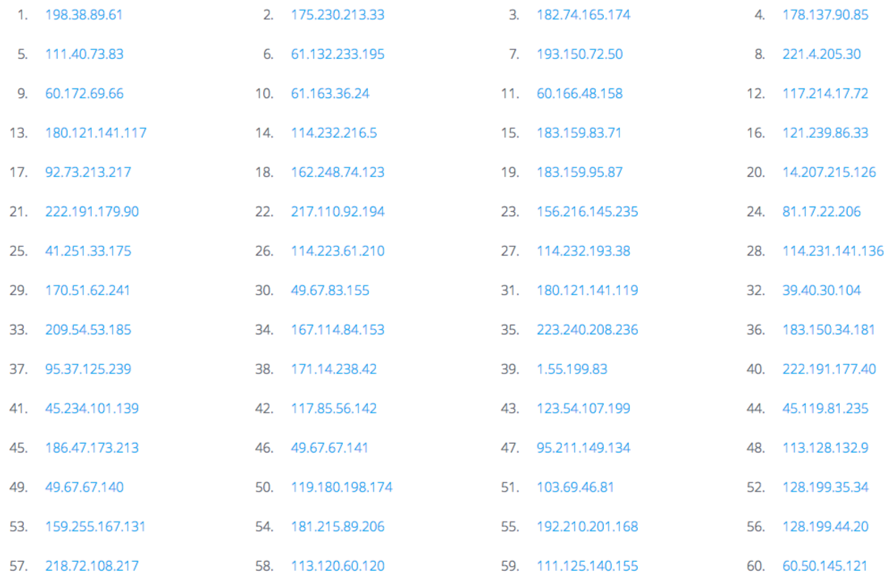
Quantifying the Impact of Blocklisting in the Age of Address Reuse

Sivaram Ramanthan , Anushah Hossain, Jelena Mirkovic, Minlan Yu and Sadia Afroz

IP Blocklists

- IP Blocklists contain a list of known malicious IP addresses.

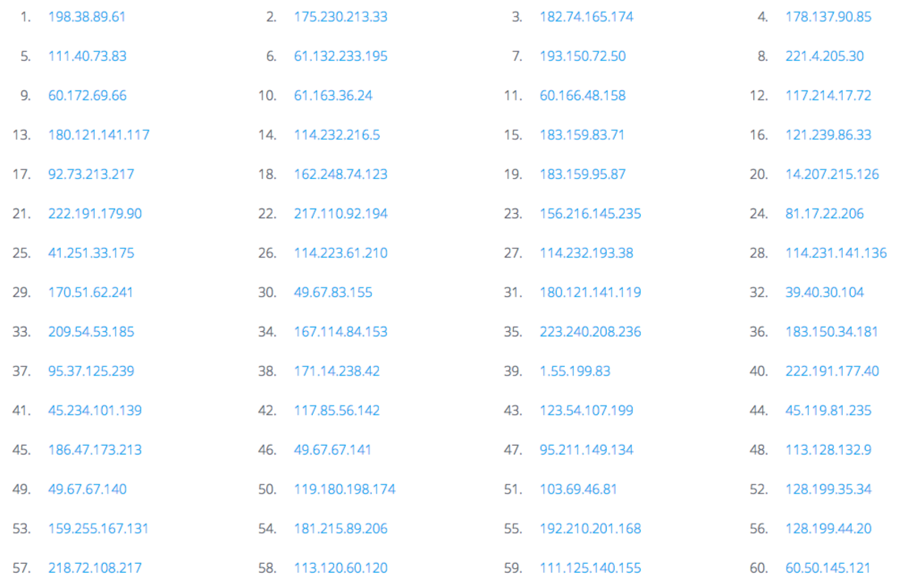
- IP Blocklists are commonly used to block attack traffic.



