DarkVec: Clustering Report

1 Cluster 0. Silhouette: 0.337

965 distinct senders with the following ground truth classes:

- Unknown. 950 senders
- Stretchoid. 14 senders
- Mirai-like. 1 sender

92547 packets sent in the last day. 2.7% of the last day traffic. 0.0% of cluster traffic has the Mirai fingerprint.

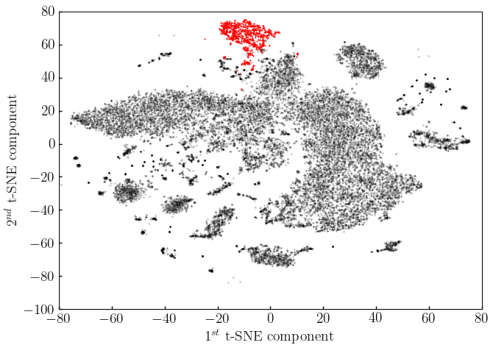


Figure 1: Cluster 0. t-SNE projection

882 distinct /24 subnets. The top-5 are:

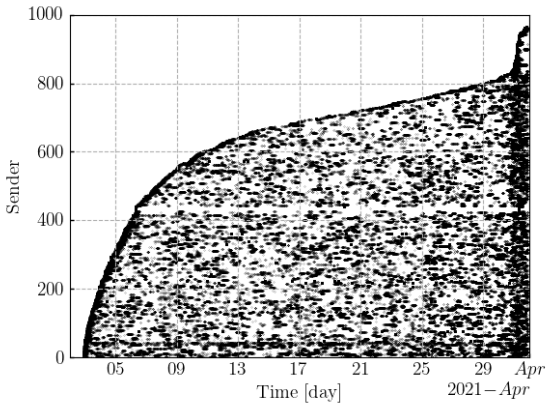
- 165.225.106.0 with 14 senders, 118.186.203.0 with 13 senders, 27.115.32.0 with 8 senders, 103.62.152.0 with 8 senders, 192.241.227.0 with 7 senders,

786 distinct /16 subnets. The top-5 are:

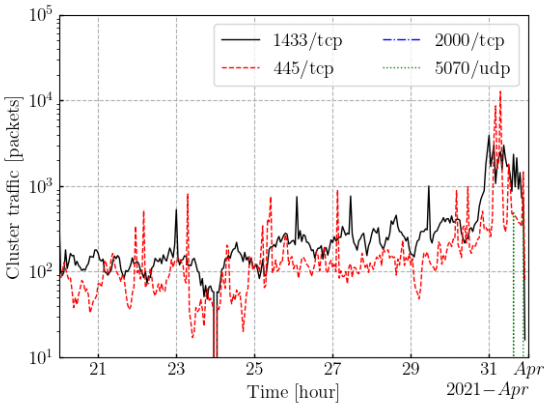
- 192.241.0.0 with 14 senders, 103.62.0.0 with 14 senders, 165.225.0.0 with 14 senders, 118.186.0.0 with 13 senders, 27.115.0.0 with 9 senders,

109 ports contacted. The top-5 are:

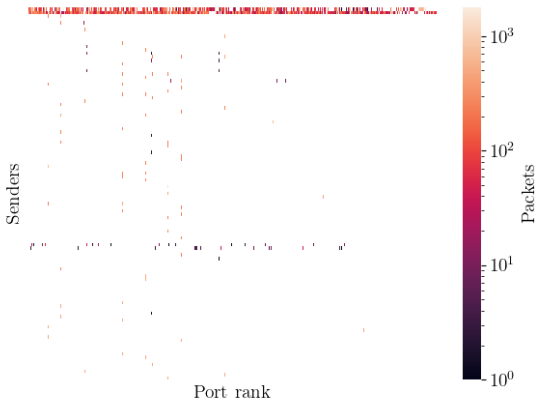
- 1433/tcp : 146834 sent packets (48.9 % of the monthly cluster traffic.) 845 senders contacted the port(87.6 % of the cluster senders.)
- 445/tcp : 110777 sent packets (36.9 % of the monthly cluster traffic.) 583 senders contacted the port(60.4 % of the cluster senders.)
- 2000/tcp : 1512 sent packets (0.5 % of the monthly cluster traffic.) 1 senders contacted the port(0.1 % of the cluster senders.)
- 5070/udp : 1265 sent packets (0.4 % of the monthly cluster traffic.) 2 senders contacted the port(0.2 % of the cluster senders.)
- 9200/tcp : 1264 sent packets (0.4 % of the monthly cluster traffic.) 5 senders contacted the port(0.5 % of the cluster senders.)



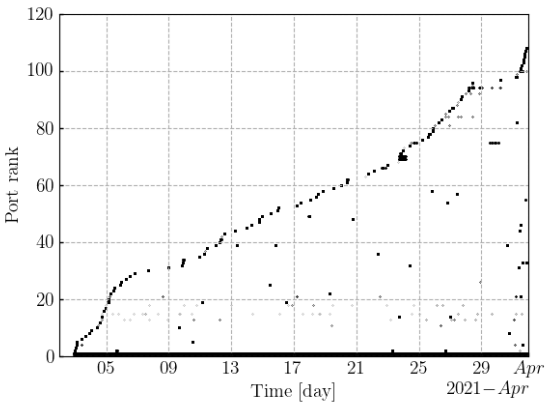
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 2: Cluster0 temporal patterns

2 Cluster 1. Silhouette: -0.025

166 distinct senders with the following ground truth classes:

- Censys. 112 senders
- Unknown. 52 senders
- Shodan. 2 senders

1548226 packets sent in the last day. 45.5% of the last day traffic.

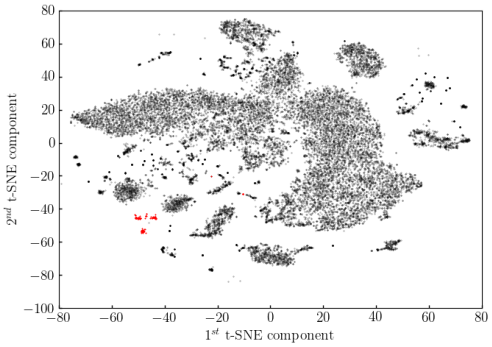


Figure 3: Cluster 1. t-SNE projection

35 distinct /24 subnets. The top-5 are:

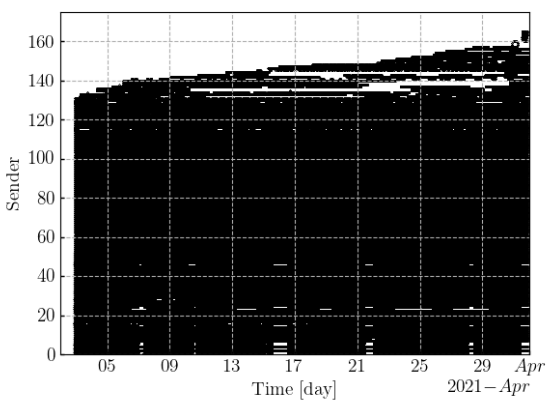
- 162.142.125.0 with 48 senders, 167.248.133.0 with 32 senders, 74.120.14.0 with 32 senders, 45.146.165.0 with 7 senders, 81.91.190.0 with 5 senders,

32 distinct /16 subnets. The top-5 are:

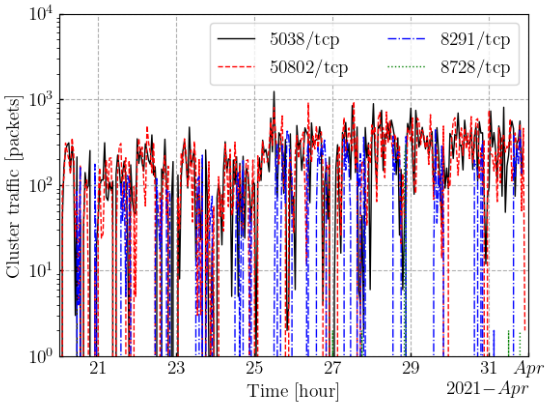
- 162.142.0.0 with 48 senders, 167.248.0.0 with 32 senders, 74.120.0.0 with 32 senders, 45.146.0.0 with 12 senders, 81.91.0.0 with 5 senders,

72796 ports contacted. The top-5 are:

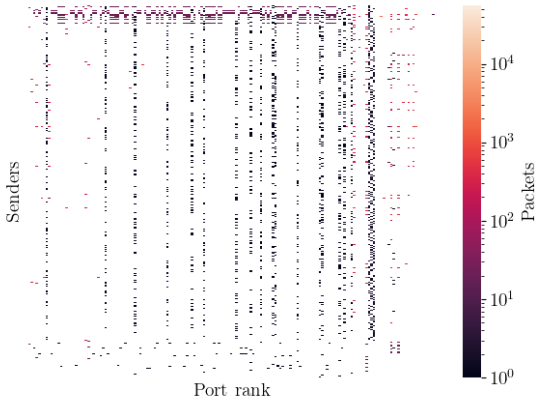
- 5038/tcp : 112634 sent packets (0.7 % of the monthly cluster traffic.) 15 senders contacted the port(9.0 % of the cluster senders.)
- 50802/tcp : 107134 sent packets (0.6 % of the monthly cluster traffic.) 8 senders contacted the port(4.8 % of the cluster senders.)
- 8291/tcp : 18401 sent packets (0.1 % of the monthly cluster traffic.) 9 senders contacted the port(5.4 % of the cluster senders.)
- 8728/tcp : 18138 sent packets (0.1 % of the monthly cluster traffic.) 8 senders contacted the port(4.8 % of the cluster senders.)
- 6666/tcp : 12769 sent packets (0.1 % of the monthly cluster traffic.) 68 senders contacted the port(41.0 % of the cluster senders.)



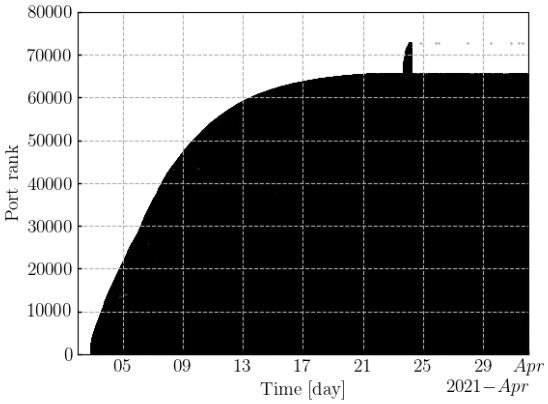
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 4: Cluster1 temporal patterns

3 Cluster 2. Silhouette: 0.506

794 distinct senders with the following ground truth classes:

- Mirai-like. 499 senders
- Unknown. 295 senders

261991 packets sent in the last day. 7.7% of the last day traffic. 0.7% of cluster traffic has the Mirai fingerprint.

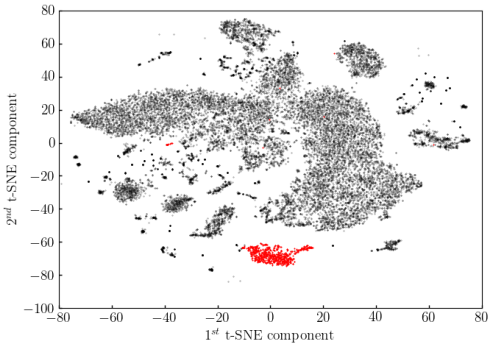


Figure 5: Cluster 2. t-SNE projection

773 distinct /24 subnets. The top-5 are:

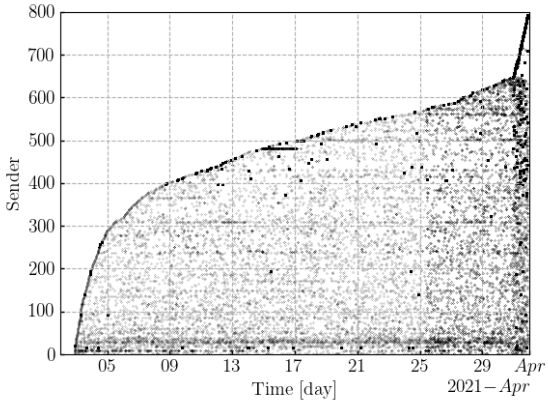
- 202.164.139.0 with 5 senders, 202.164.138.0 with 5 senders, 45.229.54.0 with 3 senders, 45.229.55.0 with 3 senders, 187.188.74.0 with 2 senders,

637 distinct /16 subnets. The top-5 are:

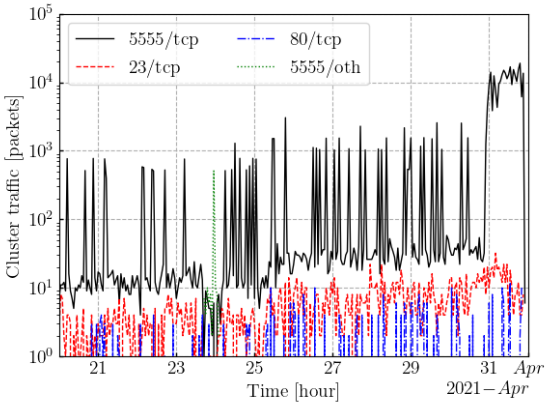
- 202.164.0.0 with 10 senders, 178.175.0.0 with 8 senders, 178.72.0.0 with 7 senders, 58.153.0.0 with 7 senders, 45.229.0.0 with 6 senders,

85 ports contacted. The top-5 are:

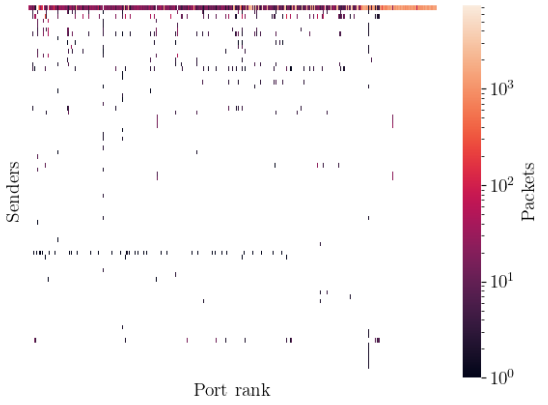
- 5555/tcp : 356505 sent packets (98.1 % of the monthly cluster traffic.) 784 senders contacted the port(98.7 % of the cluster senders.)
- 23/tcp : 3111 sent packets (0.9 % of the monthly cluster traffic.) 109 senders contacted the port(13.7 % of the cluster senders.)
- 80/tcp : 578 sent packets (0.2 % of the monthly cluster traffic.) 58 senders contacted the port(7.3 % of the cluster senders.)
- 5555/oth : 568 sent packets (0.2 % of the monthly cluster traffic.) 64 senders contacted the port(8.1 % of the cluster senders.)
- 8080/tcp : 420 sent packets (0.1 % of the monthly cluster traffic.) 54 senders contacted the port(6.8 % of the cluster senders.)



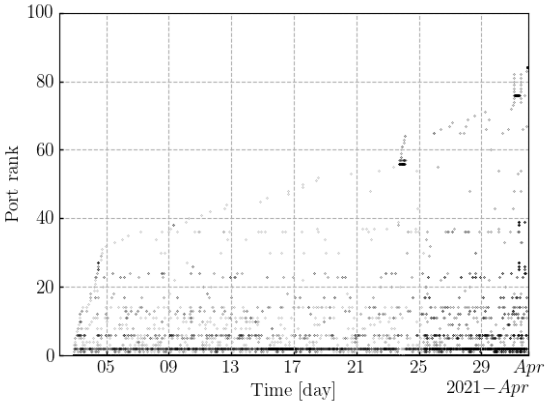
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 6: Cluster2 temporal patterns

4 Cluster 3. Silhouette: 0.738

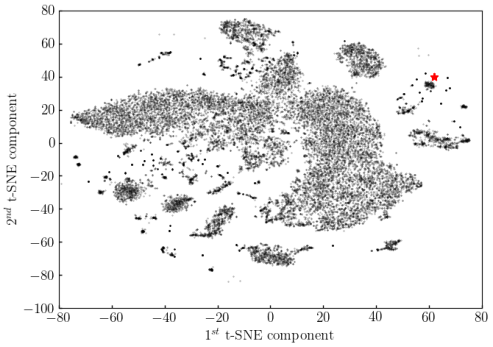


Figure 7: Cluster 3. t-SNE projection

14 distinct senders with the following ground truth classes:

- Shadowserver. 14 senders

784 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

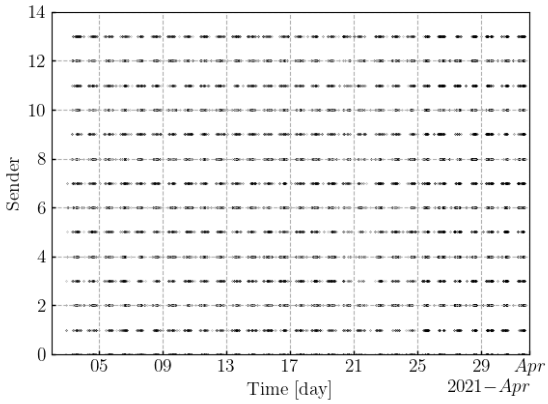
- 184.105.139.0 with 14 senders,

1 distinct /16 subnets. The top-5 are:

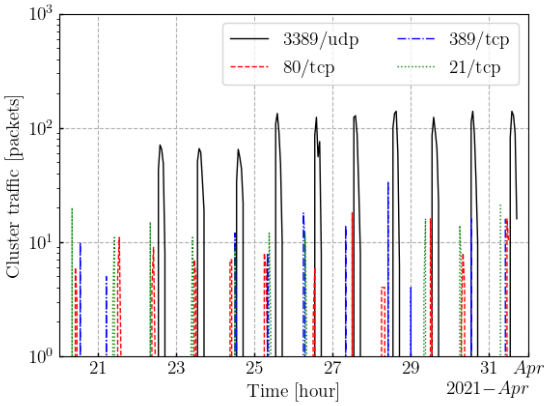
- 184.105.0.0 with 14 senders,

39 ports contacted. The top-5 are:

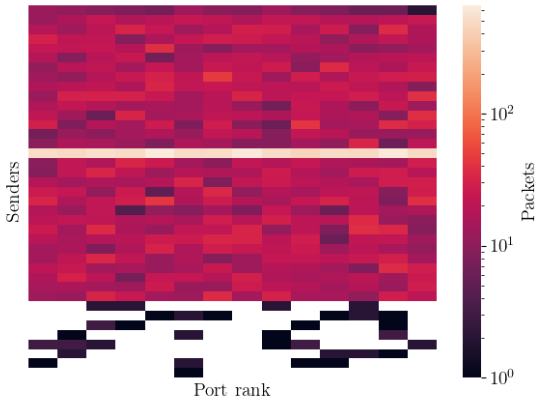
- 3389/udp : 7399 sent packets (48.1 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 80/tcp : 343 sent packets (2.2 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 389/tcp : 340 sent packets (2.2 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 21/tcp : 323 sent packets (2.1 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 449/tcp : 298 sent packets (1.9 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)



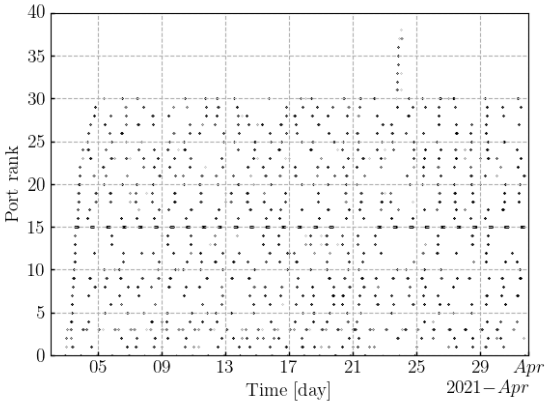
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 8: Cluster3 temporal patterns

5 Cluster 4. Silhouette: 0.452

1769 distinct senders with the following ground truth classes:

- Unknown. 1753 senders
- Mirai-like. 8 senders
- Ipip. 6 senders
- Stretchoid. 2 senders

61505 packets sent in the last day. 1.8% of the last day traffic. 0.2% of cluster traffic has the Mirai fingerprint.

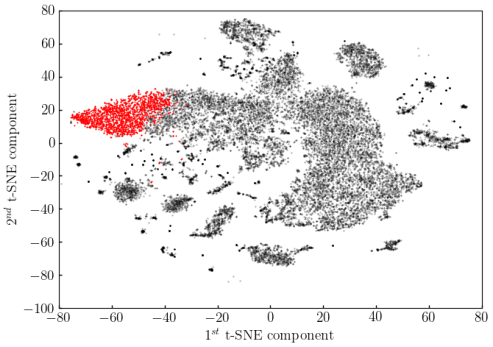


Figure 9: Cluster 4. t-SNE projection

1727 distinct /24 subnets. The top-5 are:

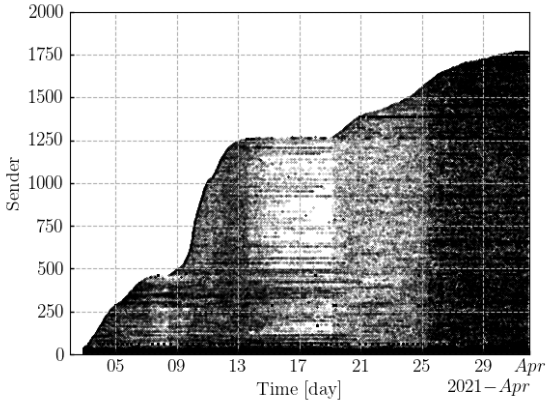
- 36.103.225.0 with 3 senders, 170.210.46.0 with 3 senders, 117.73.8.0 with 3 senders, 134.209.118.0 with 3 senders, 36.134.69.0 with 3 senders,

768 distinct /16 subnets. The top-5 are:

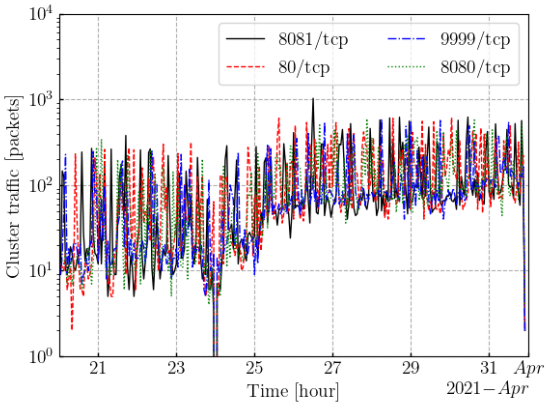
- 128.199.0.0 with 30 senders, 139.59.0.0 with 24 senders, 161.35.0.0 with 24 senders, 157.230.0.0 with 22 senders, 167.71.0.0 with 19 senders,

182 ports contacted. The top-5 are:

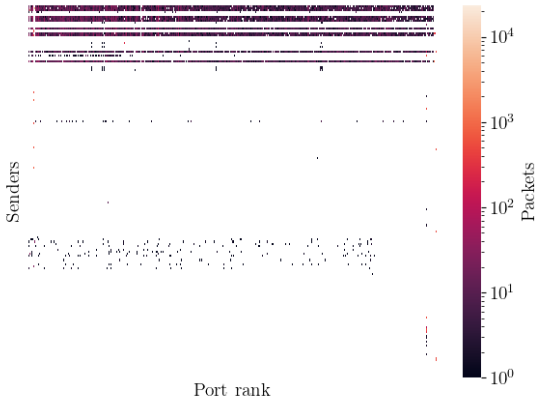
- 8081/tcp : 47850 sent packets (7.4 % of the monthly cluster traffic.) 1645 senders contacted the port(93.0 % of the cluster senders.)
- 80/tcp : 45553 sent packets (7.0 % of the monthly cluster traffic.) 1606 senders contacted the port(90.8 % of the cluster senders.)
- 9999/tcp : 38048 sent packets (5.9 % of the monthly cluster traffic.) 1650 senders contacted the port(93.3 % of the cluster senders.)
- 8080/tcp : 36472 sent packets (5.6 % of the monthly cluster traffic.) 1651 senders contacted the port(93.3 % of the cluster senders.)
- 8088/tcp : 36136 sent packets (5.6 % of the monthly cluster traffic.) 1667 senders contacted the port(94.2 % of the cluster senders.)



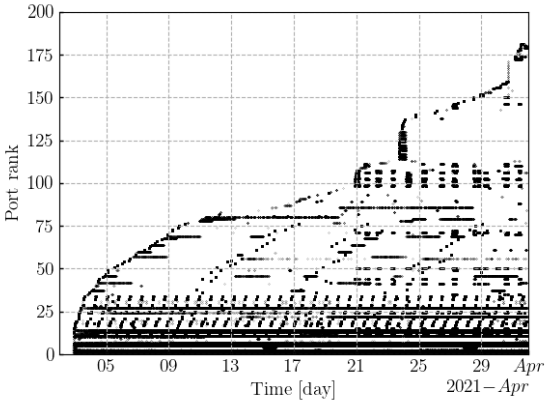
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 10: Cluster4 temporal patterns

6 Cluster 5. Silhouette: 0.469

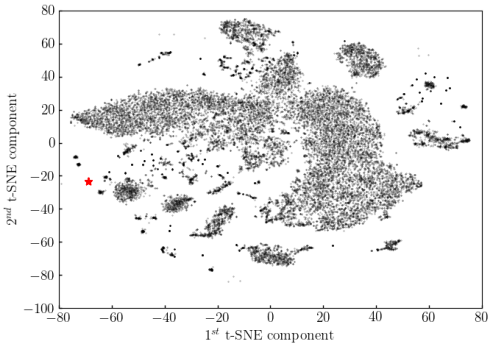


Figure 11: Cluster 5. t-SNE projection

23 distinct senders with the following ground truth classes:

- Shodan. 22 senders
- Unknown. 1 sender

20298 packets sent in the last day. 0.6% of the last day traffic.

19 distinct /24 subnets. The top-5 are:

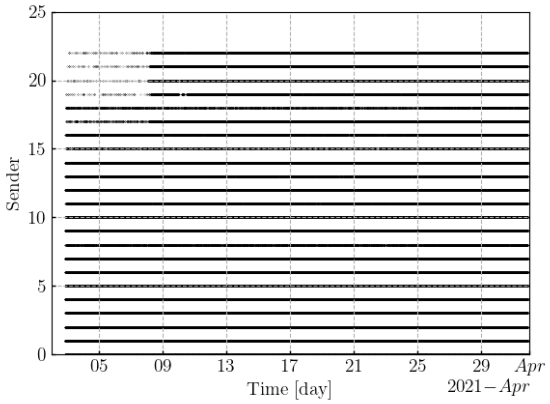
- 94.102.49.0 with 2 senders, 80.82.77.0 with 2 senders, 71.6.146.0 with 2 senders, 185.142.236.0 with 2 senders, 71.6.199.0 with 1 sender

11 distinct /16 subnets. The top-5 are:

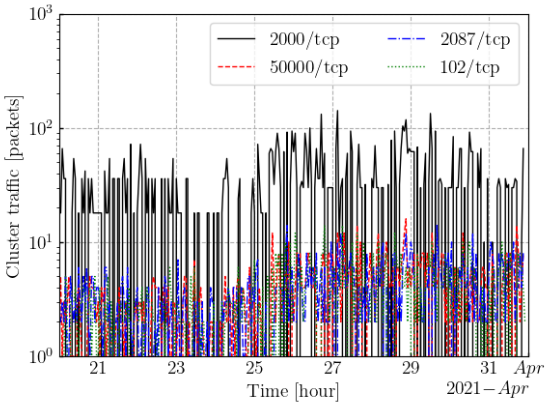
- 71.6.0.0 with 7 senders, 66.240.0.0 with 3 senders, 185.142.0.0 with 3 senders, 94.102.0.0 with 2 senders, 80.82.0.0 with 2 senders,

712 ports contacted. The top-5 are:

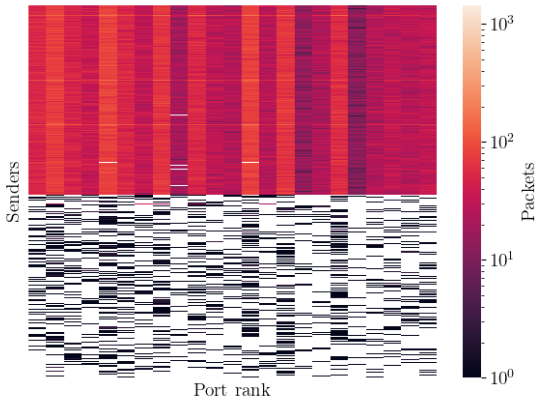
- 2000/tcp : 15523 sent packets (4.1 % of the monthly cluster traffic.) 23 senders contacted the port(100.0 % of the cluster senders.)
- 50000/tcp : 2060 sent packets (0.5 % of the monthly cluster traffic.) 23 senders contacted the port(100.0 % of the cluster senders.)
- 2087/tcp : 1998 sent packets (0.5 % of the monthly cluster traffic.) 23 senders contacted the port(100.0 % of the cluster senders.)
- 102/tcp : 1986 sent packets (0.5 % of the monthly cluster traffic.) 23 senders contacted the port(100.0 % of the cluster senders.)
- 81/tcp : 1985 sent packets (0.5 % of the monthly cluster traffic.) 23 senders contacted the port(100.0 % of the cluster senders.)



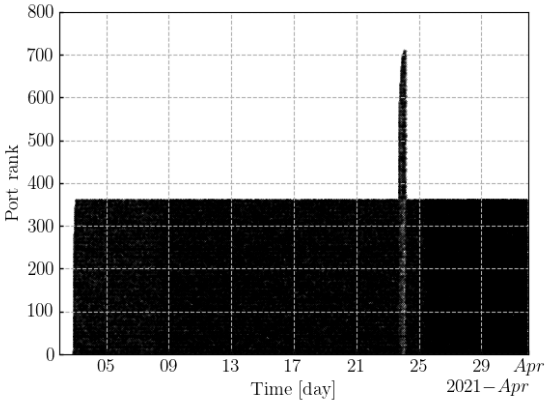
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 12: Cluster5 temporal patterns

7 Cluster 6. Silhouette: 0.43

612 distinct senders with the following ground truth classes:

- Unknown. 594 senders
- Mirai-like. 13 senders
- Stretchoid. 5 senders

38128 packets sent in the last day. 1.1% of the last day traffic. 0.1% of cluster traffic has the Mirai fingerprint.

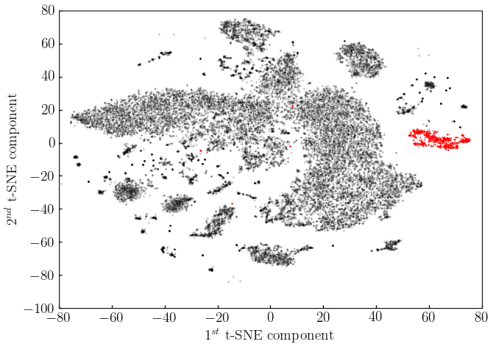


Figure 13: Cluster 6. t-SNE projection

569 distinct /24 subnets. The top-5 are:

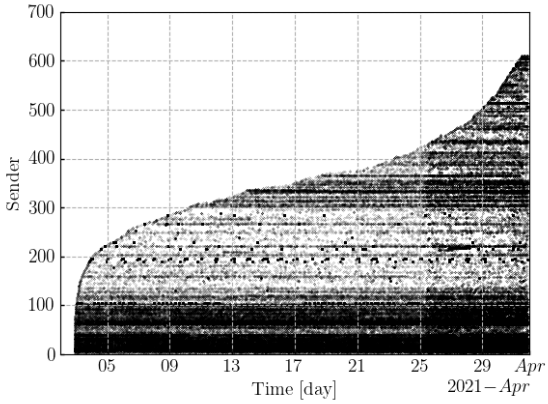
- 178.134.185.0 with 5 senders, 195.24.207.0 with 4 senders, 185.104.183.0 with 4 senders, 188.169.167.0 with 3 senders, 112.30.110.0 with 3 senders,

435 distinct /16 subnets. The top-5 are:

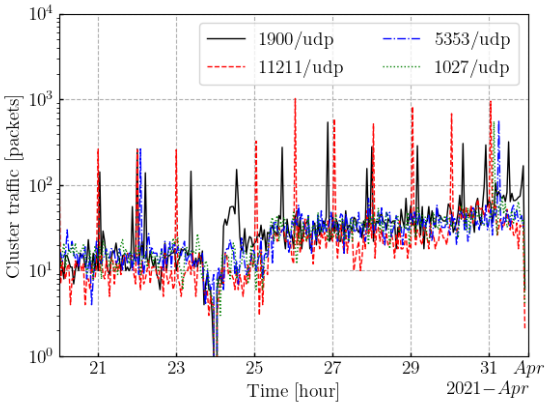
- 188.169.0.0 with 11 senders, 120.85.0.0 with 10 senders, 112.30.0.0 with 8 senders, 176.221.0.0 with 8 senders, 149.3.0.0 with 7 senders,

149 ports contacted. The top-5 are:

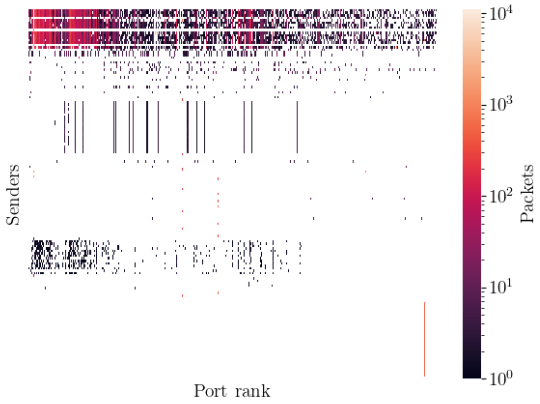
- 1900/udp : 20600 sent packets (7.9 % of the monthly cluster traffic.) 400 senders contacted the port(65.4 % of the cluster senders.)
- 11211/udp : 20438 sent packets (7.9 % of the monthly cluster traffic.) 351 senders contacted the port(57.4 % of the cluster senders.)
- 5353/udp : 14569 sent packets (5.6 % of the monthly cluster traffic.) 418 senders contacted the port(68.3 % of the cluster senders.)
- 1027/udp : 13292 sent packets (5.1 % of the monthly cluster traffic.) 395 senders contacted the port(64.5 % of the cluster senders.)
- 4000/udp : 13269 sent packets (5.1 % of the monthly cluster traffic.) 425 senders contacted the port(69.4 % of the cluster senders.)



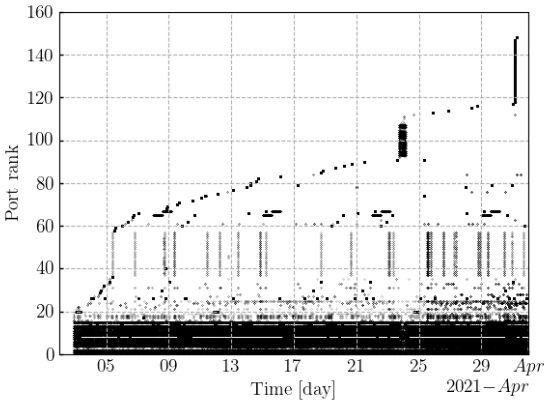
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 14: Cluster6 temporal patterns

8 Cluster 7. Silhouette: 0.688

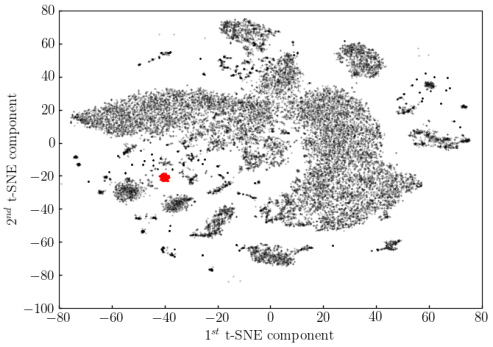


Figure 15: Cluster 7. t-SNE projection

48 distinct senders with the following ground truth classes:

- Censys. 48 senders

58484 packets sent in the last day. 1.7% of the last day traffic.

3 distinct /24 subnets. The top-5 are:

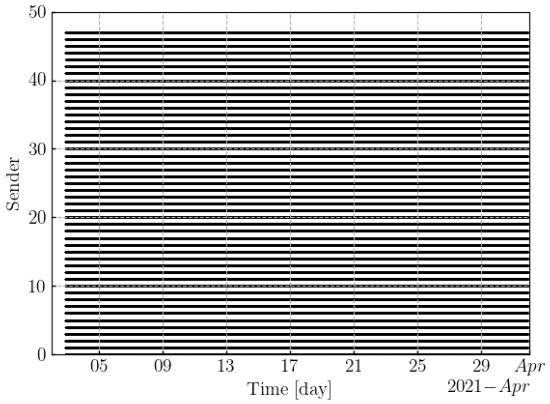
- 74.120.14.0 with 16 senders, 167.248.133.0 with 16 senders, 162.142.125.0 with 16 senders,

3 distinct /16 subnets. The top-5 are:

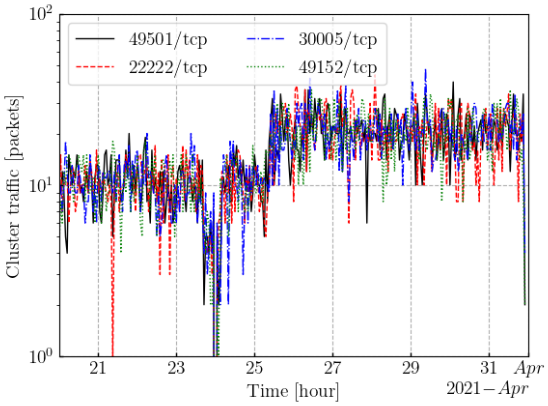
- 74.120.0.0 with 16 senders, 167.248.0.0 with 16 senders, 162.142.0.0 with 16 senders,

254 ports contacted. The top-5 are:

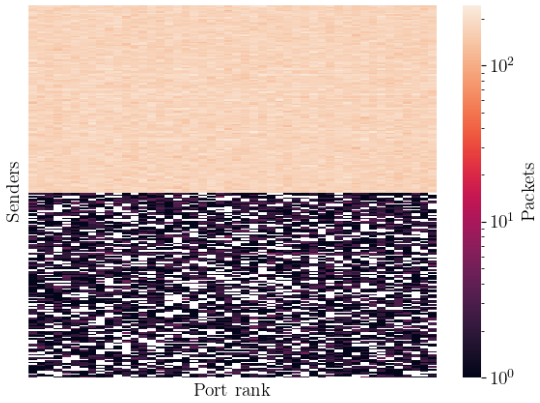
- 49501/tcp : 9023 sent packets (0.8 % of the monthly cluster traffic.) 48 senders contacted the port(100.0 % of the cluster senders.)
- 22222/tcp : 9000 sent packets (0.8 % of the monthly cluster traffic.) 48 senders contacted the port(100.0 % of the cluster senders.)
- 30005/tcp : 8992 sent packets (0.8 % of the monthly cluster traffic.) 48 senders contacted the port(100.0 % of the cluster senders.)
- 49152/tcp : 8990 sent packets (0.8 % of the monthly cluster traffic.) 48 senders contacted the port(100.0 % of the cluster senders.)
- 49502/tcp : 8978 sent packets (0.8 % of the monthly cluster traffic.) 48 senders contacted the port(100.0 % of the cluster senders.)



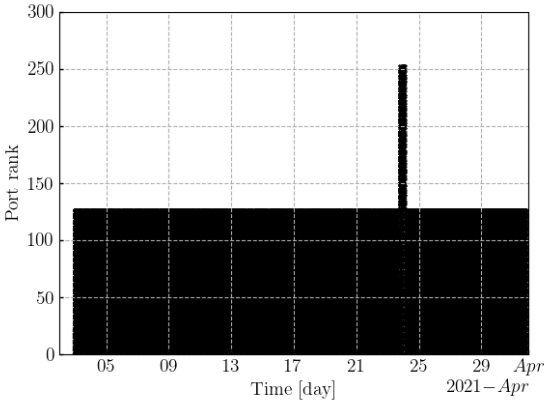
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 16: Cluster7 temporal patterns

9 Cluster 8. Silhouette: -0.358

388 distinct senders with the following ground truth classes:

- Unknown. 297 senders
- Censys. 32 senders
- Stretchoid. 22 senders
- Shadowserver. 15 senders
- AlphaStrike. 14 senders
- Ipip. 7 senders
- Mirai-like. 1 sender

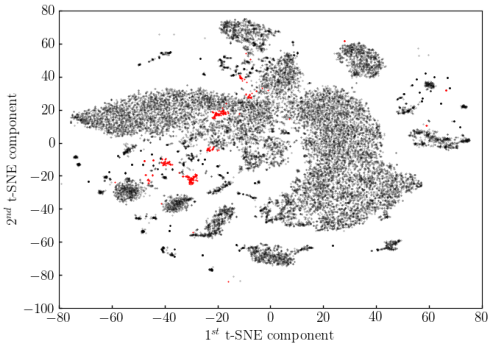


Figure 17: Cluster 8. t-SNE projection

138072 packets sent in the last day. 4.1% of the last day traffic.
0.0% of cluster traffic has the Mirai fingerprint.
296 distinct /24 subnets. The top-5 are:

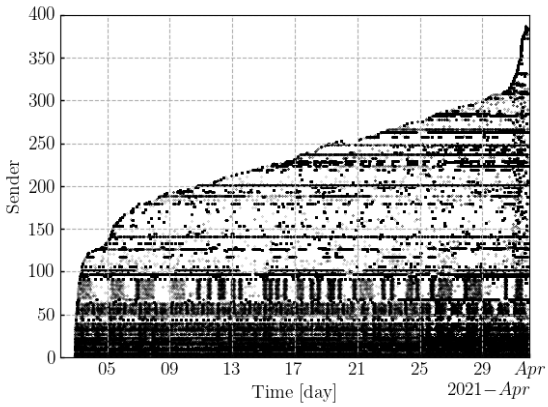
- 192.35.168.0 with 32 senders, 74.82.47.0 with 15 senders, 164.52.24.0 with 7 senders, 185.200.118.0 with 7 senders, 192.241.228.0 with 6 senders,

249 distinct /16 subnets. The top-5 are:

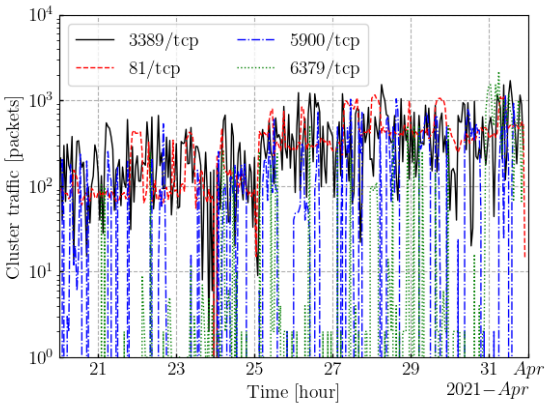
- 192.35.0.0 with 32 senders, 192.241.0.0 with 22 senders, 74.82.0.0 with 15 senders, 45.83.0.0 with 14 senders, 164.52.0.0 with 8 senders,

554 ports contacted. The top-5 are:

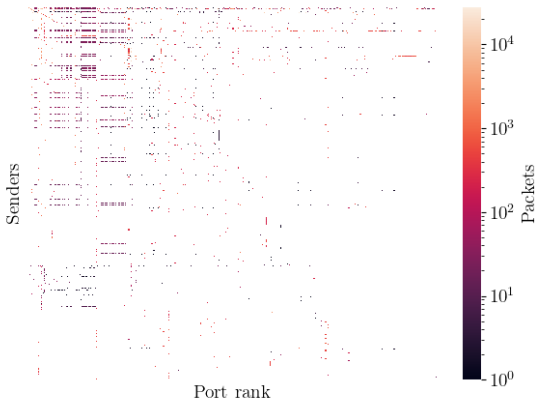
- 3389/tcp : 168319 sent packets (15.0 % of the monthly cluster traffic.) 139 senders contacted the port(35.8 % of the cluster senders.)
- 81/tcp : 110754 sent packets (9.9 % of the monthly cluster traffic.) 29 senders contacted the port(7.5 % of the cluster senders.)
- 5900/tcp : 40288 sent packets (3.6 % of the monthly cluster traffic.) 60 senders contacted the port(15.5 % of the cluster senders.)
- 6379/tcp : 31562 sent packets (2.8 % of the monthly cluster traffic.) 86 senders contacted the port(22.2 % of the cluster senders.)
- 3388/tcp : 31225 sent packets (2.8 % of the monthly cluster traffic.) 7 senders contacted the port(1.8 % of the cluster senders.)



