Darknet observability: scale and locality

Bernhard Degen

June 28, 2024

Motivation

The UCSD network telescope has been an invaluable data source for over two decades.

In 2019, UCSD-NT was reduced by 25% and got a new neighbor. A sizeable /10 prefix has become active for the first time since its inception[1].

What is the impact on the network telescope?

[1] Besides AMRPNet allocations

Research questions

1. What can learn from the darknet redimensioning regarding observability?
2. How do we distinguish between interactive and non-interactive scanners?
3. To what extent do scanners actively avoid addresses formerly part of a darknet?

RQ1 Impact on observability

How to define observability?

- Large-scale scanners
- DDoS attacks
- Internet outages
- …

Not just a matter of scale, locality must also be considered.
What are the effects of a “hypergiant in the backyard”?

Idea Replicate several studies on historical data before and after the redimensioning.

RQ2 Scanner interactivity

How do scanners traverse the darknet?

To estimate scanning rate, we must consider several dimensions

- Horizontal (*many hosts*) or vertical (*many ports*)
- Linear or (pseudo)random traversal

Intuition

s interactive $\Leftrightarrow$ time traversing *dark* space $\ll$ time traversing *light* space

RQ2 Scanner interactivity

Method

Test scale and locality in isolation, evaluate the observability metric

Scale on blocks of decreasing size, e.g. /10, /12, /16, /20, /24

Locality on blocks at varying distances from the upper and lower end

Bonus If we can reply on some addresses in the telescope range, we can also measure the effectiveness of tarpitting

RQ3 Measuring darknet avoidance

Did/do scanners actively avoid darknets? How long did it take them to become aware of the new perimeter?

Method

- We have traces from a host in 44.224.0.0/11 (AS15409, `us-west-2`) since Nov 2021.
- For each scanner identified in the darknet
  1. Compute its traversal strategy
  2. If linear, extrapolate the rate
  3. If random, compute probability of seeing it within an interval

References I

Benson, Karyn, et al., “Gaining Insight into AS-level Outages through Analysis of Internet Background Radiation”. *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Proc. of 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Apr. 2013, pp. 447–52, https://doi.org/10.1109/INFCOMW.2013.6562915.

Benson, Karyn, et al., “Leveraging Internet Background Radiation for Opportunistic Network Analysis”. *Proceedings of the 2015 Internet Measurement Conference*. IMC ’15, Association for Computing Machinery, 28 Oct. 2015, pp. 423–36, https://doi.org/10.1145/2815675.2815702.

corsaro3 contributors, *CAIDA/Corsaro3*. 22 July 2014, 2 Mar. 2024, github.com/CAIDA/corsaro3. Accessed 6 May 2024.

Dainotti, Alberto, et al., “Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet”. *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 1, 16 Jan. 2012, pp. 31–39. https://doi.org/10.1145/2096149.2096154.

De Vries, Wouter B., et al., “Global-Scale Anycast Network Management with Verfploeter”. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*. Proc. of NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Apr. 2020, pp. 1–9, https://doi.org/10.1109/NOMS47738.2020.9110449.

References II

Durumeric, Zakir, et al., “An Internet-Wide View of Internet-Wide Scanning”. *23rd USENIX Security Symposium (USENIX Security 14)*. Proc. of 23rd USENIX Security Symposium (USENIX Security 14), 2014, pp. 65–78, www.usenix.org/node/184494. Accessed 5 Feb. 2020.

Izhikevich, Liz, et al., “Cloud Watching: Understanding Attacks Against Cloud-Hosted Services”. *Proceedings of the 2023 ACM on Internet Measurement Conference*. IMC ’23, Association for Computing Machinery, 24 Oct. 2023, pp. 313–27, https://doi.org/10.1145/3618257.3624818.

Karn, Phil, et al., “AMPRNet | Amateur Radio Digital Communications”, 20 July 2019, www.ampr.org/amprnet/. Accessed 21 Oct. 2021.

Moore, David, et al., “Inferring Internet Denial-of-Service Activity”. *ACM Transactions on Computer Systems*, vol. 24, no. 2, 1 May 2006, pp. 115–39. https://doi.org/10.1145/1132026.1132027.

Pang, Ruoming, et al., “Characteristics of Internet Background Radiation”. *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement*. IMC ’04, Association for Computing Machinery, 25 Oct. 2004, pp. 27–40, https://doi.org/10.1145/1028788.1028794.

Pauley, Eric, et al., “DScope: A Cloud-Native Internet Telescope”. 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 5989–6006, www.usenix.org/conference/usenixsecurity23/presentation/pauley. Accessed 4 June 2024.

References III

Soro, Francesca, et al., “Are Darknets All The Same? On Darknet Visibility for Security Monitoring”. *2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*. Proc. of 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), July 2019, pp. 1–6, https://doi.org/10.1109/LANMAN.2019.8847113.

Soro, Francesca, et al., “Sensing the Noise: Uncovering Communities in Darknet Traffic”. *2020 Mediterranean Communication and Computer Networking Conference (MedComNet)*. Proc. of 2020 Mediterranean Communication and Computer Networking Conference (MedComNet), June 2020, pp. 1–8, https://doi.org/10.1109/MedComNet49392.2020.9191555.

Wagner, Daniel, et al., “How to Operate a Meta-Telescope in Your Spare Time”. *Proceedings of the 2023 ACM on Internet Measurement Conference*. IMC ’23, Association for Computing Machinery, 24 Oct. 2023, pp. 328–43, https://doi.org/10.1145/3618257.3624831.

Wustrow, Eric, et al., “Internet Background Radiation Revisited”. *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*. IMC ’10, Association for Computing Machinery, 1 Nov. 2010, pp. 62–74, https://doi.org/10.1145/1879141.1879149.