1. 198.38.89.61
2. 175.230.213.33
3. 182.74.165.174
4. 178.137.90.85
5. 111.40.73.83
6. 61.132.233.195
7. 193.150.72.50
8. 221.4.205.30
9. 60.172.69.66
10. 61.163.36.24
11. 60.166.48.158
12. 117.214.17.72
13. 180.121.141.117
14. 114.232.216.5
15. 183.159.83.71
16. 121.239.86.33
17. 92.73.213.217
18. 162.248.74.123
19. 183.159.95.87
20. 14.207.215.126
21. 222.191.179.90
22. 217.110.92.194
23. 156.216.145.235
24. 81.17.22.206
25. 41.251.33.175
26. 114.223.61.210
27. 114.232.193.38
28. 114.231.141.136
29. 170.51.62.241
30. 49.67.83.155
31. 180.121.141.119
32. 39.40.30.104
33. 209.54.53.185
34. 167.114.84.153
35. 223.240.208.236
36. 183.150.34.181
37. 95.37.125.239
38. 171.14.238.42
39. 1.55.199.83
40. 222.191.177.40
41. 45.234.101.139
42. 117.85.56.142
43. 123.54.107.199
44. 45.119.81.235
45. 186.47.173.213
46. 49.67.67.141
47. 95.211.149.134
48. 113.128.132.9
49. 49.67.67.140
50. 119.180.198.174
51. 103.69.46.81
52. 128.199.35.34
53. 159.255.167.131
54. 181.215.89.206
55. 192.210.201.168
56. 128.199.44.20
57. 218.72.108.217
58. 113.120.60.120
59. 111.125.140.155
60. 60.50.145.121

IP Blocklists

- IP Blocklists contain a list of known malicious IP addresses.
- IP Blocklists are commonly used to block attack traffic.
- Blocking reused addresses can lead to unjust blocking of many more users.



1. 198.38.89.61
2. 175.230.213.33
3. 182.74.165.174
4. 178.137.90.85
5. 111.40.73.83
6. 61.132.233.195
7. 193.150.72.50
8. 221.4.205.30
9. 60.172.69.66
10. 61.163.36.24
11. 60.166.48.158
12. 117.214.17.72
13. 180.121.141.117
14. 114.232.216.5
15. 183.159.83.71
16. 121.239.86.33
17. 92.73.213.217
18. 162.248.74.123
19. 183.159.95.87
20. 14.207.215.126
21. 222.191.179.90
22. 217.110.92.194
23. 156.216.145.235
24. 81.17.22.206
25. 41.251.33.175
26. 114.223.61.210
27. 114.232.193.38
28. 114.231.141.136
29. 170.51.62.241
30. 49.67.83.155
31. 180.121.141.119
32. 39.40.30.104
33. 209.54.53.185
34. 167.114.84.153
35. 223.240.208.236
36. 183.150.34.181
37. 95.37.125.239
38. 171.14.238.42
39. 1.55.199.83
40. 222.191.177.40
41. 45.234.101.139
42. 117.85.56.142
43. 123.54.107.199
44. 45.119.81.235
45. 186.47.173.213
46. 49.67.67.141
47. 95.211.149.134
48. 113.128.132.9
49. 49.67.67.140
50. 119.180.198.174
51. 103.69.46.81
52. 128.199.35.34
53. 159.255.167.131
54. 181.215.89.206
55. 192.210.201.168
56. 128.199.44.20
57. 218.72.108.217
58. 113.120.60.120
59. 111.125.140.155
60. 60.50.145.121

ALIEN VAULT

SPAMHAUS

SNORT

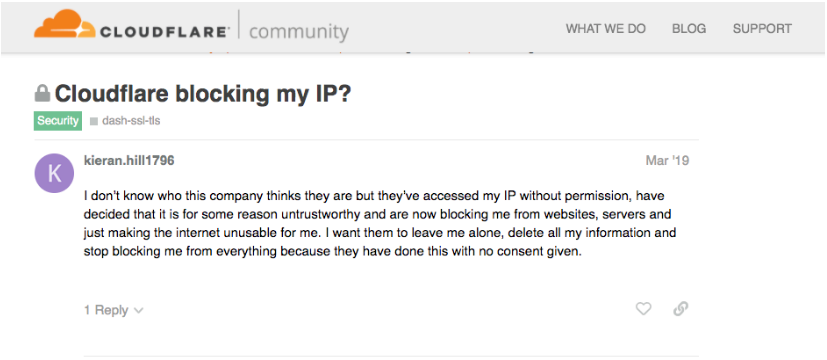
PROJECT HONEY POT

Malwarebytes

Case 1: Blocklisting Reused Addresses: NAT

https://community.cloudflare.com/t/cloudflare-blocking-my-ip/65453/57

Case 1: Blocklisting Reused Addresses: NAT



Cloudflare blocking my IP?