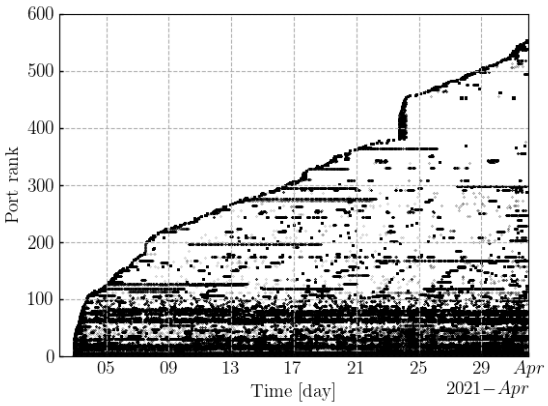
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 18: Cluster8 temporal patterns

10 Cluster 9. Silhouette: 0.557

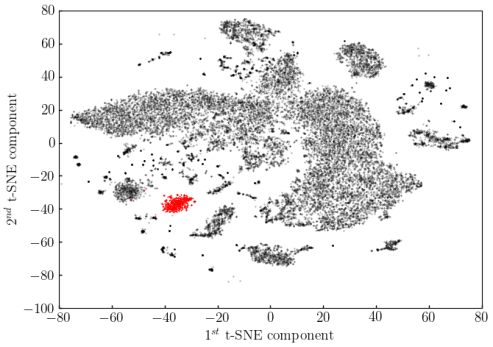


Figure 19: Cluster 9. t-SNE projection

419 distinct senders with the following ground truth classes:

- Unknown. 416 senders
- Ipip. 3 senders

92514 packets sent in the last day. 2.7% of the last day traffic.

406 distinct /24 subnets. The top-5 are:

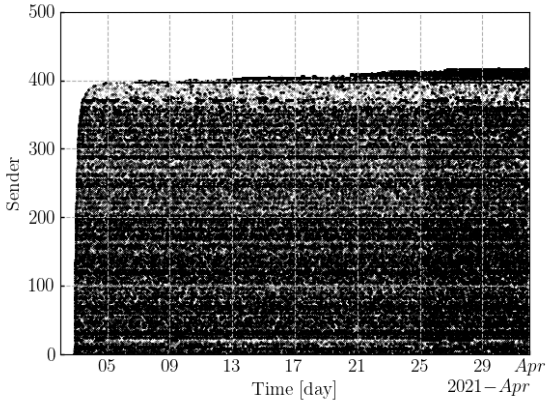
- 119.96.175.0 with 4 senders, 120.92.109.0 with 4 senders, 175.6.35.0 with 3 senders, 119.96.172.0 with 2 senders, 139.186.69.0 with 2 senders,

241 distinct /16 subnets. The top-5 are:

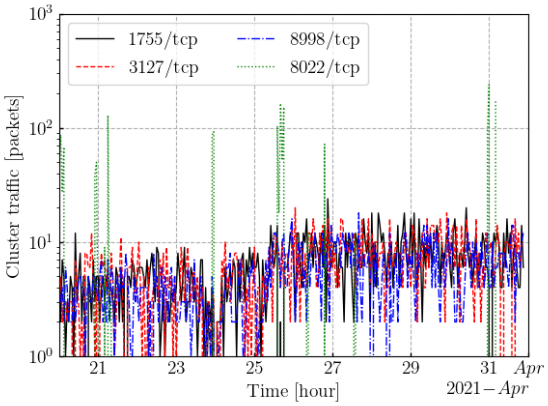
- 119.96.0.0 with 17 senders, 106.13.0.0 with 11 senders, 106.12.0.0 with 9 senders, 106.75.0.0 with 8 senders, 120.92.0.0 with 7 senders,

15699 ports contacted. The top-5 are:

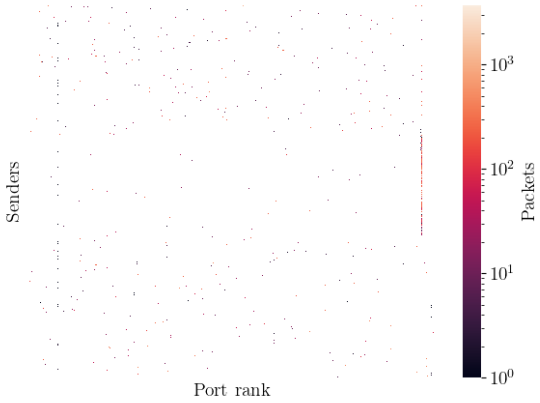
- 1755/tcp : 3680 sent packets (0.2 % of the monthly cluster traffic.) 1 senders contacted the port(0.2 % of the cluster senders.)
- 3127/tcp : 3673 sent packets (0.2 % of the monthly cluster traffic.) 2 senders contacted the port(0.5 % of the cluster senders.)
- 8998/tcp : 3209 sent packets (0.2 % of the monthly cluster traffic.) 2 senders contacted the port(0.5 % of the cluster senders.)
- 8022/tcp : 3115 sent packets (0.2 % of the monthly cluster traffic.) 3 senders contacted the port(0.7 % of the cluster senders.)
- 50808/udp : 2566 sent packets (0.1 % of the monthly cluster traffic.) 1 senders contacted the port(0.2 % of the cluster senders.)



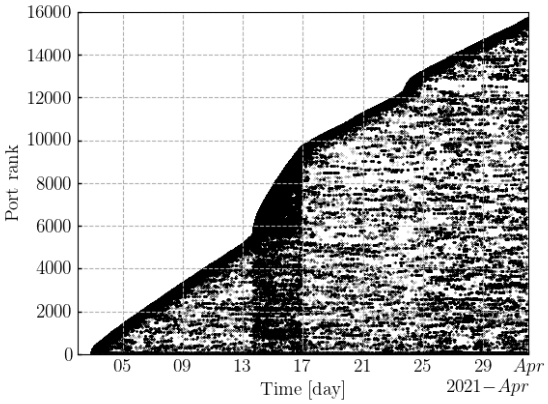
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 20: Cluster9 temporal patterns

11 Cluster 10. Silhouette: 0.826

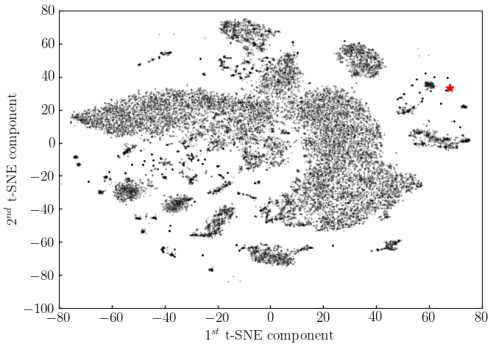


Figure 21: Cluster 10. t-SNE projection

16 distinct senders with the following ground truth classes:

- Shadowserver. 16 senders

1104 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

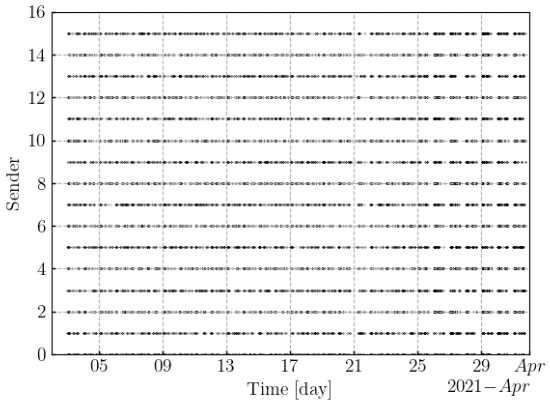
- 216.218.206.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

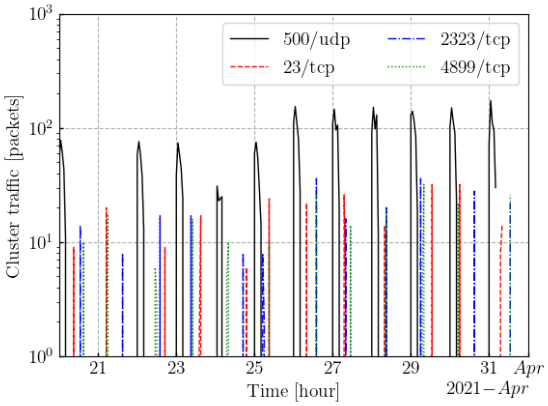
- 216.218.0.0 with 16 senders,

40 ports contacted. The top-5 are:

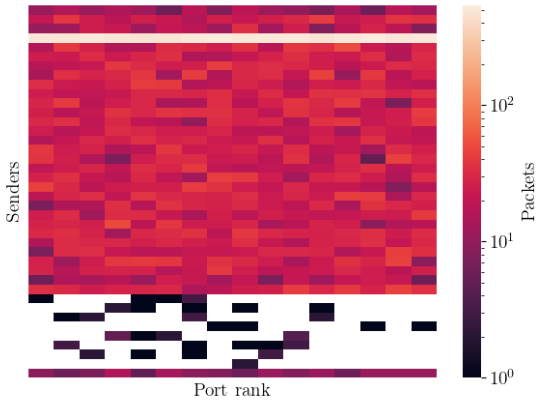
- 500/udp : 8054 sent packets (39.5 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 23/tcp : 479 sent packets (2.3 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 2323/tcp : 466 sent packets (2.3 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 4899/tcp : 460 sent packets (2.3 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 11211/tcp : 458 sent packets (2.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



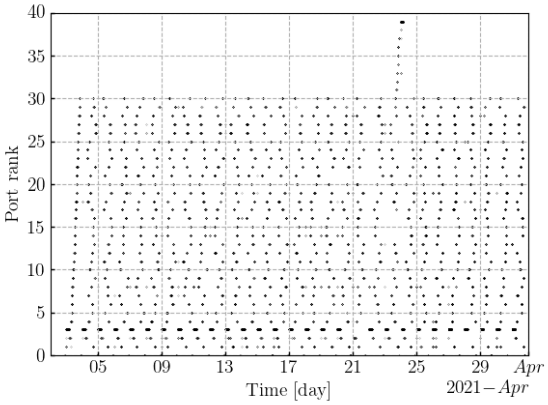
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 22: Cluster10 temporal patterns

12 Cluster 11. Silhouette: -0.244

750 distinct senders with the following ground truth classes:

- Mirai-like. 503 senders
- Unknown. 229 senders
- Shadowserver. 15 senders
- Stretchoid. 2 senders
- Ipip. 1 sender

75140 packets sent in the last day. 2.2% of the last day traffic. 52.6% of cluster traffic has the Mirai fingerprint.

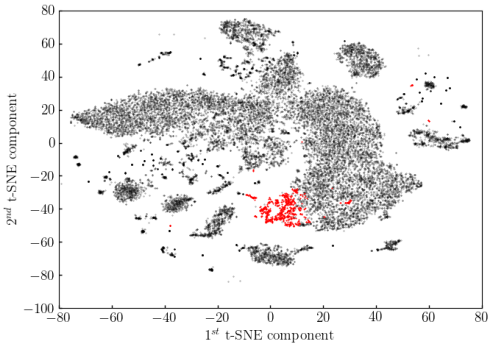


Figure 23: Cluster 11. t-SNE projection

705 distinct /24 subnets. The top-5 are:

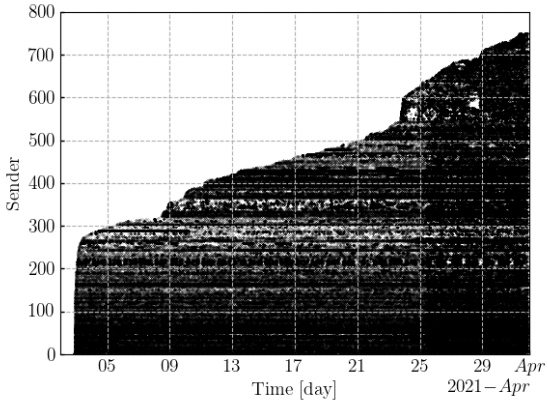
- 216.218.206.0 with 15 senders, 124.88.69.0 with 4 senders, 60.2.87.0 with 4 senders, 223.80.100.0 with 3 senders, 130.61.101.0 with 3 senders,

526 distinct /16 subnets. The top-5 are:

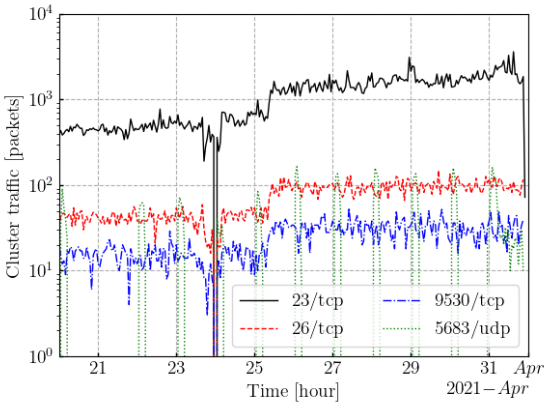
- 130.61.0.0 with 49 senders, 129.146.0.0 with 24 senders, 216.218.0.0 with 15 senders, 129.159.0.0 with 8 senders, 152.67.0.0 with 8 senders,

754 ports contacted. The top-5 are:

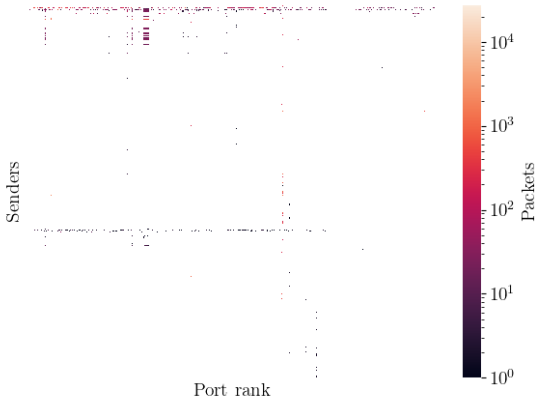
- 23/tcp : 475950 sent packets (58.2 % of the monthly cluster traffic.) 721 senders contacted the port(96.1 % of the cluster senders.)
- 26/tcp : 35521 sent packets (4.3 % of the monthly cluster traffic.) 227 senders contacted the port(30.3 % of the cluster senders.)
- 9530/tcp : 13184 sent packets (1.6 % of the monthly cluster traffic.) 9 senders contacted the port(1.2 % of the cluster senders.)
- 5683/udp : 9858 sent packets (1.2 % of the monthly cluster traffic.) 17 senders contacted the port(2.3 % of the cluster senders.)
- 2323/tcp : 9770 sent packets (1.2 % of the monthly cluster traffic.) 239 senders contacted the port(31.9 % of the cluster senders.)



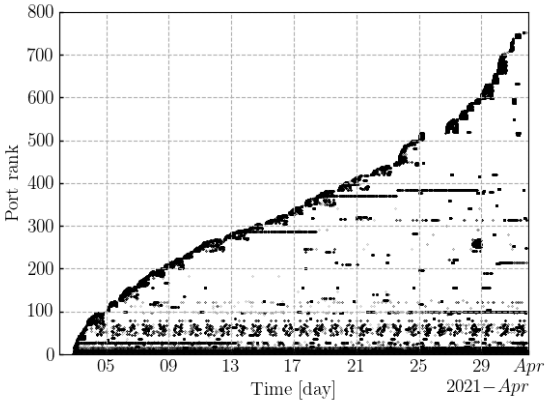
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 24: Cluster11 temporal patterns

13 Cluster 12. Silhouette: 0.905

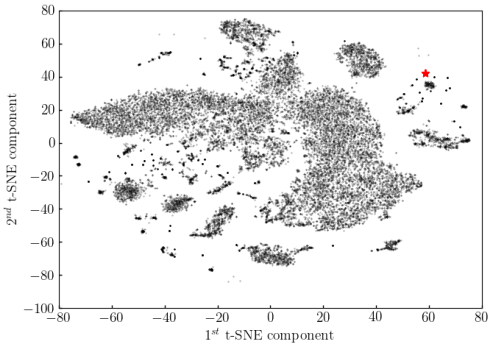


Figure 25: Cluster 12. t-SNE projection

15 distinct senders with the following ground truth classes:

- Shadowserver. 15 senders

1468 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

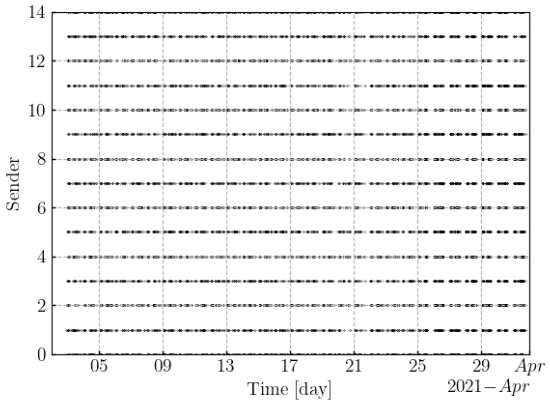
- 74.82.47.0 with 15 senders,

1 distinct /16 subnets. The top-5 are:

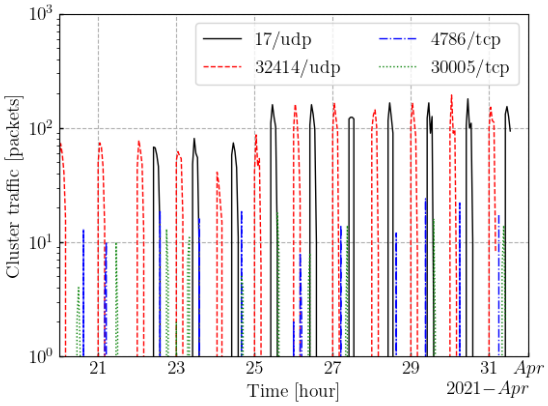
- 74.82.0.0 with 15 senders,

40 ports contacted. The top-5 are:

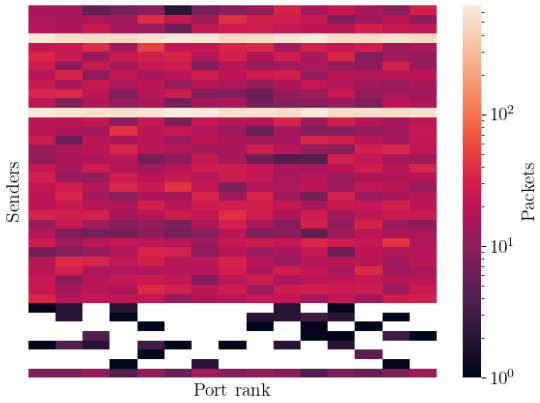
- 17/udp : 8553 sent packets (33.2 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 32414/udp : 8318 sent packets (32.3 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 4786/tcp : 387 sent packets (1.5 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 30005/tcp : 367 sent packets (1.4 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 23/tcp : 349 sent packets (1.4 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)



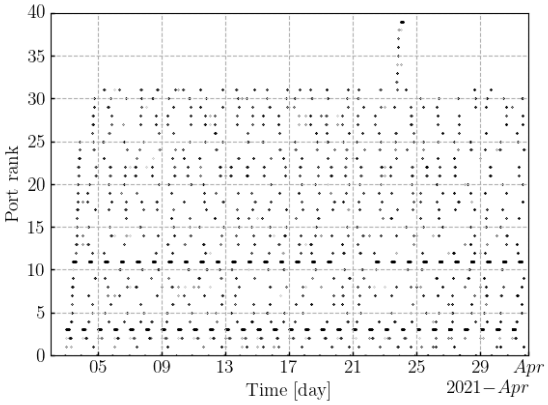
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 26: Cluster12 temporal patterns

14 Cluster 13. Silhouette: 0.174

686 distinct senders with the following ground truth classes:

- Unknown. 553 senders
- Internet-census. 55 senders
- Sharashka. 50 senders
- Ipip. 15 senders
- Censys. 8 senders
- Mirai-like. 5 senders

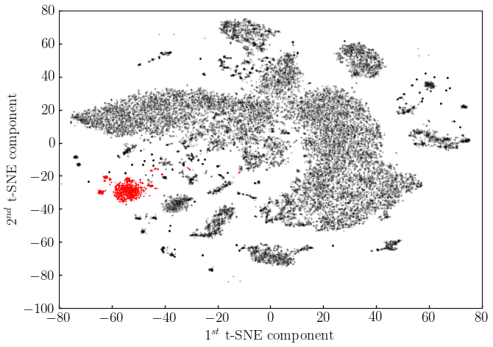


Figure 27: Cluster 13. t-SNE projection

106442 packets sent in the last day. 3.1% of the last day traffic. 0.1% of cluster traffic has the Mirai fingerprint.

237 distinct /24 subnets. The top-5 are:

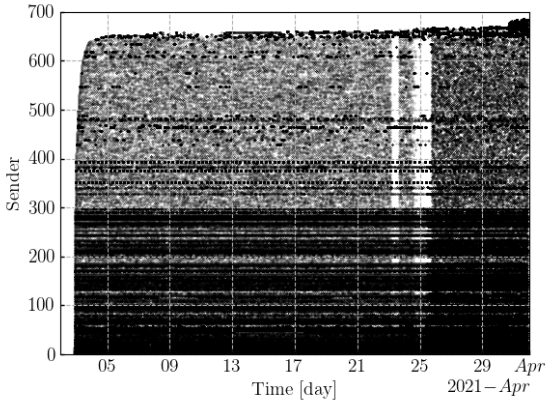
- 124.156.50.0 with 28 senders, 128.14.209.0 with 28 senders, 124.156.55.0 with 21 senders, 170.106.81.0 with 16 senders, 150.109.170.0 with 16 senders,

65 distinct /16 subnets. The top-5 are:

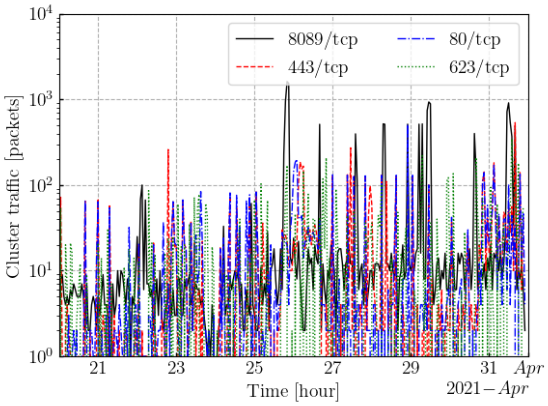
- 124.156.0.0 with 133 senders, 170.106.0.0 with 85 senders, 49.51.0.0 with 84 senders, 150.109.0.0 with 84 senders, 162.62.0.0 with 40 senders,

7731 ports contacted. The top-5 are:

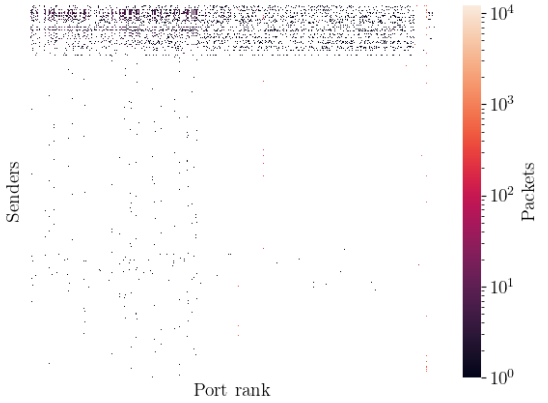
- 8089/tcp : 18866 sent packets (1.7 % of the monthly cluster traffic.) 209 senders contacted the port(30.5 % of the cluster senders.)
- 443/tcp : 12435 sent packets (1.1 % of the monthly cluster traffic.) 221 senders contacted the port(32.2 % of the cluster senders.)
- 80/tcp : 10653 sent packets (0.9 % of the monthly cluster traffic.) 216 senders contacted the port(31.5 % of the cluster senders.)
- 623/tcp : 10101 sent packets (0.9 % of the monthly cluster traffic.) 108 senders contacted the port(15.7 % of the cluster senders.)
- 8080/tcp : 9581 sent packets (0.8 % of the monthly cluster traffic.) 233 senders contacted the port(34.0 % of the cluster senders.)



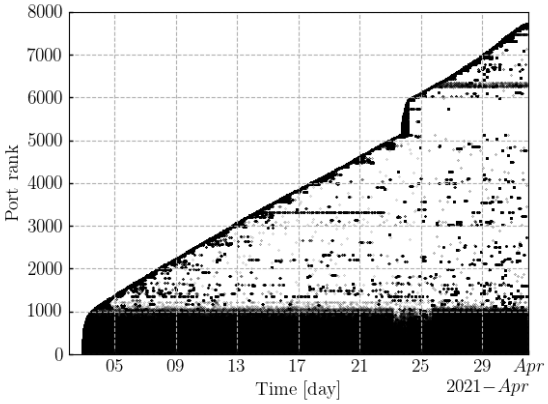
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 28: Cluster13 temporal patterns

15 Cluster 14. Silhouette: 0.629

10 distinct senders with the following ground truth classes:

- Unknown. 10 senders

7878 packets sent in the last day. 0.2% of the last day traffic.

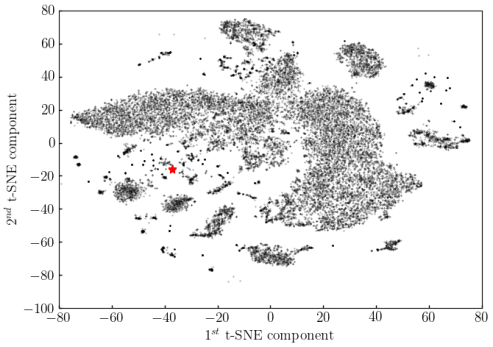


Figure 29: Cluster 14. t-SNE projection

4 distinct /24 subnets. The top-5 are:

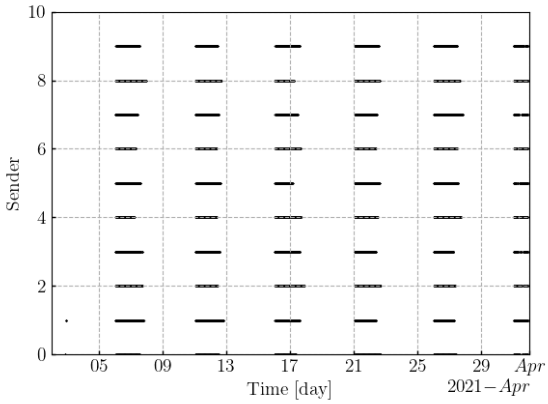
- 185.167.97.0 with 4 senders, 185.220.205.0 with 3 senders, 185.167.96.0 with 2 senders, 185.167.98.0 with 1 sender

2 distinct /16 subnets. The top-5 are:

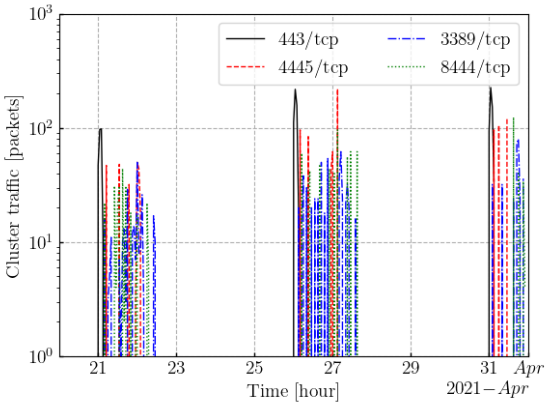
- 185.167.0.0 with 7 senders, 185.220.0.0 with 3 senders,

40 ports contacted. The top-5 are:

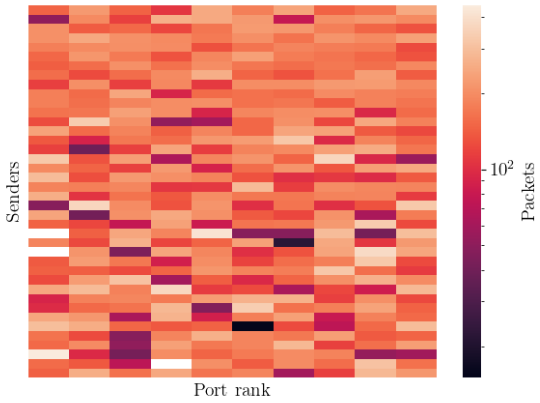
- 443/tcp : 2029 sent packets (2.9 % of the monthly cluster traffic.) 10 senders contacted the port(100.0 % of the cluster senders.)
- 4445/tcp : 1868 sent packets (2.7 % of the monthly cluster traffic.) 10 senders contacted the port(100.0 % of the cluster senders.)
- 3389/tcp : 1846 sent packets (2.7 % of the monthly cluster traffic.) 10 senders contacted the port(100.0 % of the cluster senders.)
- 8444/tcp : 1833 sent packets (2.6 % of the monthly cluster traffic.) 10 senders contacted the port(100.0 % of the cluster senders.)
- 7443/tcp : 1828 sent packets (2.6 % of the monthly cluster traffic.) 10 senders contacted the port(100.0 % of the cluster senders.)



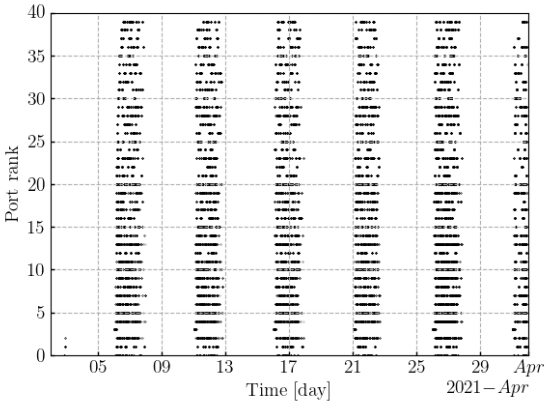
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 30: Cluster14 temporal patterns

16 Cluster 15. Silhouette: -0.043

1648 distinct senders with the following ground truth classes:

- Unknown. 1326 senders
- AlphaStrike. 162 senders
- Mirai-like. 136 senders
- Shadowserver. 15 senders
- Stretchoid. 9 senders

42038 packets sent in the last day. 1.2% of the last day traffic. 1.2% of cluster traffic has the Mirai fingerprint.

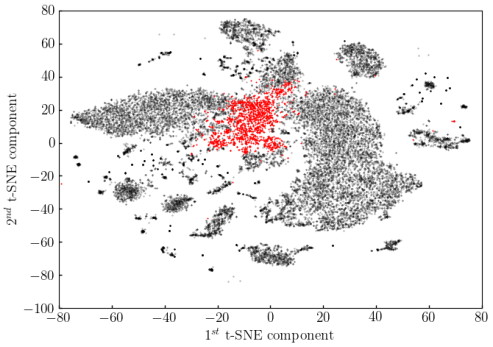


Figure 31: Cluster 15. t-SNE projection

1219 distinct /24 subnets. The top-5 are:

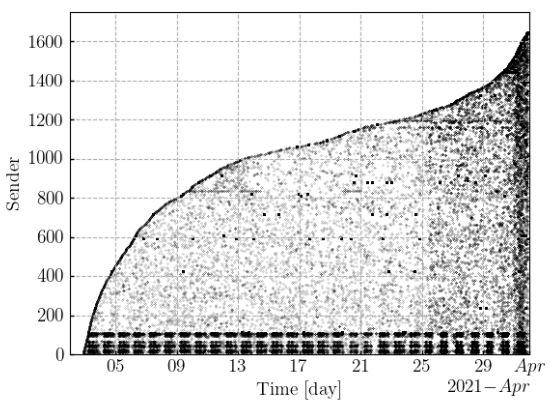
- 45.83.64.0 with 47 senders, 45.83.65.0 with 41 senders, 45.83.66.0 with 37 senders, 45.83.67.0 with 37 senders, 202.164.139.0 with 16 senders,

969 distinct /16 subnets. The top-5 are:

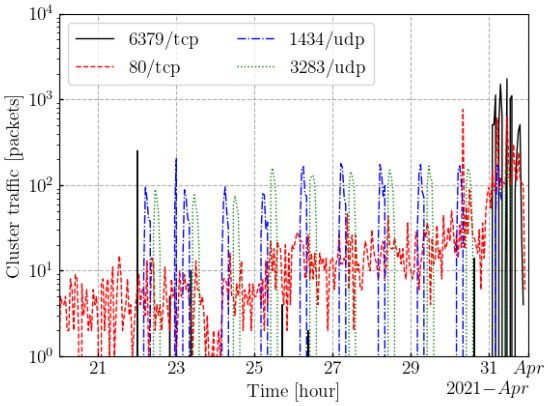
- 45.83.0.0 with 162 senders, 186.33.0.0 with 56 senders, 178.175.0.0 with 40 senders, 61.242.0.0 with 27 senders, 209.14.0.0 with 26 senders,

241 ports contacted. The top-5 are:

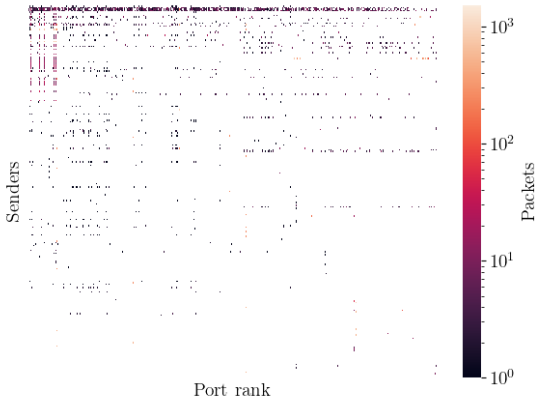
- 6379/tcp : 11705 sent packets (10.3 % of the monthly cluster traffic.) 45 senders contacted the port(2.7 % of the cluster senders.)
- 80/tcp : 9553 sent packets (8.4 % of the monthly cluster traffic.) 1135 senders contacted the port(68.9 % of the cluster senders.)
- 1434/udp : 9076 sent packets (8.0 % of the monthly cluster traffic.) 53 senders contacted the port(3.2 % of the cluster senders.)
- 3283/udp : 8541 sent packets (7.5 % of the monthly cluster traffic.) 15 senders contacted the port(0.9 % of the cluster senders.)
- 445/tcp : 6455 sent packets (5.7 % of the monthly cluster traffic.) 121 senders contacted the port(7.3 % of the cluster senders.)



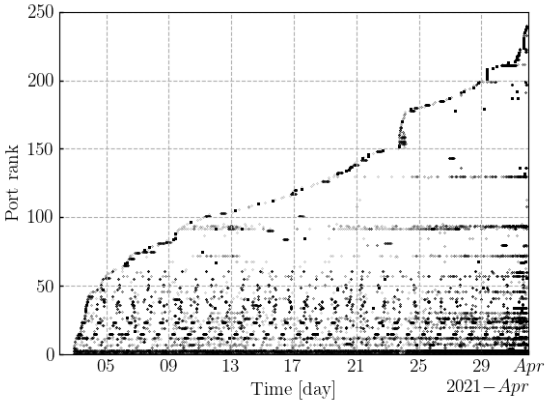
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 32: Cluster15 temporal patterns

17 Cluster 16. Silhouette: 0.935

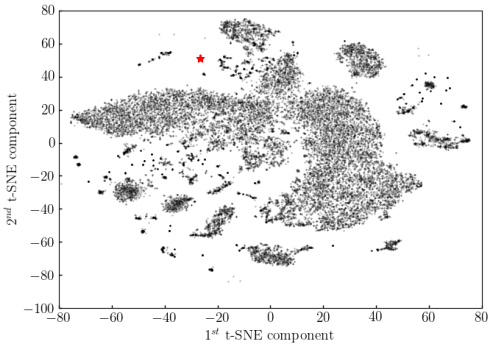


Figure 33: Cluster 16. t-SNE projection

16 distinct senders with the following ground truth classes:

- Censys. 16 senders

506 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

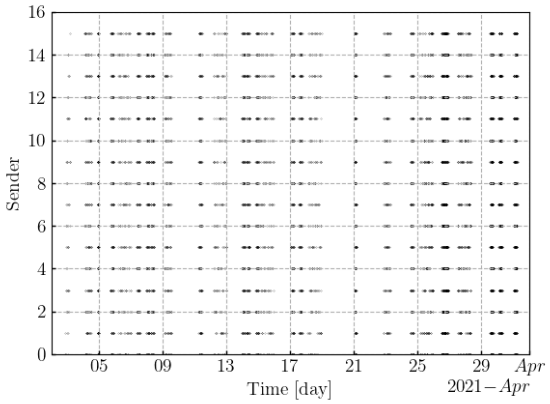
- 192.35.168.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

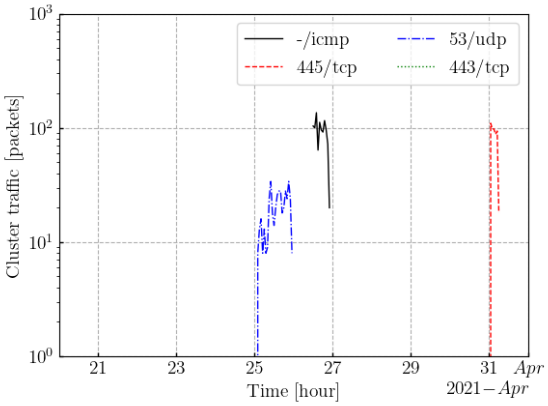
- 192.35.0.0 with 16 senders,

23 ports contacted. The top-5 are:

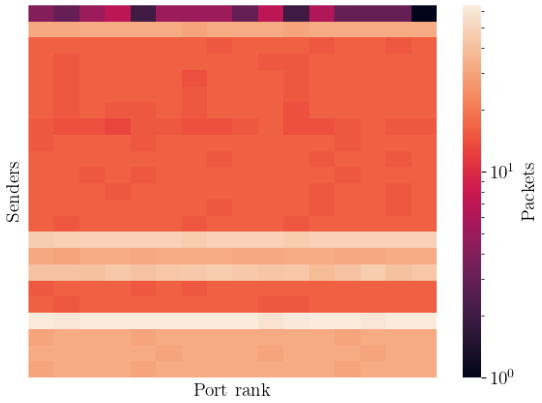
- -/icmp : 1008 sent packets (11.8 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 445/tcp : 759 sent packets (8.9 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 53/udp : 675 sent packets (7.9 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 443/tcp : 506 sent packets (5.9 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 5672/tcp : 506 sent packets (5.9 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



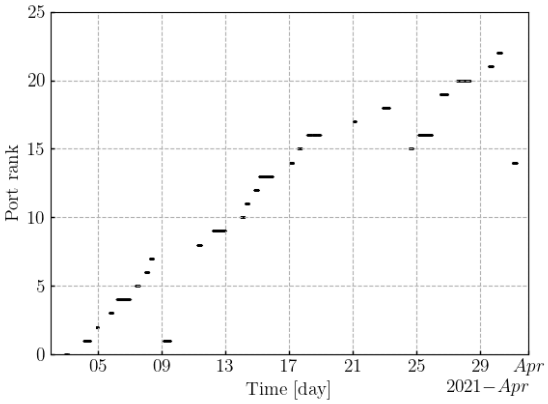
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 34: Cluster16 temporal patterns

18 Cluster 17. Silhouette: 0.806

15 distinct senders with the following ground truth classes:

- Unknown. 15 senders

3386 packets sent in the last day. 0.1% of the last day traffic.

