

Open DNS Servers, NTP monlist BCP38

Otmar Lendl
<lendl@cert.at>

About a year ago ...



The screenshot shows a news article from June 3, 2013, titled "Spamhaus-style DDoS attacks: All the hackers are doing it". The article is categorized under "SECURITY" and includes a quote: "'All you need is 10 lines of code and a lot of patience'". A comment bubble indicates 16 comments, with a snippet: "Hackers are increasingly turning to DNS reflection to amplify the volume of distributed denial of service (DDoS) attacks." The article is by John Leyden, who has 2,411 followers. A CloudFlare banner is visible at the top of the article content. At the bottom, a network traffic monitor shows Inbound and Outbound traffic statistics for a 24-hour period.

	04:00	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00	22:00	00:00	02:00
Inbound	Current: 53.01 G	Average: 46.82 G	Maximum: 118.52 G									
Outbound	Current: 49.63 G	Average: 57.51 G	Maximum: 80.33 G									

A few weeks ago ...

 **Matthew Prince**
@eastdakota Follow

Very
us r

KrebsOnSecurity

In-depth security news and investigation

Techn Radar Pro - News - New DDoS attack breaks Spamhaus records

New DDoS attack breaks Spamhaus records

D-Day for DDoS

14 The

FEB 14



By Dean Wilson 12th Feb 2014 | 14:00

COMMENTS

Over the past attacks intended to knock it offline. Earlier this week, KrebsOnSecurity was hit by easily the most massive and intense such attack yet – a nearly 200 Gbps assault leveraging a simple attack method that industry experts say is becoming alarmingly common.

