“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
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:

<table>
<thead>
<tr>
<th>PROTOCOL</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>DNS Reflection/Amplification</td>
<td>Spoofing DNS queries from the target of the attack towards DNS providers, to generate large responses that overwhelm the bandwidth of the attack target.</td>
</tr>
<tr>
<td>TCP</td>
<td>Connect</td>
<td>This flood involves a client repeatedly creating a full TCP session.</td>
</tr>
<tr>
<td>TCP</td>
<td>SYN</td>
<td>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.</td>
</tr>
<tr>
<td>UDP</td>
<td>UDP Flood</td>
<td>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.</td>
</tr>
<tr>
<td>ICMP</td>
<td>ICMP Flood</td>
<td>This flood involves ICMP packets that contain data; because ICMP does not require a session, this flood type is a good candidate for spoofing.</td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTP Flood</td>
<td>These floods inundate a target with HTTP requests (typically GET and POST requests).</td>
</tr>
<tr>
<td></td>
<td>Slowloris</td>
<td>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.</td>
</tr>
<tr>
<td>SSL</td>
<td>SSL Renegotiation</td>
<td>This attack type involves a client repeatedly performing an SSL handshake on an established SSL connection to consume a server’s resources.</td>
</tr>
</tbody>
</table>

(source: Verisign DDoS malware whitepaper)
Attack vectors

- Upstream Internet Congestion
- Internet Link Congestion
- Router CPU Exhaustion
- Router TCAM/Buffer Exhaustion
- Mitigation Exhaustion
- Firewall CPU / Memory Exhaustion
- Server CPU Exhaustion
- Server Session Exhaustion
- Application Session Exhaustion
- Database Connection Exhaustion
- Server Resource Exhaustion

CPU/Session Exhaustion
**Attack vectors (2)**

- Internet pipe (saturation): 27% (2011), 26% (2012)
- Firewall: 24% (2011), 25% (2012)
- IPS/IDS: 8% (both years)
- The server under attack: 30% (2011), 22% (2012)
- SQL Server: 5% (2011), 8% (2012)

(source: KPN presentation)
Who, for what?
Who, for what?

- Kiddies
- Distraction (from another attack)
- Blackmail
- Hacktivism
- Cyber warfare / terrorism
Who, for what?

(source: Carbon60)
What?! Gamers??

Error
You have been disconnected from the Call of Duty®: Black Ops II servers.

Disconnected.
The online lobby system has disconnected. There may be connection issues between you and the online lobby servers. Check your internet connection, firewall and router.

LAG KILLS
Gaming, gaming, gaming...

[source: http://www.twitch.tv]
Gaming sometimes is big $$$

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

(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.

(source: http://www.businessinsider.com)
Trend

(source: Radware)
Trend

(source: Arbor)
DDoS means business
DDoS means business

<mi0_ydftp> hey
<mi0_ydftp> come in pm
<Al-Majourhi>Hello
<Al-Majourhi> can you help me
<mi0_ydftp> sure
<mi0_ydftp> How much is the pay and who is the target?
<mi0_ydftp> goodbye
<Al-Majourhi> are you here
== No such nick/channel: mi0_ydftp
<Al-Majourhi> Hey back
<mi0_ydftp> 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)
<mi0_ydftp> Who?
<mi0_ydftp> basketball against US Bank?
<mi0_ydftp> 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 1GB/s right? Answer carefully.
<mi0_ydftp> We can do that. how can you pay/
<mi0_ydftp> Do you have 'name' of someone I dealt with recently so we can expedite this process.
<Al-Majourhi> Op Operation Abduit
<Al-Majourhi> Same guys.
<mi0_ydftp> got that, good.
<mi0_ydftp> Contact me on agbimrvy@sharklasers.com - and we can talk more.
<mi0_ydftp> I have to gto now.
<mi0_ydftp> You have payment means available now - I can do $200 for 1K hours, any target.
<mi0_ydftp> Make the contact we can deal.
== mi0_ydftp [web1rc@AN-143.4vr.fmlr1.IP] has quit [Quit:]
DDoS means business
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’…

(source: http://www.anonware.net/)
Step 2: IP address found

That wasn’t too hard now, was it?
Step 3: Initiate a DDoS...

My cool DDoS-stresser, I mean stress**TEST**er ;-)
Step 3: Initiate a DDoS...

Here’s another example (of the many out there)
DDoS means business
DDoS means business

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.
DDoS means business
DDoS means business

HACKFORUMS DDoS Booter Ecosystem

(source: Prolexic)
Modus operandi
of DNS amplification

• Open recursive resolvers
• Authoritative name servers
DNS Amplification/reflection
Specially crafted RR’s

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 !!
Activate botnet

Spoofed queries

Open Recursive resolvers

Problem 1: Spoofing is (still) rather easy

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

(source: https://spoofer.cmand.org/)
Problem 2: many (!) open resolvers

- Roughly 30,000,000 worldwide
- ~180,000 in the Netherlands
- ~32,000 in Norway

(source: http://openresolverproject.org)
Problem 2: many (!) open resolvers

- ~180,000 in the Netherlands
- ~120,000 in AS5390...
- Huwei 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://dnsscan.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 is even more interesting
Activate botnet

Spoofed queries (ANY .nl)
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 Nl --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.
ANY-attack on .nl (with RRL)
The good news: DNS-attacks went away!
The bad news: Kaminsky-attacks became easier...
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