Security dash-ssl-tls

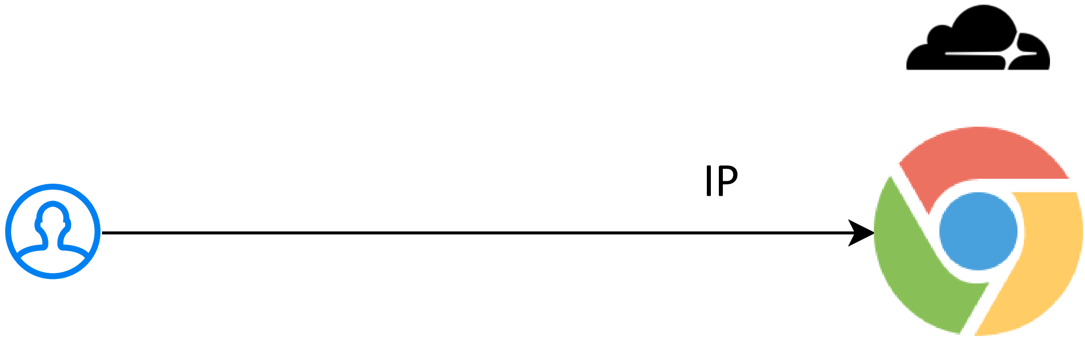
kieran.hill1796 Mar '19

I don't know who this company thinks they are but they've accessed my IP without permission, have decided that it is for some reason untrustworthy and are now blocking me from websites, servers and just making the internet unusable for me. I want them to leave me alone, delete all my information and stop blocking me from everything because they have done this with no consent given.

1 Reply

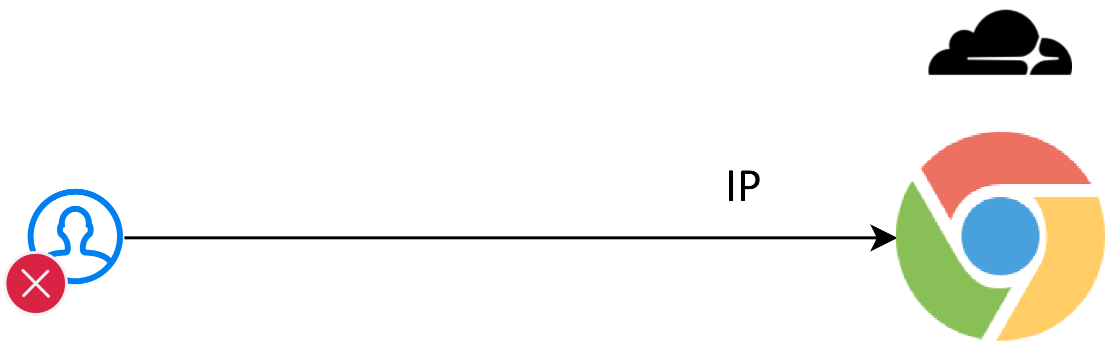
https://community.cloudflare.com/t/cloudflare-blocking-my-ip/65453/57

