Illuminating Large-Scale IPv6 Scanning in the Internet

Philipp Richter, Oliver Gasser, and Arthur Berger

IETF-115 MAPRG
What is Scanning?

TCP SYN, e.g., port 23

e.g., “do you speak Telnet?”

“the Internet”
What is Scanning?

TCP SYN, e.g., port 23

e.g., “do you speak Telnet?”

“the Internet”
What is Scanning?

TCP SYN, e.g., port 23
e.g., “do you speak Telnet?”
TCP SYN ACK
“yes, I do — what’s up?”

“the Internet”
What is Scanning?

TCP SYN, e.g., port 23
  e.g., “do you speak Telnet?”
TCP SYN ACK
  “yes, I do — what’s up?”

“the Internet”

attempt(s) to exploit or abuse
What is Scanning?

Scanning is key for cyberattacks.

TCP SYN, e.g., port 23
  e.g., “do you speak Telnet?”

TCP SYN ACK
  “yes, I do — what's up?”

attempts to exploit or abuse

“the Internet”
Scanning in IPv4

- About 4 billion target addresses
e.g., 198.51.100.17

- Full scan in <1 hour

- Scan detection readily possible
  (e.g., using darknets)**

- Millions of monthly active scanners

** with limitations
Scanning in IPv4

• About 4 billion target addresses
e.g., 198.51.100.17

• Full scan in <1 hour

• Scan detection readily possible
  (e.g., using darknets)**

• Millions of monthly active scanners

Scanning in IPv6

• About $10^{38}$ target addresses
  e.g., 2001:db8:86e7:637:106c:d7dc:248:4a5d

• Trillions of years needed for full scan

• Detection not readily possible
  (need vantage points!)

• Extent of active scanning unknown

** with limitations
Scanning in IPv4

• About 4 billion target addresses
e.g., 198.51.100.17

• Full scan in <1 hour

• Scan detection readily possible
(e.g., using darknets)**

• Millions of monthly active scanners

Scanning in IPv6

• About $10^{38}$ target addresses
e.g., 2001:db8:86e7:637:106c:d7dc:248:4a5d

• Trillions of years needed for full scan

• Detection not readily possible
(need vantage points!)

• Extent of active scanning unknown

What’s going on in the IPv6 space?

** with limitations
First Longitudinal Study of Large-Scale IPv6 Scans

• 15 months of firewall logs of some 200,000+ CDN servers

• Double-check with publicly available traffic traces (MAWI)
First Longitudinal Study of Large-Scale IPv6 Scans

• 15 months of firewall logs of some 200,000+ CDN servers

• Double-check with publicly available traffic traces (MAWI)
First Longitudinal Study of Large-Scale IPv6 Scans

- 15 months of firewall logs of some 200,000+ CDN servers
- Double-check with publicly available traffic traces (MAWI)

Large-Scale IPv6 Scans:
Sources that target at least 100 DST IPs in either vantage point.
IPv6 Scan Sources over Time

IPv6 is now actively scanned. We find between ~10 and ~100 active weekly sources.
Traffic heavily concentrated on datacenter/cloud ASes.
## Top IPv6 Scan Source Networks

| rank | AS type                  | packets       | scan sources |
|------|--------------------------|---------------|--------------|
|      |                          | /48s /64s /128s |              |
| #1   | Datacenter (CN)          | 839M (39.2%)  | 1 1 1        |
| #2   | Datacenter (CN)          | 744M (34.8%)  | 1 1 5        |
| #3   | Cybersecurity (US)       | 275M (12.9%)  | 1 1 12       |
| #4   | Cloud (US/global)        | 78M (3.7%)    | 2 2 512      |
| #5   | Cloud (DE)               | 48M (2.3%)    | 3 59 59      |
| #6   | Cloud (US/global)        | 45M (2.1%)    | 10 15 205    |
| #7   | Cloud (US/global)        | 39M (1.8%)    | 9 9 123      |
| #8   | Cloud (CN)               | 30M (1.4%)    | 5 5 53       |
| #9   | Transit (global)         | 11M (0.5%)    | 1 2 956      |
| #10  | Cloud (CN)               | 10M (0.5%)    | 1 1 7        |
| #11  | Cloud (US/global)        | 4.7M (0.2%)   | 1 1 353      |
| #12  | Datacenter (CN)          | 3.1M (0.1%)   | 9 12 19      |
| #13  | ISP (VN)                 | 2.5M (0.1%)   | 1 1 1        |
| #14  | Datacenter (CN)          | 1.6M (≤ 0.1%) | 1 1 2        |
| #15  | Research (DE)            | 1.1M (≤ 0.1%) | 1 1 1        |
| #16  | ISP (RU)                 | 0.9M (≤ 0.1%) | 1 1 2        |
| #17  | University (DE)          | 0.8M (≤ 0.1%) | 1 1 2        |
| #18  | Cloud/Transit (DE)       | 0.6M (≤ 0.1%) | 1,092 1,057 1,057 |
| #19  | ISP (RU)                 | 0.6M (≤ 0.1%) | 1 1 1        |
| #20  | University (DE)          | 0.5M (≤ 0.1%) | 1 1 1        |

Traffic heavily concentrated on datacenter/cloud ASes.
Topmost Active IPv6 Scan Source

• Single most active source in CDN firewall and passive MAWI trace!