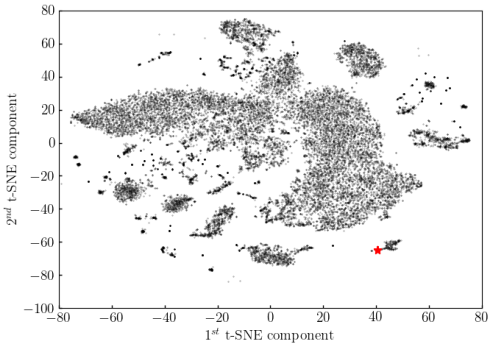


Figure 35: Cluster 17. t-SNE projection

15 distinct /24 subnets. The top-5 are:

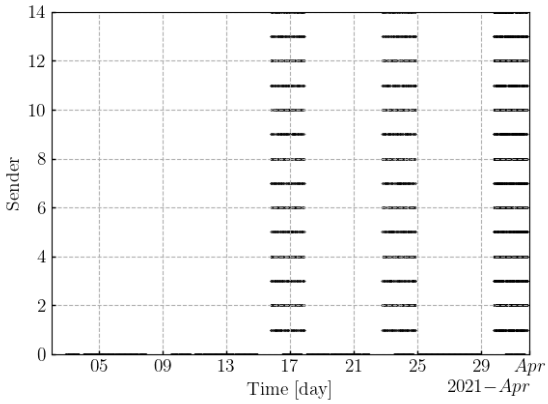
- 71.6.232.0 with 1 sender 69.230.247.0 with 1 sender 54.252.233.0 with 1 sender 54.153.91.0 with 1 sender 52.80.152.0 with 1 sender

15 distinct /16 subnets. The top-5 are:

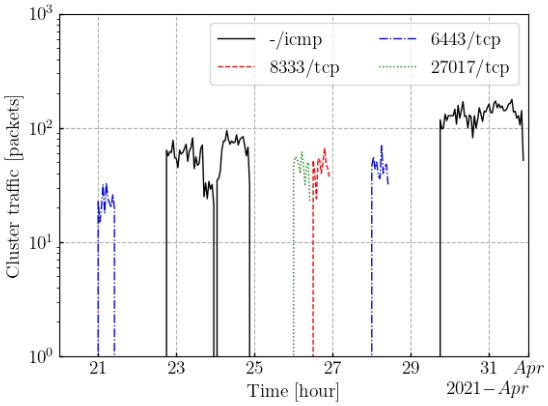
- 71.6.0.0 with 1 sender 69.230.0.0 with 1 sender 54.252.0.0 with 1 sender 54.153.0.0 with 1 sender 52.80.0.0 with 1 sender

12 ports contacted. The top-5 are:

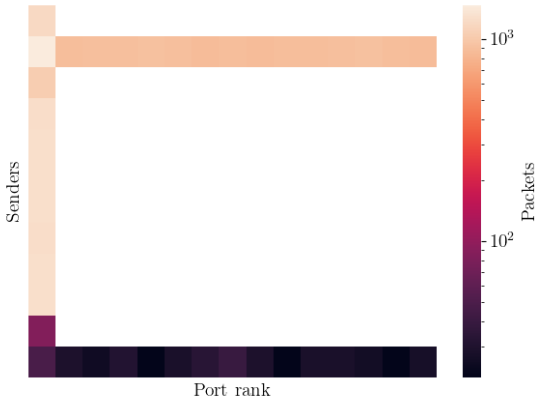
- -/icmp : 13930 sent packets (54.6 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 8333/tcp : 1265 sent packets (5.0 % of the monthly cluster traffic.) 1 senders contacted the port(6.7 % of the cluster senders.)
- 6443/tcp : 1265 sent packets (5.0 % of the monthly cluster traffic.) 1 senders contacted the port(6.7 % of the cluster senders.)
- 27017/tcp : 1265 sent packets (5.0 % of the monthly cluster traffic.) 1 senders contacted the port(6.7 % of the cluster senders.)
- 7210/tcp : 1264 sent packets (4.9 % of the monthly cluster traffic.) 1 senders contacted the port(6.7 % of the cluster senders.)



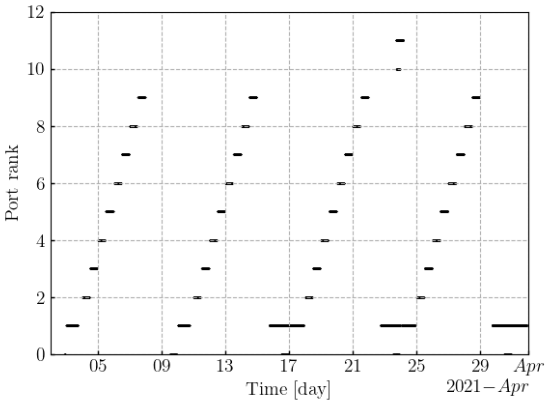
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 36: Cluster17 temporal patterns

19 Cluster 18. Silhouette: 0.637

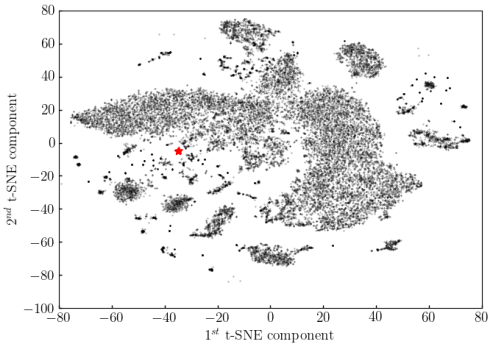


Figure 37: Cluster 18. t-SNE projection

5 distinct senders with the following ground truth classes:

- Unknown. 4 senders
- Binaryedge. 1 sender

30 packets sent in the last day. 0.0% of the last day traffic.

5 distinct /24 subnets. The top-5 are:

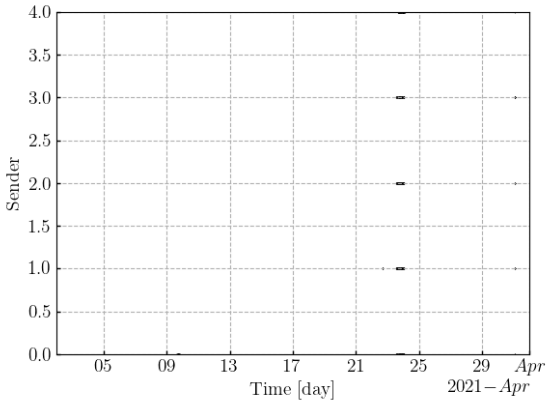
- 64.227.23.0 with 1 sender 45.79.70.0 with 1 sender 45.56.88.0 with 1 sender 178.79.160.0 with 1 sender 172.105.106.0 with 1 sender

5 distinct /16 subnets. The top-5 are:

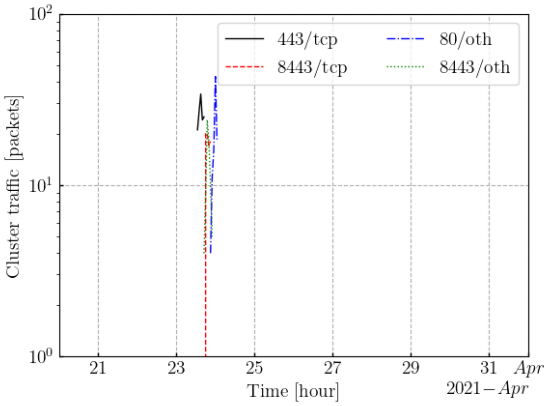
- 64.227.0.0 with 1 sender 45.79.0.0 with 1 sender 45.56.0.0 with 1 sender 178.79.0.0 with 1 sender 172.105.0.0 with 1 sender

10 ports contacted. The top-5 are:

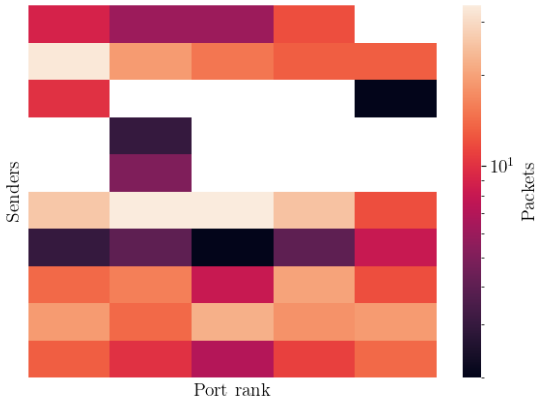
- 443/tcp : 131 sent packets (25.4 % of the monthly cluster traffic.) 5 senders contacted the port(100.0 % of the cluster senders.)
- 8443/tcp : 93 sent packets (18.1 % of the monthly cluster traffic.) 5 senders contacted the port(100.0 % of the cluster senders.)
- 80/oth : 92 sent packets (17.9 % of the monthly cluster traffic.) 5 senders contacted the port(100.0 % of the cluster senders.)
- 8443/oth : 70 sent packets (13.6 % of the monthly cluster traffic.) 5 senders contacted the port(100.0 % of the cluster senders.)
- 80/tcp : 55 sent packets (10.7 % of the monthly cluster traffic.) 5 senders contacted the port(100.0 % of the cluster senders.)



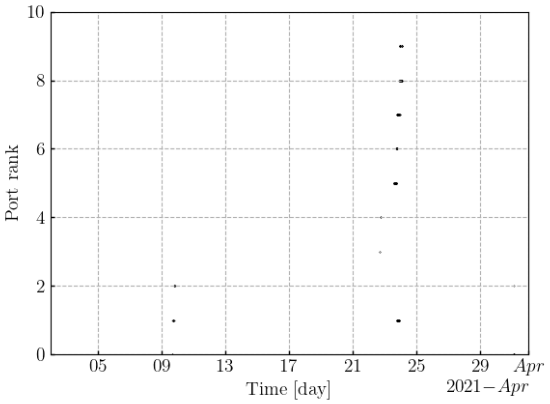
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 38: Cluster18 temporal patterns

20 Cluster 19. Silhouette: 0.11

2237 distinct senders with the following ground truth classes:

- Mirai-like. 1416 senders
- Unknown. 814 senders
- AlphaStrike. 6 senders
- Stretchoid. 1 sender

27089 packets sent in the last day. 0.8% of the last day traffic. 27.0% of cluster traffic has the Mirai fingerprint.

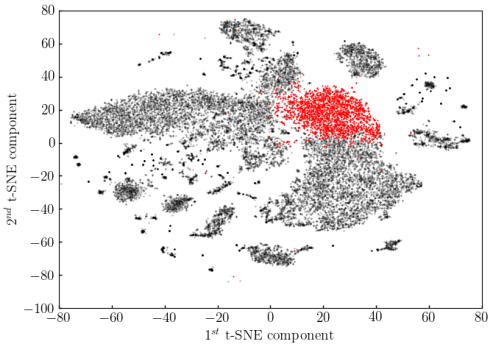


Figure 39: Cluster 19. t-SNE projection

1863 distinct /24 subnets. The top-5 are:

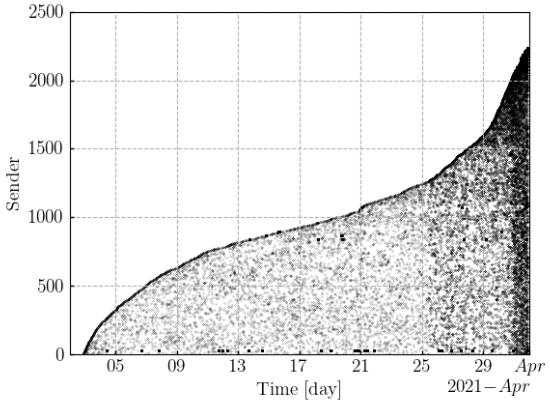
- 178.72.75.0 with 31 senders, 178.72.68.0 with 26 senders, 178.72.78.0 with 24 senders, 178.72.70.0 with 20 senders, 178.72.76.0 with 19 senders,

1359 distinct /16 subnets. The top-5 are:

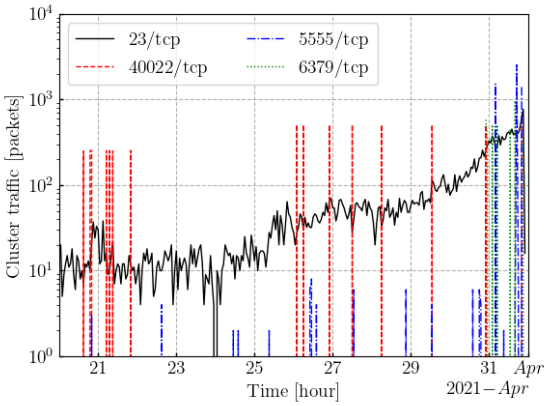
- 178.72.0.0 with 160 senders, 202.44.0.0 with 61 senders, 120.85.0.0 with 37 senders, 186.33.0.0 with 32 senders, 178.141.0.0 with 21 senders,

120 ports contacted. The top-5 are:

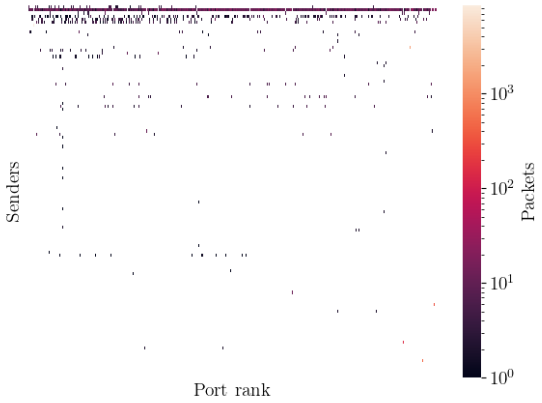
- 23/tcp : 23400 sent packets (35.9 % of the monthly cluster traffic.) 2144 senders contacted the port(95.8 % of the cluster senders.)
- 40022/tcp : 8583 sent packets (13.2 % of the monthly cluster traffic.) 1 senders contacted the port(0.0 % of the cluster senders.)
- 5555/tcp : 5605 sent packets (8.6 % of the monthly cluster traffic.) 39 senders contacted the port(1.7 % of the cluster senders.)
- 6379/tcp : 3722 sent packets (5.7 % of the monthly cluster traffic.) 11 senders contacted the port(0.5 % of the cluster senders.)
- 8080/tcp : 1597 sent packets (2.5 % of the monthly cluster traffic.) 401 senders contacted the port(17.9 % of the cluster senders.)



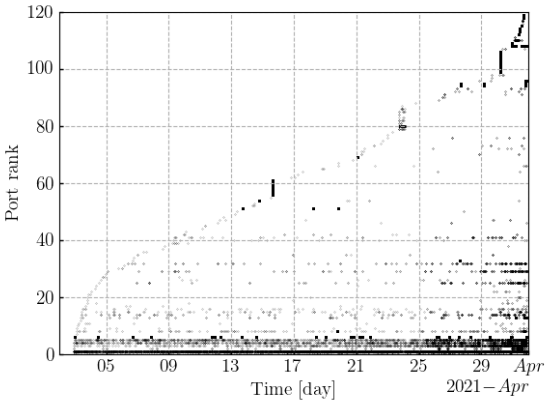
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 40: Cluster19 temporal patterns

21 Cluster 20. Silhouette: 0.916

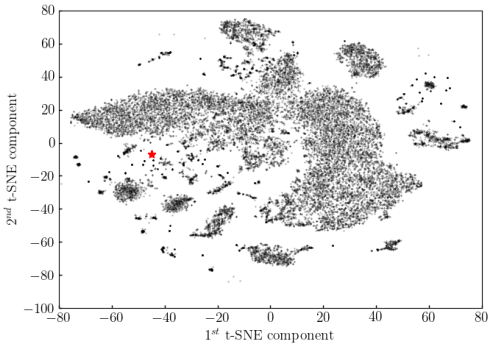


Figure 41: Cluster 20. t-SNE projection

16 distinct senders with the following ground truth classes:

- Censys. 16 senders

506 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

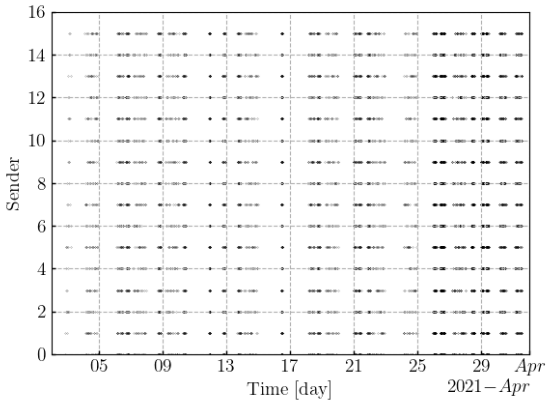
- 192.35.168.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

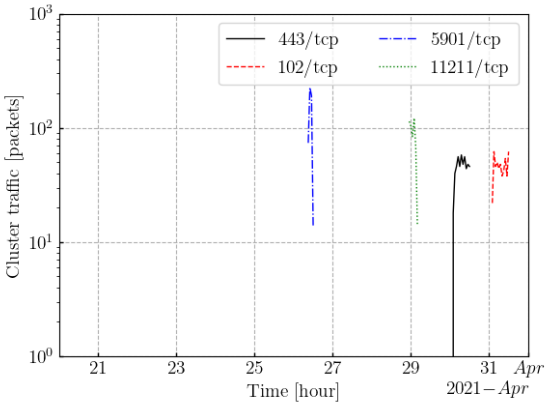
- 192.35.0.0 with 16 senders,

27 ports contacted. The top-5 are:

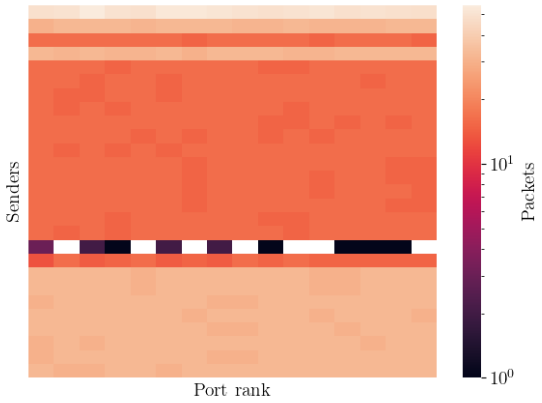
- 443/tcp : 806 sent packets (8.3 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 102/tcp : 506 sent packets (5.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 5901/tcp : 506 sent packets (5.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 11211/tcp : 506 sent packets (5.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 25/tcp : 506 sent packets (5.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



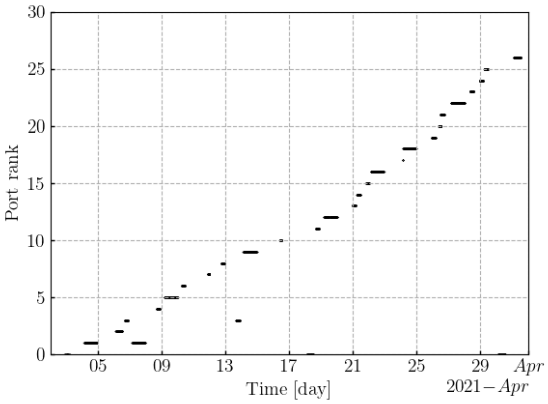
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 42: Cluster20 temporal patterns

22 Cluster 21. Silhouette: -0.139

388 distinct senders with the following ground truth classes:

- Unknown. 193 senders
- Mirai-like. 189 senders
- Stretchoid. 3 senders
- Ipip. 3 senders

24751 packets sent in the last day. 0.7% of the last day traffic. 4.7% of cluster traffic has the Mirai fingerprint.

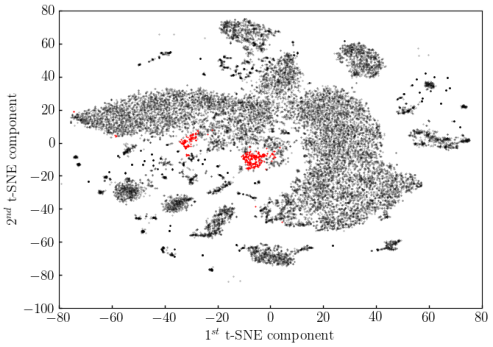


Figure 43: Cluster 21. t-SNE projection

265 distinct /24 subnets. The top-5 are:

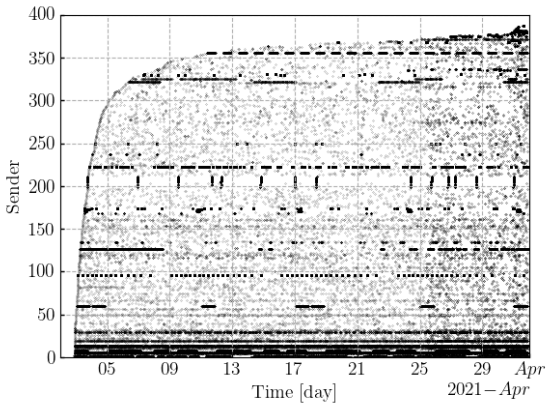
- 172.172.30.0 with 27 senders, 180.182.245.0 with 17 senders, 172.172.26.0 with 13 senders, 113.131.183.0 with 8 senders, 113.131.125.0 with 8 senders,

222 distinct /16 subnets. The top-5 are:

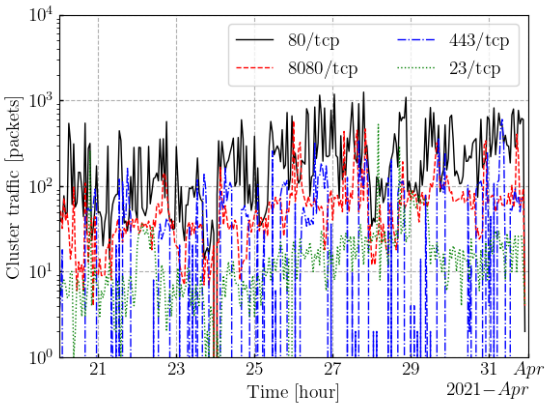
- 172.172.0.0 with 46 senders, 113.131.0.0 with 39 senders, 180.182.0.0 with 30 senders, 110.46.0.0 with 8 senders, 113.130.0.0 with 7 senders,

553 ports contacted. The top-5 are:

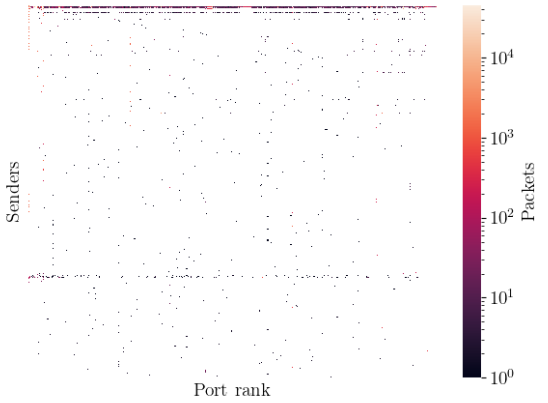
- 80/tcp : 121157 sent packets (40.1 % of the monthly cluster traffic.) 373 senders contacted the port(96.1 % of the cluster senders.)
- 8080/tcp : 34315 sent packets (11.4 % of the monthly cluster traffic.) 309 senders contacted the port(79.6 % of the cluster senders.)
- 443/tcp : 20116 sent packets (6.7 % of the monthly cluster traffic.) 13 senders contacted the port(3.4 % of the cluster senders.)
- 23/tcp : 9670 sent packets (3.2 % of the monthly cluster traffic.) 270 senders contacted the port(69.6 % of the cluster senders.)
- 60001/tcp : 6055 sent packets (2.0 % of the monthly cluster traffic.) 7 senders contacted the port(1.8 % of the cluster senders.)



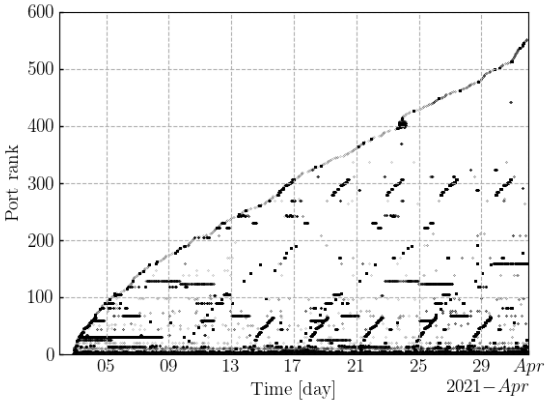
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 44: Cluster21 temporal patterns

23 Cluster 22. Silhouette: 0.435

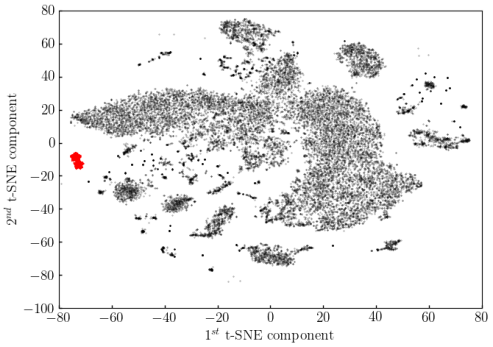


Figure 45: Cluster 22. t-SNE projection

95 distinct senders with the following ground truth classes:

- Unknown. 48 senders
- NetSys. 47 senders

54276 packets sent in the last day. 1.6% of the last day traffic.

6 distinct /24 subnets. The top-5 are:

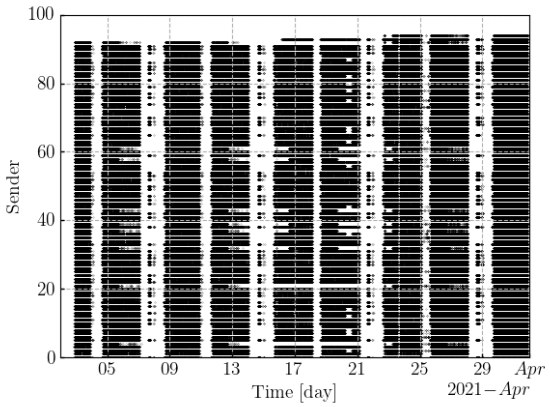
- 104.206.128.0 with 19 senders, 92.118.161.0 with 16 senders, 185.173.35.0 with 16 senders, 92.118.160.0 with 15 senders, 170.130.187.0 with 15 senders,

5 distinct /16 subnets. The top-5 are:

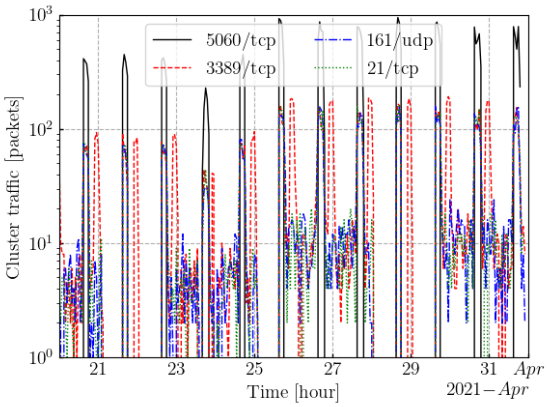
- 92.118.0.0 with 31 senders, 104.206.0.0 with 19 senders, 185.173.0.0 with 16 senders, 170.130.0.0 with 15 senders, 104.140.0.0 with 14 senders,

416 ports contacted. The top-5 are:

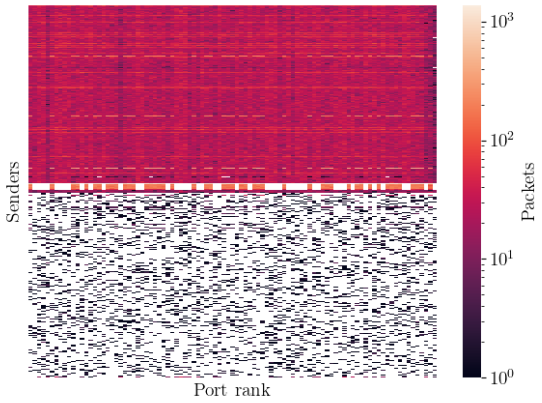
- 5060/tcp : 51643 sent packets (7.3 % of the monthly cluster traffic.) 48 senders contacted the port(50.5 % of the cluster senders.)
- 3389/tcp : 19833 sent packets (2.8 % of the monthly cluster traffic.) 95 senders contacted the port(100.0 % of the cluster senders.)
- 161/udp : 11362 sent packets (1.6 % of the monthly cluster traffic.) 95 senders contacted the port(100.0 % of the cluster senders.)
- 21/tcp : 11347 sent packets (1.6 % of the monthly cluster traffic.) 95 senders contacted the port(100.0 % of the cluster senders.)
- 5900/tcp : 8825 sent packets (1.3 % of the monthly cluster traffic.) 48 senders contacted the port(50.5 % of the cluster senders.)



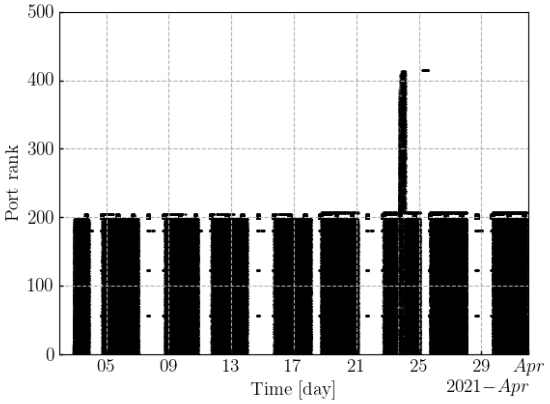
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 46: Cluster22 temporal patterns

24 Cluster 23. Silhouette: 0.696

125 distinct senders with the following ground truth classes:

- Unknown. 96 senders
- Censys. 26 senders
- Stretchoid. 2 senders
- Ipip. 1 sender

43568 packets sent in the last day. 1.3% of the last day traffic.

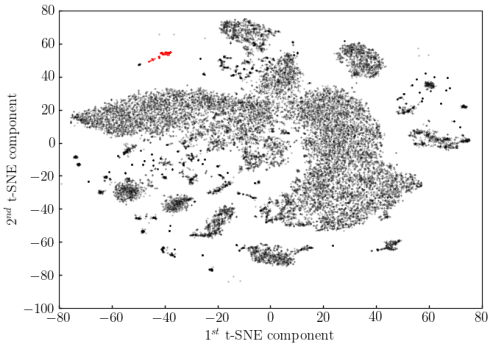


Figure 47: Cluster 23. t-SNE projection

42 distinct /24 subnets. The top-5 are:

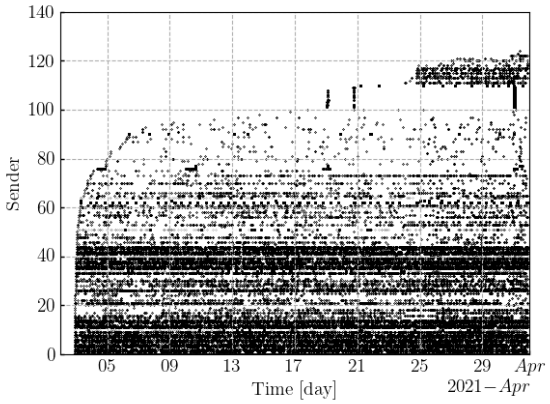
- 23.129.64.0 with 35 senders, 185.220.100.0 with 10 senders, 185.220.101.0 with 10 senders, 162.142.125.0 with 10 senders, 167.248.133.0 with 8 senders,

33 distinct /16 subnets. The top-5 are:

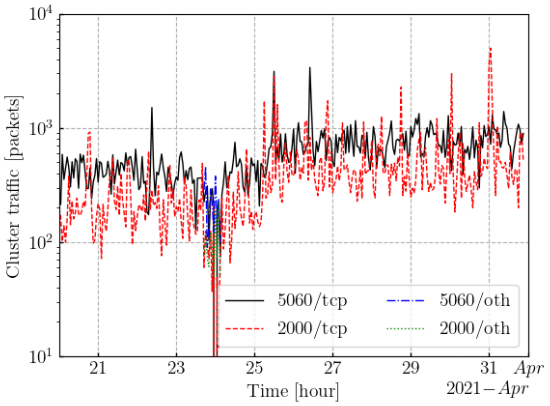
- 23.129.0.0 with 35 senders, 185.220.0.0 with 20 senders, 162.142.0.0 with 10 senders, 74.120.0.0 with 8 senders, 167.248.0.0 with 8 senders,

119 ports contacted. The top-5 are:

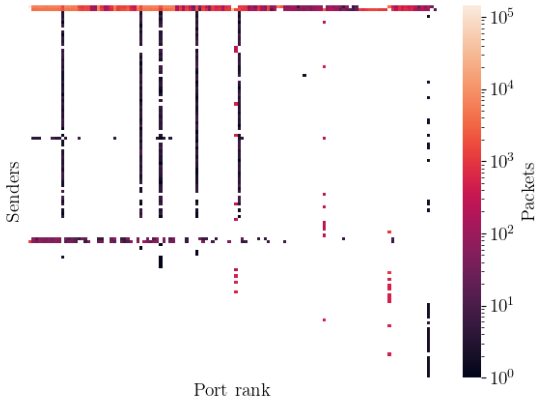
- 5060/tcp : 349276 sent packets (61.0 % of the monthly cluster traffic.) 111 senders contacted the port(88.8 % of the cluster senders.)
- 2000/tcp : 205673 sent packets (35.9 % of the monthly cluster traffic.) 120 senders contacted the port(96.0 % of the cluster senders.)
- 5060/oth : 2476 sent packets (0.4 % of the monthly cluster traffic.) 42 senders contacted the port(33.6 % of the cluster senders.)
- 2000/oth : 1127 sent packets (0.2 % of the monthly cluster traffic.) 40 senders contacted the port(32.0 % of the cluster senders.)
- 5061/tcp : 1012 sent packets (0.2 % of the monthly cluster traffic.) 1 senders contacted the port(0.8 % of the cluster senders.)



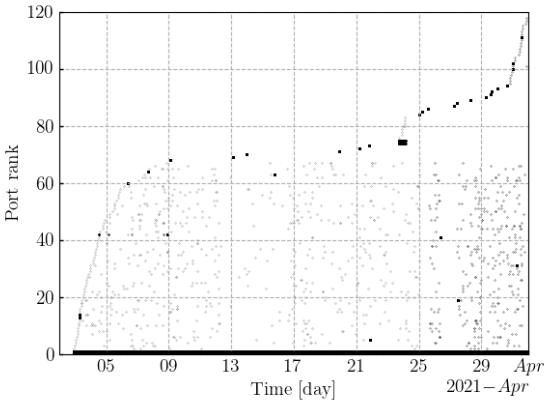
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 48: Cluster23 temporal patterns

25 Cluster 24. Silhouette: 0.591

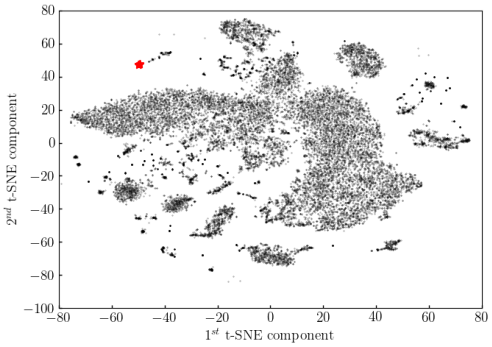


Figure 49: Cluster 24. t-SNE projection

26 distinct senders with the following ground truth classes:

- Unknown. 26 senders

1268 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

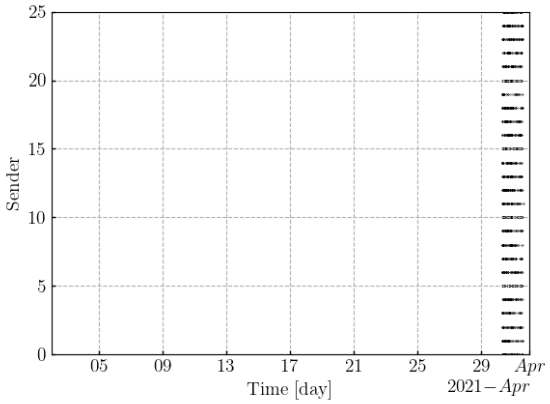
- 34.86.35.0 with 26 senders,

1 distinct /16 subnets. The top-5 are:

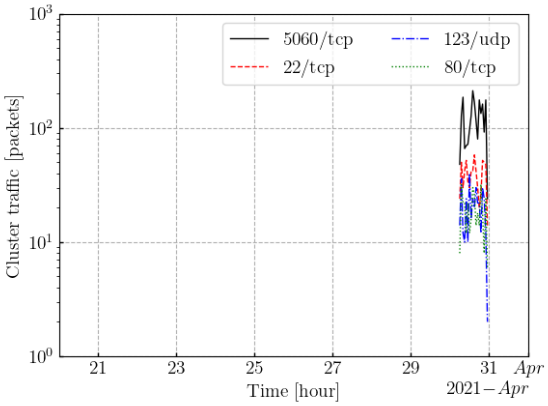
- 34.86.0.0 with 26 senders,

15 ports contacted. The top-5 are:

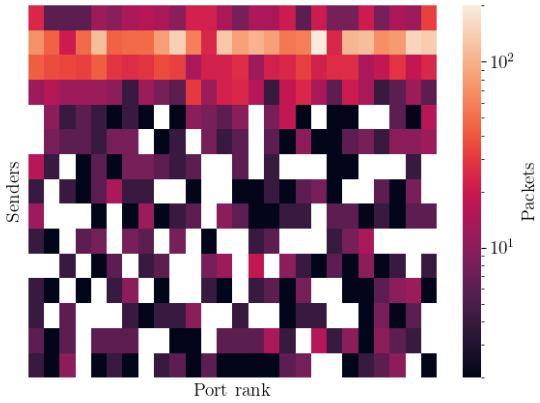
- 5060/tcp : 2134 sent packets (46.6 % of the monthly cluster traffic.) 26 senders contacted the port(100.0 % of the cluster senders.)
- 22/tcp : 686 sent packets (15.0 % of the monthly cluster traffic.) 26 senders contacted the port(100.0 % of the cluster senders.)
- 123/udp : 360 sent packets (7.9 % of the monthly cluster traffic.) 26 senders contacted the port(100.0 % of the cluster senders.)
- 80/tcp : 336 sent packets (7.3 % of the monthly cluster traffic.) 26 senders contacted the port(100.0 % of the cluster senders.)
- 28769/tcp : 136 sent packets (3.0 % of the monthly cluster traffic.) 22 senders contacted the port(84.6 % of the cluster senders.)



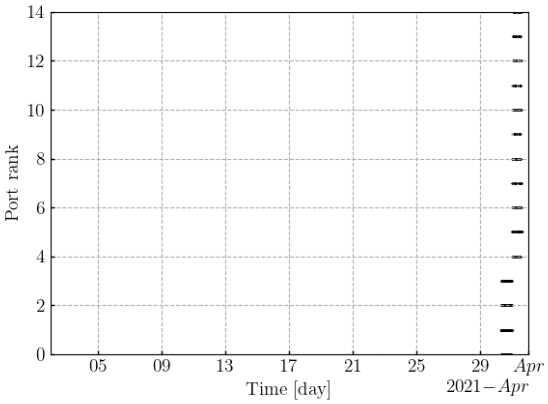
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 50: Cluster24 temporal patterns

26 Cluster 25. Silhouette: 0.397

629 distinct senders with the following ground truth classes:

- Unknown. 611 senders
- Stretchoid. 10 senders
- Ipip. 3 senders
- AlphaStrike. 3 senders
- Mirai-like. 2 senders

46128 packets sent in the last day. 1.4% of the last day traffic. 0.0% of cluster traffic has the Mirai fingerprint.

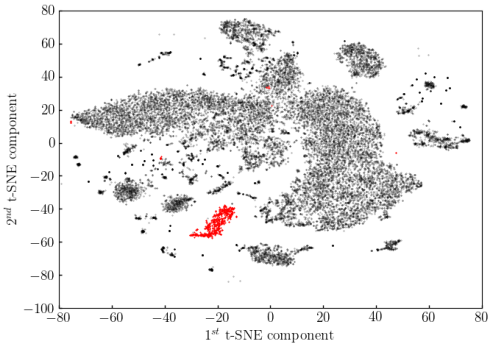


Figure 51: Cluster 25. t-SNE projection

612 distinct /24 subnets. The top-5 are:

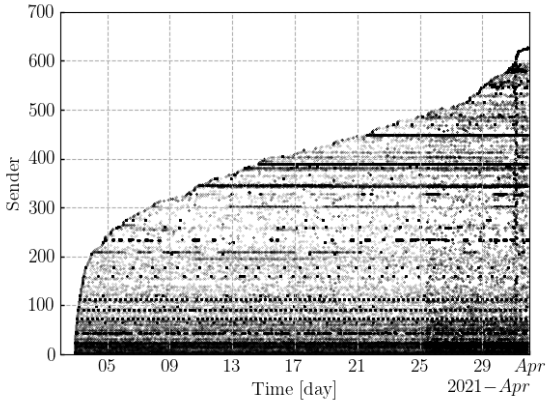
- 161.35.18.0 with 4 senders, 185.90.107.0 with 4 senders, 192.241.227.0 with 2 senders, 45.83.64.0 with 2 senders, 134.122.85.0 with 2 senders,

551 distinct /16 subnets. The top-5 are:

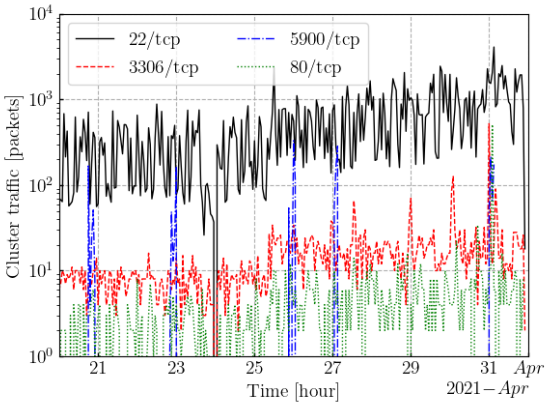
- 192.241.0.0 with 10 senders, 82.65.0.0 with 8 senders, 161.35.0.0 with 7 senders, 185.90.0.0 with 4 senders, 82.64.0.0 with 4 senders,

151 ports contacted. The top-5 are:

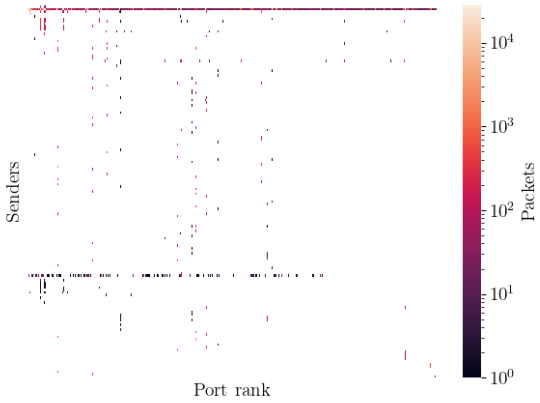
- 22/tcp : 260755 sent packets (79.8 % of the monthly cluster traffic.) 604 senders contacted the port(96.0 % of the cluster senders.)
- 3306/tcp : 8041 sent packets (2.5 % of the monthly cluster traffic.) 23 senders contacted the port(3.7 % of the cluster senders.)
- 5900/tcp : 5278 sent packets (1.6 % of the monthly cluster traffic.) 1 senders contacted the port(0.2 % of the cluster senders.)
- 80/tcp : 3088 sent packets (0.9 % of the monthly cluster traffic.) 19 senders contacted the port(3.0 % of the cluster senders.)
- 2000/tcp : 2530 sent packets (0.8 % of the monthly cluster traffic.) 1 senders contacted the port(0.2 % of the cluster senders.)



