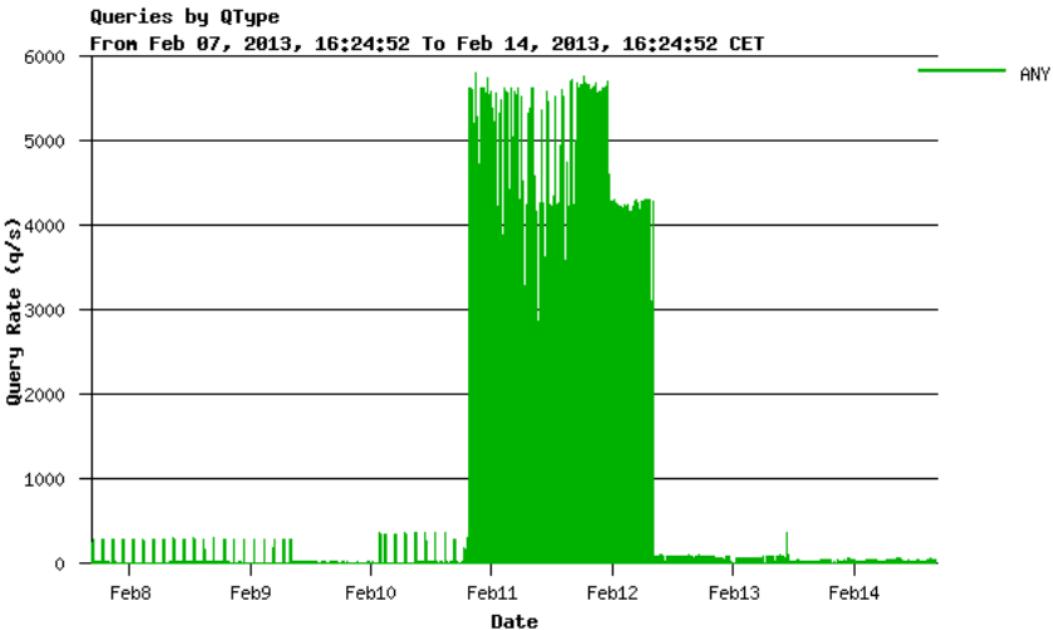


Problem 3: Not limited to open resolvers

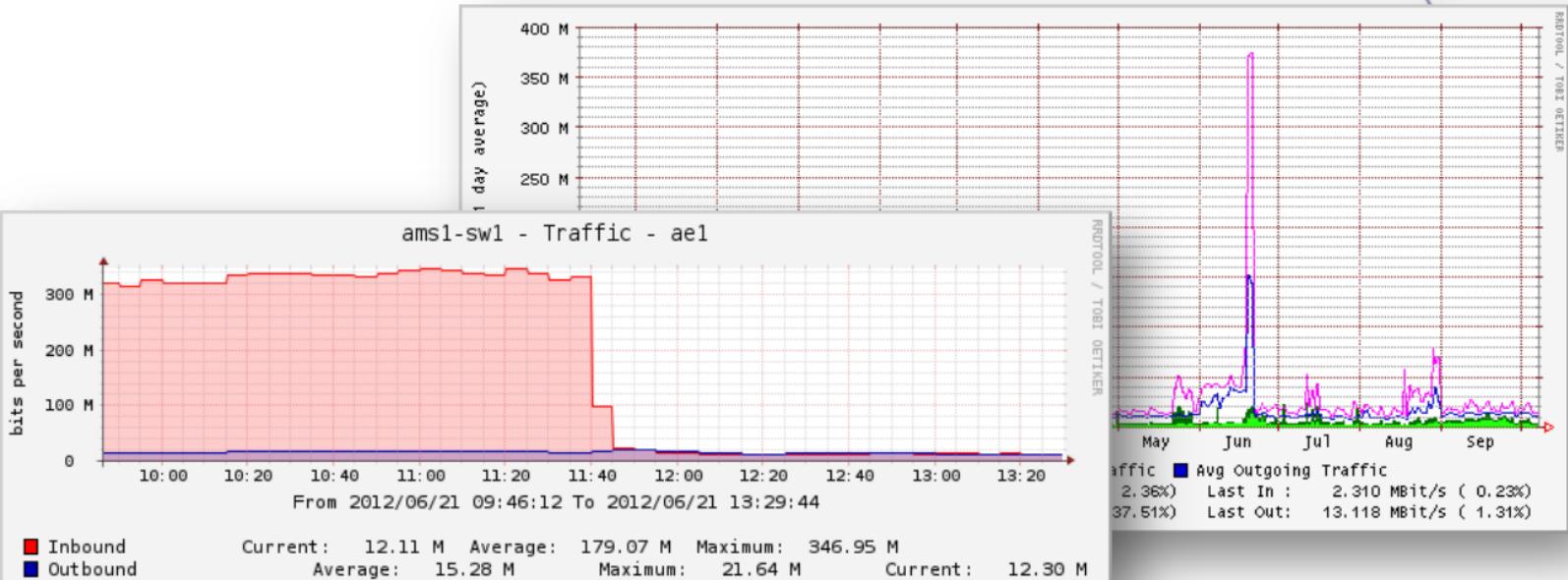
- Authoritative name servers work well too
 - Now it's our problem as well...
 - Con's: competent management (mostly)
 - Pro's: Good infrastructure
- TLD, second-level, doesn't really matter
- DNSSEC makes it even more interesting