• Continually active for almost 2 years

• Scanning right now! (though changing ports targeted)

• Reported 1000s of times in open-source reputation data
Ports Targeted

• Majority of scans target *multiple* port numbers / services

• Behavior resembling that of general penetration testing as opposed to exploitation of specific vulnerabilities
## Top IPv6 Scan Source Networks

| rank | AS type            | packets    | scan sources |
|------|--------------------|------------|--------------|
|      |                    | 48s | /64s | /128s |
| #1   | Datacenter (CN)    | 839M | 1   | 1     | 1     |
| #2   | Datacenter (CN)    | 744M | 1   | 1     | 5     |
| #3   | Cybersecurity (US) | 275M | 1   | 1     | 12    |
| #4   | Cloud (US/global)  | 78M  | 2   | 2     | 512   |
| #5   | Cloud (DE)         | 48M  | 3   | 59    | 59    |
| #6   | Cloud (US/global)  | 45M  | 10  | 15    | 205   |
| #7   | Cloud (US/global)  | 39M  | 9   | 9     | 123   |
| #8   | Cloud (CN)         | 30M  | 5   | 5     | 53    |
| #9   | Transit (global)   | 11M  | 1   | 2     | 956   |
| #10  | Cloud (CN)         | 10M  | 1   | 1     | 7     |
| #11  | Cloud (US/global)  | 4.7M | 1   | 1     | 353   |
| #12  | Datacenter (CN)    | 3.1M | 9   | 12    | 19    |
| #13  | ISP (VN)           | 2.5M | 1   | 1     | 1     |
| #14  | Datacenter (CN)    | 1.6M | 1   | 1     | 2     |
| #15  | Research (DE)      | 1.1M | 1   | 1     | 1     |
| #16  | ISP (RU)           | 0.9M | 1   | 1     | 2     |
| #17  | University (DE)    | 0.8M | 1   | 1     | 2     |
| #18  | Cloud/Transit (DE) | 0.6M | 1,092 | 1,057 | 1,057 |
| #19  | ISP (RU)           | 0.6M | 1   | 1     | 1     |
| #20  | University (DE)    | 0.5M | 1   | 1     | 1     |

### Major Challenge: Identifying and isolating scan sources.
Key Challenge: Source Aggregation/Isolation

BGP announced prefix: 2001:db8::/32

SOURCE IP
2001:db8:86e7:3637:106c:d7dc:e248:4a5d
2001:db8:2c7a:b1e7:e808:499c:d5b8:35b9
2001:db8:16cd:3fe3:3210:e49f:70f4:e081
2001:db8:3af5:a3e0:d5f1:8885:f3f3:da78
2001:db8:bd8:72c4:5b7e:01da7:88cc:99e1
2001:db8:69eb:ade2:a2f8:da13:11ed:5702
2001:db8:fc5:3a12:3506:37eb:61c6:9322
2001:db8:b794:67d9:ec6c:38d7:daa3:71e9
2001:db8:a1f4:2409:f182:02d2:96c3:f96f
2001:db8:748e:22f1:fa81:0062:e3c6:8183
Key Challenge: Source Aggregation/Isolation

BGP announced prefix: 2001:db8::/32

AS A – cybersecurity company

one single scanning entity

SOURCE IP
2001:db8:86e7:3637:106c:d7dc:e248:4a5d
2001:db8:2c7a:b1e7:e808:499c:d5b8:35b9
2001:db8:16cd:3fe3:3210:e49f:70f4:e081
2001:db8:3af5:a3e0:d5f1:8885:f3f3:da78
2001:db8:bd8:72c4:5b7e:01da7:88cc:99e1
2001:db8:69eb:ade2:a2f8:da13:11ed:5702
2001:db8:flc5:3a12:3506:37eb:61c6:9322
2001:db8:b794:67d9:ec6c:38d7:daa3:71e9
2001:db8:a1f4:2409:f182:02d2:96c3:f96f
2001:db8:748e:22f1:fb9:0062:e3c6:8183

one single scan entity entire /32 prefix

BGP announced prefix: 2001:db9::/32

AS B – major cloud provider

VM-assinged ::/124

SOURCE IP
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:ba01
2001:db9:2143:11e4:6083:4e9f:ca01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:ba01
2001:db9:2143:11e4:6083:4e9f:ca01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:ba01
2001:db9:2143:11e4:6083:4e9f:ca01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:ba01
2001:db9:2143:11e4:6083:4e9f:ca01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:ba01
2001:db9:2143:11e4:6083:4e9f:ca01
Key Challenge: Source Aggregation/Isolation

AS A — cybersecurity company

SOURCE IP
2001:db8:86e7:3637:106c:d7dc:e248:4a5d
2001:db8:2c7a:b1e7:e808:499c:d5b8:35b9
2001:db8:16cd:3fe3:3210:e49f:70f4:e081
2001:db8:3af5:a3e0:d5f1:8885:f3f3:da78
2001:db8:bd8:72c4:5b7e:01da7:88cc:99e1
2001:db8:69eb:ade2:a2f8:da13:1led:5702
2001:db8:flc5:3a12:3506:37eb:61c6:9322
2001:db8:b794:67d9:ec6c:38d7:daa3:7le9
2001:db8:a1f4:2409:f182:02d2:96c3:ef6f
2001:db8:748e:22f1:fba1:0062:e3c6:8183

one single scan entity entire /32 prefix

AS B — major cloud provider

SOURCE IP
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01
2001:db9:2143:11e4:6083:4e9f:aa01

scanner A /124 prefix

scanner B /124 prefix

scanner C /124 prefix

Without aggregation, we miss some (or all) of scanning activity! With too much aggregation, we conflate scanners / block too much.
Key Findings

- The IPv6 space is actively being scanned!
- Detection - especially real-time - challenging
- More details in the paper!
  - Vantage points
  - Detection methodology
  - Details on services targeted, addresses targeted
  - And much more!

get the paper here:  https://tinyurl.com/v6scan
points to: https://dl.acm.org/doi/10.1145/3517745.3561452