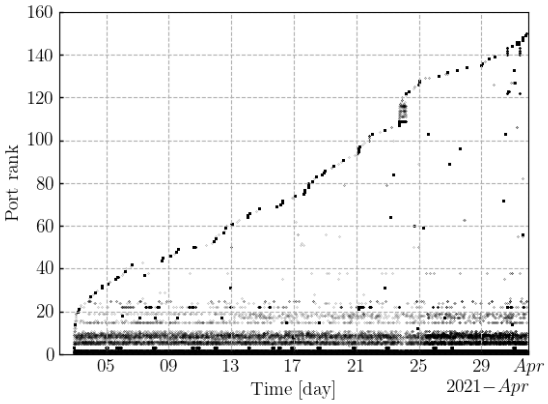
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 52: Cluster25 temporal patterns

27 Cluster 26. Silhouette: -0.055

223 distinct senders with the following ground truth classes:

- Unknown. 127 senders
- AlphaStrike. 78 senders
- Shadowserver. 15 senders
- Stretchoid. 3 senders

59214 packets sent in the last day. 1.7% of the last day traffic.

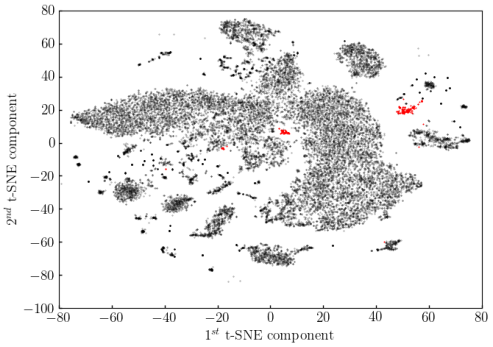


Figure 53: Cluster 26. t-SNE projection

98 distinct /24 subnets. The top-5 are:

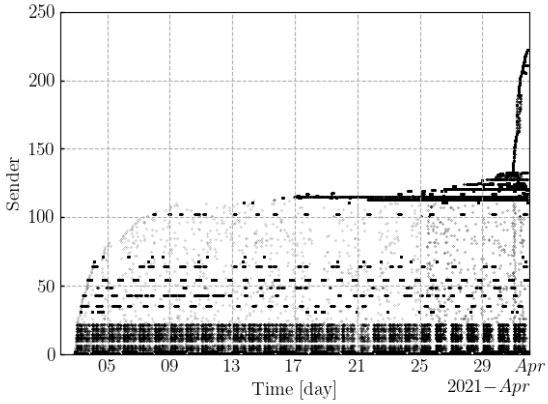
- 103.142.141.0 with 29 senders, 45.83.67.0 with 23 senders, 45.83.64.0 with 20 senders, 45.83.66.0 with 18 senders, 45.83.65.0 with 17 senders,

89 distinct /16 subnets. The top-5 are:

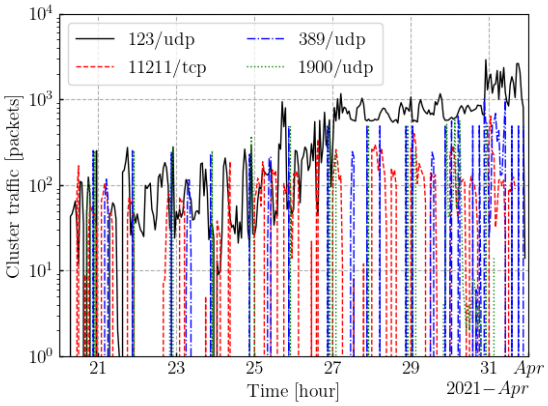
- 45.83.0.0 with 78 senders, 103.142.0.0 with 29 senders, 184.105.0.0 with 15 senders, 103.138.0.0 with 9 senders, 209.141.0.0 with 3 senders,

142 ports contacted. The top-5 are:

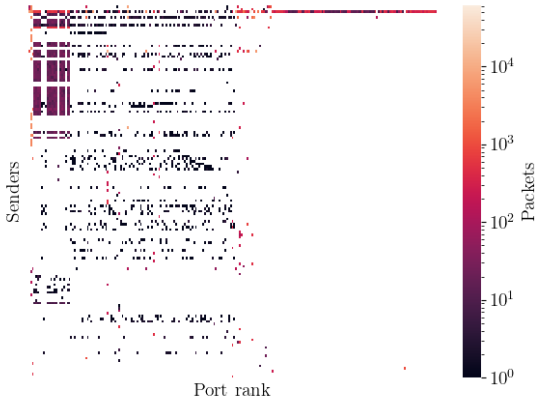
- 123/udp : 153031 sent packets (44.8 % of the monthly cluster traffic.) 172 senders contacted the port(77.1 % of the cluster senders.)
- 11211/tcp : 25218 sent packets (7.4 % of the monthly cluster traffic.) 24 senders contacted the port(10.8 % of the cluster senders.)
- 389/udp : 24321 sent packets (7.1 % of the monthly cluster traffic.) 69 senders contacted the port(30.9 % of the cluster senders.)
- 1900/udp : 14416 sent packets (4.2 % of the monthly cluster traffic.) 10 senders contacted the port(4.5 % of the cluster senders.)
- 53/udp : 13646 sent packets (4.0 % of the monthly cluster traffic.) 3 senders contacted the port(1.3 % of the cluster senders.)



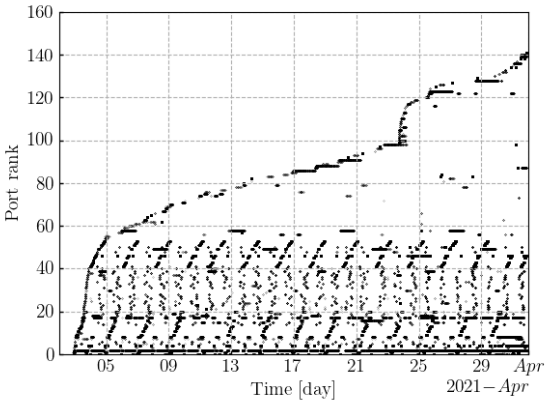
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 54: Cluster26 temporal patterns

28 Cluster 27. Silhouette: 0.593

12 distinct senders with the following ground truth classes:

- Internet-census. 12 senders

2930 packets sent in the last day. 0.1% of the last day traffic.

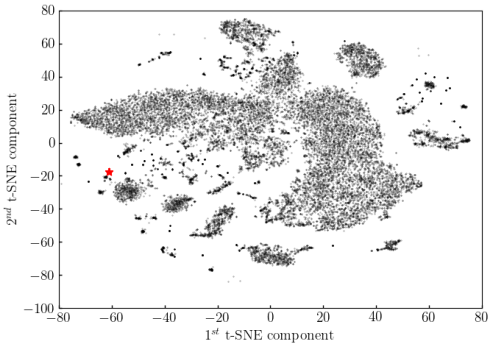


Figure 55: Cluster 27. t-SNE projection

5 distinct /24 subnets. The top-5 are:

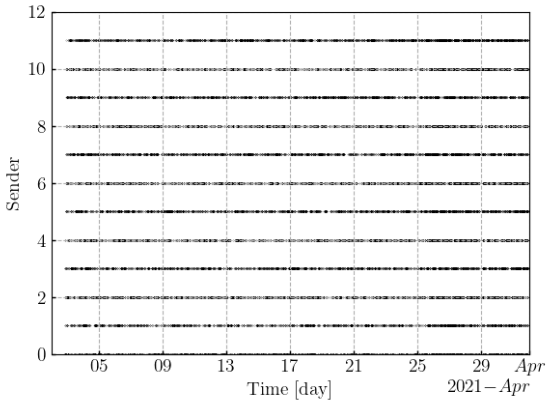
- 128.14.209.0 with 7 senders, 193.118.53.0 with 2 senders, 193.118.55.0 with 1 sender 128.14.136.0 with 1 sender 128.14.133.0 with 1 sender

2 distinct /16 subnets. The top-5 are:

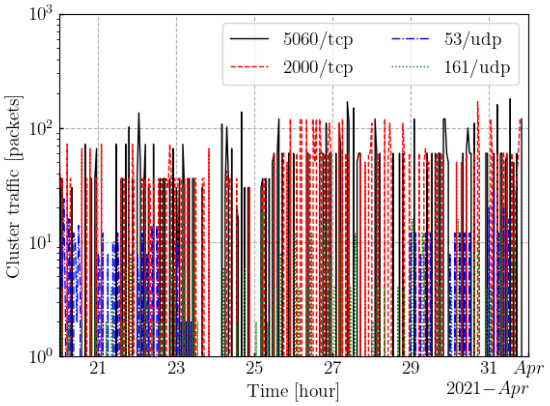
- 128.14.0.0 with 9 senders, 193.118.0.0 with 3 senders,

355 ports contacted. The top-5 are:

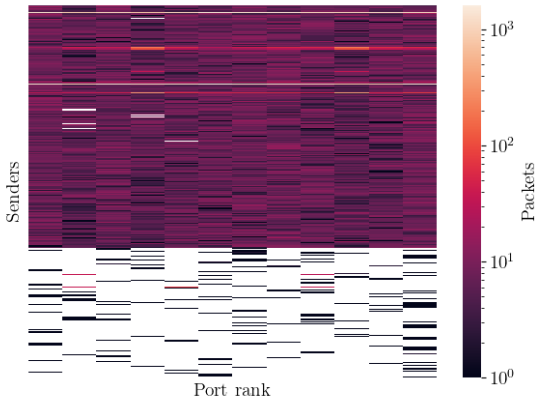
- 5060/tcp : 14032 sent packets (28.3 % of the monthly cluster traffic.) 12 senders contacted the port(100.0 % of the cluster senders.)
- 2000/tcp : 13023 sent packets (26.3 % of the monthly cluster traffic.) 12 senders contacted the port(100.0 % of the cluster senders.)
- 53/udp : 1209 sent packets (2.4 % of the monthly cluster traffic.) 12 senders contacted the port(100.0 % of the cluster senders.)
- 161/udp : 891 sent packets (1.8 % of the monthly cluster traffic.) 12 senders contacted the port(100.0 % of the cluster senders.)
- 1434/udp : 446 sent packets (0.9 % of the monthly cluster traffic.) 12 senders contacted the port(100.0 % of the cluster senders.)



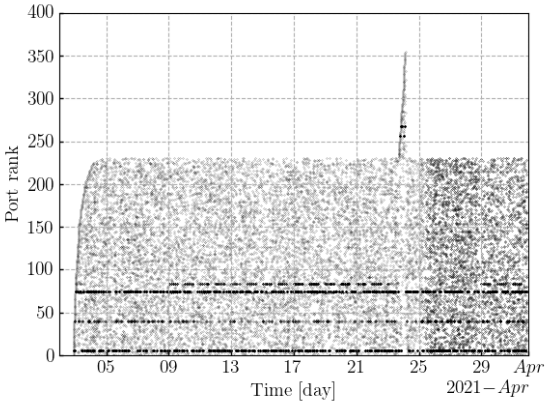
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 56: Cluster27 temporal patterns

29 Cluster 28. Silhouette: 0.971

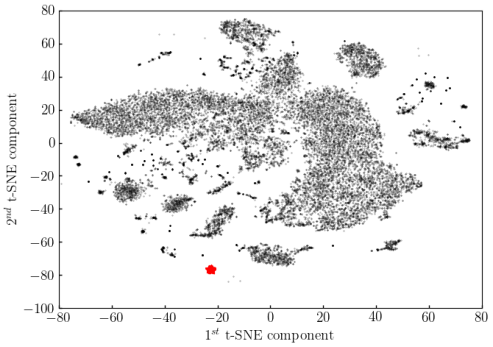


Figure 57: Cluster 28. t-SNE projection

46 distinct senders with the following ground truth classes:

- CSN. 46 senders

486 packets sent in the last day. 0.0% of the last day traffic.

2 distinct /24 subnets. The top-5 are:

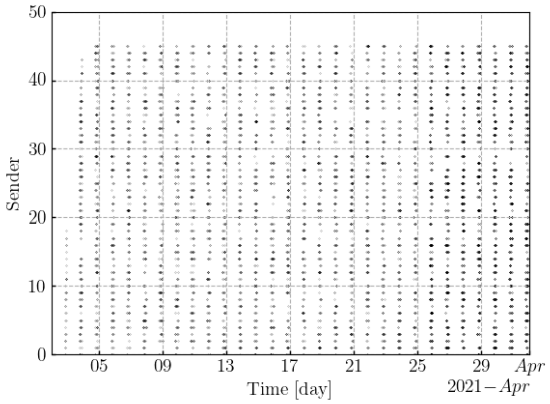
- 209.17.96.0 with 31 senders, 209.17.97.0 with 15 senders,

1 distinct /16 subnets. The top-5 are:

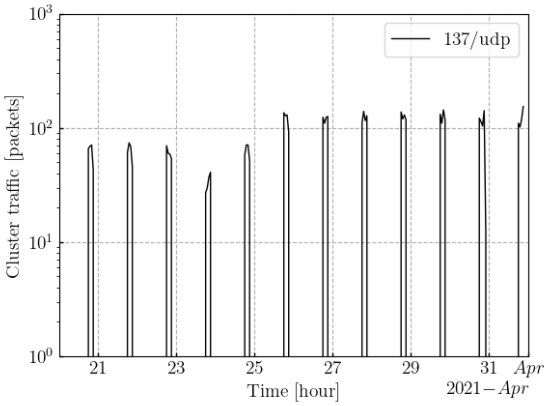
- 209.17.0.0 with 46 senders,

2 ports contacted. The top-5 are:

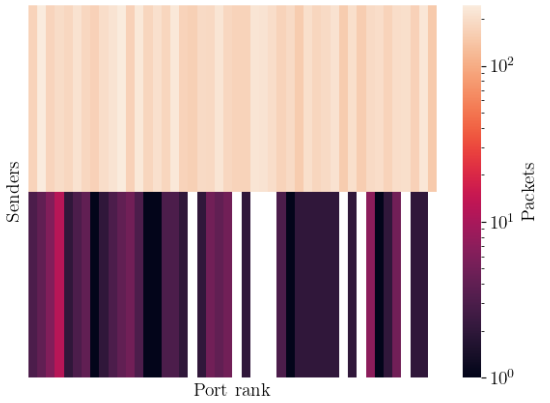
- 137/udp : 8798 sent packets (98.7 % of the monthly cluster traffic.) 46 senders contacted the port(100.0 % of the cluster senders.)
- 137/oth : 115 sent packets (1.3 % of the monthly cluster traffic.) 37 senders contacted the port(80.4 % of the cluster senders.)



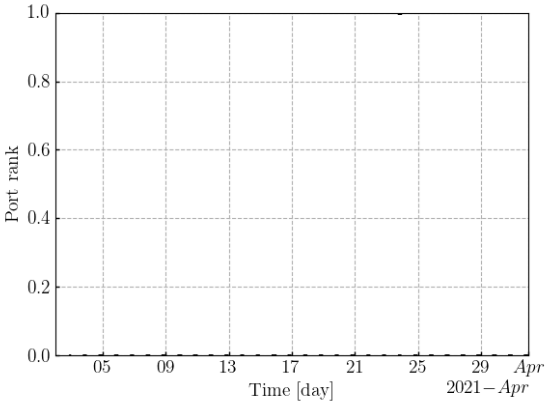
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 58: Cluster28 temporal patterns

30 Cluster 29. Silhouette: 0.197

1769 distinct senders with the following ground truth classes:

- Unknown. 1726 senders
- Mirai-like. 22 senders
- AlphaStrike. 12 senders
- Stretchoid. 8 senders
- Binaryedge. 1 sender

20544 packets sent in the last day. 0.6% of the last day traffic. 0.4% of cluster traffic has the Mirai fingerprint.

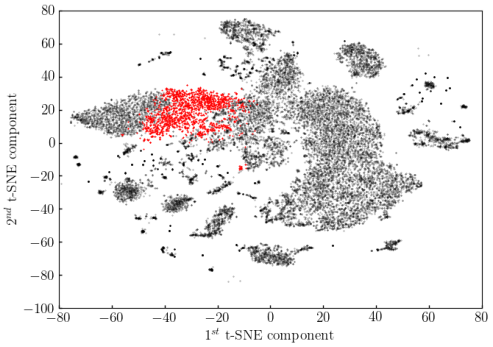


Figure 59: Cluster 29. t-SNE projection

1700 distinct /24 subnets. The top-5 are:

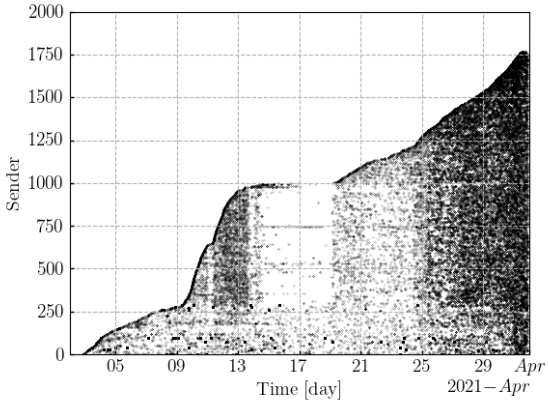
- 202.164.139.0 with 9 senders, 202.164.138.0 with 6 senders, 116.236.231.0 with 5 senders, 113.142.72.0 with 4 senders, 209.14.31.0 with 4 senders,

969 distinct /16 subnets. The top-5 are:

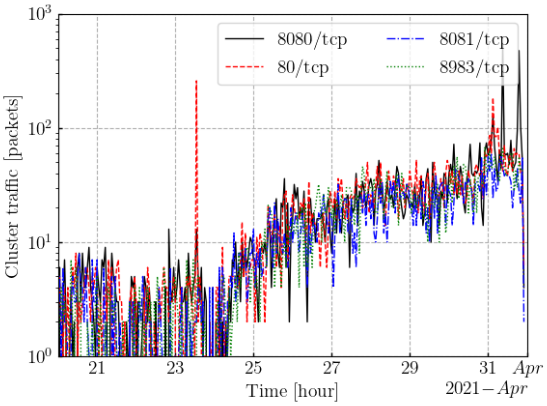
- 161.35.0.0 with 31 senders, 157.230.0.0 with 26 senders, 128.199.0.0 with 21 senders, 167.99.0.0 with 19 senders, 68.183.0.0 with 18 senders,

175 ports contacted. The top-5 are:

- 8080/tcp : 8244 sent packets (9.3 % of the monthly cluster traffic.) 1339 senders contacted the port(75.7 % of the cluster senders.)
- 80/tcp : 7220 sent packets (8.2 % of the monthly cluster traffic.) 1310 senders contacted the port(74.1 % of the cluster senders.)
- 8081/tcp : 5423 sent packets (6.1 % of the monthly cluster traffic.) 1110 senders contacted the port(62.7 % of the cluster senders.)
- 8983/tcp : 5277 sent packets (6.0 % of the monthly cluster traffic.) 1126 senders contacted the port(63.7 % of the cluster senders.)
- 7001/tcp : 5097 sent packets (5.8 % of the monthly cluster traffic.) 1108 senders contacted the port(62.6 % of the cluster senders.)

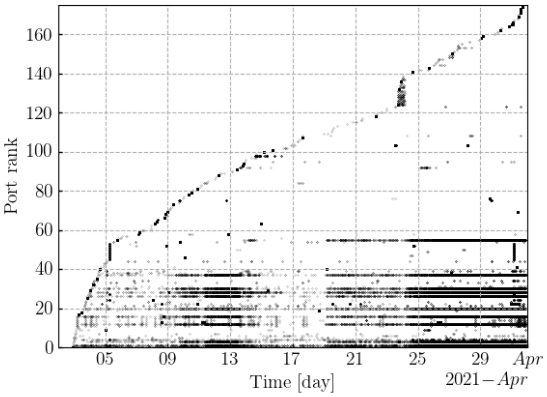


(a) Activity pattern



(b) Top-4 ports traffic

(c) Port Heatmap



(d) Port pattern

Figure 60: Cluster29 temporal patterns

31 Cluster 30. Silhouette: 0.669

14 distinct senders with the following ground truth classes:

- Unknown. 14 senders

3436 packets sent in the last day. 0.1% of the last day traffic.

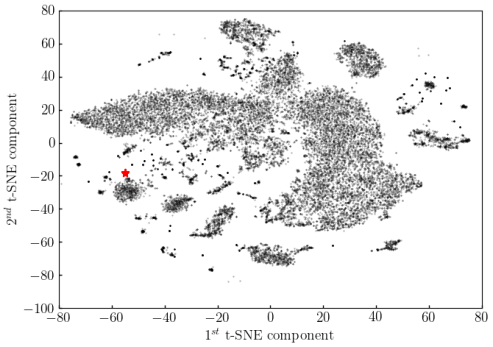


Figure 61: Cluster 30. t-SNE projection

14 distinct /24 subnets. The top-5 are:

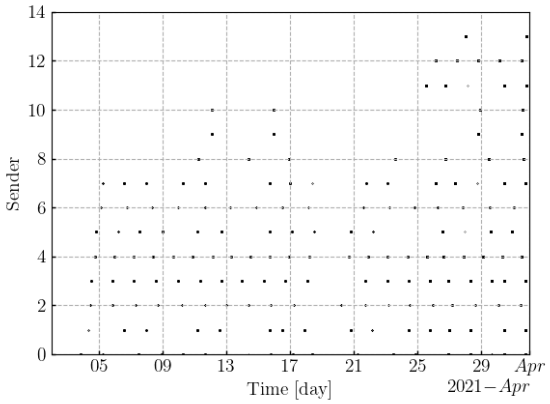
- 95.46.114.0 with 1 sender 95.142.37.0 with 1 sender 82.146.54.0 with 1 sender 81.29.143.0 with 1 sender 62.173.140.0 with 1 sender

14 distinct /16 subnets. The top-5 are:

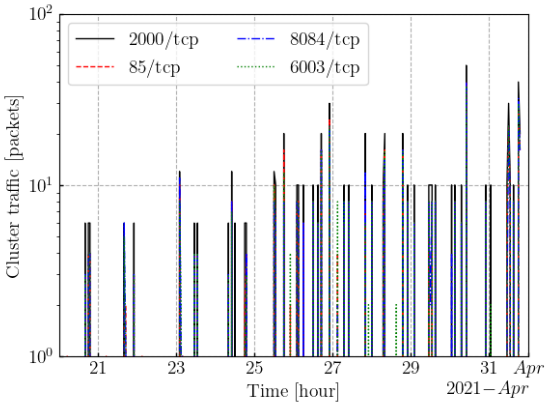
- 95.46.0.0 with 1 sender 95.142.0.0 with 1 sender 82.146.0.0 with 1 sender 81.29.0.0 with 1 sender 62.173.0.0 with 1 sender

35 ports contacted. The top-5 are:

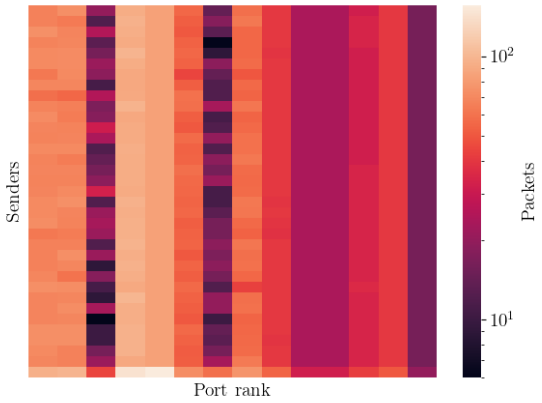
- 2000/tcp : 972 sent packets (4.3 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 85/tcp : 649 sent packets (2.9 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 8084/tcp : 648 sent packets (2.9 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 6003/tcp : 647 sent packets (2.9 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 8081/tcp : 646 sent packets (2.9 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)



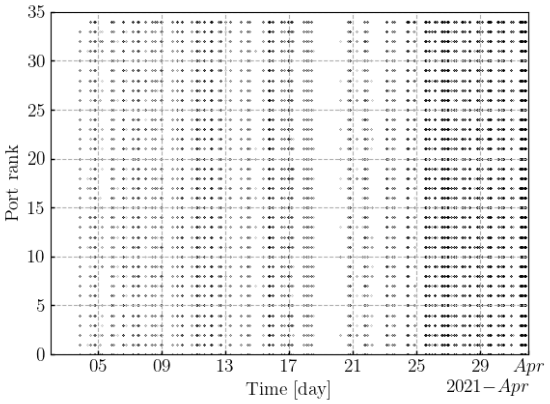
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 62: Cluster30 temporal patterns

32 Cluster 31. Silhouette: 0.371

33 distinct senders with the following ground truth classes:

- Unknown. 27 senders
- Mirai-like. 6 senders

11248 packets sent in the last day. 0.3% of the last day traffic. 1.0% of cluster traffic has the Mirai fingerprint.

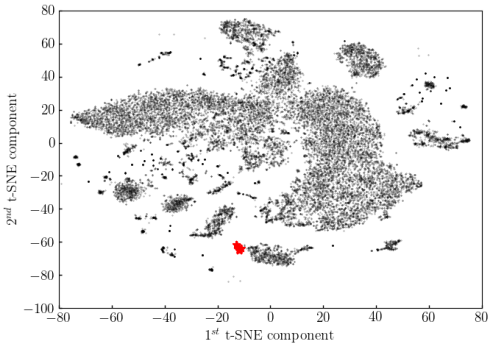


Figure 63: Cluster 31. t-SNE projection

25 distinct /24 subnets. The top-5 are:

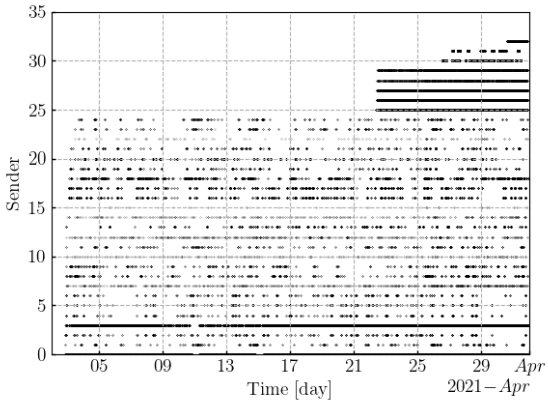
- 103.40.172.0 with 4 senders, 4.71.37.0 with 2 senders, 140.206.86.0 with 2 senders, 203.248.175.0 with 2 senders, 216.4.95.0 with 2 senders,

24 distinct /16 subnets. The top-5 are:

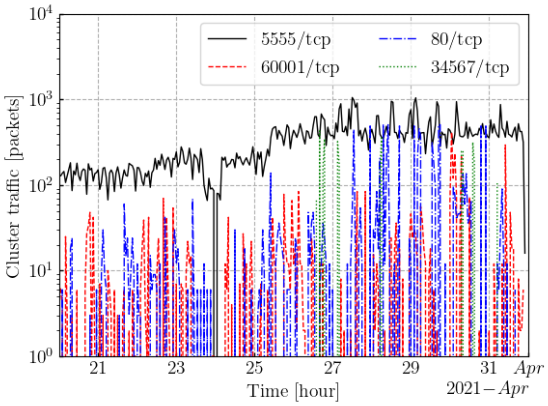
- 103.40.0.0 with 4 senders, 4.71.0.0 with 2 senders, 140.206.0.0 with 2 senders, 167.172.0.0 with 2 senders, 203.248.0.0 with 2 senders,

16 ports contacted. The top-5 are:

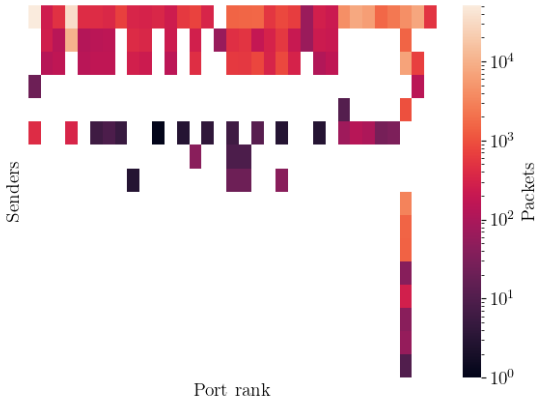
- 5555/tcp : 132129 sent packets (77.2 % of the monthly cluster traffic.) 32 senders contacted the port(97.0 % of the cluster senders.)
- 60001/tcp : 17066 sent packets (10.0 % of the monthly cluster traffic.) 21 senders contacted the port(63.6 % of the cluster senders.)
- 80/tcp : 13132 sent packets (7.7 % of the monthly cluster traffic.) 19 senders contacted the port(57.6 % of the cluster senders.)
- 34567/tcp : 3110 sent packets (1.8 % of the monthly cluster traffic.) 1 senders contacted the port(3.0 % of the cluster senders.)
- 81/tcp : 1460 sent packets (0.9 % of the monthly cluster traffic.) 1 senders contacted the port(3.0 % of the cluster senders.)



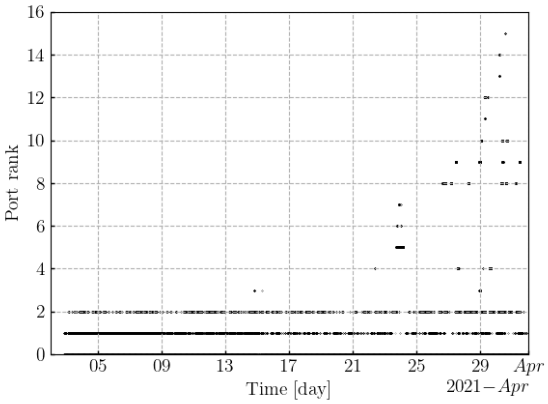
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 64: Cluster31 temporal patterns

33 Cluster 32. Silhouette: 0.836

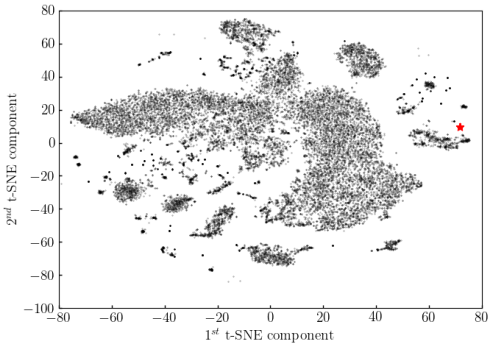


Figure 65: Cluster 32. t-SNE projection

14 distinct senders with the following ground truth classes:

- Shadowserver. 12 senders
- Unknown. 2 senders

1904 packets sent in the last day. 0.1% of the last day traffic.

2 distinct /24 subnets. The top-5 are:

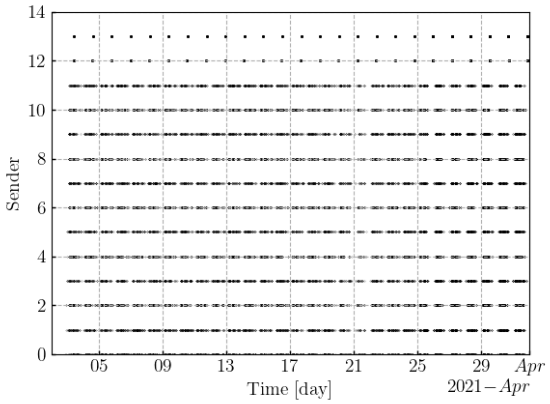
- 184.105.247.0 with 12 senders, 185.217.1.0 with 2 senders,

2 distinct /16 subnets. The top-5 are:

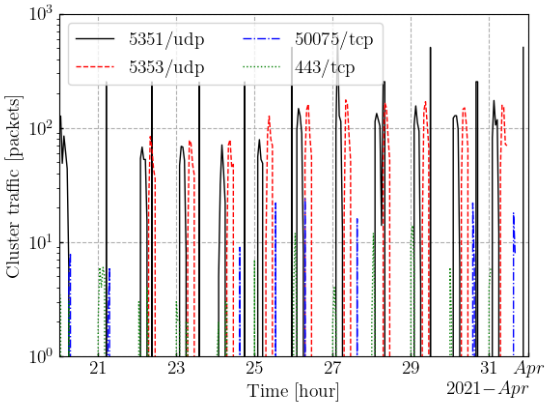
- 184.105.0.0 with 12 senders, 185.217.0.0 with 2 senders,

41 ports contacted. The top-5 are:

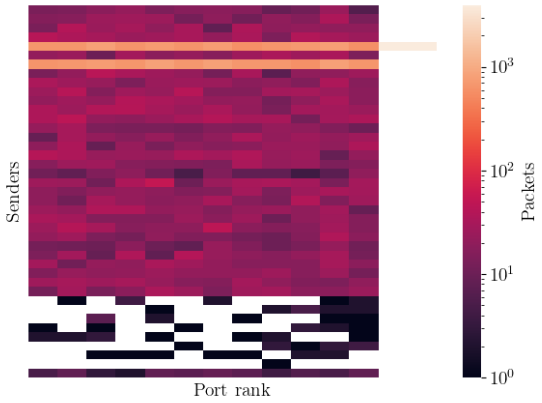
- 5351/udp : 15976 sent packets (49.3 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 5353/udp : 8388 sent packets (25.9 % of the monthly cluster traffic.) 12 senders contacted the port(85.7 % of the cluster senders.)
- 50075/tcp : 350 sent packets (1.1 % of the monthly cluster traffic.) 12 senders contacted the port(85.7 % of the cluster senders.)
- 443/tcp : 348 sent packets (1.1 % of the monthly cluster traffic.) 12 senders contacted the port(85.7 % of the cluster senders.)
- 50070/tcp : 338 sent packets (1.0 % of the monthly cluster traffic.) 12 senders contacted the port(85.7 % of the cluster senders.)



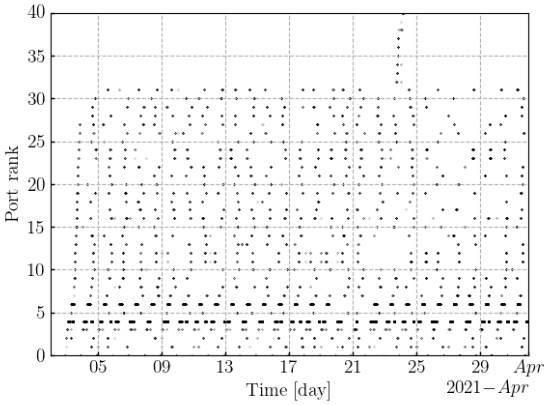
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 66: Cluster32 temporal patterns

34 Cluster 33. Silhouette: 0.905

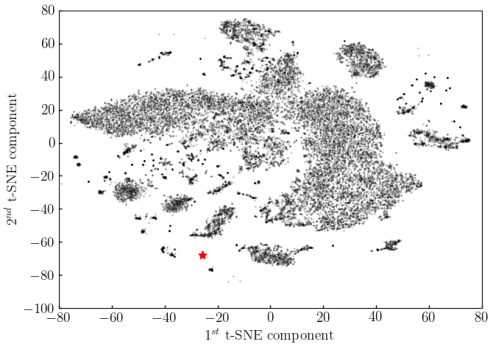


Figure 67: Cluster 33. t-SNE projection

32 distinct senders with the following ground truth classes:

- Unknown. 32 senders

1098 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

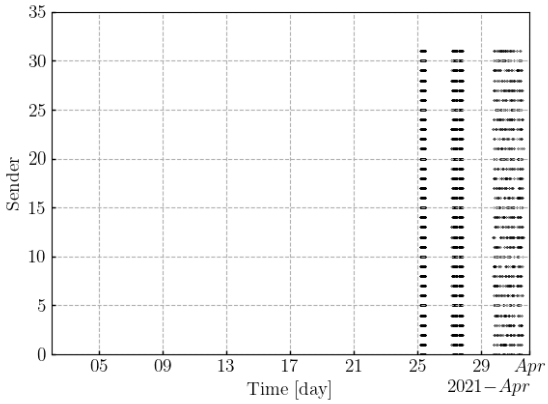
- 34.77.162.0 with 32 senders,

1 distinct /16 subnets. The top-5 are:

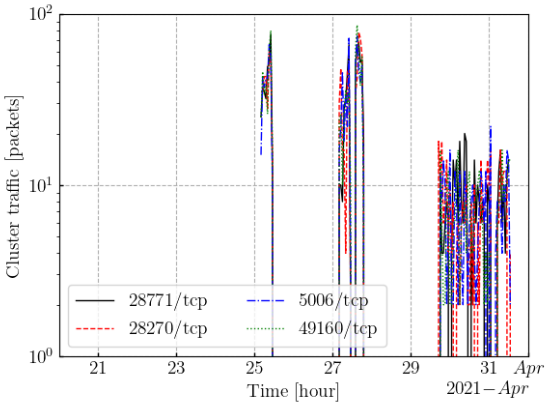
- 34.77.0.0 with 32 senders,

16 ports contacted. The top-5 are:

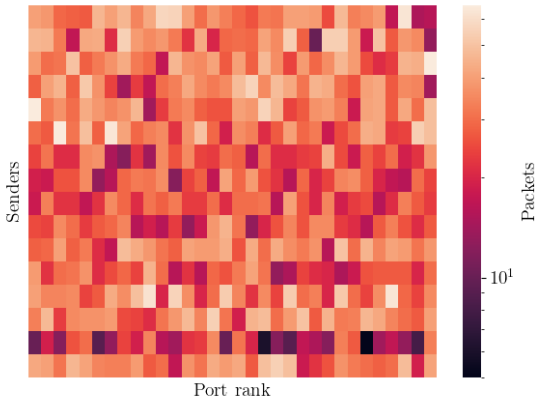
- 28771/tcp : 1151 sent packets (7.2 % of the monthly cluster traffic.) 32 senders contacted the port(100.0 % of the cluster senders.)
- 28270/tcp : 1144 sent packets (7.2 % of the monthly cluster traffic.) 32 senders contacted the port(100.0 % of the cluster senders.)
- 5006/tcp : 1143 sent packets (7.1 % of the monthly cluster traffic.) 32 senders contacted the port(100.0 % of the cluster senders.)
- 49160/tcp : 1142 sent packets (7.1 % of the monthly cluster traffic.) 32 senders contacted the port(100.0 % of the cluster senders.)
- 5008/tcp : 1136 sent packets (7.1 % of the monthly cluster traffic.) 32 senders contacted the port(100.0 % of the cluster senders.)



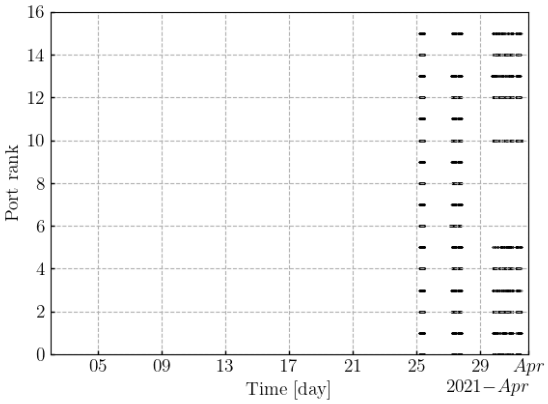
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 68: Cluster33 temporal patterns

35 Cluster 34. Silhouette: 0.869

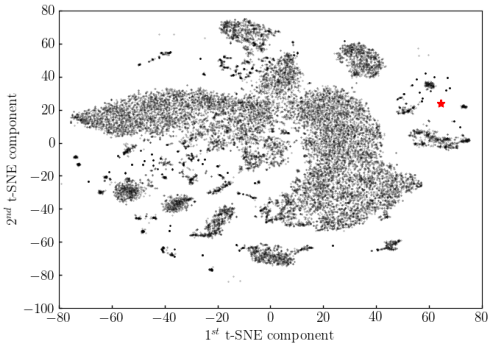


Figure 69: Cluster 34. t-SNE projection

16 distinct senders with the following ground truth classes:

- Shadowserver. 15 senders
- Unknown. 1 sender

2734 packets sent in the last day. 0.1% of the last day traffic.

2 distinct /24 subnets. The top-5 are:

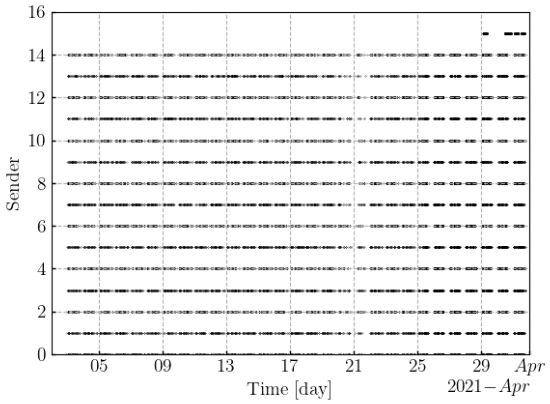
- 184.105.139.0 with 15 senders, 103.139.45.0 with 1 sender

2 distinct /16 subnets. The top-5 are:

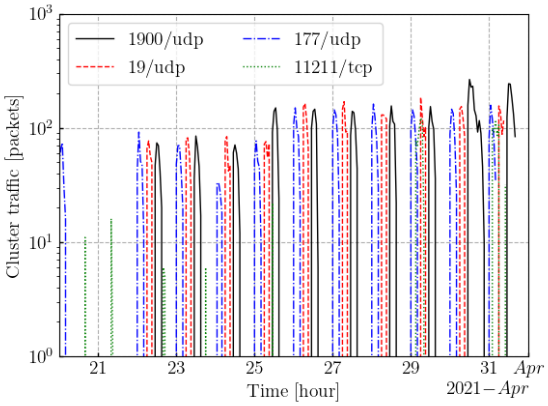
- 184.105.0.0 with 15 senders, 103.139.0.0 with 1 sender

42 ports contacted. The top-5 are:

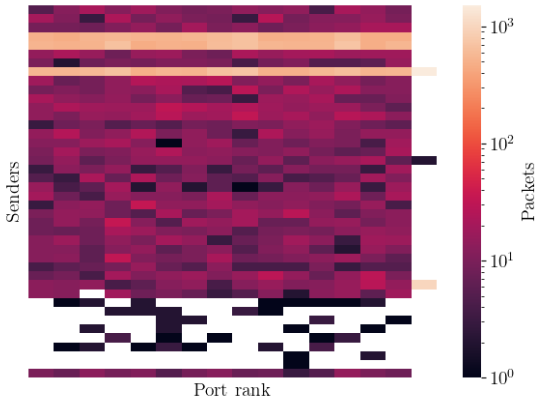
- 1900/udp : 10070 sent packets (30.4 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 19/udp : 8302 sent packets (25.0 % of the monthly cluster traffic.) 15 senders contacted the port(93.8 % of the cluster senders.)
- 177/udp : 8015 sent packets (24.2 % of the monthly cluster traffic.) 15 senders contacted the port(93.8 % of the cluster senders.)
- 11211/tcp : 1181 sent packets (3.6 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 873/tcp : 285 sent packets (0.9 % of the monthly cluster traffic.) 15 senders contacted the port(93.8 % of the cluster senders.)