 **Oles**
@olesovh

En ce mo
réseau re
350Gbps
VAC fait s

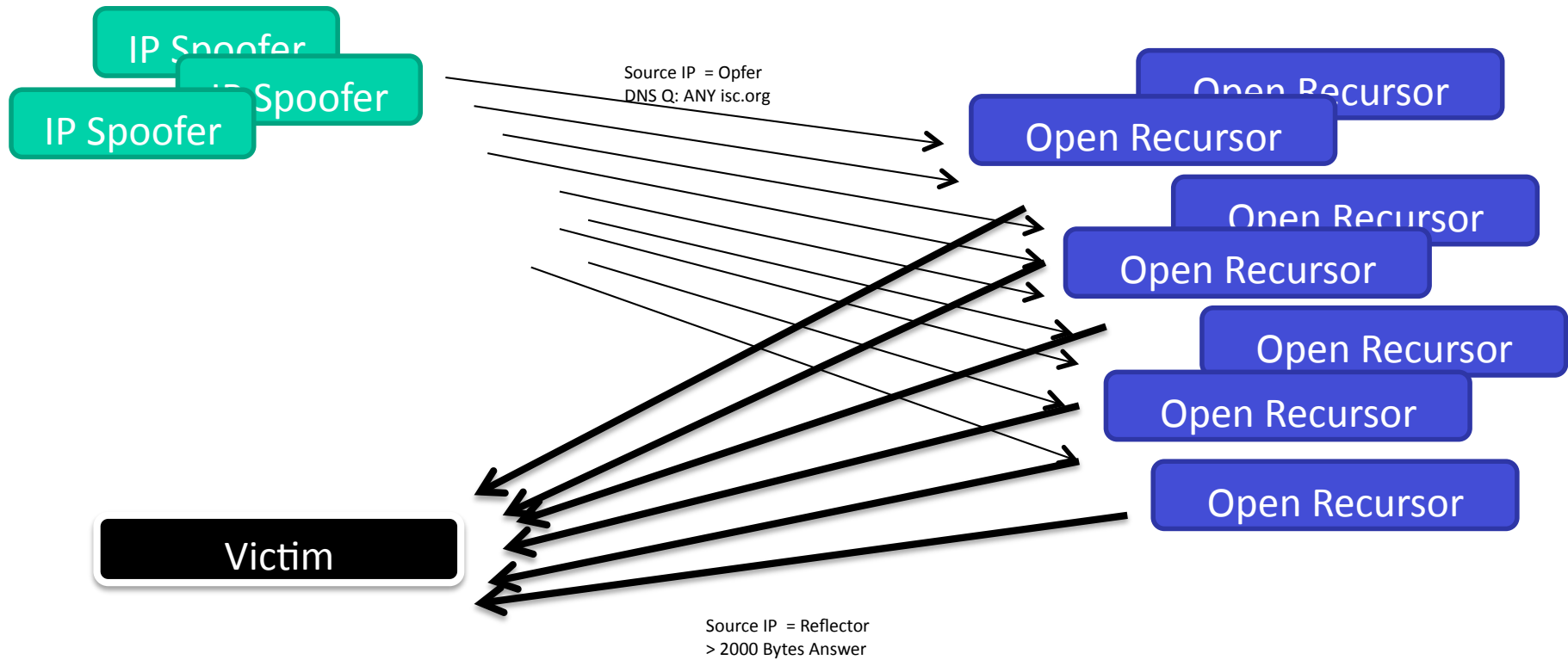
Reply Retweet Favorite more

RETWEETS 40 FAVORITES 18



4:36 PM - 10 Feb 2014

DNS Reflection Attack



Summary Reflected DDOS



- The victim only sees packets from the reflectors, not the attacker
- The reflectors only see the spoofed packets
- Amplification:
 - DNS: up to factor 100
 - NTP: with monlist, up to 1000
- Mitigation by filtering/rate-limiting might be possible

- See also
 - <http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks>
 - Other protocols as well:
http://www.internetsociety.org/sites/default/files/01_5.pdf

What do we need to do?



- Prevent IP Address Spoofing
- Reduce number of reflectors/amplificators
- Trace-back capabilities
- Control Plane protection
- Cooperation during attacks

TODO 1: Anti-Spoofing



- Prohibit IP Address Spoofing
 - BCP38: Network Ingress Filtering
 - <http://tools.ietf.org/html/bcp38>
 - <http://www.bcp38.info/>
 - BCP84: Ingress Filtering for Multihomed Networks
 - <https://tools.ietf.org/html/bcp84>
 - The closer to the customer, the easier and better
 - **Datacenter**, DSL, Cable, leased lines, ...
 - Small ISPs: filter towards the upstream
 - Automate!

TODO 2: Secure Servers



- Remove amplifiers from our networks
 - Analogue to open SMTP relays or smurf amplifiers
- DNS
 - No open recursors
 - <http://openresolverproject.org/>
 - Rate-Limit on authoritative servers
 - <http://www.redbarn.org/dns/ratelimits>
- NTP
 - Restrict access
 - Disable control commands
 - <http://openntpproject.org/>
- chargin
 - No, it is not 1992 any more
- ...

TODO 3: Traceback!

- We need to know who is generating spoofed packets
 - Otherwise we will not get the required pressure
- Assuming an amplicator in **your** network: can you trace back the forged packets?
- Tools & Processes & Skills
 - Netflow -> Interface
 - How to trace back over shared IXP LANs?

TODO 4: Protect yourself

- The Spamhaus DDOS last year:
 - Initially against web servers
 - Then against the unicast addresses of Cloudflare sites
 - Then against the interface address of the supporting routers
 - Then against the IXP address of the ISP
- Thus:
 - Protect your control plane
 - Ideally: filter traffic towards routers as early as possible
 - Do we need to announce the IXP prefix?

TODO 5: Cooperation!



- Smaller (i.e. not Tier1) networks cannot mitigate every attack
- Mitigation needs cooperation
 - Establish rapport with your upstreams
 - What can they do manually?
 - Automatic features (remote triggered blackholing?)
 - Get to know your peers / CERTs / LE
- Plan ahead:
 - See Barry Greene's „The Service Provider Tool Kit”
<http://www.nanog.org/meetings/abstract?meet=54>

Outlook

- We're seeing significant DDOS activity
- Booter services offer that for minimal money
- Extortion racket in Asia

- **We need to fix this.**

- If not, we're opening ourselves up for regulatory intervention.

Questions?



Otmar Lendl <lendl@cert.at>

+43 1 5056416 711