Case 1: Blocklisting Reused Addresses: NAT



https://community.cloudflare.com/t/cloudflare-blocking-my-ip/65453/57

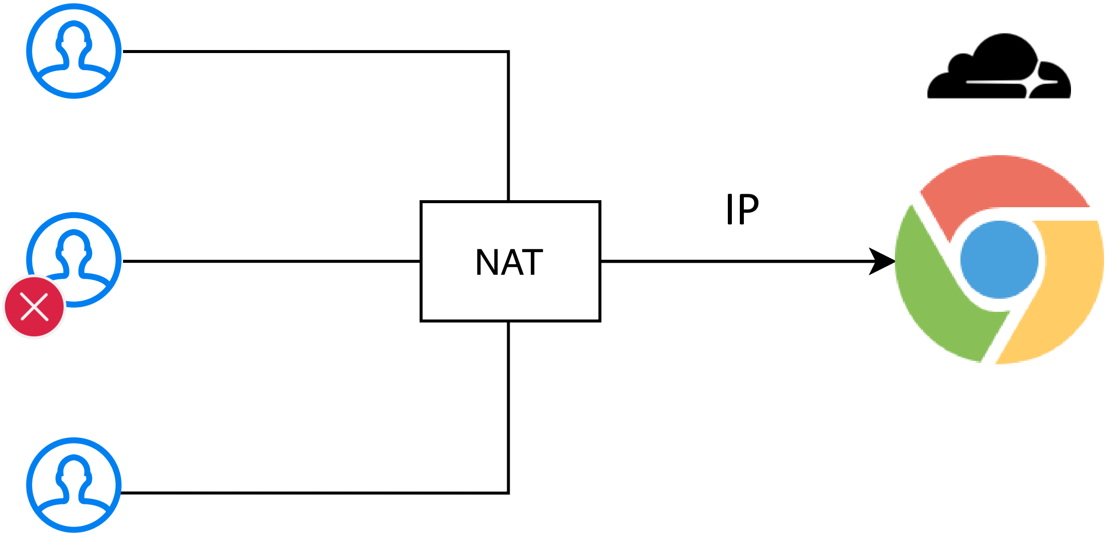
Case 1: Blocklisting Reused Addresses: NAT



Cloudflare uses Dshield blocklist.

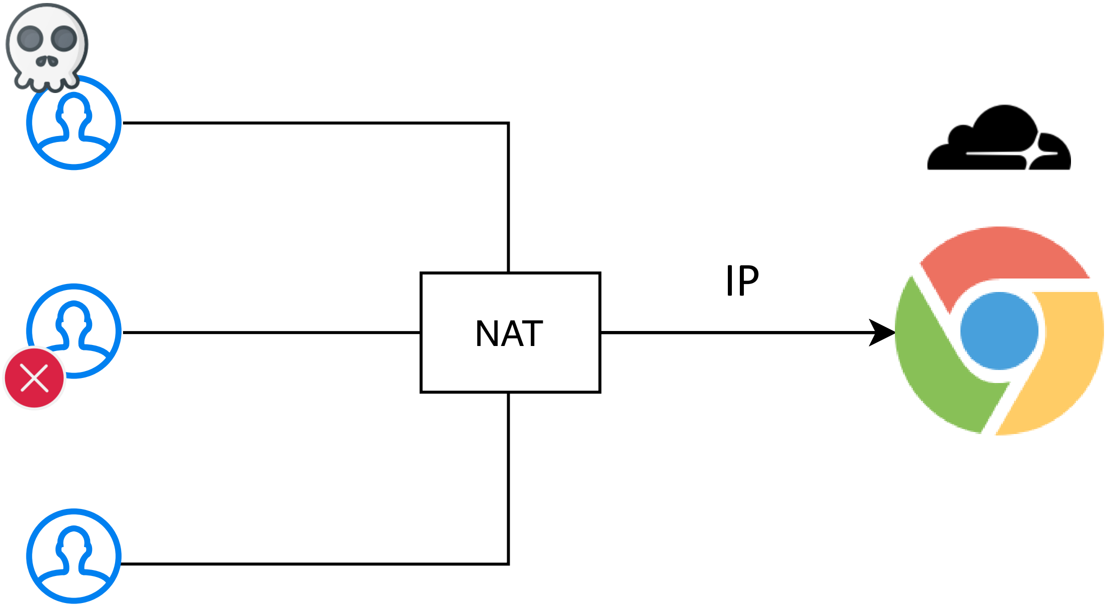
https://community.cloudflare.com/t/cloudflare-blocking-my-ip/65453/57