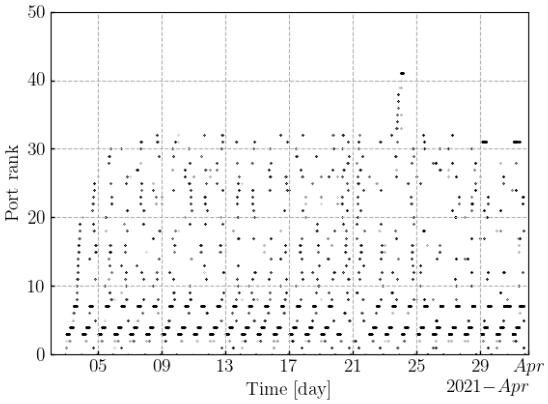
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 70: Cluster34 temporal patterns

36 Cluster 35. Silhouette: -0.144

137 distinct senders with the following ground truth classes:

- Unknown. 54 senders
- Internet-census. 41 senders
- Censys. 14 senders
- Stretchoid. 11 senders
- Shodan. 9 senders
- Ipip. 5 senders
- Mirai-like. 2 senders
- Shadowserver. 1 sender

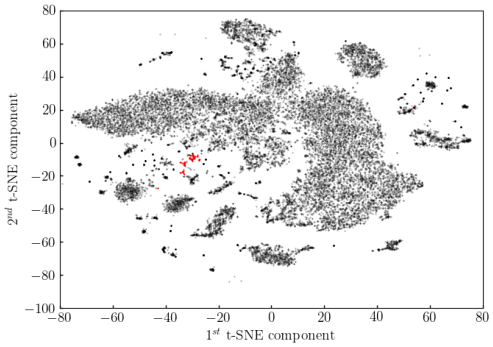


Figure 71: Cluster 35. t-SNE projection

34540 packets sent in the last day. 1.0% of the last day traffic. 0.0% of cluster traffic has the Mirai fingerprint.
86 distinct /24 subnets. The top-5 are:

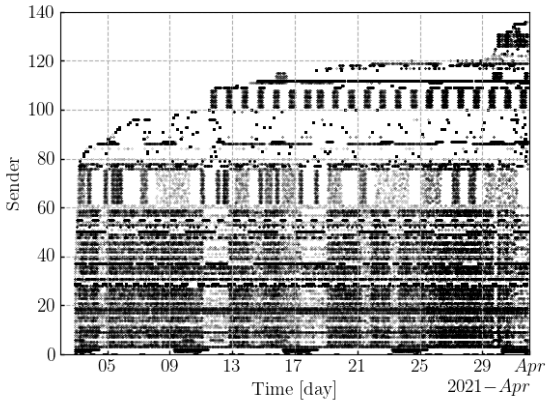
- 193.118.53.0 with 15 senders, 192.35.168.0 with 14 senders, 128.14.152.0 with 5 senders, 128.1.91.0 with 5 senders, 128.14.137.0 with 4 senders,

63 distinct /16 subnets. The top-5 are:

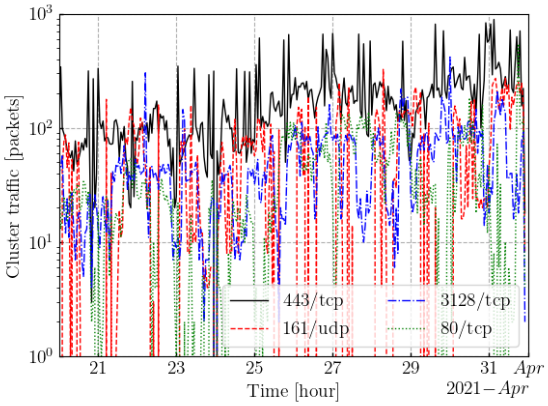
- 128.14.0.0 with 15 senders, 193.118.0.0 with 15 senders, 192.35.0.0 with 14 senders, 192.241.0.0 with 11 senders, 128.1.0.0 with 5 senders,

207 ports contacted. The top-5 are:

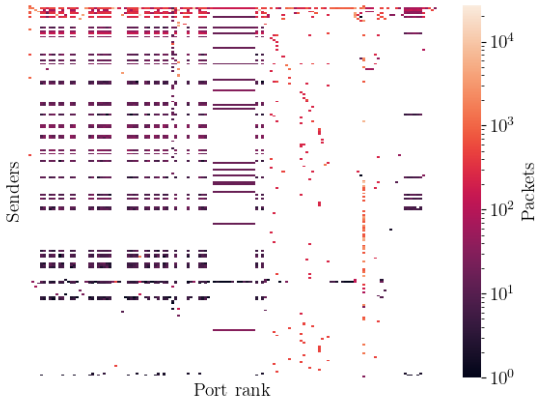
- 443/tcp : 106927 sent packets (26.4 % of the monthly cluster traffic.) 114 senders contacted the port(83.2 % of the cluster senders.)
- 161/udp : 31039 sent packets (7.7 % of the monthly cluster traffic.) 29 senders contacted the port(21.2 % of the cluster senders.)
- 3128/tcp : 30574 sent packets (7.5 % of the monthly cluster traffic.) 14 senders contacted the port(10.2 % of the cluster senders.)
- 80/tcp : 19935 sent packets (4.9 % of the monthly cluster traffic.) 59 senders contacted the port(43.1 % of the cluster senders.)
- 8080/tcp : 16138 sent packets (4.0 % of the monthly cluster traffic.) 64 senders contacted the port(46.7 % of the cluster senders.)



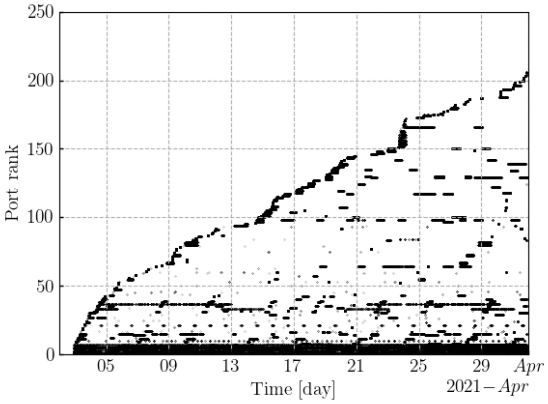
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 72: Cluster35 temporal patterns

37 Cluster 36. Silhouette: 0.174

1354 distinct senders with the following ground truth classes:

- Mirai-like. 1204 senders
- Unknown. 150 senders

7650 packets sent in the last day. 0.2% of the last day traffic. 82.4% of cluster traffic has the Mirai fingerprint.

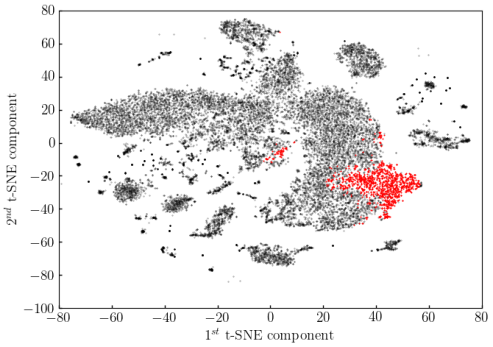


Figure 73: Cluster 36. t-SNE projection

1297 distinct /24 subnets. The top-5 are:

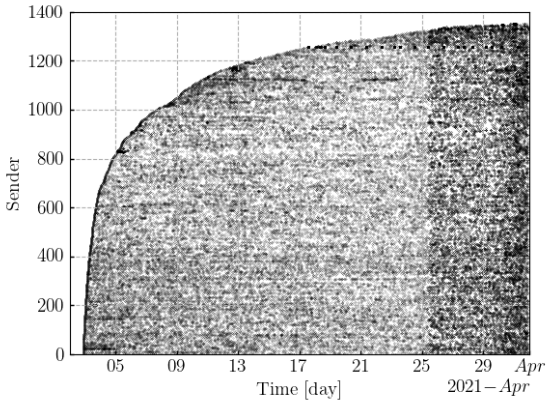
- 178.72.75.0 with 10 senders, 178.72.70.0 with 8 senders, 178.72.76.0 with 8 senders, 178.72.68.0 with 7 senders, 178.72.78.0 with 3 senders,

1055 distinct /16 subnets. The top-5 are:

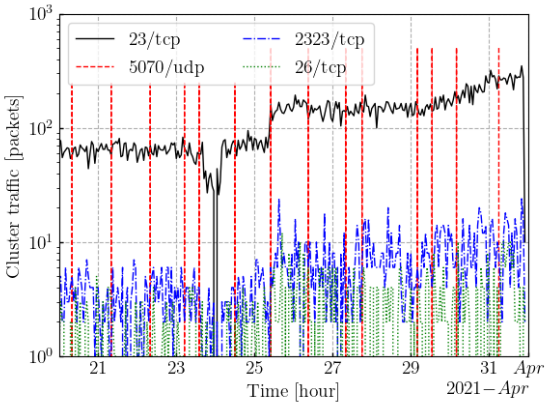
- 178.72.0.0 with 42 senders, 220.135.0.0 with 12 senders, 114.35.0.0 with 12 senders, 122.117.0.0 with 11 senders, 114.33.0.0 with 9 senders,

58 ports contacted. The top-5 are:

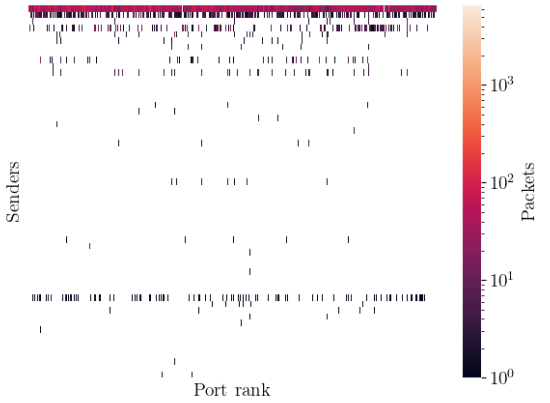
- 23/tcp : 64728 sent packets (81.5 % of the monthly cluster traffic.) 1347 senders contacted the port(99.5 % of the cluster senders.)
- 5070/udp : 6569 sent packets (8.3 % of the monthly cluster traffic.) 1 senders contacted the port(0.1 % of the cluster senders.)
- 2323/tcp : 3126 sent packets (3.9 % of the monthly cluster traffic.) 766 senders contacted the port(56.6 % of the cluster senders.)
- 26/tcp : 1892 sent packets (2.4 % of the monthly cluster traffic.) 288 senders contacted the port(21.3 % of the cluster senders.)
- 8081/tcp : 754 sent packets (0.9 % of the monthly cluster traffic.) 104 senders contacted the port(7.7 % of the cluster senders.)



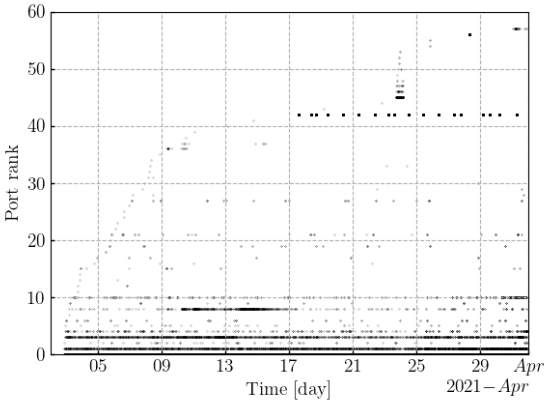
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 74: Cluster36 temporal patterns

38 Cluster 37. Silhouette: 0.393

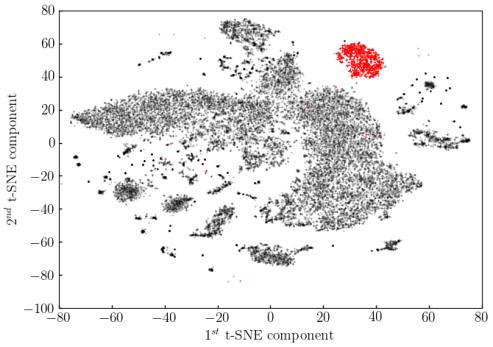


Figure 75: Cluster 37. t-SNE projection

909 distinct senders with the following ground truth classes:

- Unknown. 885 senders
- Mirai-like. 24 senders

4192 packets sent in the last day. 0.1% of the last day traffic. 1.6% of cluster traffic has the Mirai fingerprint.

889 distinct /24 subnets. The top-5 are:

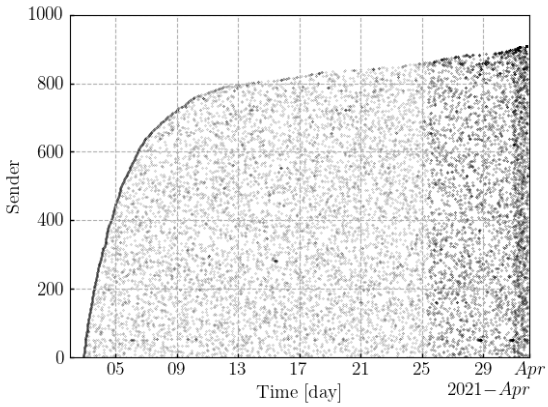
- 202.164.138.0 with 5 senders, 178.72.75.0 with 3 senders, 209.14.31.0 with 2 senders, 84.228.112.0 with 2 senders, 78.23.172.0 with 2 senders,

628 distinct /16 subnets. The top-5 are:

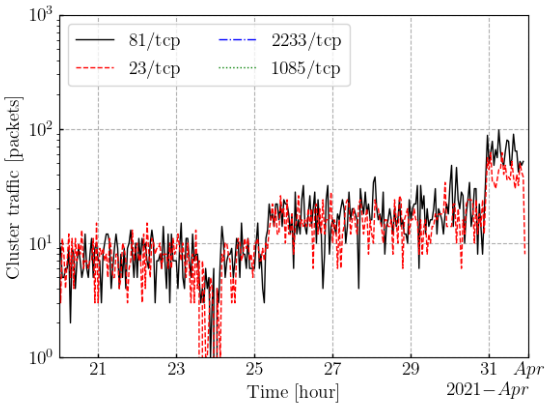
- 122.117.0.0 with 15 senders, 114.32.0.0 with 15 senders, 114.33.0.0 with 13 senders, 220.132.0.0 with 12 senders, 220.133.0.0 with 12 senders,

39 ports contacted. The top-5 are:

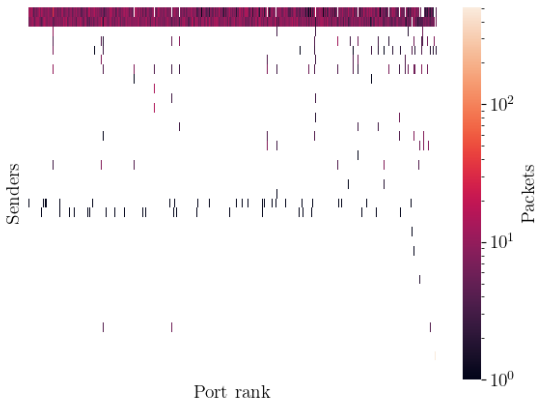
- 81/tcp : 7912 sent packets (44.6 % of the monthly cluster traffic.) 905 senders contacted the port(99.6 % of the cluster senders.)
- 23/tcp : 7115 sent packets (40.1 % of the monthly cluster traffic.) 860 senders contacted the port(94.6 % of the cluster senders.)
- 2233/tcp : 506 sent packets (2.9 % of the monthly cluster traffic.) 1 senders contacted the port(0.1 % of the cluster senders.)
- 1085/tcp : 506 sent packets (2.9 % of the monthly cluster traffic.) 1 senders contacted the port(0.1 % of the cluster senders.)
- 34567/tcp : 500 sent packets (2.8 % of the monthly cluster traffic.) 1 senders contacted the port(0.1 % of the cluster senders.)



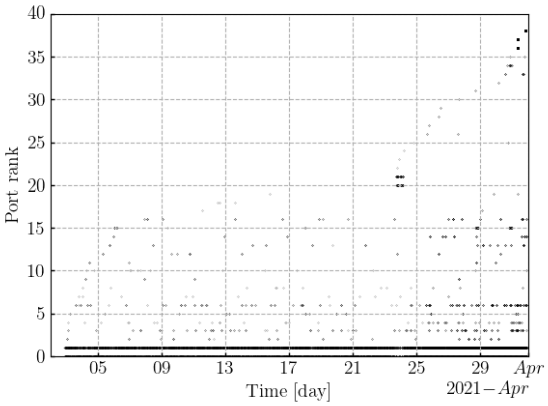
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 76: Cluster37 temporal patterns

39 Cluster 38. Silhouette: 0.416

893 distinct senders with the following ground truth classes:

- Unknown. 867 senders
- Mirai-like. 20 senders
- Stretchoid. 3 senders
- AlphaStrike. 3 senders

124348 packets sent in the last day. 3.7% of the last day traffic. 0.0% of cluster traffic has the Mirai fingerprint.

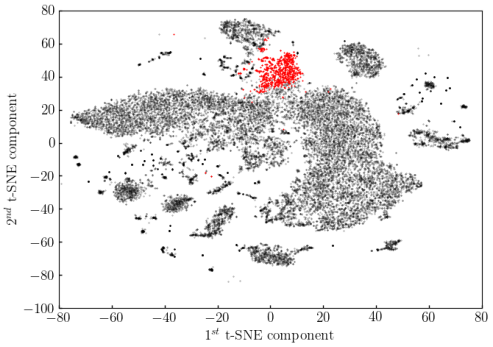


Figure 77: Cluster 38. t-SNE projection

797 distinct /24 subnets. The top-5 are:

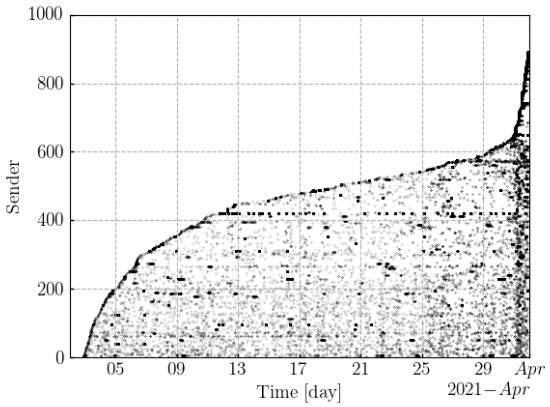
- 103.201.137.0 with 20 senders, 60.172.0.0 with 12 senders, 165.225.104.0 with 11 senders, 112.133.244.0 with 8 senders, 182.148.122.0 with 8 senders,

700 distinct /16 subnets. The top-5 are:

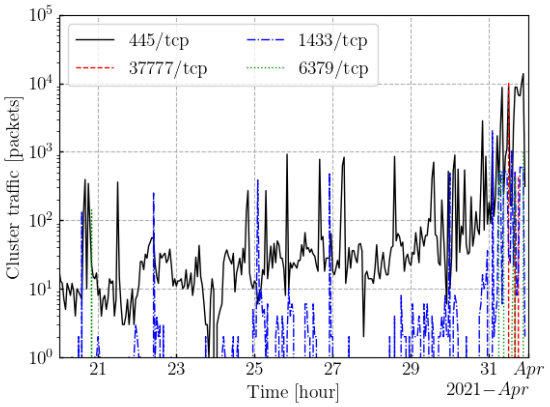
- 103.201.0.0 with 20 senders, 165.225.0.0 with 12 senders, 60.172.0.0 with 12 senders, 112.133.0.0 with 12 senders, 182.148.0.0 with 8 senders,

272 ports contacted. The top-5 are:

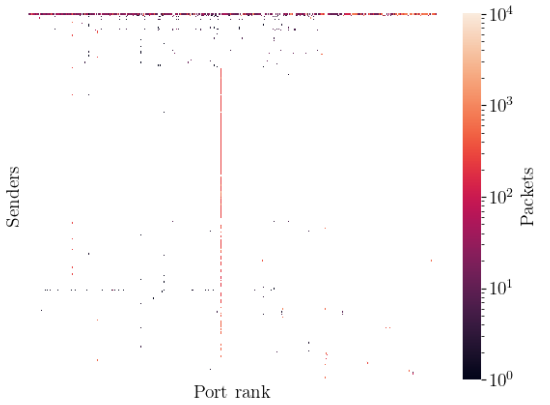
- 445/tcp : 121637 sent packets (54.4 % of the monthly cluster traffic.) 715 senders contacted the port(80.1 % of the cluster senders.)
- 37777/tcp : 11108 sent packets (5.0 % of the monthly cluster traffic.) 3 senders contacted the port(0.3 % of the cluster senders.)
- 1433/tcp : 10940 sent packets (4.9 % of the monthly cluster traffic.) 108 senders contacted the port(12.1 % of the cluster senders.)
- 6379/tcp : 3579 sent packets (1.6 % of the monthly cluster traffic.) 9 senders contacted the port(1.0 % of the cluster senders.)
- 139/tcp : 3461 sent packets (1.5 % of the monthly cluster traffic.) 6 senders contacted the port(0.7 % of the cluster senders.)



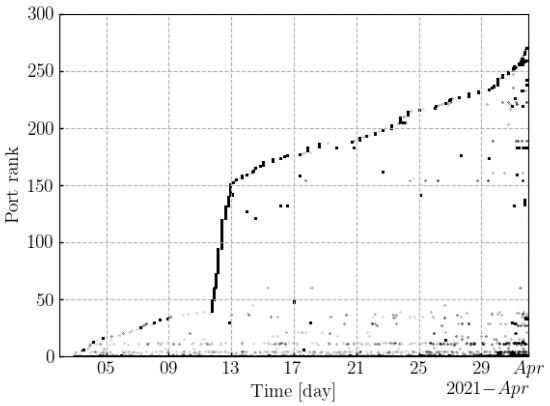
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 78: Cluster38 temporal patterns

40 Cluster 39. Silhouette: 0.244

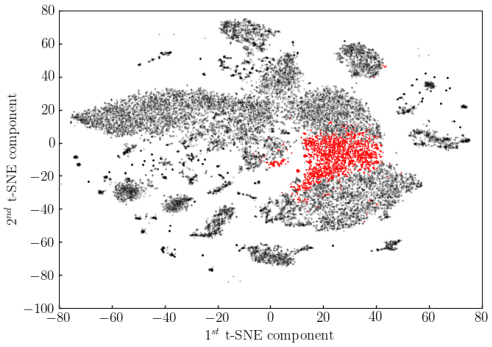


Figure 79: Cluster 39. t-SNE projection

1885 distinct senders with the following ground truth classes:

- Mirai-like. 1676 senders
- Unknown. 209 senders

19408 packets sent in the last day. 0.6% of the last day traffic. 84.7% of cluster traffic has the Mirai fingerprint.

1738 distinct /24 subnets. The top-5 are:

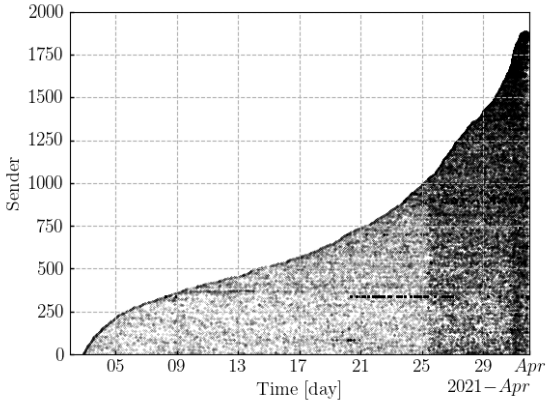
- 202.44.249.0 with 13 senders, 178.72.75.0 with 11 senders, 178.72.77.0 with 10 senders, 178.72.68.0 with 10 senders, 178.72.78.0 with 9 senders,

1339 distinct /16 subnets. The top-5 are:

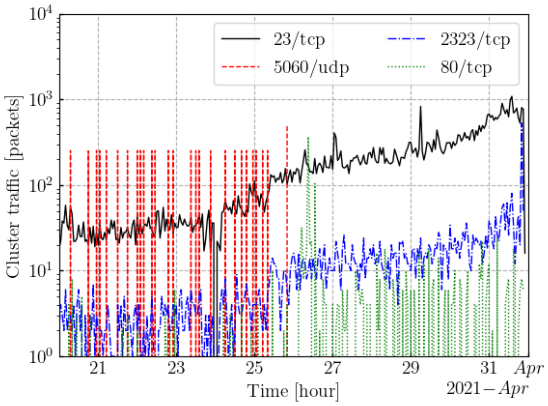
- 178.72.0.0 with 59 senders, 202.44.0.0 with 28 senders, 117.192.0.0 with 18 senders, 31.163.0.0 with 16 senders, 178.141.0.0 with 16 senders,

85 ports contacted. The top-5 are:

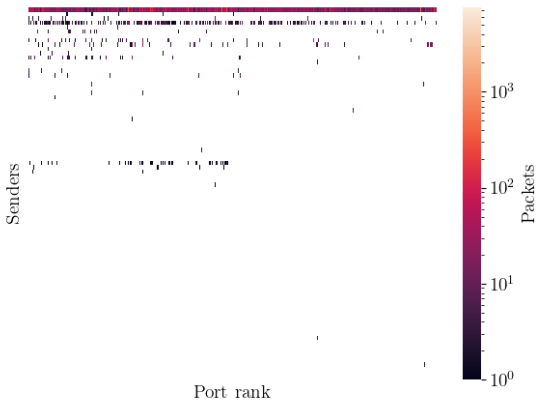
- 23/tcp : 58399 sent packets (67.9 % of the monthly cluster traffic.) 1882 senders contacted the port(99.8 % of the cluster senders.)
- 5060/udp : 7579 sent packets (8.8 % of the monthly cluster traffic.) 1 senders contacted the port(0.1 % of the cluster senders.)
- 2323/tcp : 4046 sent packets (4.7 % of the monthly cluster traffic.) 854 senders contacted the port(45.3 % of the cluster senders.)
- 80/tcp : 1379 sent packets (1.6 % of the monthly cluster traffic.) 138 senders contacted the port(7.3 % of the cluster senders.)
- 26/tcp : 1042 sent packets (1.2 % of the monthly cluster traffic.) 158 senders contacted the port(8.4 % of the cluster senders.)



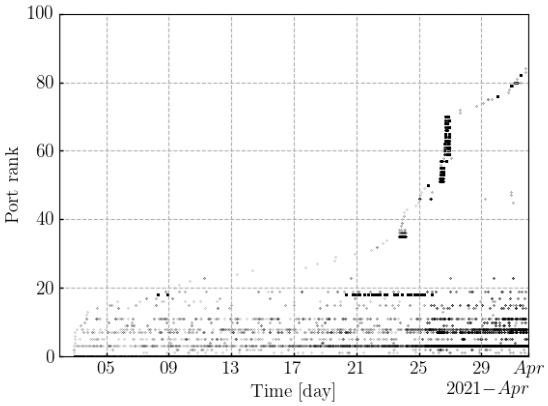
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 80: Cluster39 temporal patterns

41 Cluster 40. Silhouette: 0.227

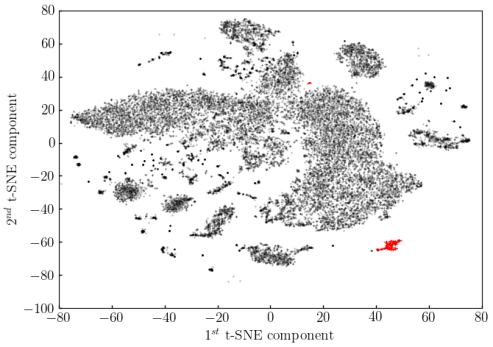


Figure 81: Cluster 40. t-SNE projection

194 distinct senders with the following ground truth classes:

- Unknown. 191 senders
- Ipip. 3 senders

14984 packets sent in the last day. 0.4% of the last day traffic.

184 distinct /24 subnets. The top-5 are:

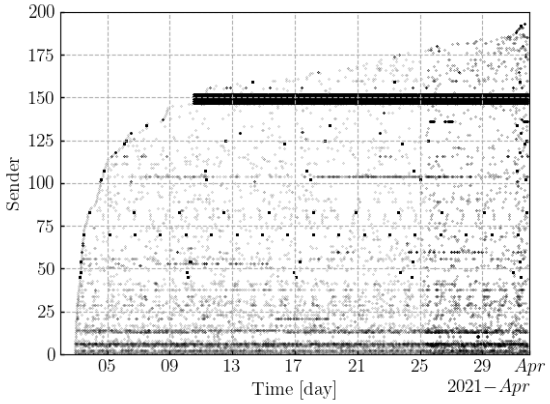
- 212.220.11.0 with 4 senders, 222.175.50.0 with 2 senders, 218.59.231.0 with 2 senders, 176.16.93.0 with 2 senders, 58.58.251.0 with 2 senders,

178 distinct /16 subnets. The top-5 are:

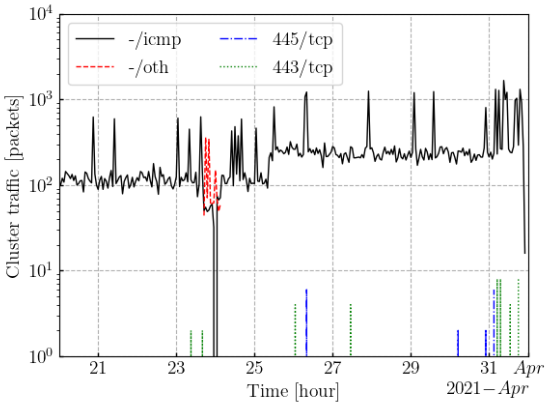
- 212.220.0.0 with 4 senders, 176.16.0.0 with 3 senders, 45.170.0.0 with 2 senders, 84.22.0.0 with 2 senders, 58.58.0.0 with 2 senders,

28 ports contacted. The top-5 are:

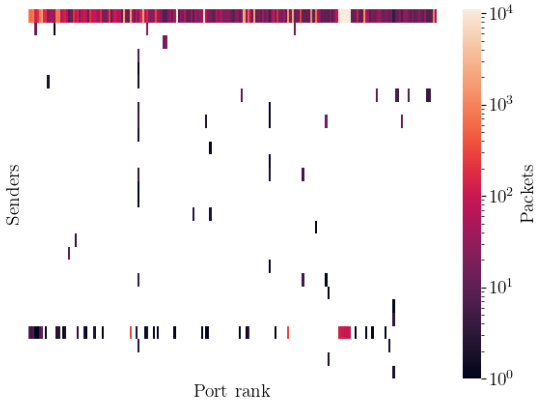
- -/icmp : 114148 sent packets (98.6 % of the monthly cluster traffic.) 194 senders contacted the port(100.0 % of the cluster senders.)
- -/oth : 1324 sent packets (1.1 % of the monthly cluster traffic.) 42 senders contacted the port(21.6 % of the cluster senders.)
- 445/tcp : 50 sent packets (0.0 % of the monthly cluster traffic.) 4 senders contacted the port(2.1 % of the cluster senders.)
- 443/tcp : 48 sent packets (0.0 % of the monthly cluster traffic.) 7 senders contacted the port(3.6 % of the cluster senders.)
- 1433/tcp : 33 sent packets (0.0 % of the monthly cluster traffic.) 2 senders contacted the port(1.0 % of the cluster senders.)



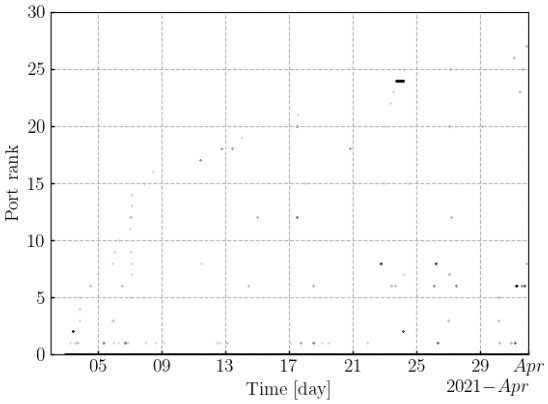
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 82: Cluster40 temporal patterns

42 Cluster 41. Silhouette: -0.425

153 distinct senders with the following ground truth classes:

- Unknown. 123 senders
- Shadowserver. 15 senders
- Mirai-like. 9 senders
- AlphaStrike. 3 senders
- Stretchoid. 2 senders
- Ipip. 1 sender

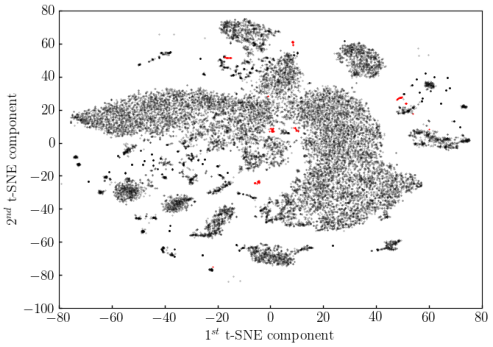


Figure 83: Cluster 41. t-SNE projection

71956 packets sent in the last day. 2.1% of the last day traffic. 0.0% of cluster traffic has the Mirai fingerprint.

129 distinct /24 subnets. The top-5 are:

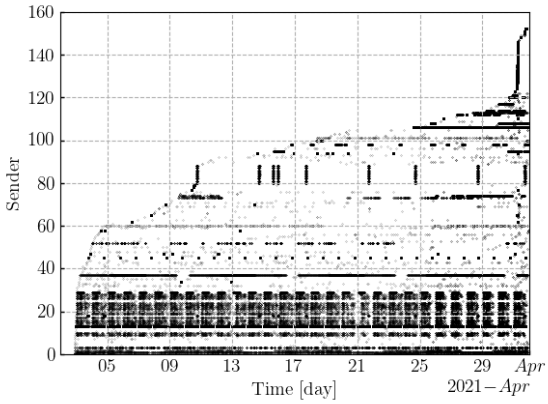
- 216.218.206.0 with 15 senders, 141.212.123.0 with 10 senders, 37.49.230.0 with 2 senders, 141.22.28.0 with 1 sender 143.137.87.0 with 1 sender

117 distinct /16 subnets. The top-5 are:

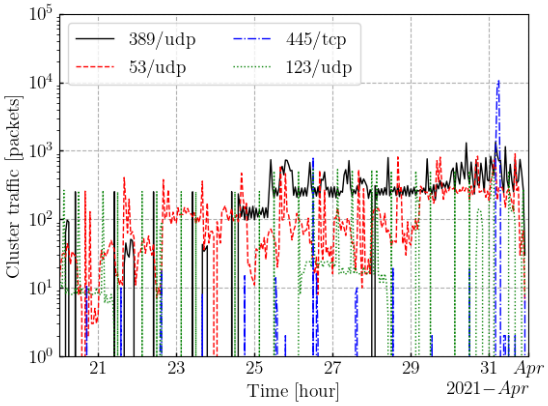
- 216.218.0.0 with 15 senders, 141.212.0.0 with 10 senders, 178.72.0.0 with 4 senders, 45.83.0.0 with 3 senders, 178.175.0.0 with 2 senders,

142 ports contacted. The top-5 are:

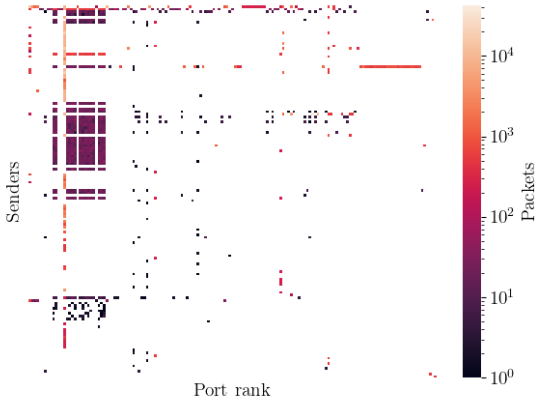
- 389/udp : 70065 sent packets (13.0 % of the monthly cluster traffic.) 12 senders contacted the port(7.8 % of the cluster senders.)
- 53/udp : 60612 sent packets (11.2 % of the monthly cluster traffic.) 30 senders contacted the port(19.6 % of the cluster senders.)
- 445/tcp : 25818 sent packets (4.8 % of the monthly cluster traffic.) 49 senders contacted the port(32.0 % of the cluster senders.)
- 123/udp : 23912 sent packets (4.4 % of the monthly cluster traffic.) 7 senders contacted the port(4.6 % of the cluster senders.)
- 1900/udp : 19290 sent packets (3.6 % of the monthly cluster traffic.) 4 senders contacted the port(2.6 % of the cluster senders.)



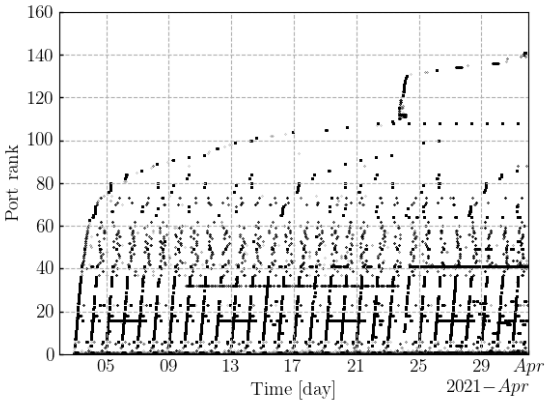
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 84: Cluster41 temporal patterns

43 Cluster 42. Silhouette: -0.027

120 distinct senders with the following ground truth classes:

- Unknown. 117 senders
- Stretchoid. 3 senders

5310 packets sent in the last day. 0.2% of the last day traffic.

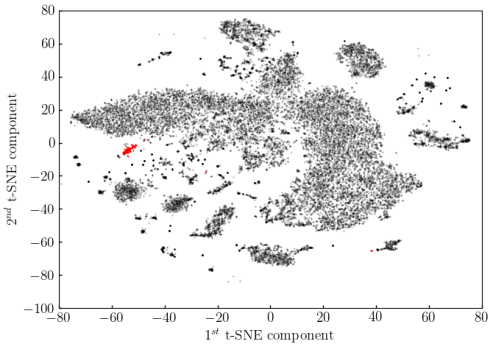


Figure 85: Cluster 42. t-SNE projection

117 distinct /24 subnets. The top-5 are:

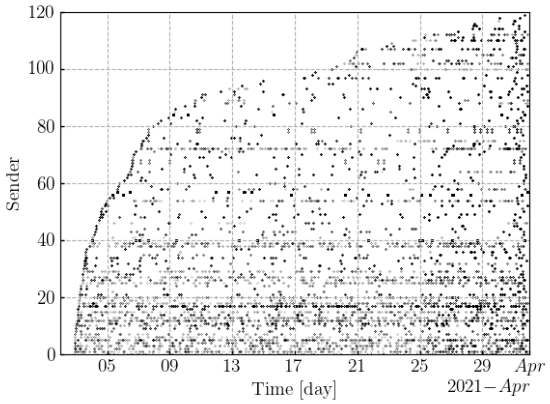
- 150.138.145.0 with 2 senders, 8.131.65.0 with 2 senders, 192.241.227.0 with 2 senders, 124.160.165.0 with 1 sender 121.4.74.0 with 1 sender

99 distinct /16 subnets. The top-5 are:

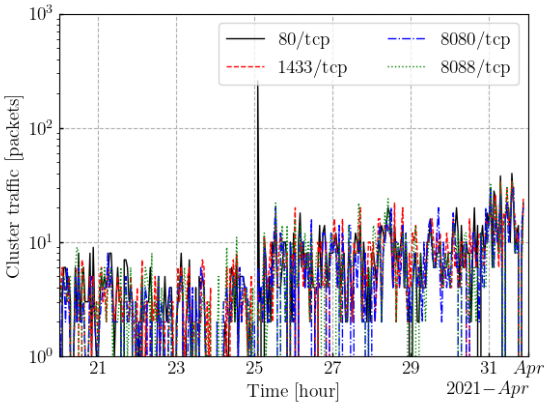
- 8.131.0.0 with 5 senders, 49.234.0.0 with 4 senders, 106.53.0.0 with 4 senders, 119.45.0.0 with 3 senders, 192.241.0.0 with 3 senders,

74 ports contacted. The top-5 are:

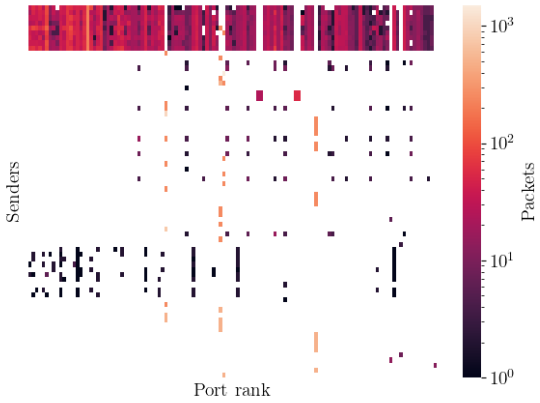
- 80/tcp : 3242 sent packets (7.6 % of the monthly cluster traffic.) 109 senders contacted the port(90.8 % of the cluster senders.)
- 1433/tcp : 3124 sent packets (7.3 % of the monthly cluster traffic.) 109 senders contacted the port(90.8 % of the cluster senders.)
- 8080/tcp : 2933 sent packets (6.8 % of the monthly cluster traffic.) 108 senders contacted the port(90.0 % of the cluster senders.)
- 8088/tcp : 2898 sent packets (6.8 % of the monthly cluster traffic.) 109 senders contacted the port(90.8 % of the cluster senders.)
- 9200/tcp : 2881 sent packets (6.7 % of the monthly cluster traffic.) 109 senders contacted the port(90.8 % of the cluster senders.)



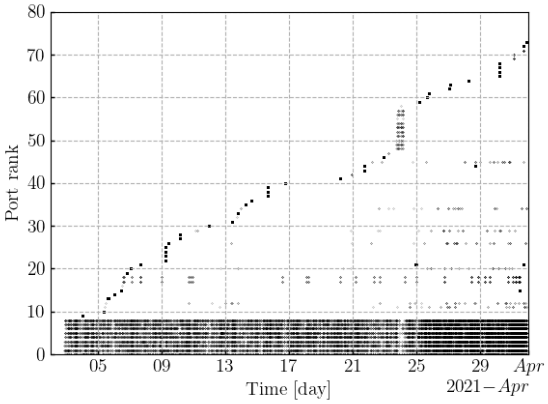
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 86: Cluster42 temporal patterns

44 Cluster 43. Silhouette: 0.94

28 distinct senders with the following ground truth classes:

- Unknown. 28 senders

342 packets sent in the last day. 0.0% of the last day traffic.