ANY-attack on .nl



ANY-attack on .nl



ANY-attack on .nl

```
rule=$(python generate-netfilter-u32-dns-rule.py --qname nl --qtype ANY)  
  
iptables -A INPUT -p udp --dport 53 --match u32 --u32 "$rule" -j RATELIMITER  
  
iptables -A RATELIMITER -m hashlimit \  
  --hashlimit-name DNS --hashlimit-above 20/second --hashlimit-mode srcip \  
  --hashlimit-burst 100 --hashlimit-srcmask 28 -j DROP
```

(source: <http://www.bortzmeyer.org/files/generate-netfilter-u32-dns-rule.py>)

ANY-attack on .nl

rule=\$(python generate-netfilter-u32-dns-rule.py --qname **nl** --qtype ANY)

rule=\$(python generate-netfilter-u32-dns-rule.py --qname **NL** --qtype ANY)

rule=\$(python generate-netfilter-u32-dns-rule.py --qname **NI** --qtype ANY)

rule=\$(python generate-netfilter-u32-dns-rule.py --qname **nL** --qtype ANY)

ANY-attack on .nl

~~-A RL -s 2001:db8::/32 -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT~~
~~-A RL -s 2001:db8::/32 -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT~~
~~-A RL -m state --state NEW -m udp -p udp --dport 53 -m limit --limit 30/minute --limit-burst 90 -j ACCEPT~~
~~-A RL -m state --state NEW -m tcp -p tcp --dport 53 -m limit --limit 30/minute --limit-burst 90 -j ACCEPT~~

Response Rate Limiting (RRL)

- Available for BIND, NSD and Knot
- <http://www.redbarn.org/dns/ratelimits>

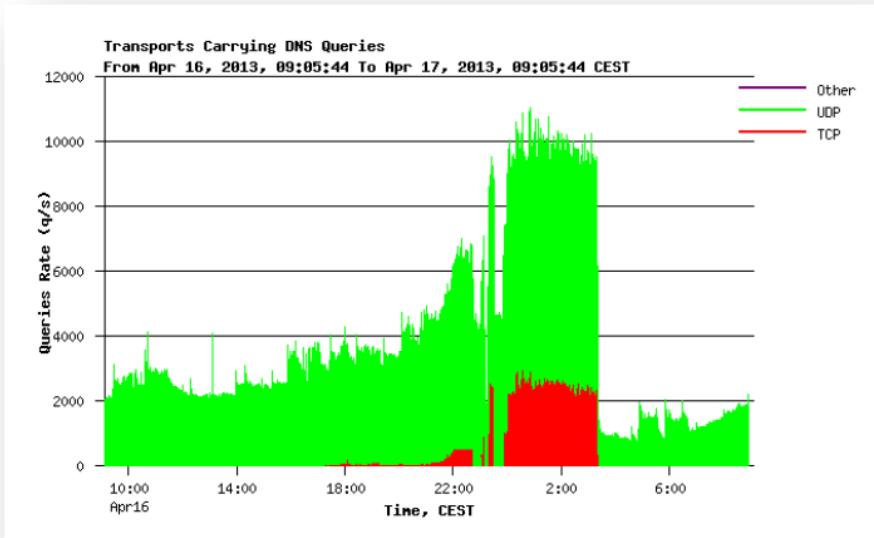
Response Rate Limiting (RRL)