Case 1: Blocklisting Reused Addresses: NAT



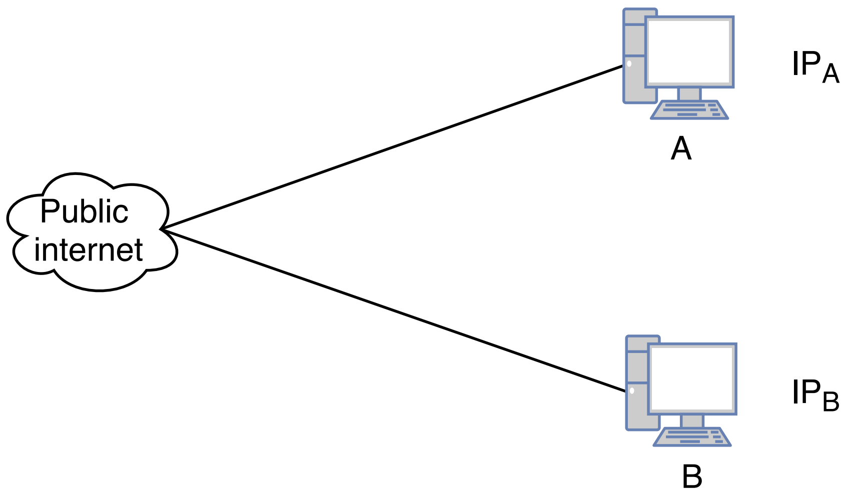
https://community.cloudflare.com/t/cloudflare-blocking-my-ip/65453/57