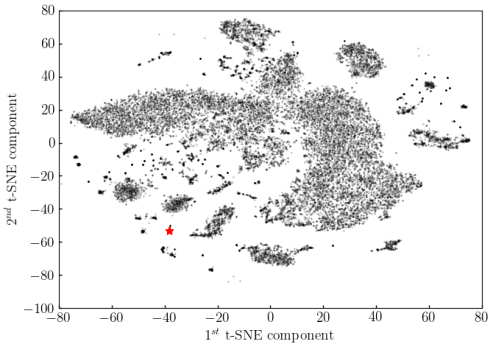


Figure 87: Cluster 43. t-SNE projection

18 distinct /24 subnets. The top-5 are:

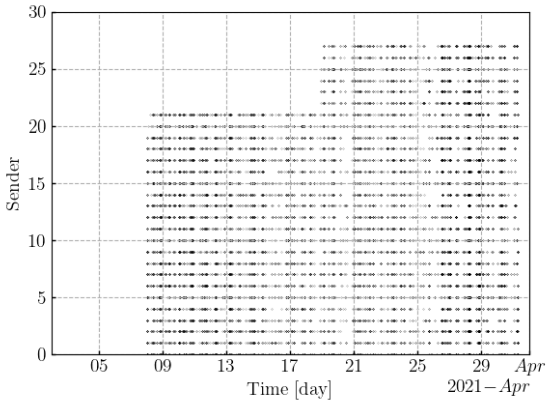
- 138.68.138.0 with 5 senders, 138.68.133.0 with 4 senders, 138.68.173.0 with 3 senders, 138.68.137.0 with 2 senders, 46.101.23.0 with 1 sender

5 distinct /16 subnets. The top-5 are:

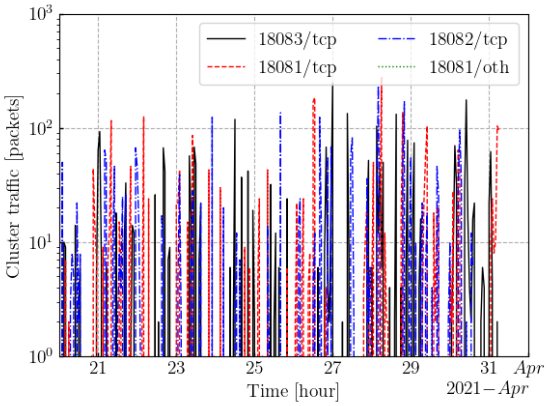
- 138.68.0.0 with 18 senders, 178.62.0.0 with 4 senders, 46.101.0.0 with 3 senders, 188.166.0.0 with 2 senders, 139.59.0.0 with 1 sender

5 ports contacted. The top-5 are:

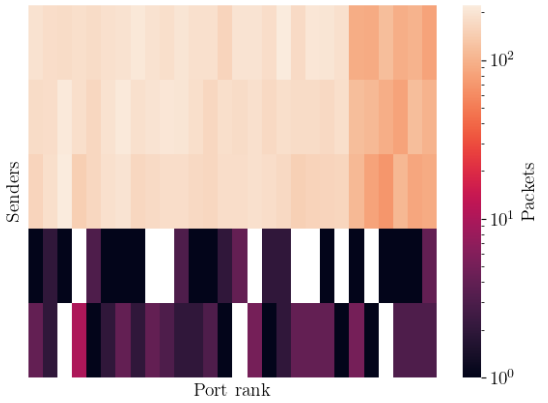
- 18083/tcp : 4753 sent packets (34.1 % of the monthly cluster traffic.) 28 senders contacted the port(100.0 % of the cluster senders.)
- 18081/tcp : 4710 sent packets (33.8 % of the monthly cluster traffic.) 28 senders contacted the port(100.0 % of the cluster senders.)
- 18082/tcp : 4366 sent packets (31.3 % of the monthly cluster traffic.) 28 senders contacted the port(100.0 % of the cluster senders.)
- 18081/oth : 76 sent packets (0.5 % of the monthly cluster traffic.) 25 senders contacted the port(89.3 % of the cluster senders.)
- 18082/oth : 34 sent packets (0.2 % of the monthly cluster traffic.) 20 senders contacted the port(71.4 % of the cluster senders.)



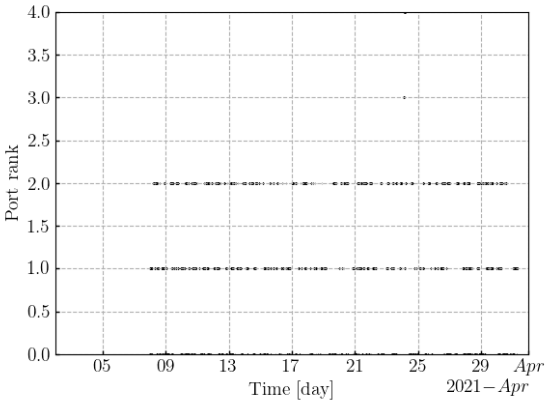
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 88: Cluster43 temporal patterns

45 Cluster 44. Silhouette: 0.688

119 distinct senders with the following ground truth classes:

- Binaryedge. 106 senders
- Unknown. 12 senders
- Stretchoid. 1 sender

11202 packets sent in the last day. 0.3% of the last day traffic.

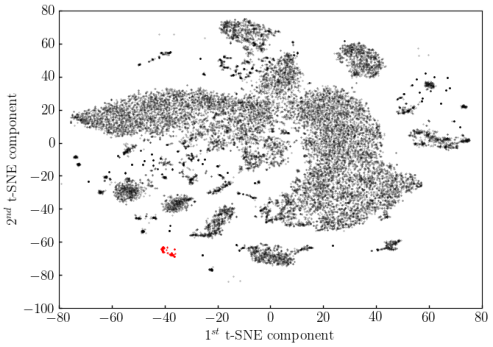


Figure 89: Cluster 44. t-SNE projection

110 distinct /24 subnets. The top-5 are:

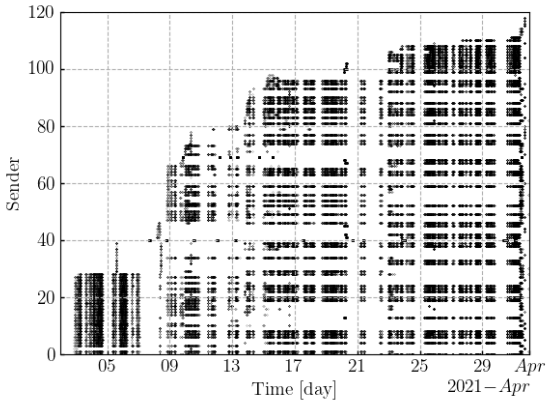
- 46.101.48.0 with 5 senders, 159.65.194.0 with 3 senders, 172.105.11.0 with 2 senders, 45.33.50.0 with 2 senders, 64.227.38.0 with 2 senders,

44 distinct /16 subnets. The top-5 are:

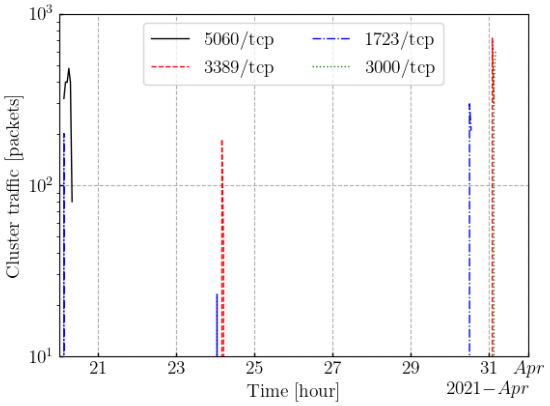
- 172.105.0.0 with 17 senders, 46.101.0.0 with 6 senders, 178.62.0.0 with 5 senders, 159.65.0.0 with 5 senders, 64.227.0.0 with 5 senders,

245 ports contacted. The top-5 are:

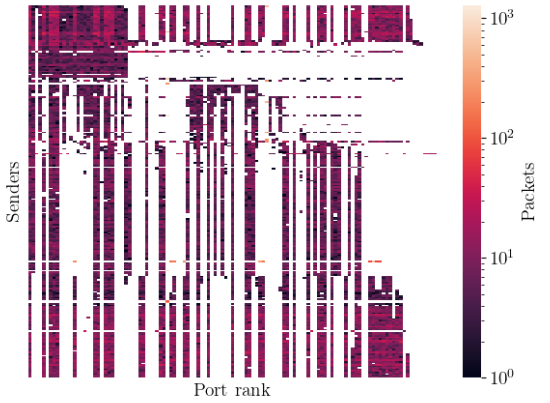
- 5060/tcp : 2076 sent packets (2.1 % of the monthly cluster traffic.) 10 senders contacted the port(8.4 % of the cluster senders.)
- 3389/tcp : 1519 sent packets (1.5 % of the monthly cluster traffic.) 69 senders contacted the port(58.0 % of the cluster senders.)
- 1723/tcp : 1485 sent packets (1.5 % of the monthly cluster traffic.) 39 senders contacted the port(32.8 % of the cluster senders.)
- 3000/tcp : 1305 sent packets (1.3 % of the monthly cluster traffic.) 67 senders contacted the port(56.3 % of the cluster senders.)
- 5222/tcp : 1282 sent packets (1.3 % of the monthly cluster traffic.) 66 senders contacted the port(55.5 % of the cluster senders.)



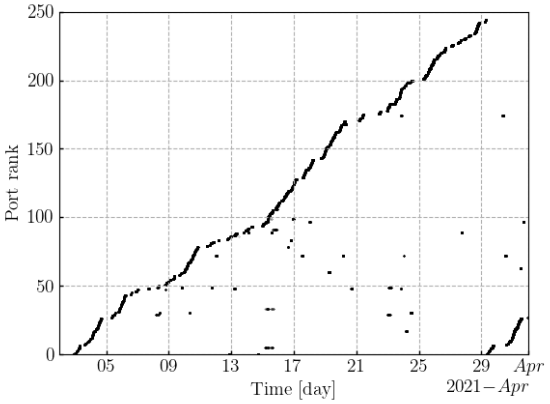
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 90: Cluster44 temporal patterns

46 Cluster 45. Silhouette: 0.292

1669 distinct senders with the following ground truth classes:

- Mirai-like. 1575 senders
- Unknown. 92 senders
- Stretchoid. 2 senders

16966 packets sent in the last day. 0.5% of the last day traffic. 84.9% of cluster traffic has the Mirai fingerprint.

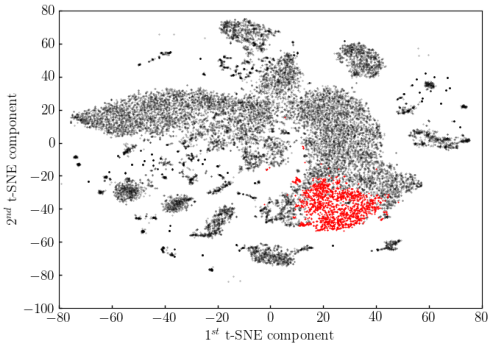


Figure 91: Cluster 45. t-SNE projection

1640 distinct /24 subnets. The top-5 are:

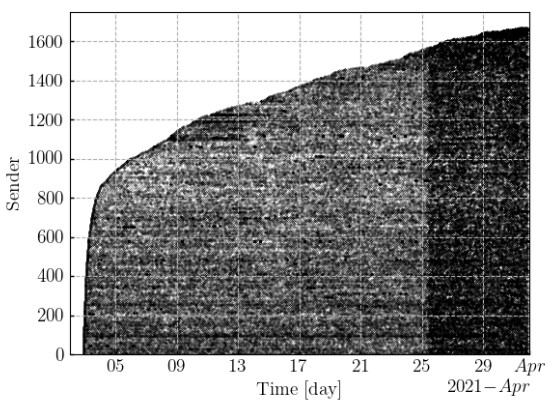
- 178.174.137.0 with 3 senders, 103.198.10.0 with 3 senders, 186.251.6.0 with 3 senders, 90.150.90.0 with 2 senders, 59.126.177.0 with 2 senders,

1223 distinct /16 subnets. The top-5 are:

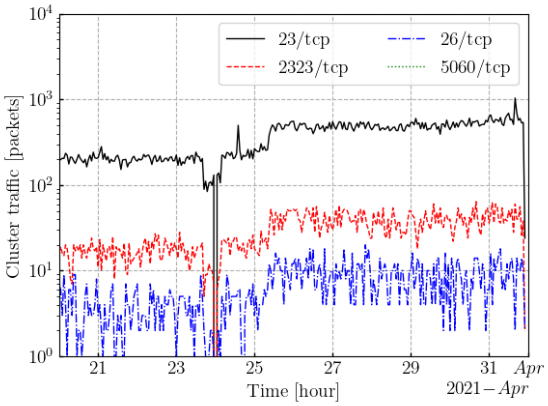
- 220.133.0.0 with 20 senders, 114.35.0.0 with 20 senders, 59.127.0.0 with 19 senders, 114.33.0.0 with 18 senders, 122.117.0.0 with 16 senders,

73 ports contacted. The top-5 are:

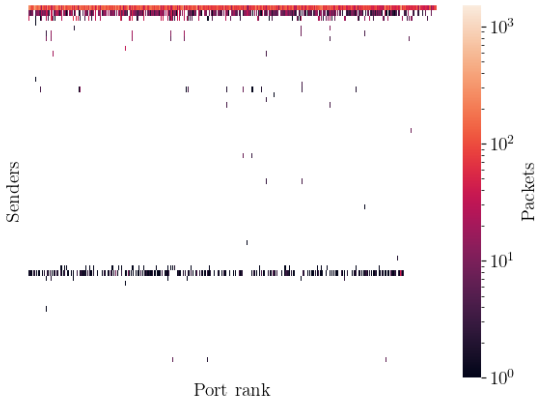
- 23/tcp : 173131 sent packets (84.8 % of the monthly cluster traffic.) 1666 senders contacted the port(99.8 % of the cluster senders.)
- 2323/tcp : 14466 sent packets (7.1 % of the monthly cluster traffic.) 1275 senders contacted the port(76.4 % of the cluster senders.)
- 26/tcp : 4313 sent packets (2.1 % of the monthly cluster traffic.) 278 senders contacted the port(16.7 % of the cluster senders.)
- 5060/tcp : 1518 sent packets (0.7 % of the monthly cluster traffic.) 1 senders contacted the port(0.1 % of the cluster senders.)
- 23/oth : 1340 sent packets (0.7 % of the monthly cluster traffic.) 761 senders contacted the port(45.6 % of the cluster senders.)



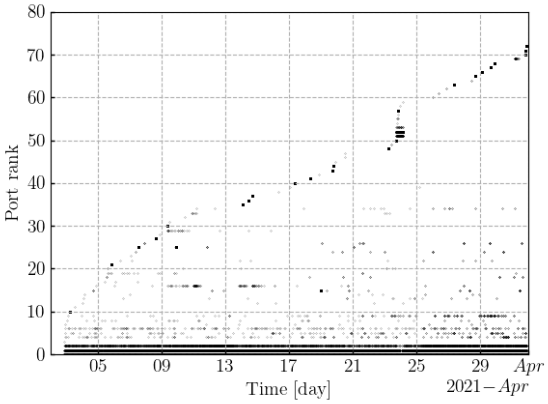
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 92: Cluster45 temporal patterns

47 Cluster 46. Silhouette: 0.783

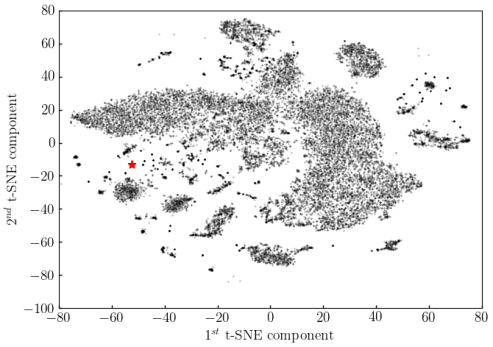


Figure 93: Cluster 46. t-SNE projection

22 distinct senders with the following ground truth classes:

- Unknown. 22 senders

1268 packets sent in the last day. 0.0% of the last day traffic.

18 distinct /24 subnets. The top-5 are:

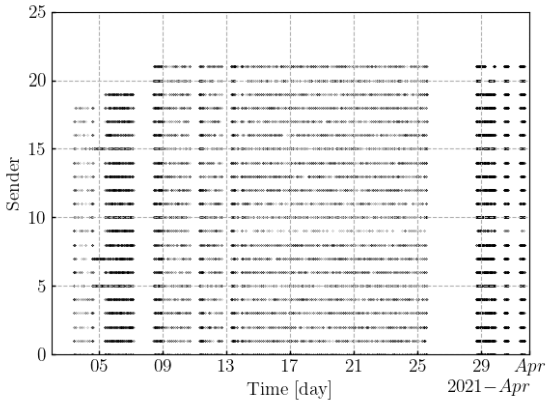
- 71.6.231.0 with 5 senders, 91.207.175.0 with 1 sender 185.94.188.0 with 1 sender 141.98.216.0 with 1 sender 172.107.94.0 with 1 sender

16 distinct /16 subnets. The top-5 are:

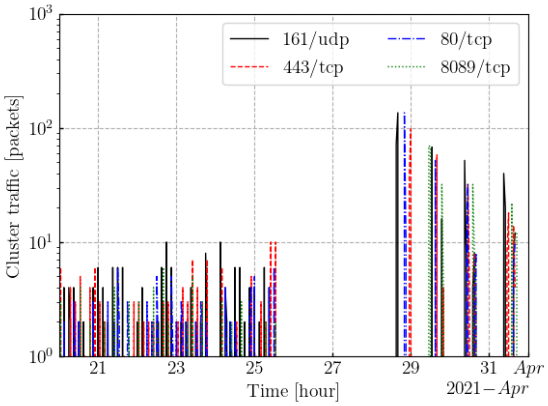
- 71.6.0.0 with 5 senders, 185.94.0.0 with 2 senders, 172.107.0.0 with 2 senders, 91.207.0.0 with 1 sender 91.196.0.0 with 1 sender

69 ports contacted. The top-5 are:

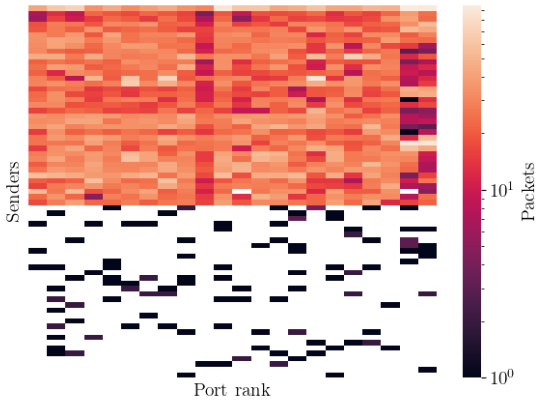
- 161/udp : 1154 sent packets (5.2 % of the monthly cluster traffic.) 22 senders contacted the port(100.0 % of the cluster senders.)
- 443/tcp : 788 sent packets (3.5 % of the monthly cluster traffic.) 22 senders contacted the port(100.0 % of the cluster senders.)
- 80/tcp : 765 sent packets (3.4 % of the monthly cluster traffic.) 22 senders contacted the port(100.0 % of the cluster senders.)
- 8089/tcp : 720 sent packets (3.2 % of the monthly cluster traffic.) 22 senders contacted the port(100.0 % of the cluster senders.)
- 8081/tcp : 715 sent packets (3.2 % of the monthly cluster traffic.) 22 senders contacted the port(100.0 % of the cluster senders.)



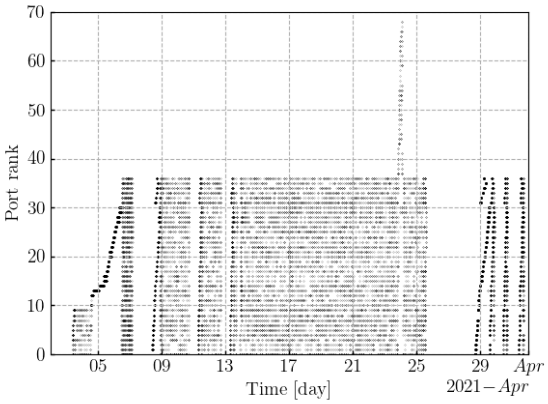
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 94: Cluster46 temporal patterns

48 Cluster 47. Silhouette: 0.34

12 distinct senders with the following ground truth classes:

- Unknown. 11 senders
- Ipip. 1 sender

1988 packets sent in the last day. 0.1% of the last day traffic.

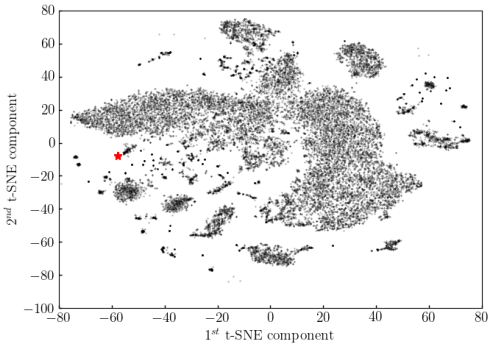


Figure 95: Cluster 47. t-SNE projection

12 distinct /24 subnets. The top-5 are:

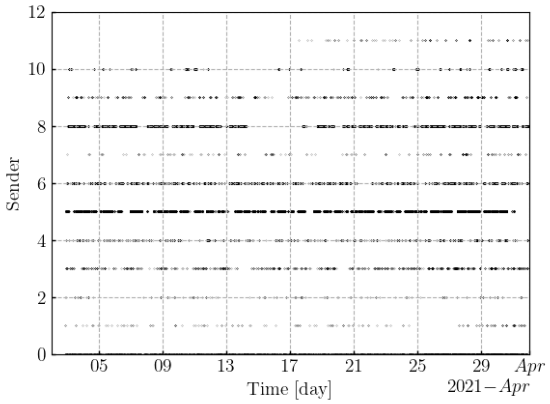
- 27.150.31.0 with 1 sender 222.93.39.0 with 1 sender 202.85.223.0 with 1 sender 182.151.46.0 with 1 sender 14.215.45.0 with 1 sender

12 distinct /16 subnets. The top-5 are:

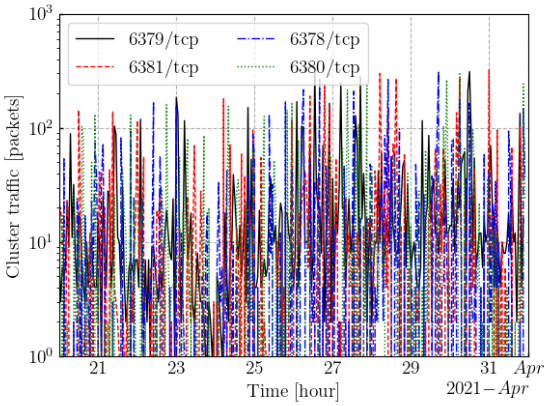
- 27.150.0.0 with 1 sender 222.93.0.0 with 1 sender 202.85.0.0 with 1 sender 182.151.0.0 with 1 sender 14.215.0.0 with 1 sender

8 ports contacted. The top-5 are:

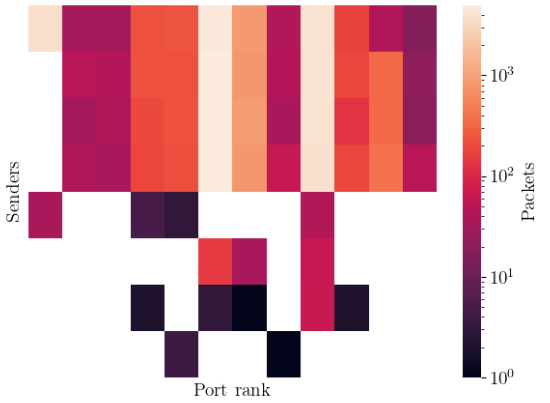
- 6379/tcp : 14104 sent packets (29.9 % of the monthly cluster traffic.) 12 senders contacted the port(100.0 % of the cluster senders.)
- 6381/tcp : 10963 sent packets (23.2 % of the monthly cluster traffic.) 11 senders contacted the port(91.7 % of the cluster senders.)
- 6378/tcp : 10875 sent packets (23.1 % of the monthly cluster traffic.) 11 senders contacted the port(91.7 % of the cluster senders.)
- 6380/tcp : 10807 sent packets (22.9 % of the monthly cluster traffic.) 11 senders contacted the port(91.7 % of the cluster senders.)
- 6381/oth : 252 sent packets (0.5 % of the monthly cluster traffic.) 3 senders contacted the port(25.0 % of the cluster senders.)



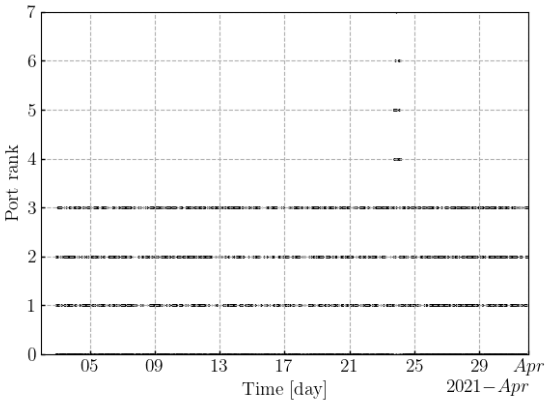
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 96: Cluster47 temporal patterns

49 Cluster 48. Silhouette: 0.935

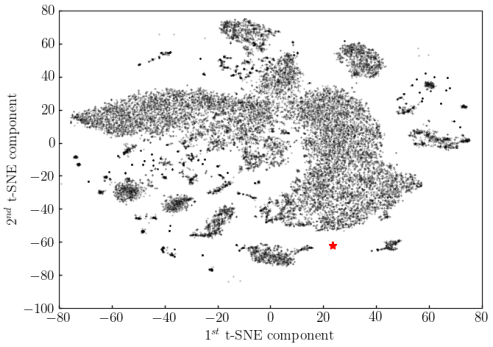


Figure 97: Cluster 48. t-SNE projection

16 distinct senders with the following ground truth classes:

- Censys. 16 senders

532 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

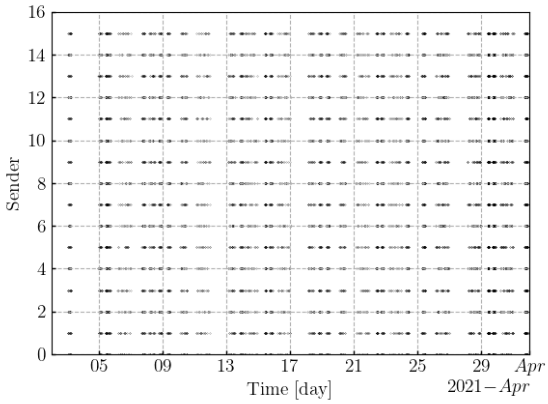
- 192.35.168.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

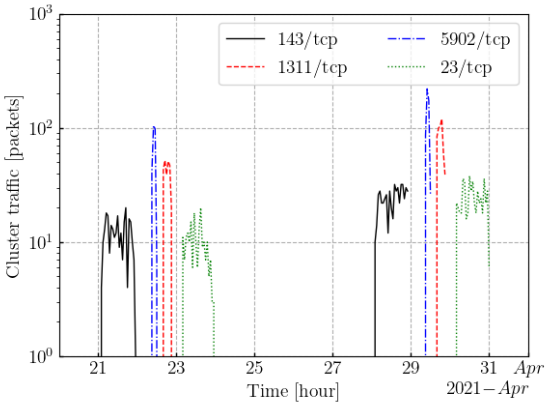
- 192.35.0.0 with 16 senders,

26 ports contacted. The top-5 are:

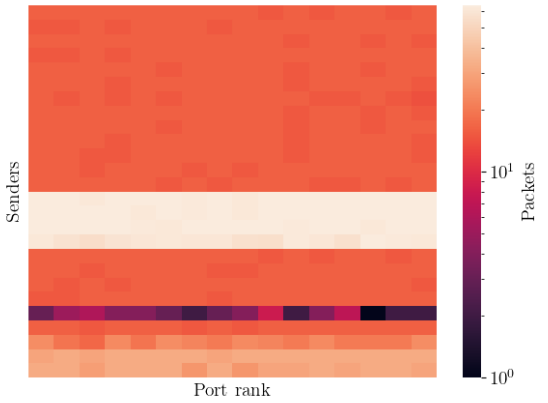
- 143/tcp : 1012 sent packets (10.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 1311/tcp : 1011 sent packets (10.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 5902/tcp : 1010 sent packets (10.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 23/tcp : 952 sent packets (9.6 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 8080/tcp : 506 sent packets (5.1 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



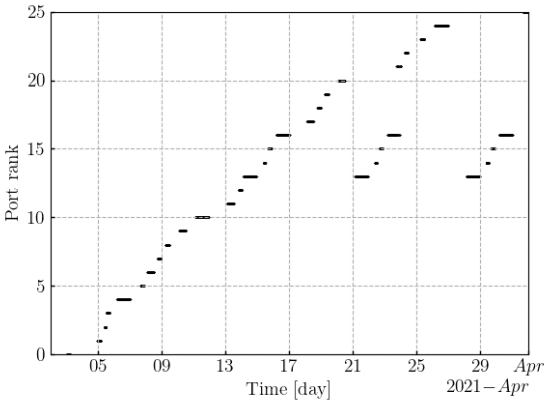
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 98: Cluster48 temporal patterns

50 Cluster 49. Silhouette: 0.489

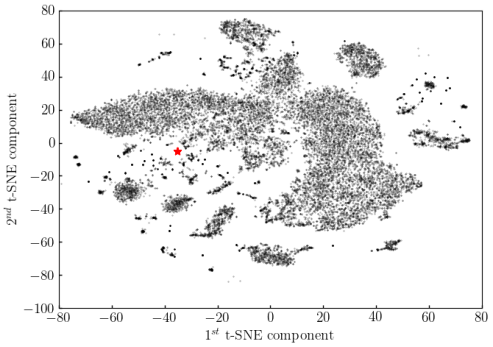


Figure 99: Cluster 49. t-SNE projection

13 distinct senders with the following ground truth classes:

- Binaryedge. 13 senders

88 packets sent in the last day. 0.0% of the last day traffic.

13 distinct /24 subnets. The top-5 are:

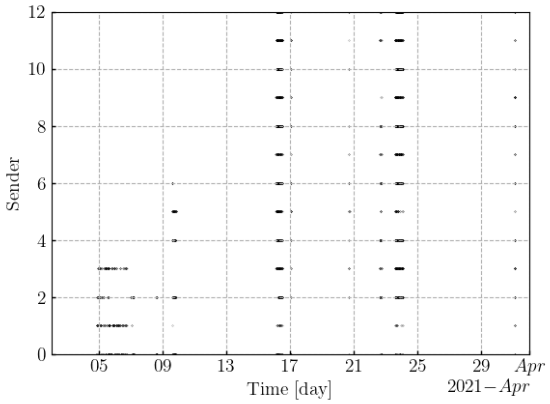
- 67.207.95.0 with 1 sender 67.205.187.0 with 1 sender 46.101.3.0 with 1 sender 46.101.17.0 with 1 sender 198.199.83.0 with 1 sender

11 distinct /16 subnets. The top-5 are:

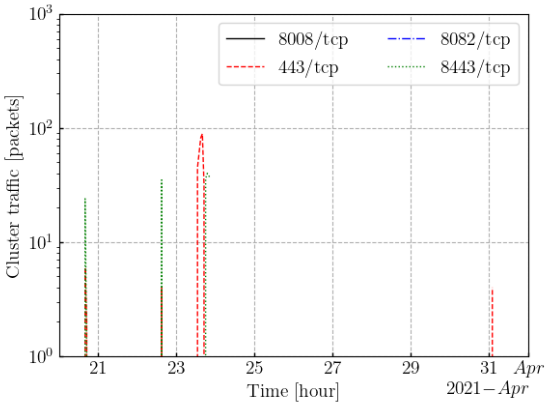
- 46.101.0.0 with 2 senders, 172.105.0.0 with 2 senders, 67.207.0.0 with 1 sender 67.205.0.0 with 1 sender 198.199.0.0 with 1 sender

17 ports contacted. The top-5 are:

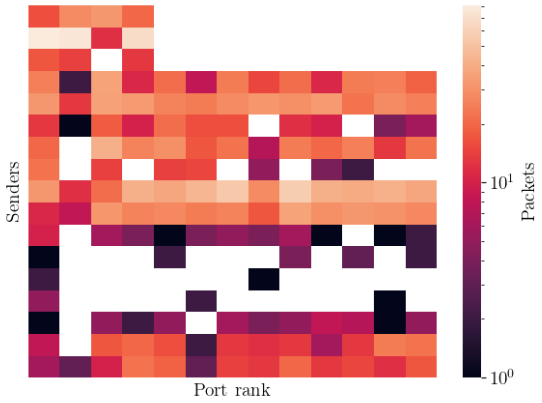
- 8008/tcp : 485 sent packets (17.9 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)
- 443/tcp : 359 sent packets (13.3 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)
- 8082/tcp : 324 sent packets (12.0 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)
- 8443/tcp : 266 sent packets (9.8 % of the monthly cluster traffic.) 12 senders contacted the port(92.3 % of the cluster senders.)
- 80/tcp : 242 sent packets (8.9 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)



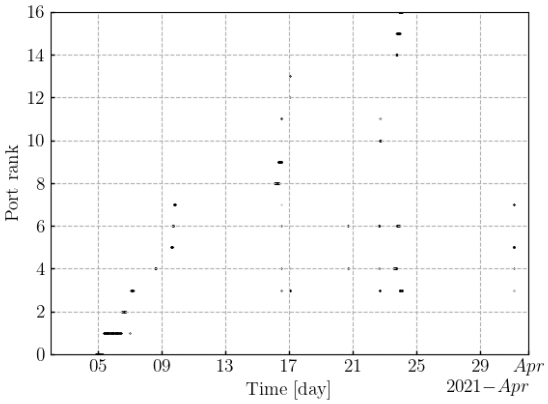
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 100: Cluster49 temporal patterns

51 Cluster 50. Silhouette: 0.772

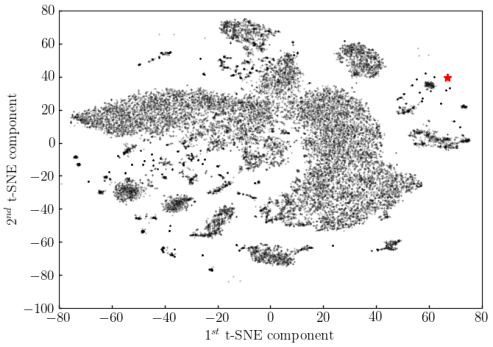


Figure 101: Cluster 50. t-SNE projection

18 distinct senders with the following ground truth classes:

- Shadowserver. 15 senders
- Unknown. 3 senders

2246 packets sent in the last day. 0.1% of the last day traffic.

4 distinct /24 subnets. The top-5 are:

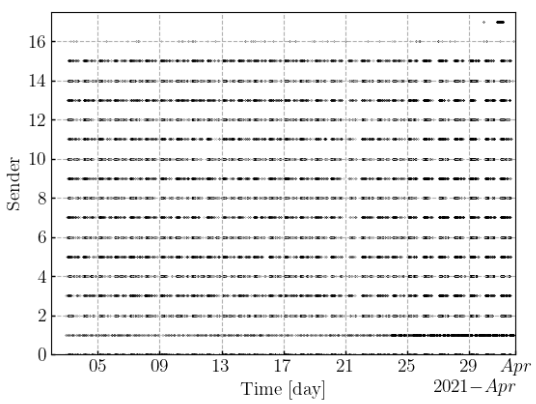
- 74.82.47.0 with 15 senders, 79.181.121.0 with 1 sender 31.210.20.0 with 1 sender 164.52.24.0 with 1 sender

4 distinct /16 subnets. The top-5 are:

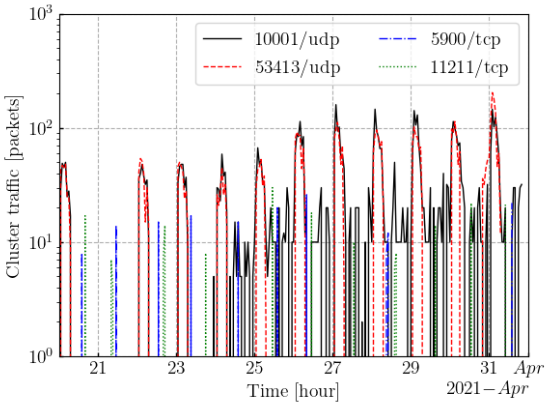
- 74.82.0.0 with 15 senders, 79.181.0.0 with 1 sender 31.210.0.0 with 1 sender 164.52.0.0 with 1 sender

46 ports contacted. The top-5 are:

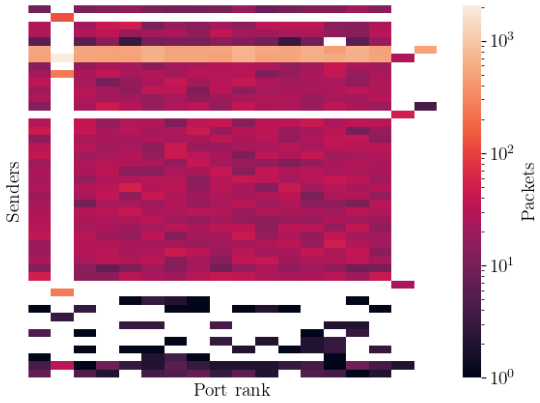
- 10001/udp : 10311 sent packets (33.1 % of the monthly cluster traffic.) 17 senders contacted the port(94.4 % of the cluster senders.)
- 53413/udp : 8753 sent packets (28.1 % of the monthly cluster traffic.) 16 senders contacted the port(88.9 % of the cluster senders.)
- 5900/tcp : 640 sent packets (2.1 % of the monthly cluster traffic.) 16 senders contacted the port(88.9 % of the cluster senders.)
- 11211/tcp : 447 sent packets (1.4 % of the monthly cluster traffic.) 15 senders contacted the port(83.3 % of the cluster senders.)
- 449/tcp : 445 sent packets (1.4 % of the monthly cluster traffic.) 15 senders contacted the port(83.3 % of the cluster senders.)



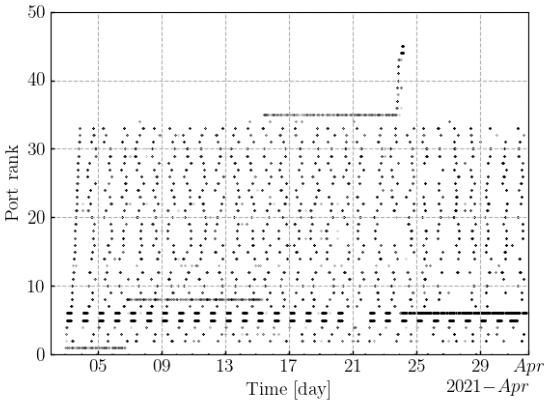
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 102: Cluster50 temporal patterns

52 Cluster 51. Silhouette: 0.464

8 distinct senders with the following ground truth classes:

- Unknown. 8 senders

878 packets sent in the last day. 0.0% of the last day traffic.

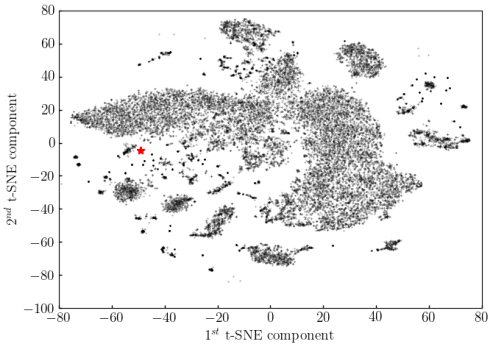


Figure 103: Cluster 51. t-SNE projection

8 distinct /24 subnets. The top-5 are:

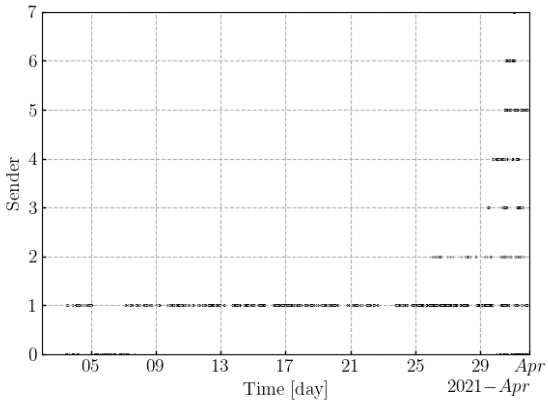
- 91.232.135.0 with 1 sender 75.49.159.0 with 1 sender 54.36.34.0 with 1 sender 203.232.194.0 with 1 sender 188.166.114.0 with 1 sender

8 distinct /16 subnets. The top-5 are:

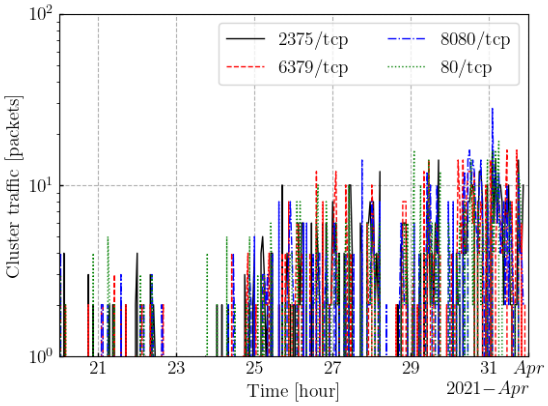
- 91.232.0.0 with 1 sender 75.49.0.0 with 1 sender 54.36.0.0 with 1 sender 203.232.0.0 with 1 sender 188.166.0.0 with 1 sender

11 ports contacted. The top-5 are:

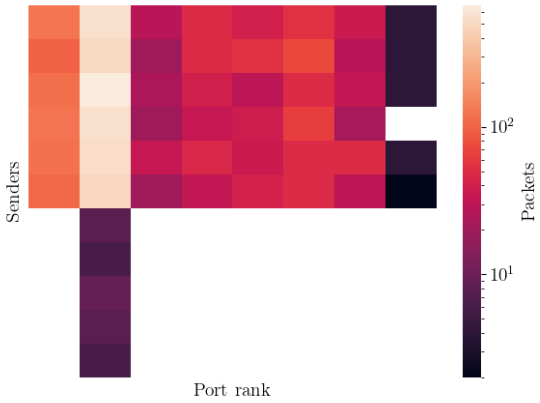
- 2375/tcp : 958 sent packets (18.3 % of the monthly cluster traffic.) 8 senders contacted the port(100.0 % of the cluster senders.)
- 6379/tcp : 899 sent packets (17.2 % of the monthly cluster traffic.) 8 senders contacted the port(100.0 % of the cluster senders.)
- 8080/tcp : 877 sent packets (16.8 % of the monthly cluster traffic.) 8 senders contacted the port(100.0 % of the cluster senders.)
- 80/tcp : 861 sent packets (16.5 % of the monthly cluster traffic.) 7 senders contacted the port(87.5 % of the cluster senders.)
- 6380/tcp : 826 sent packets (15.8 % of the monthly cluster traffic.) 8 senders contacted the port(100.0 % of the cluster senders.)