- Several configurable parameters
- In particular: ‘slip’

When a query would be dropped due to rate limiting, RRL randomly sends back a truncated response instead, once per ‘TC-RATE’ queries. This tells a victim whose address is being forged to retry using TCP.

```
+ Internet Protocol Version 4, Src: 91.203.212.8 (91.203.212.8), Dst: 192.168.100.2 (192.168.100.2)
+ User Datagram Protocol, Src Port: domain (53), Dst Port: 8577 (8577)
- Domain Name System (response)
  [Request In: 511]
  [time: 0.014566000 seconds]
  Transaction ID: 0x8175
  Flags: 0x8620 (Standard query response, No error)
    1.... .... .... = Response: Message is a response
    .000 0.... .... = Opcode: Standard query (0)
      1..... .... = Authoritative: Server is an authority for domain
      ....1.... .... = Truncated: Message is truncated
      ....0.... .... = Recursion desired: don't do query recursively
      ....0.... .... = Recursion available: Server can't do recursive queries
      ....0.... .... = Z: reserved (0)
      ....1.... .... = Answer authenticated: Answer/authority portion was authenticated by the server
      0..... .... = Non-authenticated data: Unacceptable
```

ANY-attack on .nl (with RRL)



The good news: DNS-attacks went away!

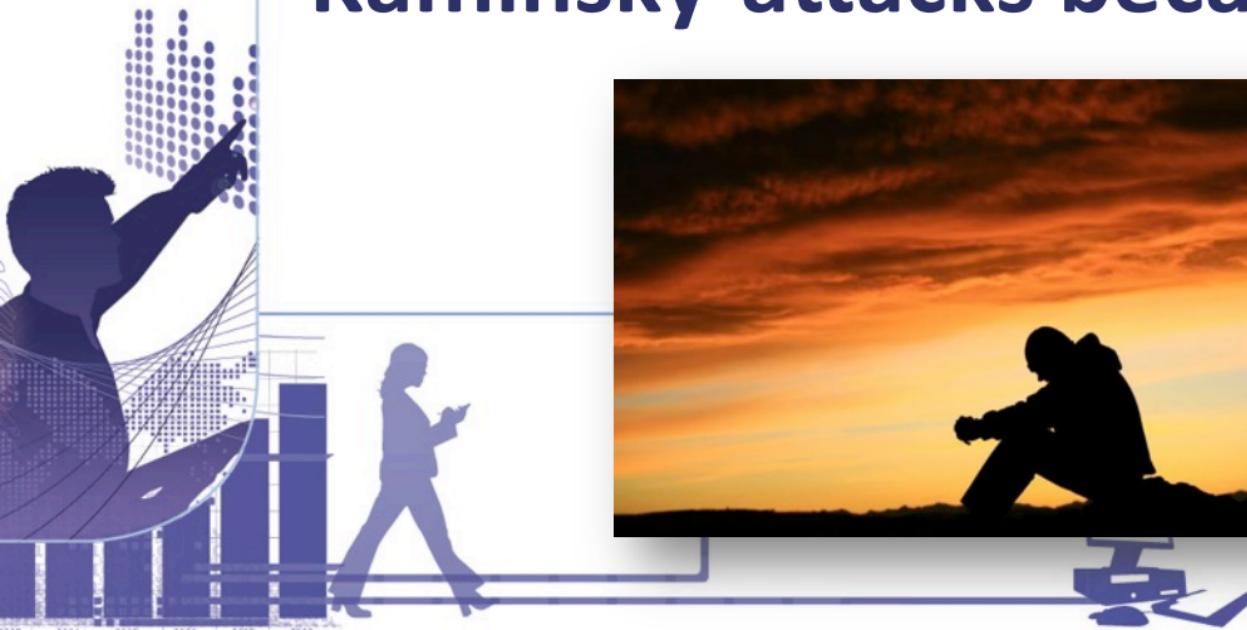




The bad news: Kaminsky-attacks became easier...



CVE-2013-5661



What can I do?

- **Implement BCP38**
- **Shut down ‘open resolvers’**
- **Enable RRL**
- **Monitor your infrastructure**
- **Enable DNSSEC (validation)**



Questions?

Marco Davids

Technical Advisor

marco.davids@sidn.nl

@marcodavids