Case 1: Blocklisting Reused Addresses: NAT

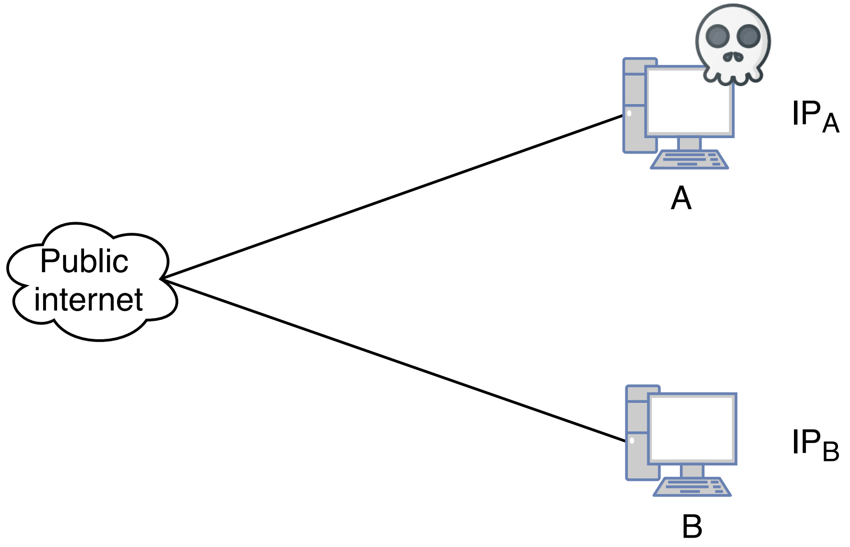


https://community.cloudflare.com/t/cloudflare-blocking-my-ip/65453/57

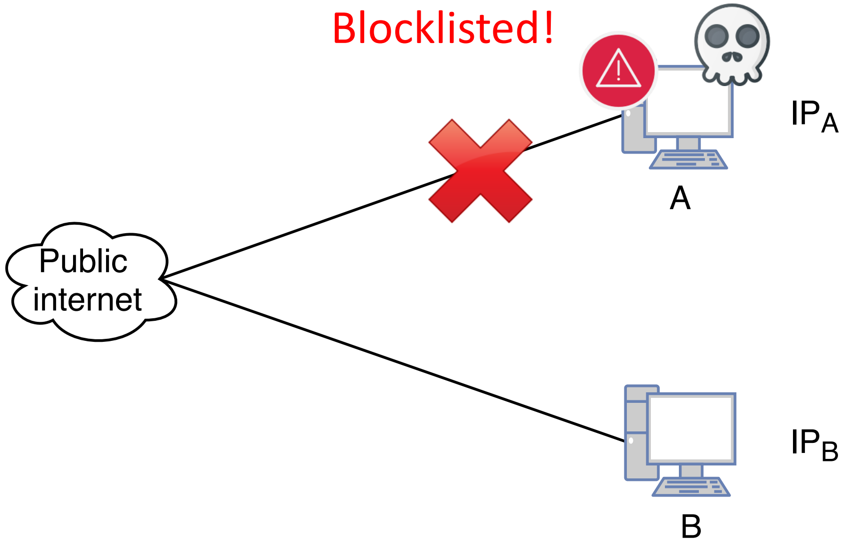
Case 2: Blocklisting Reused Addresses: Dynamic Addressing



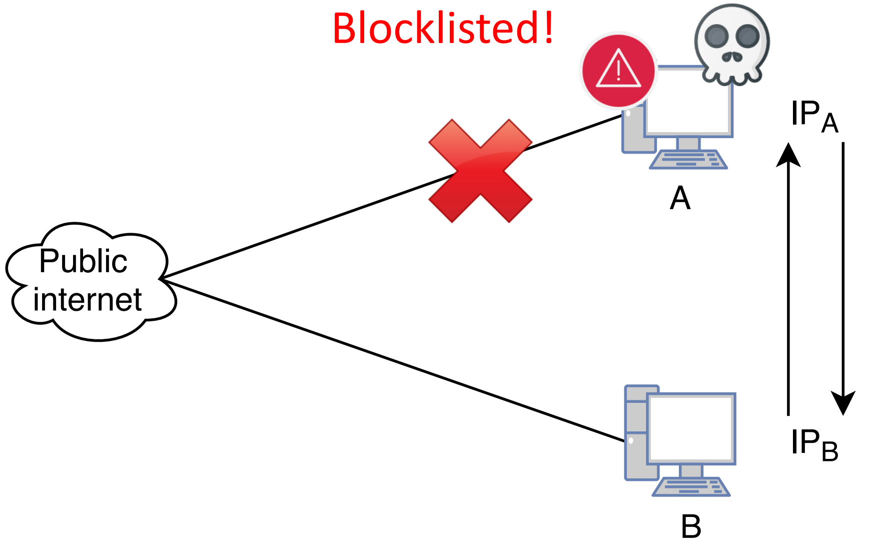
Case 2: Blocklisting Reused Addresses: Dynamic Addressing



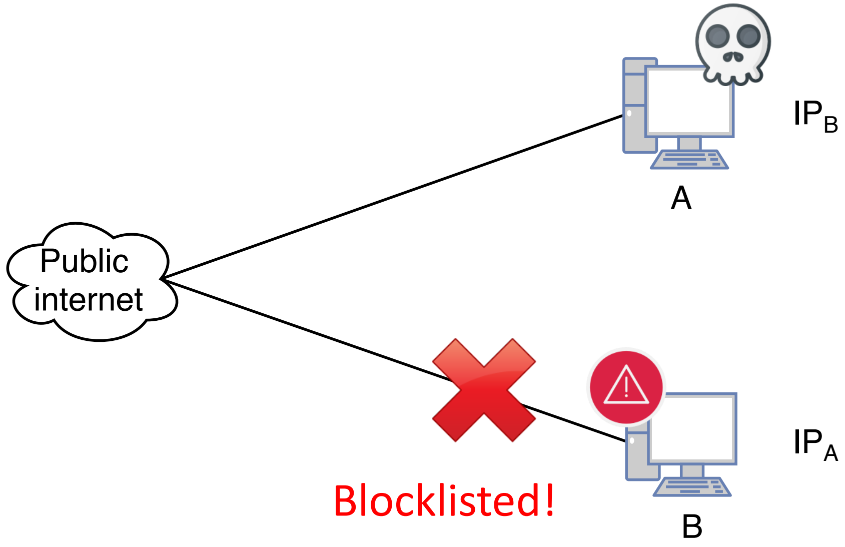
Case 2: Blocklisting Reused Addresses: Dynamic Addressing



Case 2: Blocklisting Reused Addresses: Dynamic Addressing



Case 2: Blocklisting Reused Addresses: Dynamic Addressing



Public internet

IP_B

A

Blocklisted!