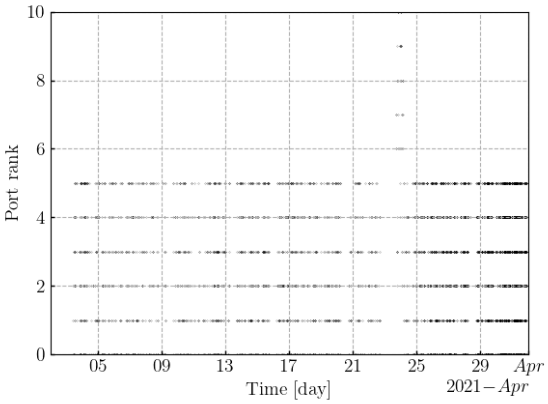
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 104: Cluster51 temporal patterns

53 Cluster 52. Silhouette: 0.904

16 distinct senders with the following ground truth classes:

- Censys. 16 senders

506 packets sent in the last day. 0.0% of the last day traffic.

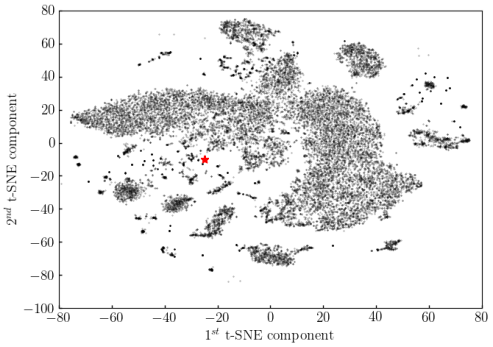


Figure 105: Cluster 52. t-SNE projection

1 distinct /24 subnets. The top-5 are:

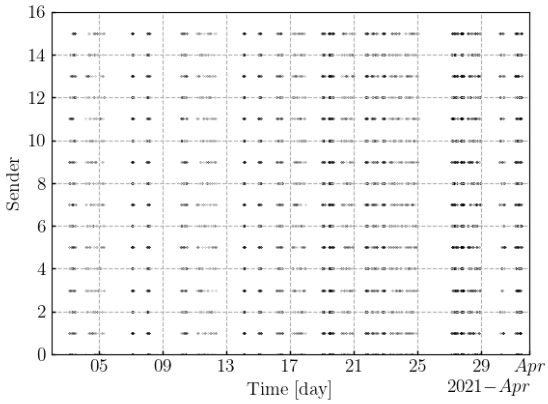
- 192.35.168.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

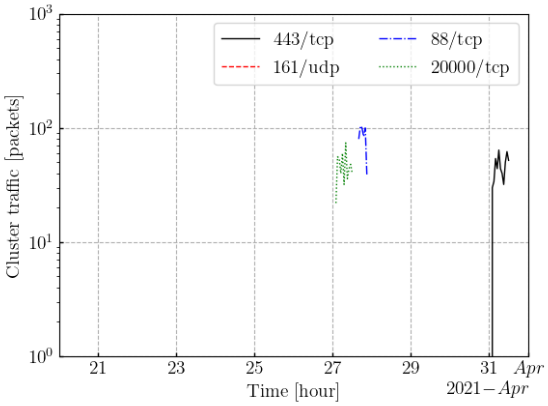
- 192.35.0.0 with 16 senders,

20 ports contacted. The top-5 are:

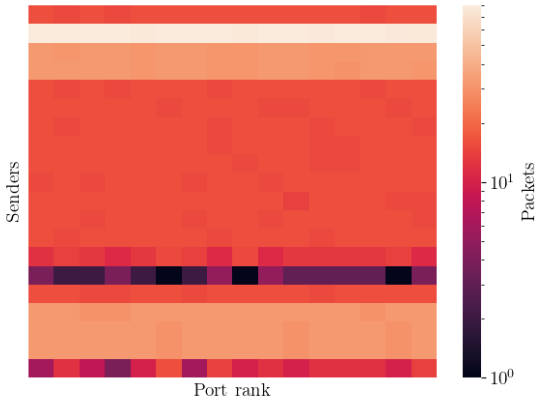
- 443/tcp : 1264 sent packets (18.1 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 161/udp : 506 sent packets (7.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 88/tcp : 506 sent packets (7.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 20000/tcp : 506 sent packets (7.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 53/udp : 506 sent packets (7.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



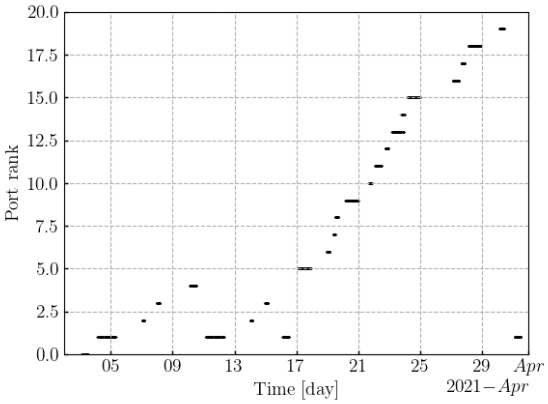
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 106: Cluster52 temporal patterns

54 Cluster 53. Silhouette: 0.944

14 distinct senders with the following ground truth classes:

- Unknown. 14 senders

5266 packets sent in the last day. 0.2% of the last day traffic.

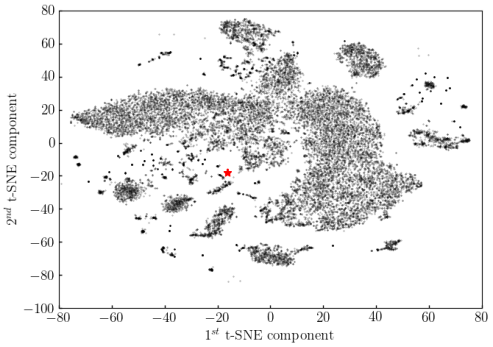


Figure 107: Cluster 53. t-SNE projection

14 distinct /24 subnets. The top-5 are:

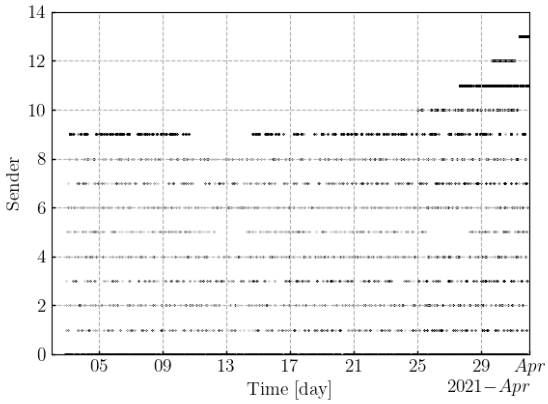
- 47.107.35.0 with 1 sender 47.101.217.0 with 1 sender 45.33.111.0 with 1 sender 39.105.54.0 with 1 sender 172.105.173.0 with 1 sender

14 distinct /16 subnets. The top-5 are:

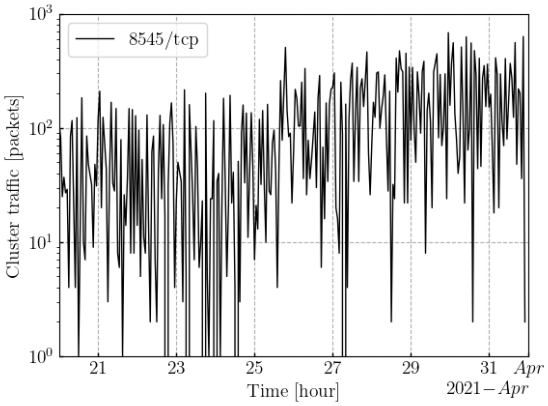
- 47.107.0.0 with 1 sender 47.101.0.0 with 1 sender 45.33.0.0 with 1 sender 39.105.0.0 with 1 sender 172.105.0.0 with 1 sender

2 ports contacted. The top-5 are:

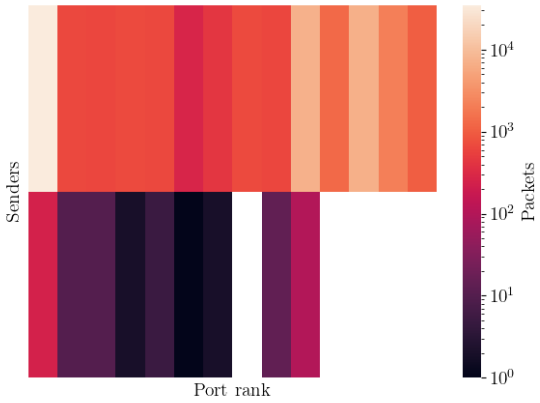
- 8545/tcp : 58210 sent packets (99.3 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 8545/oth : 386 sent packets (0.7 % of the monthly cluster traffic.) 9 senders contacted the port(64.3 % of the cluster senders.)



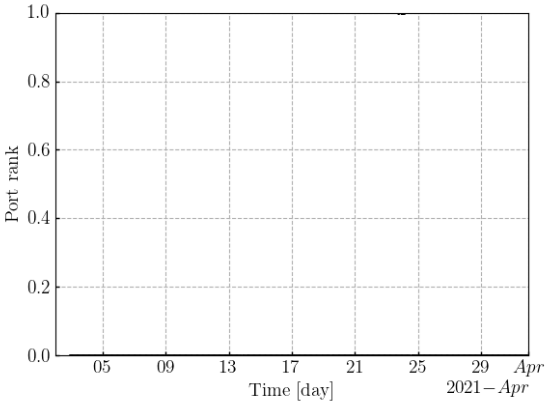
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 108: Cluster53 temporal patterns

55 Cluster 54. Silhouette: -0.097

234 distinct senders with the following ground truth classes:

- Unknown. 215 senders
- Mirai-like. 19 senders

54120 packets sent in the last day. 1.6% of the last day traffic. 0.1% of cluster traffic has the Mirai fingerprint.

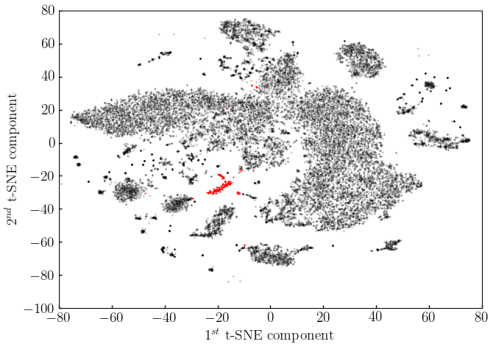


Figure 109: Cluster 54. t-SNE projection

209 distinct /24 subnets. The top-5 are:

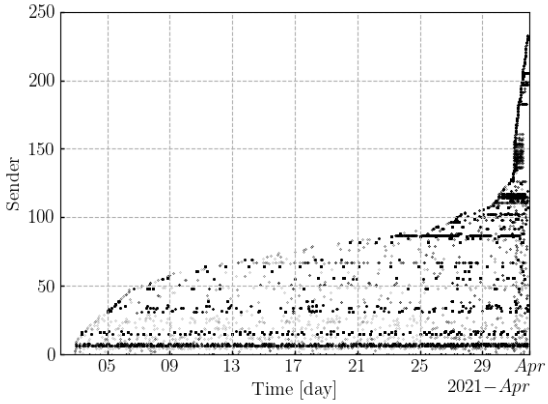
- 34.96.130.0 with 19 senders, 202.164.139.0 with 4 senders, 54.39.194.0 with 4 senders, 202.164.138.0 with 2 senders, 98.42.139.0 with 1 sender

198 distinct /16 subnets. The top-5 are:

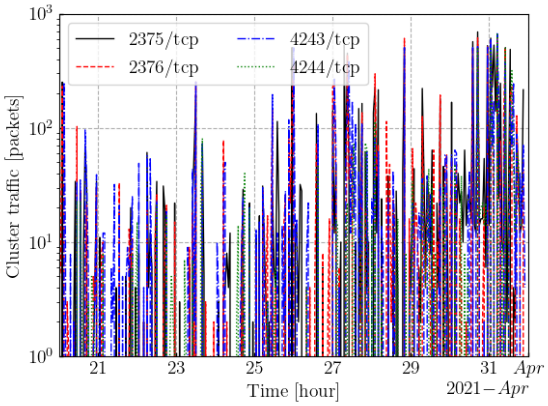
- 34.96.0.0 with 19 senders, 202.164.0.0 with 6 senders, 54.39.0.0 with 4 senders, 119.45.0.0 with 4 senders, 103.253.0.0 with 2 senders,

862 ports contacted. The top-5 are:

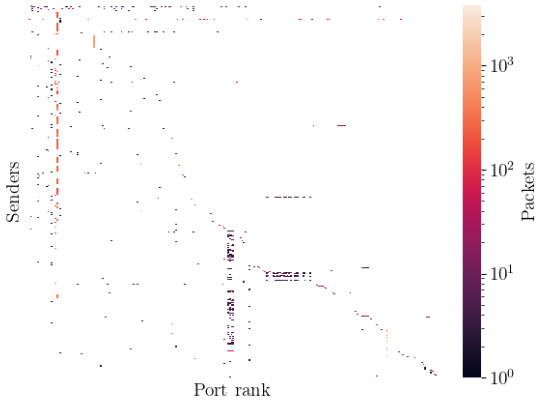
- 2375/tcp : 15977 sent packets (8.6 % of the monthly cluster traffic.) 38 senders contacted the port(16.2 % of the cluster senders.)
- 2376/tcp : 14022 sent packets (7.5 % of the monthly cluster traffic.) 36 senders contacted the port(15.4 % of the cluster senders.)
- 4243/tcp : 13609 sent packets (7.3 % of the monthly cluster traffic.) 36 senders contacted the port(15.4 % of the cluster senders.)
- 4244/tcp : 5143 sent packets (2.8 % of the monthly cluster traffic.) 23 senders contacted the port(9.8 % of the cluster senders.)
- 2377/tcp : 4868 sent packets (2.6 % of the monthly cluster traffic.) 21 senders contacted the port(9.0 % of the cluster senders.)



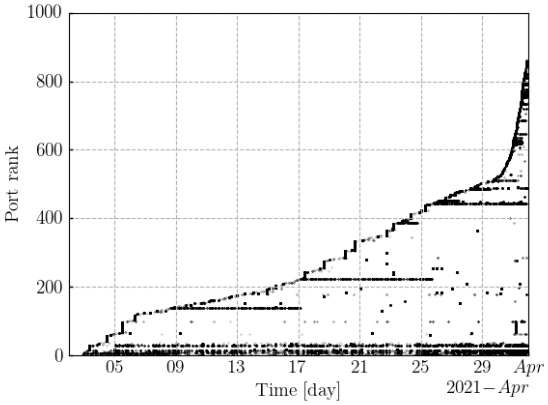
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 110: Cluster54 temporal patterns

56 Cluster 55. Silhouette: 0.909

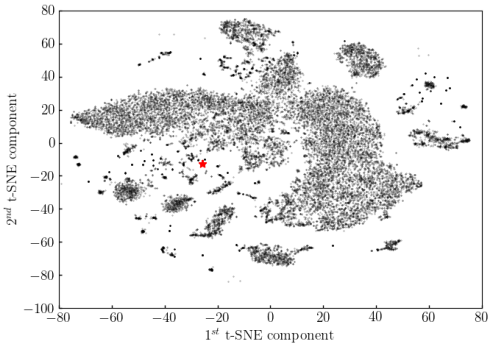


Figure 111: Cluster 55. t-SNE projection

16 distinct senders with the following ground truth classes:

- Censys. 16 senders

460 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

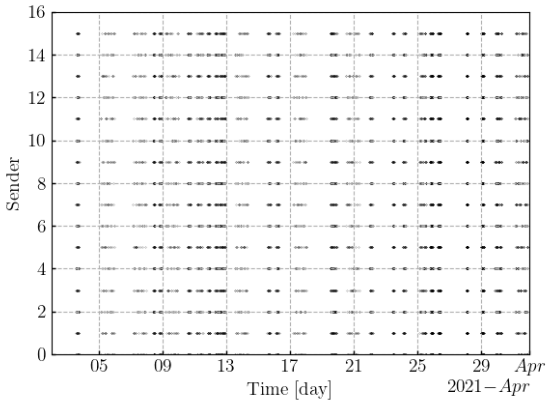
- 192.35.168.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

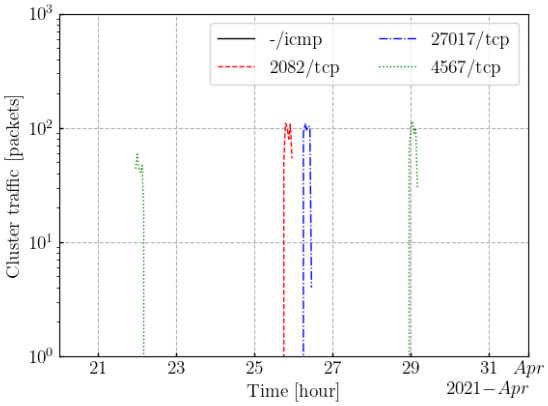
- 192.35.0.0 with 16 senders,

21 ports contacted. The top-5 are:

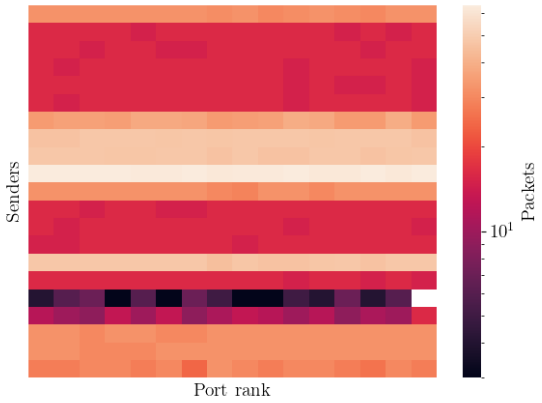
- -/icmp : 1012 sent packets (11.4 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 2082/tcp : 759 sent packets (8.6 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 27017/tcp : 757 sent packets (8.5 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 4567/tcp : 757 sent packets (8.5 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 443/tcp : 577 sent packets (6.5 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



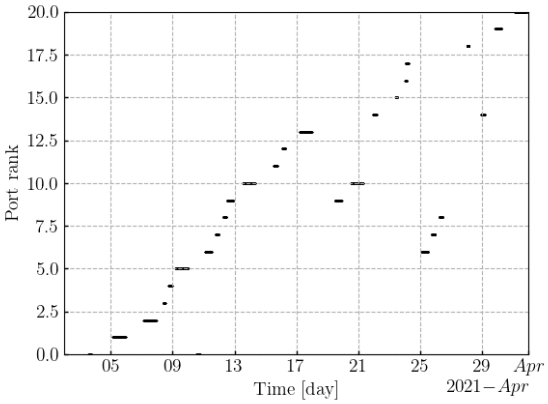
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 112: Cluster55 temporal patterns

57 Cluster 56. Silhouette: 0.843

4 distinct senders with the following ground truth classes:

- Unknown. 4 senders

556 packets sent in the last day. 0.0% of the last day traffic.

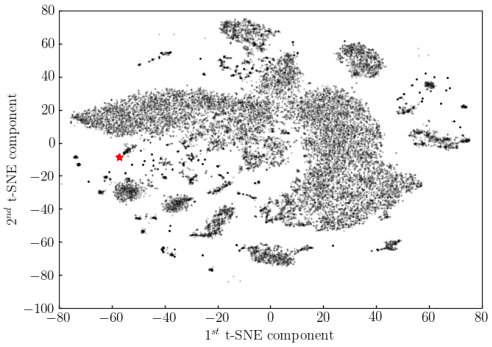


Figure 113: Cluster 56. t-SNE projection

4 distinct /24 subnets. The top-5 are:

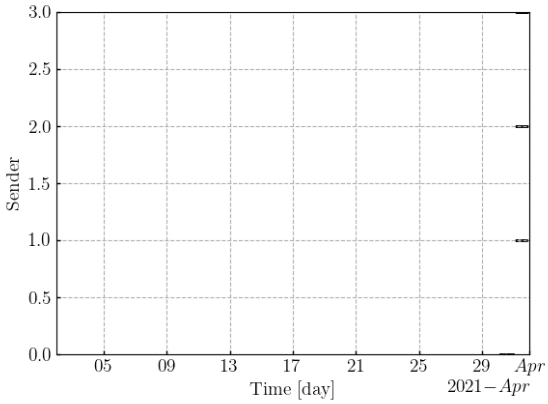
- 165.232.138.0 with 1 sender 159.65.138.0 with 1 sender 139.59.171.0 with 1 sender 138.197.210.0 with 1 sender

4 distinct /16 subnets. The top-5 are:

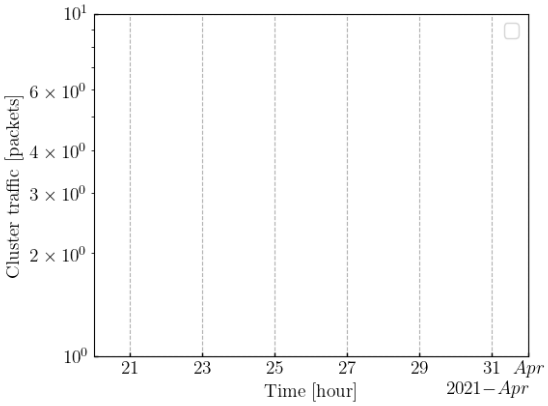
- 165.232.0.0 with 1 sender 159.65.0.0 with 1 sender 139.59.0.0 with 1 sender 138.197.0.0 with 1 sender

1 ports contacted. The top-5 are:

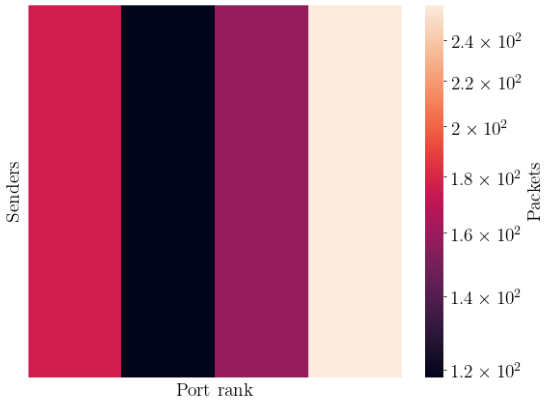
- 6379/tcp : 710 sent packets (100.0 % of the monthly cluster traffic.) 4 senders contacted the port(100.0 % of the cluster senders.)



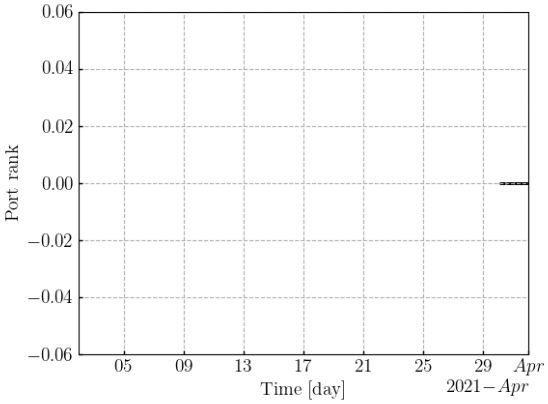
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 114: Cluster56 temporal patterns

58 Cluster 57. Silhouette: 0.492

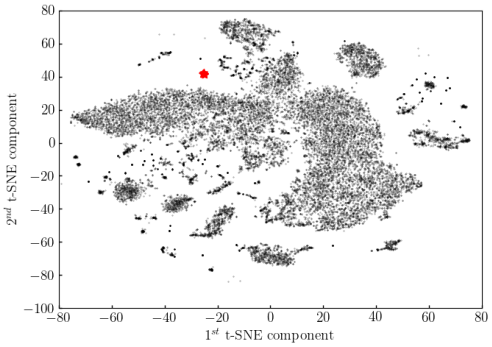


Figure 115: Cluster 57. t-SNE projection

24 distinct senders with the following ground truth classes:

- Unknown. 24 senders

31162 packets sent in the last day. 0.9% of the last day traffic.

20 distinct /24 subnets. The top-5 are:

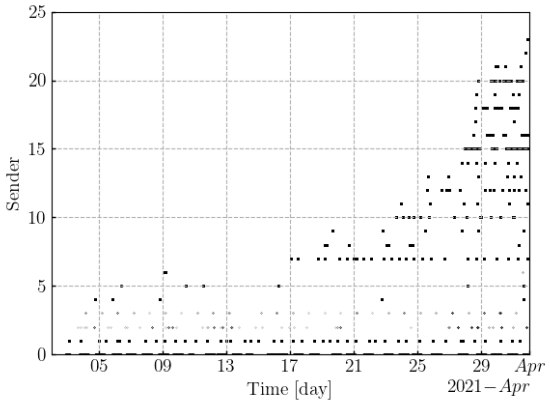
- 45.134.144.0 with 4 senders, 193.107.216.0 with 2 senders, 92.204.135.0 with 1 sender 193.46.255.0 with 1 sender 109.65.121.0 with 1 sender

19 distinct /16 subnets. The top-5 are:

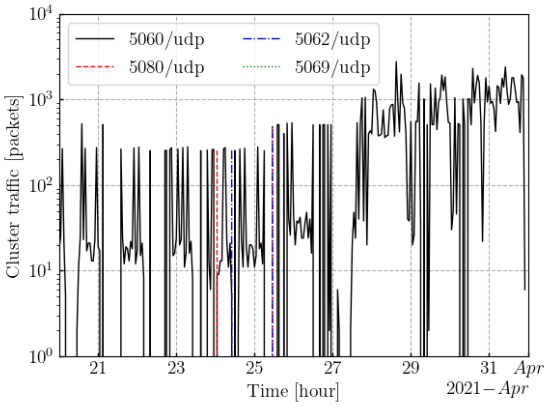
- 45.134.0.0 with 4 senders, 193.107.0.0 with 2 senders, 51.15.0.0 with 2 senders, 92.204.0.0 with 1 sender 109.65.0.0 with 1 sender

53 ports contacted. The top-5 are:

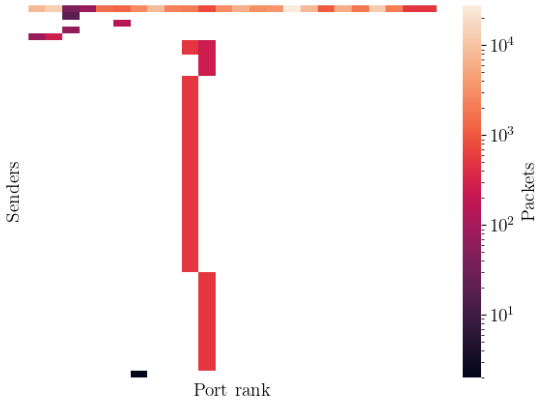
- 5060/udp : 117940 sent packets (83.0 % of the monthly cluster traffic.) 24 senders contacted the port(100.0 % of the cluster senders.)
- 5080/udp : 759 sent packets (0.5 % of the monthly cluster traffic.) 2 senders contacted the port(8.3 % of the cluster senders.)
- 5062/udp : 759 sent packets (0.5 % of the monthly cluster traffic.) 2 senders contacted the port(8.3 % of the cluster senders.)
- 5069/udp : 506 sent packets (0.4 % of the monthly cluster traffic.) 1 senders contacted the port(4.2 % of the cluster senders.)
- 8032/udp : 506 sent packets (0.4 % of the monthly cluster traffic.) 1 senders contacted the port(4.2 % of the cluster senders.)



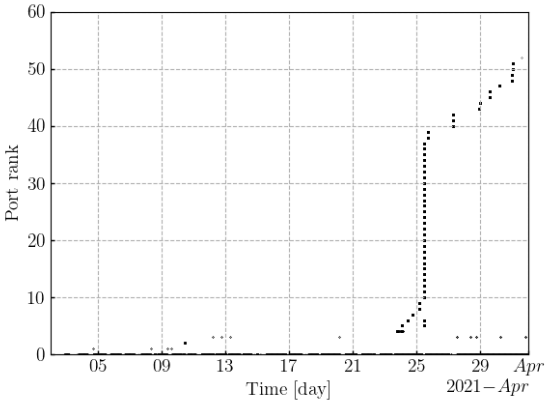
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 116: Cluster57 temporal patterns

59 Cluster 58. Silhouette: 0.227

182 distinct senders with the following ground truth classes:

- Unknown. 178 senders
- Mirai-like. 4 senders

116930 packets sent in the last day. 3.4% of the last day traffic. 0.0% of cluster traffic has the Mirai fingerprint.

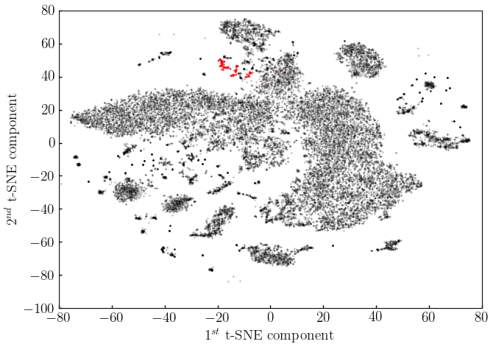


Figure 117: Cluster 58. t-SNE projection

182 distinct /24 subnets. The top-5 are:

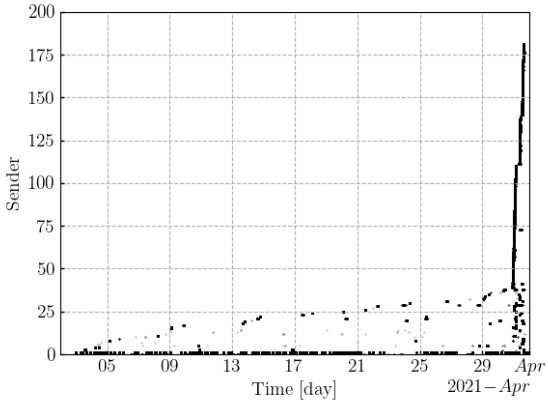
- 95.179.127.0 with 1 sender 164.155.88.0 with 1 sender 153.212.215.0 with 1 sender 153.187.165.0 with 1 sender 148.102.25.0 with 1 sender

175 distinct /16 subnets. The top-5 are:

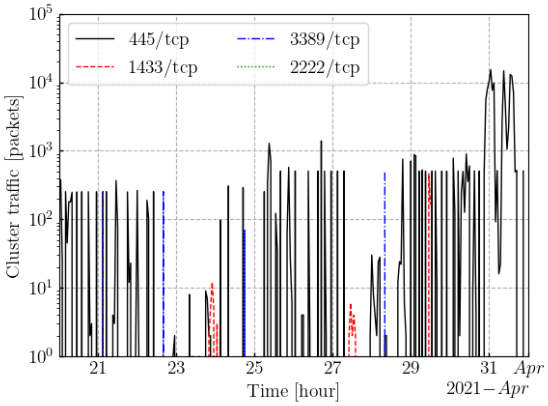
- 130.204.0.0 with 3 senders, 130.164.0.0 with 3 senders, 36.78.0.0 with 2 senders, 103.97.0.0 with 2 senders, 197.50.0.0 with 2 senders,

24 ports contacted. The top-5 are:

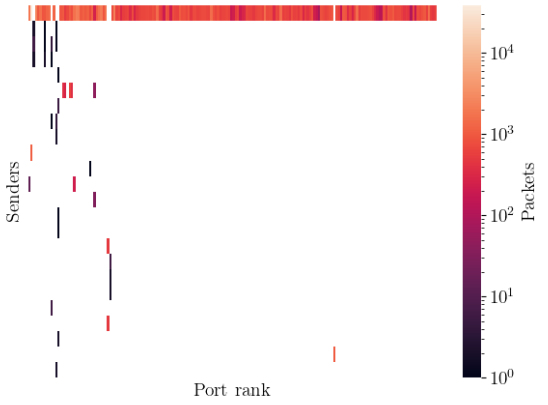
- 445/tcp : 169219 sent packets (97.0 % of the monthly cluster traffic.) 175 senders contacted the port(96.2 % of the cluster senders.)
- 1433/tcp : 1731 sent packets (1.0 % of the monthly cluster traffic.) 5 senders contacted the port(2.7 % of the cluster senders.)
- 3389/tcp : 1081 sent packets (0.6 % of the monthly cluster traffic.) 1 senders contacted the port(0.5 % of the cluster senders.)
- 2222/tcp : 1012 sent packets (0.6 % of the monthly cluster traffic.) 1 senders contacted the port(0.5 % of the cluster senders.)
- 30443/tcp : 506 sent packets (0.3 % of the monthly cluster traffic.) 1 senders contacted the port(0.5 % of the cluster senders.)



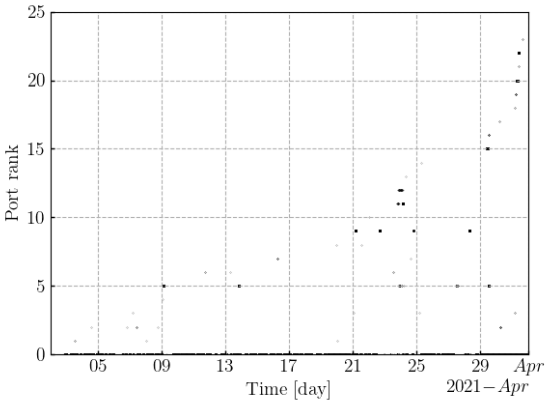
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 118: Cluster58 temporal patterns

60 Cluster 59. Silhouette: 0.555

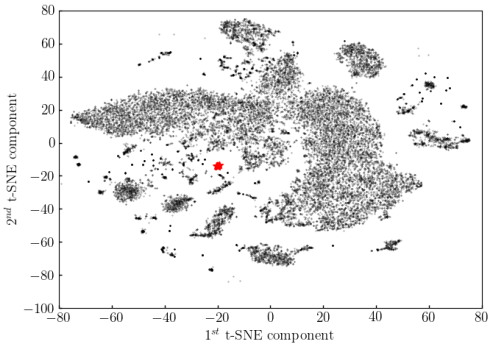


Figure 119: Cluster 59. t-SNE projection

29 distinct senders with the following ground truth classes:

- Unknown. 29 senders

9314 packets sent in the last day. 0.3% of the last day traffic.

28 distinct /24 subnets. The top-5 are:

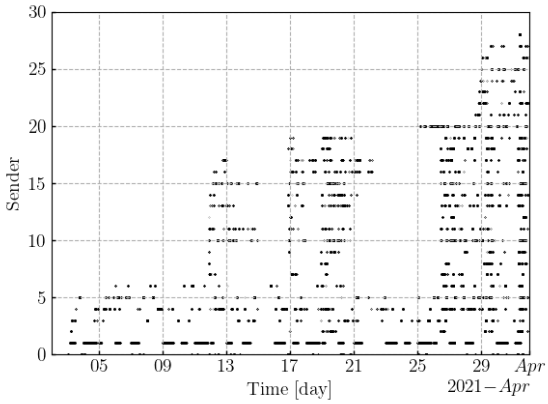
- 218.17.208.0 with 2 senders, 91.236.177.0 with 1 sender 173.249.51.0 with 1 sender 117.119.83.0 with 1 sender 138.197.122.0 with 1 sender

24 distinct /16 subnets. The top-5 are:

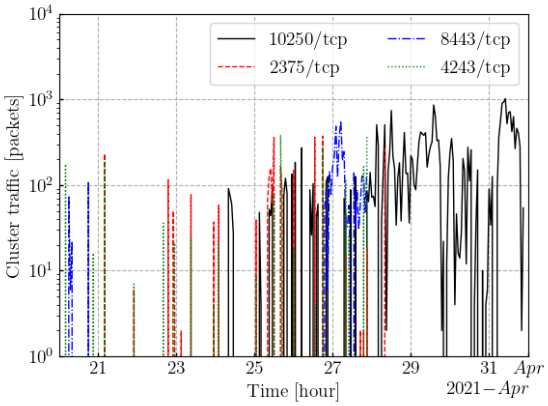
- 138.197.0.0 with 2 senders, 138.68.0.0 with 2 senders, 218.17.0.0 with 2 senders, 188.166.0.0 with 2 senders, 167.71.0.0 with 2 senders,

24 ports contacted. The top-5 are:

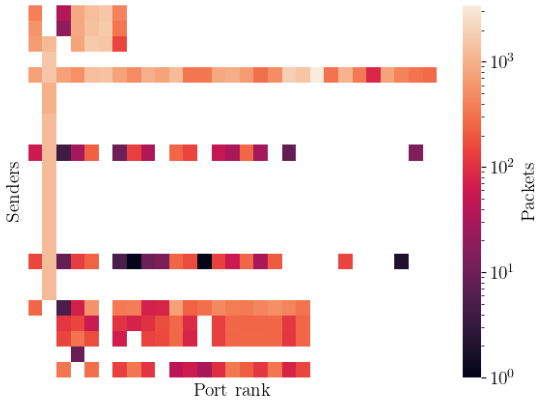
- 10250/tcp : 24601 sent packets (32.5 % of the monthly cluster traffic.) 29 senders contacted the port(100.0 % of the cluster senders.)
- 2375/tcp : 5935 sent packets (7.8 % of the monthly cluster traffic.) 6 senders contacted the port(20.7 % of the cluster senders.)
- 8443/tcp : 5869 sent packets (7.8 % of the monthly cluster traffic.) 18 senders contacted the port(62.1 % of the cluster senders.)
- 4243/tcp : 4868 sent packets (6.4 % of the monthly cluster traffic.) 6 senders contacted the port(20.7 % of the cluster senders.)
- 2376/tcp : 4523 sent packets (6.0 % of the monthly cluster traffic.) 6 senders contacted the port(20.7 % of the cluster senders.)



