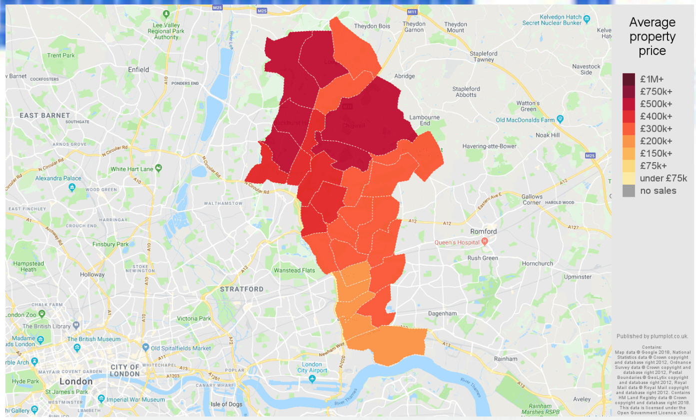
Wrong, **wrong, WRONG!** methods of DDoS mitigation

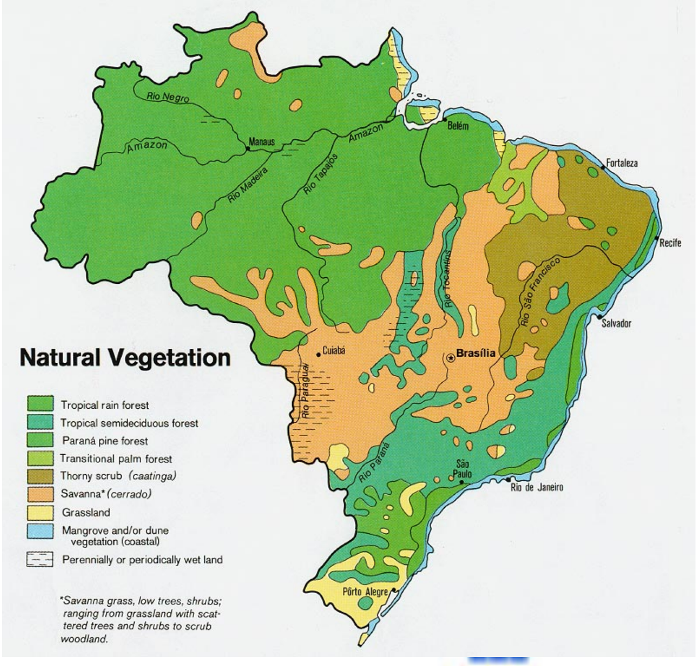
Töma Gavrichenkov <ag@qrator.net>

“On the wrong day
of the wrong week
I used the wrong method
with the wrong technique.”

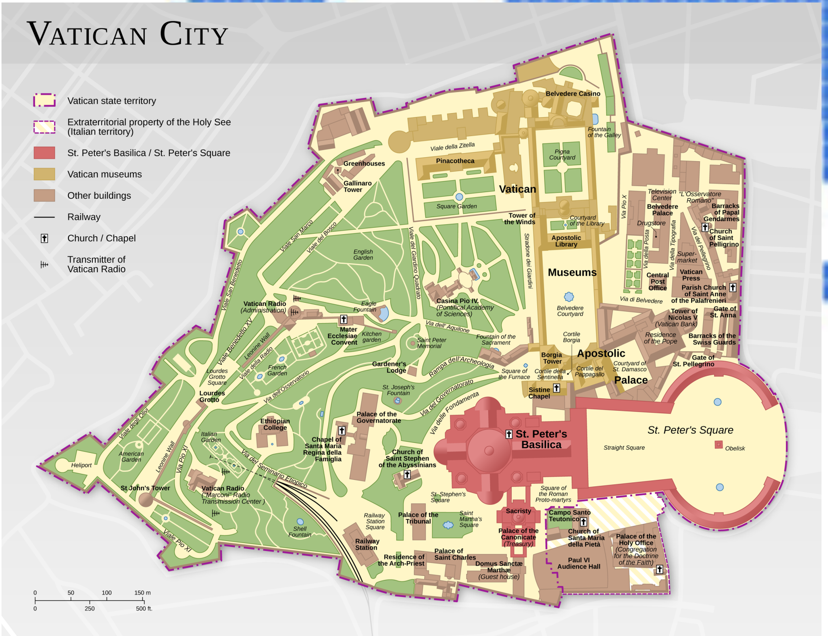
— Depeche Mode.