IP_A

B

Usage and Perception of Blocklists

- Surveyed 40 network operators to understand usage of blocklists and their anecdotal experiences on blocklisting reused addresses.
- Blocklists are commonly used and used for active defense:
  - 70% of operators used blocklists and 60% of them use blocklists to directly block traffic.

Usage and Perception of Blocklists

- Surveyed 40 network operators to understand usage of blocklists and their anecdotal experiences on blocklisting reused addresses.
- Blocklists are commonly used and used for active defense:
    - 70% of operators used blocklists and 60% of them use blocklists to directly block traffic.
- Blocklists can have inaccuracies due to reused addresses:
    - About 56--76% of operators feel inaccuracies in blocklists due to reused addresses.

What is our study?

Quantifying the Impact of Blocklisting

- Accurately identifying reused addresses.

- Identifying blocklists that list such reused addresses.

- Quantifying the impact of blocking reused addresses.

Quantifying the Impact of Blocklisting

- Accurately identifying reused addresses.
  - Two techniques using a BitTorrent DHT crawler and RIPE atlas measurement logs.
- Identifying blocklists that list such reused addresses.
- Quantifying the impact of blocking reused addresses.

Quantifying the Impact of Blocklisting

- Accurately identifying reused addresses.
  - Two techniques using a BitTorrent DHT crawler and RIPE atlas measurement logs.
- Identifying blocklists that list such reused addresses.
  - 151 publicly available blocklists used for detecting variety of malicious users.
- Quantifying the impact of blocking reused addresses.

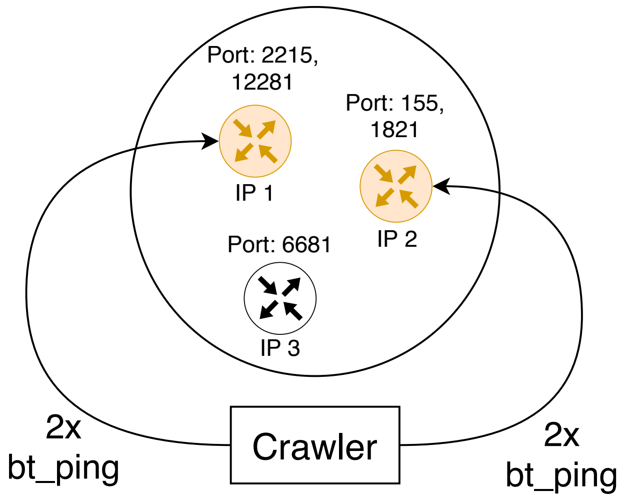
Quantifying the Impact of Blocklisting

- Accurately identifying reused addresses.
  - Two techniques using a BitTorrent DHT crawler and RIPE atlas measurement logs.
- Identifying blocklists that list such reused addresses.
  - 151 publicly available blocklists used for detecting variety of malicious users.
- Quantifying the impact of blocking reused addresses.
  - Impact on the number of addresses potentially affected due to blocking reused addresses.

Our Techniques.