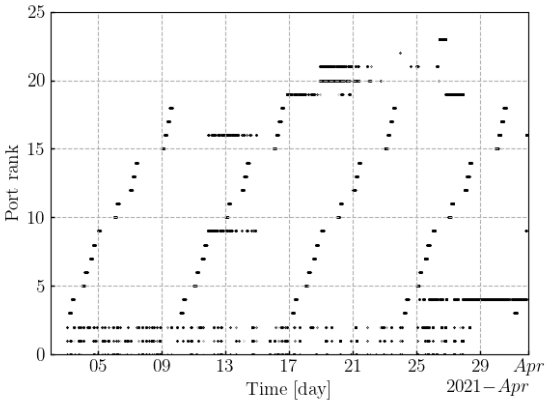
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 120: Cluster59 temporal patterns

61 Cluster 60. Silhouette: 0.929

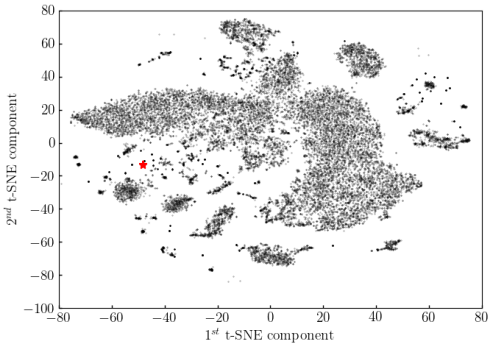


Figure 121: Cluster 60. t-SNE projection

16 distinct senders with the following ground truth classes:

- Censys. 16 senders

1074 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

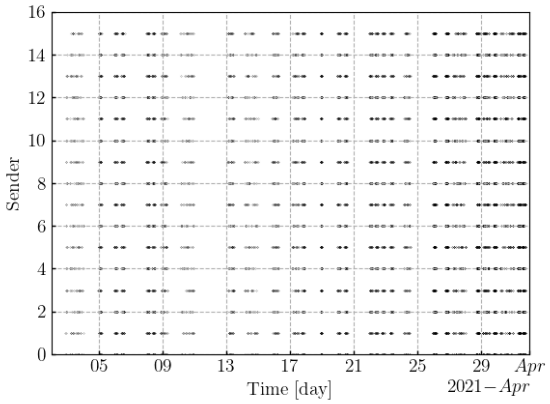
- 192.35.168.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

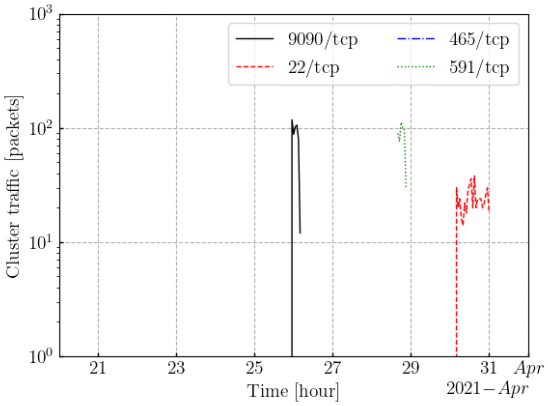
- 192.35.0.0 with 16 senders,

26 ports contacted. The top-5 are:

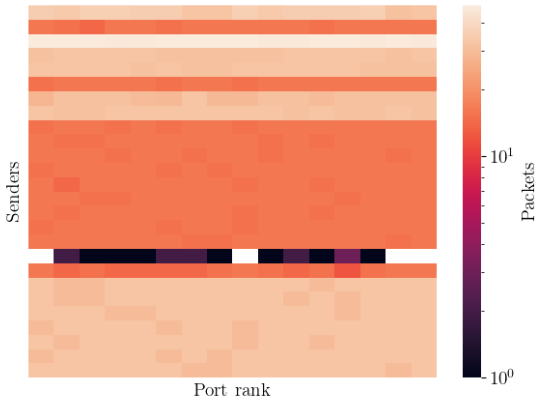
- 9090/tcp : 758 sent packets (7.7 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 22/tcp : 549 sent packets (5.6 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 465/tcp : 506 sent packets (5.1 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 591/tcp : 506 sent packets (5.1 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 1911/tcp : 506 sent packets (5.1 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



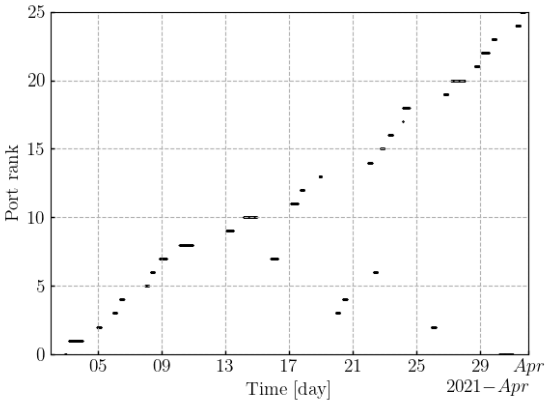
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 122: Cluster60 temporal patterns

62 Cluster 61. Silhouette: 0.906

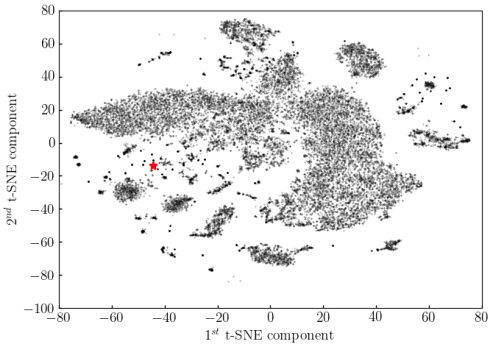


Figure 123: Cluster 61. t-SNE projection

10 distinct senders with the following ground truth classes:

- Unknown. 10 senders

402 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

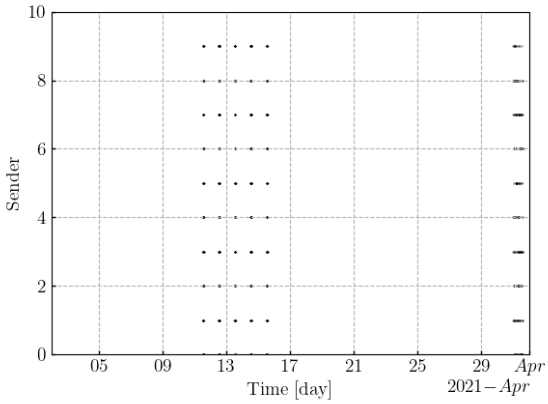
- 34.96.130.0 with 10 senders,

1 distinct /16 subnets. The top-5 are:

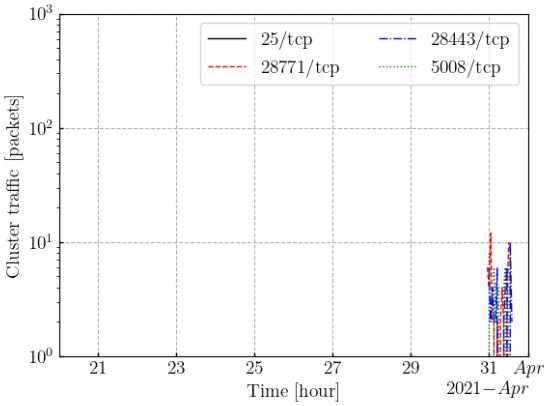
- 34.96.0.0 with 10 senders,

12 ports contacted. The top-5 are:

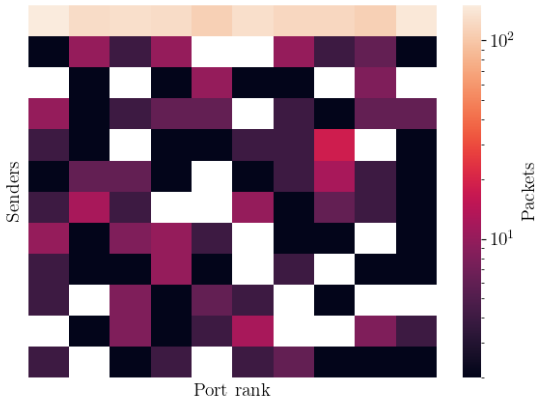
- 25/tcp : 1263 sent packets (75.9 % of the monthly cluster traffic.) 10 senders contacted the port(100.0 % of the cluster senders.)
- 28771/tcp : 48 sent packets (2.9 % of the monthly cluster traffic.) 8 senders contacted the port(80.0 % of the cluster senders.)
- 28443/tcp : 46 sent packets (2.8 % of the monthly cluster traffic.) 9 senders contacted the port(90.0 % of the cluster senders.)
- 5008/tcp : 44 sent packets (2.6 % of the monthly cluster traffic.) 8 senders contacted the port(80.0 % of the cluster senders.)
- 5986/tcp : 40 sent packets (2.4 % of the monthly cluster traffic.) 7 senders contacted the port(70.0 % of the cluster senders.)



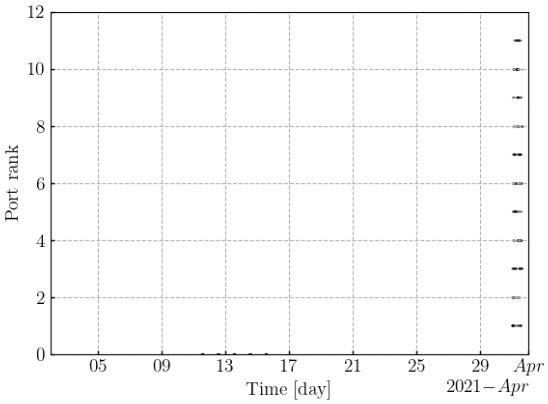
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 124: Cluster61 temporal patterns

63 Cluster 62. Silhouette: 0.659

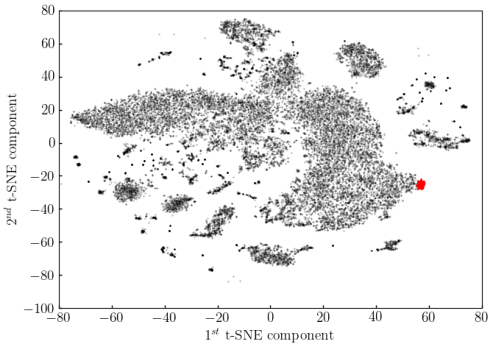


Figure 125: Cluster 62. t-SNE projection

18 distinct senders with the following ground truth classes:

- Mirai-like. 17 senders
- Unknown. 1 sender

90 packets sent in the last day. 0.0% of the last day traffic. 97.8% of cluster traffic has the Mirai fingerprint.

17 distinct /24 subnets. The top-5 are:

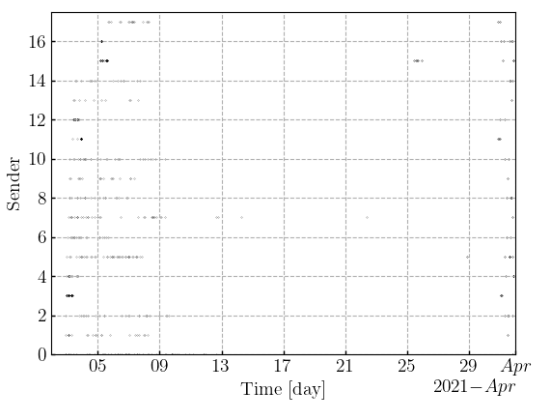
- 5.26.164.0 with 2 senders, 5.26.198.0 with 1 sender 176.30.199.0 with 1 sender 117.192.84.0 with 1 sender 117.220.184.0 with 1 sender

16 distinct /16 subnets. The top-5 are:

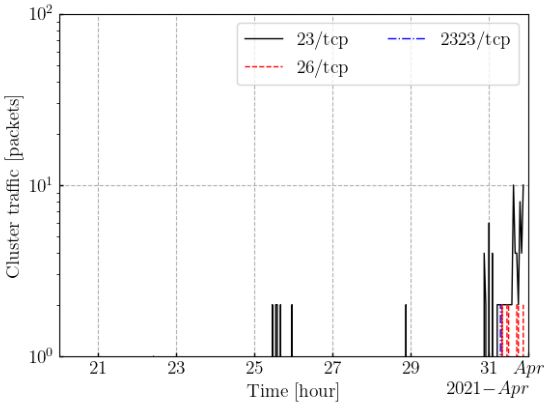
- 5.26.0.0 with 3 senders, 5.11.0.0 with 1 sender 220.133.0.0 with 1 sender 213.57.0.0 with 1 sender 211.210.0.0 with 1 sender

4 ports contacted. The top-5 are:

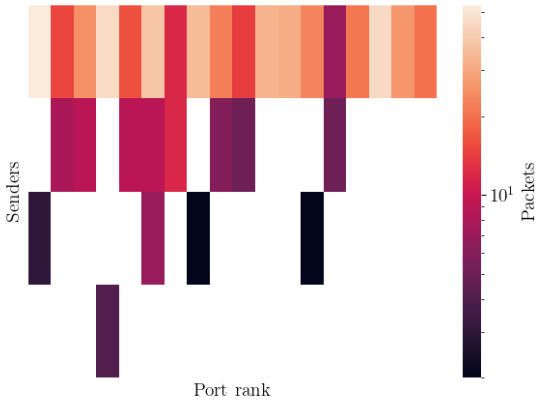
- 23/tcp : 482 sent packets (85.6 % of the monthly cluster traffic.) 18 senders contacted the port(100.0 % of the cluster senders.)
- 26/tcp : 63 sent packets (11.2 % of the monthly cluster traffic.) 8 senders contacted the port(44.4 % of the cluster senders.)
- 2323/tcp : 14 sent packets (2.5 % of the monthly cluster traffic.) 4 senders contacted the port(22.2 % of the cluster senders.)
- 55555/tcp : 4 sent packets (0.7 % of the monthly cluster traffic.) 1 senders contacted the port(5.6 % of the cluster senders.)



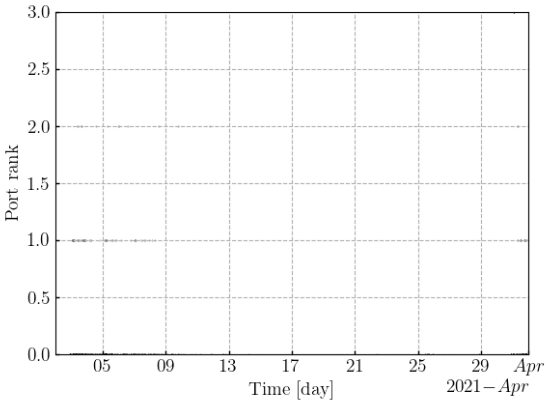
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 126: Cluster62 temporal patterns

64 Cluster 63. Silhouette: 0.794

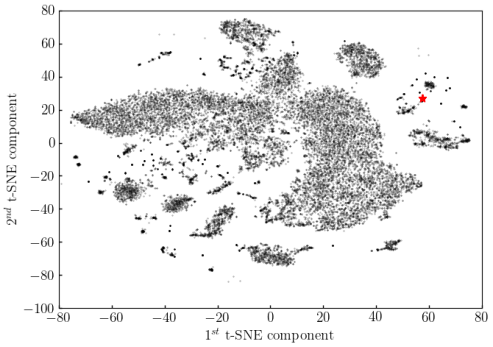


Figure 127: Cluster 63. t-SNE projection

15 distinct senders with the following ground truth classes:

- Shadowserver. 15 senders

1122 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

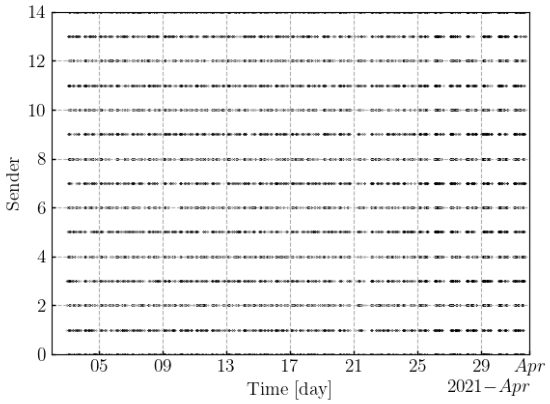
- 184.105.139.0 with 15 senders,

1 distinct /16 subnets. The top-5 are:

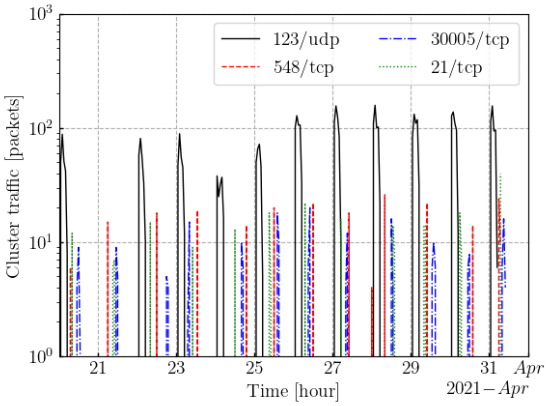
- 184.105.0.0 with 15 senders,

40 ports contacted. The top-5 are:

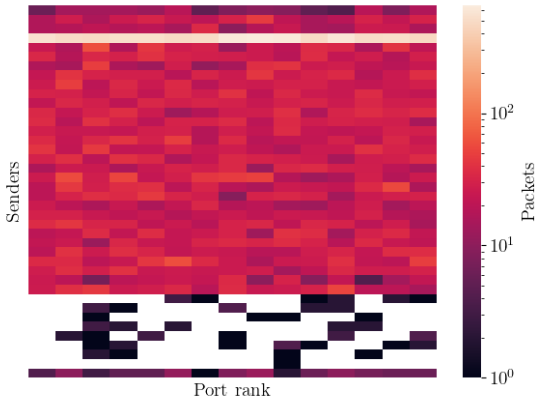
- 123/udp : 8072 sent packets (40.0 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 548/tcp : 474 sent packets (2.4 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 30005/tcp : 472 sent packets (2.3 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 21/tcp : 446 sent packets (2.2 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)
- 23/tcp : 439 sent packets (2.2 % of the monthly cluster traffic.) 15 senders contacted the port(100.0 % of the cluster senders.)



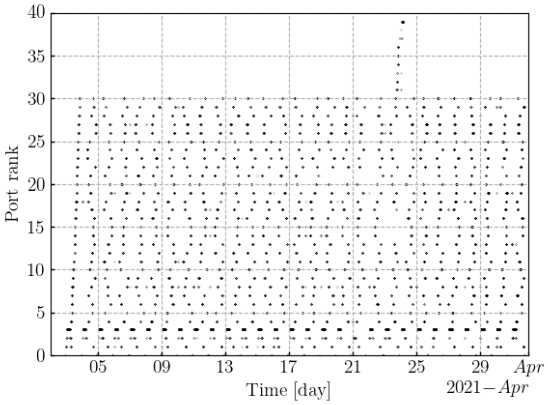
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 128: Cluster63 temporal patterns

65 Cluster 64. Silhouette: 0.724

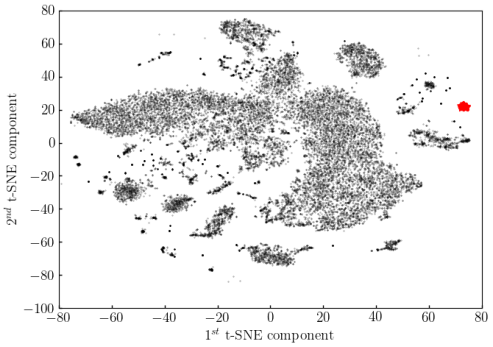


Figure 129: Cluster 64. t-SNE projection

61 distinct senders with the following ground truth classes:

- Shadowserver. 61 senders

3028 packets sent in the last day. 0.1% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

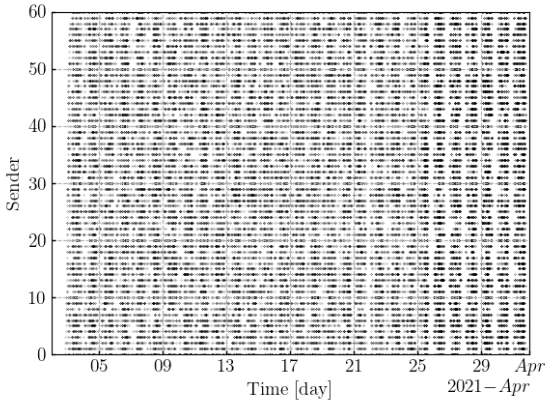
- 65.49.20.0 with 61 senders,

1 distinct /16 subnets. The top-5 are:

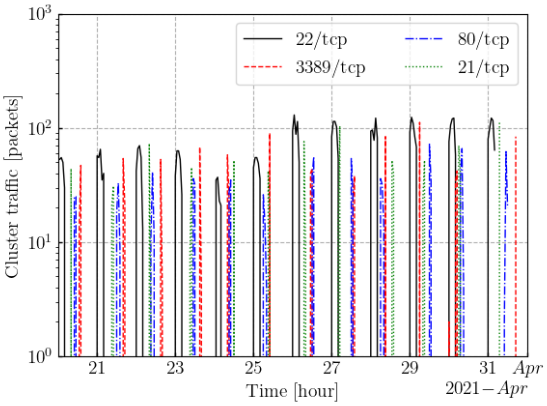
- 65.49.0.0 with 61 senders,

40 ports contacted. The top-5 are:

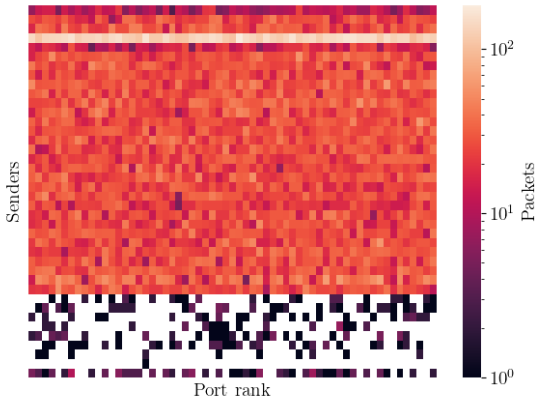
- 22/tcp : 8211 sent packets (14.2 % of the monthly cluster traffic.) 61 senders contacted the port(100.0 % of the cluster senders.)
- 3389/tcp : 2209 sent packets (3.8 % of the monthly cluster traffic.) 61 senders contacted the port(100.0 % of the cluster senders.)
- 80/tcp : 1935 sent packets (3.3 % of the monthly cluster traffic.) 61 senders contacted the port(100.0 % of the cluster senders.)
- 21/tcp : 1894 sent packets (3.3 % of the monthly cluster traffic.) 61 senders contacted the port(100.0 % of the cluster senders.)
- 4786/tcp : 1783 sent packets (3.1 % of the monthly cluster traffic.) 61 senders contacted the port(100.0 % of the cluster senders.)



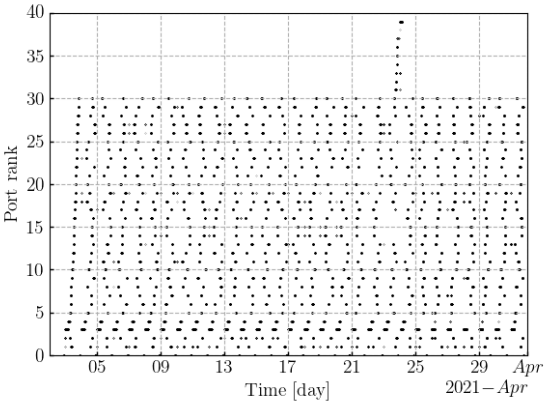
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 130: Cluster64 temporal patterns

66 Cluster 65. Silhouette: 0.849

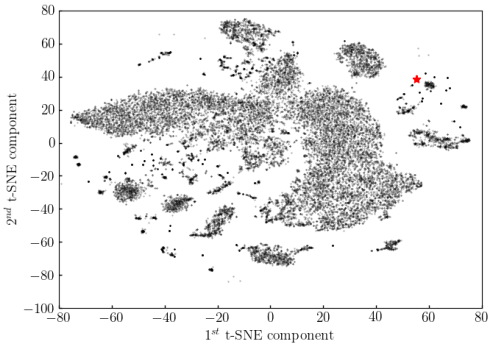


Figure 131: Cluster 65. t-SNE projection

14 distinct senders with the following ground truth classes:

- Shadowserver. 14 senders

1098 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

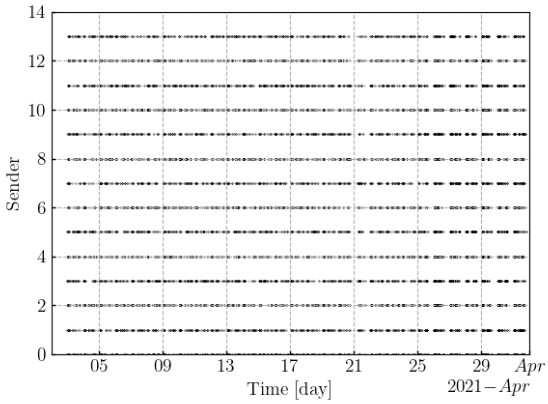
- 184.105.247.0 with 14 senders,

1 distinct /16 subnets. The top-5 are:

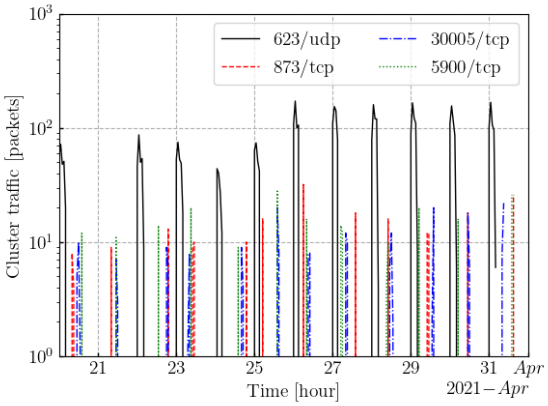
- 184.105.0.0 with 14 senders,

39 ports contacted. The top-5 are:

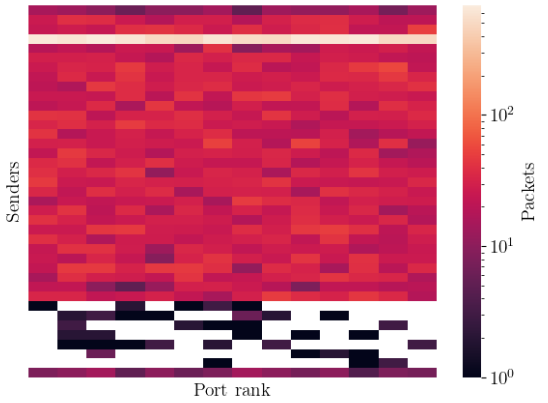
- 623/udp : 8083 sent packets (39.9 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 873/tcp : 478 sent packets (2.4 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 30005/tcp : 470 sent packets (2.3 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 5900/tcp : 461 sent packets (2.3 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)
- 5555/tcp : 456 sent packets (2.3 % of the monthly cluster traffic.) 14 senders contacted the port(100.0 % of the cluster senders.)



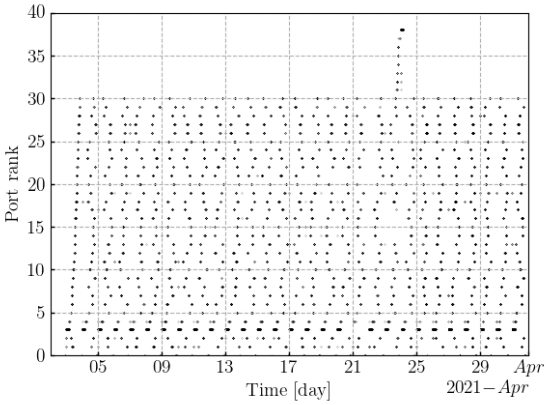
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 132: Cluster65 temporal patterns

67 Cluster 66. Silhouette: 0.494

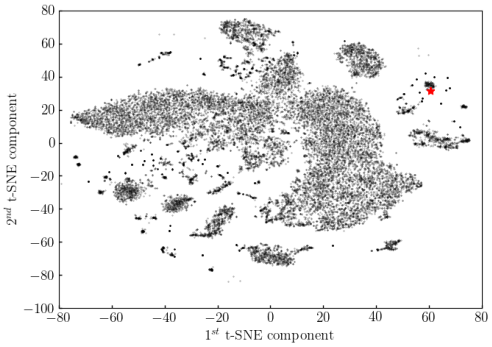


Figure 133: Cluster 66. t-SNE projection

7 distinct senders with the following ground truth classes:

- Shadowserver. 7 senders

1408 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

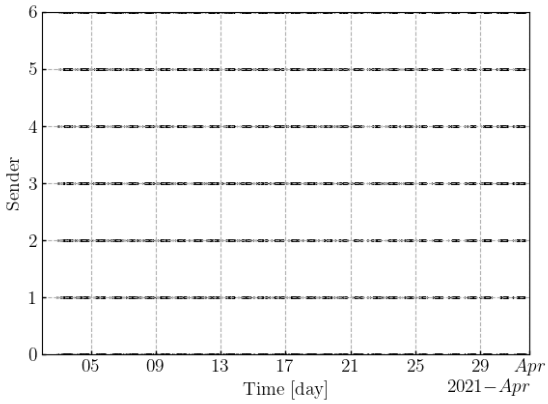
- 184.105.247.0 with 7 senders,

1 distinct /16 subnets. The top-5 are:

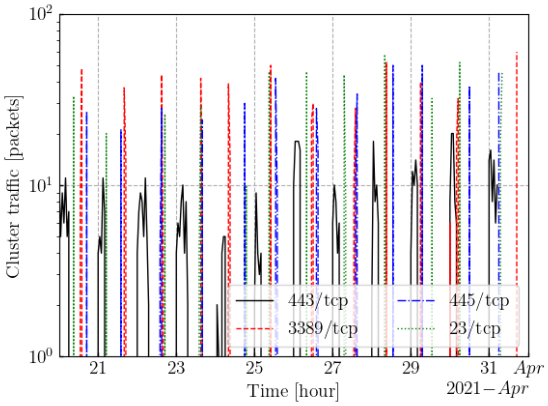
- 184.105.0.0 with 7 senders,

39 ports contacted. The top-5 are:

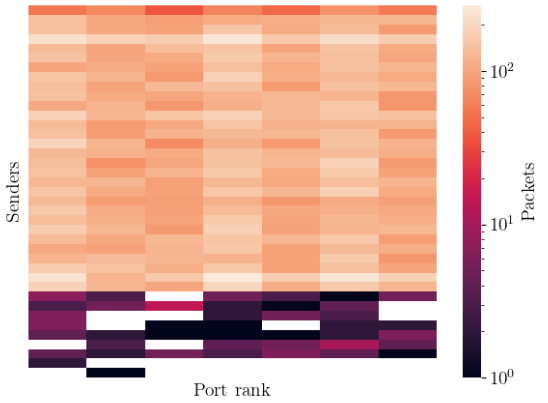
- 443/tcp : 1376 sent packets (5.2 % of the monthly cluster traffic.) 7 senders contacted the port(100.0 % of the cluster senders.)
- 3389/tcp : 1376 sent packets (5.2 % of the monthly cluster traffic.) 7 senders contacted the port(100.0 % of the cluster senders.)
- 445/tcp : 1067 sent packets (4.0 % of the monthly cluster traffic.) 7 senders contacted the port(100.0 % of the cluster senders.)
- 23/tcp : 999 sent packets (3.8 % of the monthly cluster traffic.) 7 senders contacted the port(100.0 % of the cluster senders.)
- 389/tcp : 922 sent packets (3.5 % of the monthly cluster traffic.) 7 senders contacted the port(100.0 % of the cluster senders.)



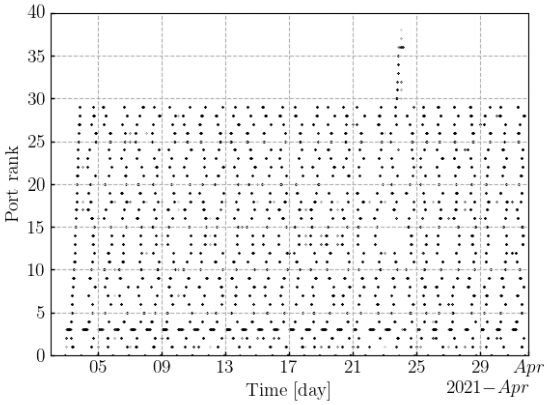
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 134: Cluster66 temporal patterns

68 Cluster 67. Silhouette: 0.51

126 distinct senders with the following ground truth classes:

- Unknown. 125 senders
- Stretchoid. 1 sender

5476 packets sent in the last day. 0.2% of the last day traffic.

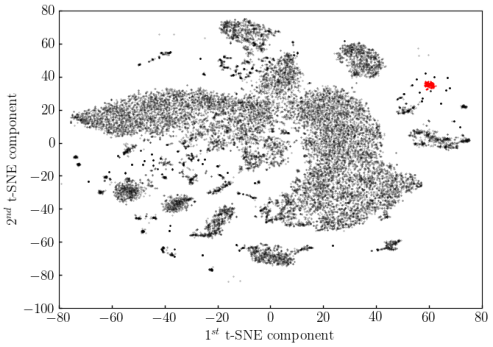


Figure 135: Cluster 67. t-SNE projection

7 distinct /24 subnets. The top-5 are:

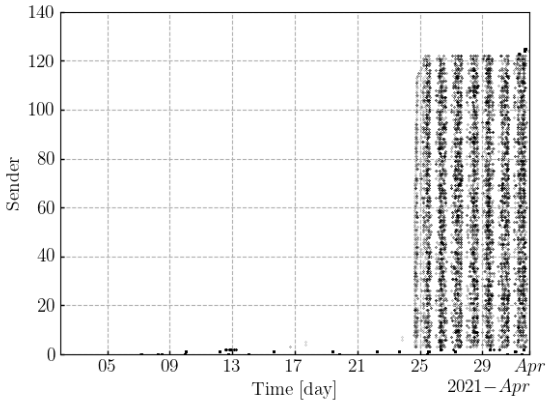
- 64.62.197.0 with 120 senders, 45.155.205.0 with 1 sender 35.178.190.0 with 1 sender 34.83.17.0 with 1 sender 192.241.226.0 with 1 sender

7 distinct /16 subnets. The top-5 are:

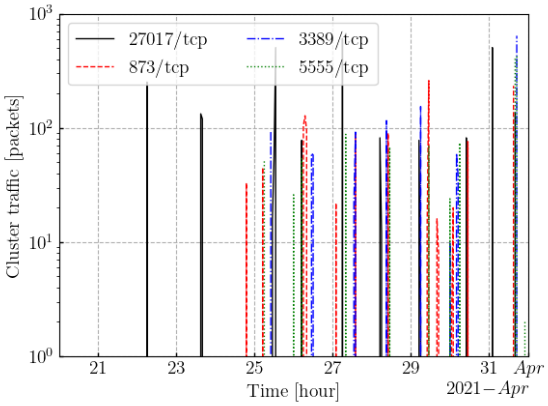
- 64.62.0.0 with 120 senders, 45.155.0.0 with 1 sender 35.178.0.0 with 1 sender 34.83.0.0 with 1 sender 192.241.0.0 with 1 sender

36 ports contacted. The top-5 are:

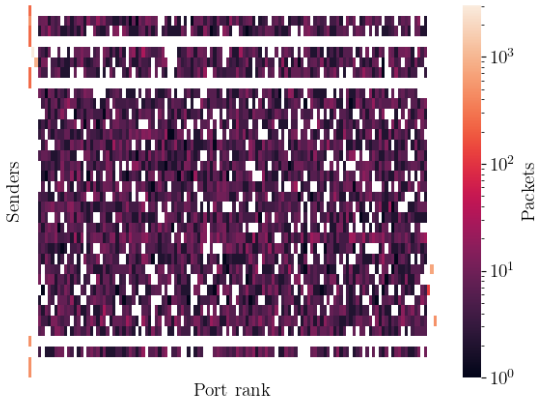
- 27017/tcp : 3677 sent packets (13.7 % of the monthly cluster traffic.) 94 senders contacted the port(74.6 % of the cluster senders.)
- 873/tcp : 1489 sent packets (5.6 % of the monthly cluster traffic.) 103 senders contacted the port(81.7 % of the cluster senders.)
- 3389/tcp : 1344 sent packets (5.0 % of the monthly cluster traffic.) 111 senders contacted the port(88.1 % of the cluster senders.)
- 5555/tcp : 1281 sent packets (4.8 % of the monthly cluster traffic.) 100 senders contacted the port(79.4 % of the cluster senders.)
- 9200/tcp : 1154 sent packets (4.3 % of the monthly cluster traffic.) 104 senders contacted the port(82.5 % of the cluster senders.)



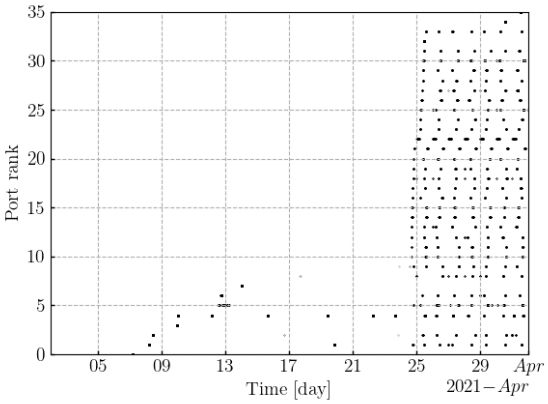
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 136: Cluster67 temporal patterns

69 Cluster 68. Silhouette: 0.78

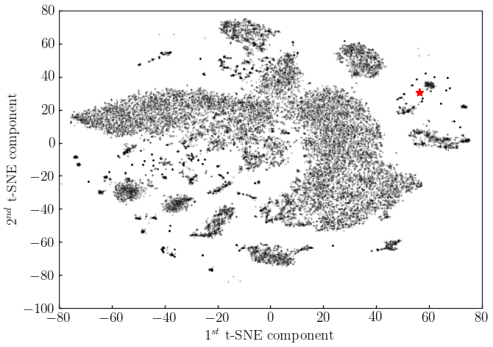


Figure 137: Cluster 68. t-SNE projection

13 distinct senders with the following ground truth classes:

- Shadowserver. 13 senders

1158 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

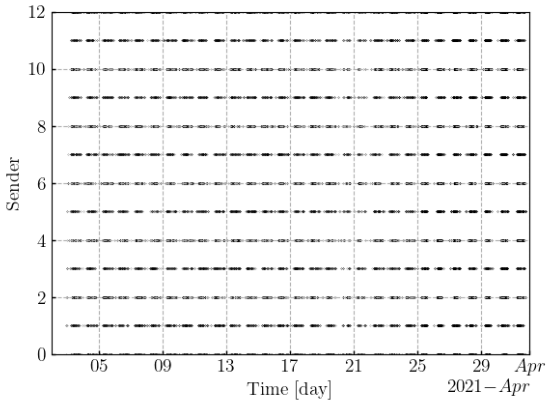
- 184.105.247.0 with 13 senders,

1 distinct /16 subnets. The top-5 are:

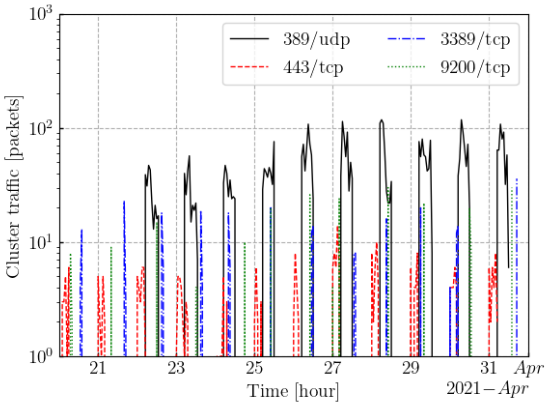
- 184.105.0.0 with 13 senders,

38 ports contacted. The top-5 are:

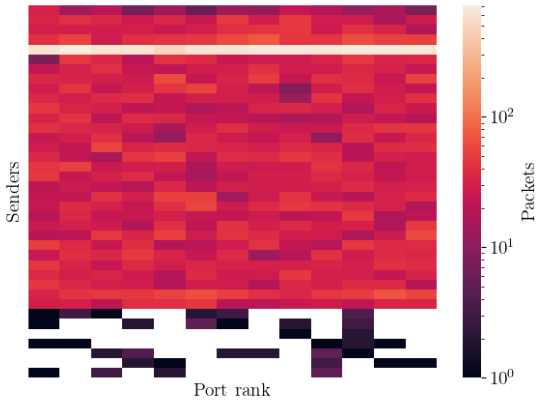
- 389/udp : 8370 sent packets (40.0 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)
- 443/tcp : 644 sent packets (3.1 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)
- 3389/tcp : 631 sent packets (3.0 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)
- 9200/tcp : 470 sent packets (2.2 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)
- 4899/tcp : 457 sent packets (2.2 % of the monthly cluster traffic.) 13 senders contacted the port(100.0 % of the cluster senders.)



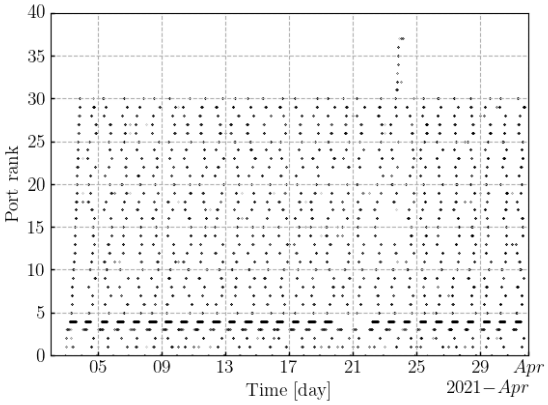
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 138: Cluster68 temporal patterns

70 Cluster 69. Silhouette: 0.857

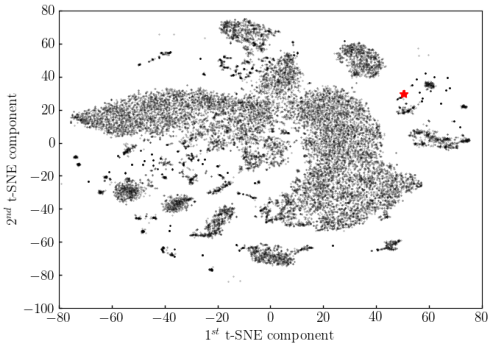


Figure 139: Cluster 69. t-SNE projection

16 distinct senders with the following ground truth classes:

- Shadowserver. 16 senders

1130 packets sent in the last day. 0.0% of the last day traffic.

1 distinct /24 subnets. The top-5 are:

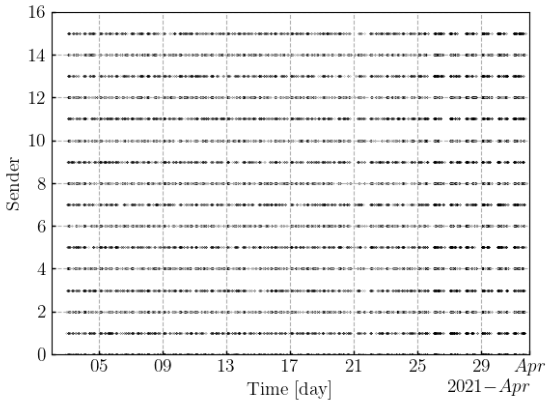
- 74.82.47.0 with 16 senders,

1 distinct /16 subnets. The top-5 are:

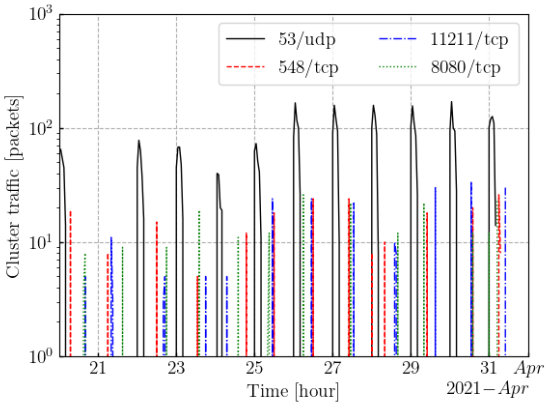
- 74.82.0.0 with 16 senders,

40 ports contacted. The top-5 are:

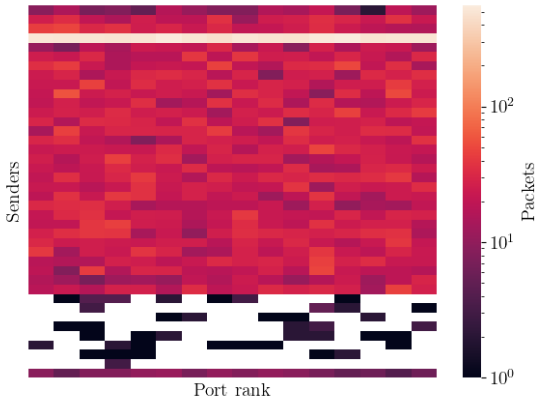
- 53/udp : 8068 sent packets (40.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 548/tcp : 459 sent packets (2.3 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 11211/tcp : 457 sent packets (2.3 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 8080/tcp : 452 sent packets (2.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)
- 2323/tcp : 450 sent packets (2.2 % of the monthly cluster traffic.) 16 senders contacted the port(100.0 % of the cluster senders.)



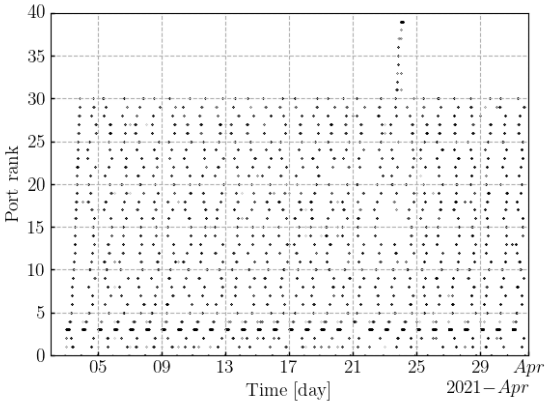
(a) Activity pattern



(b) Top-4 ports traffic



(c) Port Heatmap



(d) Port pattern

Figure 140: Cluster69 temporal patterns