Average property price
£1M+
£750k+
£500k+
£400k+
£300k+
£200k+
£150k+
£75k+
under £75k
no sales
Published by plumplot.co.uk



Natural Vegetation
Tropical rain forest
Tropical semideciduous forest
Paraná pine forest
Transitional palm forest
Thorny scrub (caatinga)
Savanna* (cerrado)
Grassland
Mangrove and/or dune vegetation (coastal)
Perennially or periodically wet land
*Savanna grass, low trees, shrubs; ranging from grassland with scattered trees and shrubs to scrub woodland.
Rio Negro
Amazon
Manaus
Belém
Fortaleza
Recife
Salvador
Cuiabá
Brasília
Rio de Janeiro
São Paulo
Pôrto Alegre
Rio Madeira
Rio Tapajós
Rio São Francisco
Rio Paraná
Rio Paraguai



Vatican City
Vatican state territory
Extraterritorial property of the Holy See (Italian territory)
St. Peter's Basilica / St. Peter's Square
Vatican museums
Other buildings
Railway
Church / Chapel
Transmitter of Vatican Radio
St. Peter's Square
St. Peter's Basilica
Apostolic Palace
Museums
Vatican
Belvedere Casino
Pinacotheca
Sistine Chapel

中国茶叶博物馆
China National Tea Museum
示意图
Map
Twin fragrant paths
双香径
本馆质量方针：
零缺陷，传承茶叶文化；
零起点，创建名胜景观；
零距离，增进观众满意。
本馆环境方针：
严格守法，致力文物保护；
全员进取，提供绿色服务；
节能降耗，提高环境绩效。
0571-87964221

Blocking *known attack sources*

- Also known as:
  “I’m not expecting Chinese customers,
  why don’t we just deny access to the Chinese IPs?”

Redlining

"...In the United States, ***redlining*** *is the systematic denial of various services to residents of specific neighborhoods or communities, either directly or through the selective raising of prices."*

— Wikipedia.

Network Redlining

Why is it a bad idea?

- GeoIP databases are unofficial
  and have no mandatory policy on corrections
- IP addresses get sold and bought
- Some IP networks are being used
  far from the original RIR
- Anycast