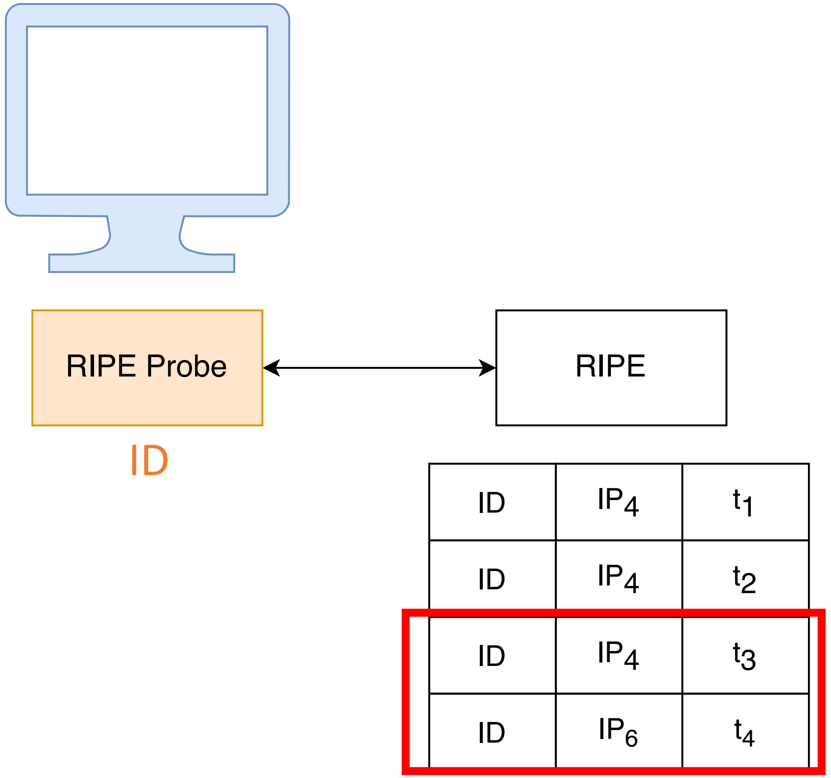
Detecting Reused NATed addresses

- We use the BitTorrent Network to identify users that are allocated the same IP address.
- The BitTorrent protocol allows two messages that helps us identify NATted users accurately.
  - *get_nodes*: Returns a list of active neighbors to a node.
  - *bt_ping*: Periodically pings active neighbors.



Detecting Dynamic Addresses

- RIPE atlas measurement logs contain the IP addresses allocated to RIPE probes over time.
- Analyzing the monitoring logs, we can obtain RIPE probes that are potentially in dynamically allocated address spaces.



ID	IP_4	t_1
ID	IP_4	t_2
ID	IP_4	t_3
ID	IP_6	t_4

IP4 and IP6 are potentially dynamically allocated.

Quantifying Impact with Blocklists

- We use the BLAG dataset that actively maintains blocklisted addresses from public blocklists.
- 151 blocklists that monitor variety of attacks including Spam, DDoS, malware hosting or reputation of IP addresses.
- Monitoring period of 83 days over two measurement periods.
- Observed 2.2M blocklisted IP addresses.

Key Results.

Key Results

- How many Blocklists list reused addresses?
  - NATed reused addresses: 29.7K addresses in 61 blocklists
  - Dynamic reused addresses: 22.7K addresses in 72 blocklists

Key Results

- How many Blocklists list reused addresses?
  - NATed reused addresses: 29.7K addresses in 61 blocklists
  - Dynamic reused addresses: 22.7K addresses in 72 blocklists
- How long are reused addresses present in blocklists?
  - Reused addresses are removed quicker than other blocklisted addresses (3—9 days).
  - 77% of all dynamic addresses are removed within 2 days.

Key Results

- How many Blocklists list reused addresses?
  - NATed reused addresses: 29.7K addresses in 61 blocklists
  - Dynamic reused addresses: 22.7K addresses in 72 blocklists
- How long are reused addresses present in blocklists?
  - Reused addresses are removed quicker than other blocklisted addresses (3—9 days).
  - 77% of all dynamic addresses are removed within 2 days.
- How many users are affected?
  - As many as 78 users can be potentially affected.

Thank You! Questions?

All detected reused addresses are present in:

https://steel.isi.edu/members/sivaram/blocklisting_impact/

All monitored blocklists are available at:

https://steel.isi.edu/Projects/BLAG/

USC University of Southern California

ICSI

VE RI TAS HARVARD