IP Anti Spoofing

How to avoid the "bad guys"

Fernando García/Tecnocom
Juan Pedro Cerezo/BT GS

Tecnocom

What is?

- A document to help configure routers
- Sponsored by Daniel Karrenberg & Nina Hjorth Bargisen
- Writen by Fernando Garcia & Juan Pedro Cerezo

Tecnocom

Reasons behind

- Botnets usually employ forged addresses to avoid trace of origin
- This botnets are used for DoS attacks, spam, etc.
- We can reduce the impact of this attacks

Tecnocom

Benefits

- For the ISP
  - Reduced bandwidth
  - Avoid being filtered by other ISPs
- For the community
  - Reduce the attacks
- Long-term strategy

Tecnocom

Purpose

- How to filter bad address
- Simple set of rules and examples
- Not a perfect solution
  - But if everybody follows it, we would reduce the impact of attacks
- For IPv4 and IPv6

Tecnocom

What to do

- Filter prefixes that CLEARLY are incorrect
- Filter BOGON prefixes
- Use uRPF
  - Strict
  - Feasible
  - Loose

Tecnocom

BOGON

- No, It's not a StarTrek name
- "a route that should never appear in the Internet routing table" (cymru)

Tecnocom

BOGONS in IPv4:

- RFC 1918 (172.16.x.x, 192.168.x.x 10.x.x.x)
- Loopbacks (127.x.x.x)
- Rendezvous (169.254.x.x)
- Example (192.0.2.x)
- Testing (198.18.x.x)
- Reserved (240.x.x.x)

Tecnocom

BOGONS in IPv6:

- 3FFE::/16 are explicit denied - this /16 is not in use anymore according to 6bone and ICANN rules
- 2001:db8::/32 is explicitely denied because is reserved for documentation purposes
- 0000::/8 is denied (loopback, unspecified, v4-mapped)
- •0000::/8 is denied (loopback, unspecified,

Tecnocom

More BOGONS

- Unasigned:
  - IANA reserved for the future:
    - 0/8, 1/8, 2/8, 5/8, 7/8, 10/8, 23/8, 27/8, 31/8, 36/8, 37/8, 39/8, 42/8, 46/8, 94/8, 95/8, 100-115/8, 173-187/8, 197/8
- BE CAREFULL: This list changes!!!
- If you don't keep current, risk of blocking legal addresses to your customers/users

Tecnocom

Vendor specifics

- Cisco & Juniper (no information from other vendors)
- Both support source address filtering
- Both support uRPF
- Juniper by default allows source address routing: disable it

Tecnocom

Scenarios

- Single router, single provider
- Multiple router, single provider, redundant
- Multiple router, single provider, load balancing
- Multiple providers
- Internal networks
- Access networks

Tecnocom

Scenarios (2)

- Logical explanation
- Examples/Templates for Cisco & Juniper

Tecnocom

Single router/Single provider

- CPE: Reject bogons + my own address
- PE: Accept only customer prefixes
- uRPF strict

Tecnocom

Multiple router/Single provider, redundant

- CPE: similar to the previous one
- PE: uRPF strict & filtering of prefix

Tecnocom

Multiple router/Single provider, load balancing

- Customer side, similar and/or dynamic routing
- Provider: dynamic routing
- uRPF loose

Tecnocom

Single router/Multiple providers

- CPE: BOGON filter lists, uRPF loose
- PE: Customer prefix lists, uRPF loose

Tecnocom

CPE inner networks

- Internal networks with public addresses
- One interface:
  - stric uRPF + BOGON list
- Many interfaces:
  - feasible path uRPF + BOGON list

Tecnocom

Access Networks

- Usually: dynamic address assignement (RADIUS, DHCP)
- strict uRPF

Tecnocom

Core networks

- Usually, only BOGON filtering feasible
- scripts based on routing database registries

Tecnocom

Conclusion

- Not the perfect solution
- Not the best solution
- but if everybody implements it, we could reduce the attacks by a very important scale

Tecnocom

Draft document

- http://www.lab.bt.es/tf-spoofing/howto.txt

Tecnocom

Q&A

fernando.garcia@tecnocom.es

Tecnocom