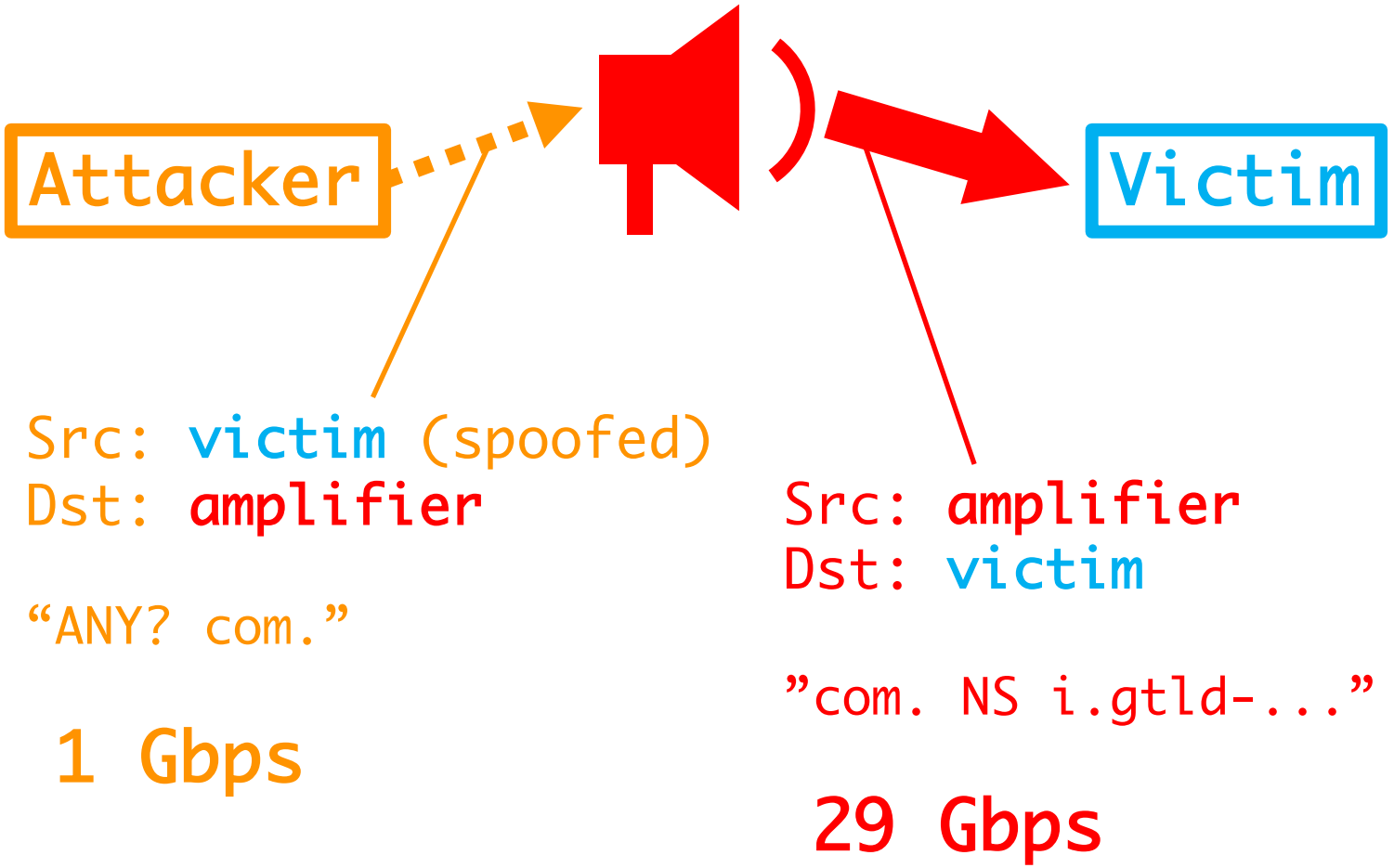
Network Redlining

- GeoIP databases are unofficial
  and have no mandatory policy on corrections
- IP addresses get sold and bought
- Some IP networks are being used
  far from the original RIR
- Anycast

Some of the above might be better with IPv6.

Amplification DDoS?

A premise:
40 Gbps of unwanted DNS traffic coming from source port 53



Amplification DDoS?

A premise: 40 Gbps of unwanted DNS traffic coming from source port 53

- A solution here?
  Use blocklists/Flowspec/RTBH to drop traffic from known reflection *sources*!

- Why is it a bad idea?

A True Story

- An enterprise got those 40 Gbps of DNS traffic
- Decided to parse the source IP addresses of reflectors and populate a blocklist

A True Story

- An enterprise got those 40 Gbps of DNS traffic
- Decided to parse the source IP addresses of reflectors and populate a blocklist

- 2 hours after, the attacker started enumerating IPv4 0/0 within empty packets' sources (with source UDP port 53)
- Started with most popular ISP access prefixes

A True Story

- An enterprise got those 40 Gbps of DNS traffic
- Decided to parse the source IP addresses of reflectors and populate a blocklist

- 2 hours after, the attacker started enumerating IPv4 0/0 within empty packets' sources (with source UDP port 53)
- Started with most popular ISP access prefixes
- 8 hours later, nothing is working, ~1 bln IPv4 in blocklist

Lesson 2

- **No** blocklists without remote IP address authentication
- **Especially** in the case of amplification/reflection

But what if...

...we check that there’s actually an amplifier?

But what if...

...we check that there’s actually an amplifier?

Then such a check may fail due to a
(..tada..)

But what if...

...we check that there's actually an amplifier?

Then such a check may fail due to a
(..tada..)

network redlining on the other side!

Sound bytes

- **No** blocklists without remote IP address authentication
- **Avoid** network redlining
- **Stop** breaking the Internet!

mailto: Töma Gavrichenkov <ag@qrator.net>

CC BY-SA credits

- https://commons.wikimedia.org/wiki/File:DaveGahanbyNOA-HASSIN.JPG
- https://commons.wikimedia.org/wiki/Atlas_of_Brazil