A Decade's-worth Perspective on Operating a Large Network Telescope (Abstract)

Michalis Kallitsis[1] (mgkallit@ieee.org), Bob Stovall (bes@merit.edu)

Network telescopes have been useful Internet monitoring sensors to security researchers for the past two decades. They have been employed to study several macroscopic Internet activities such as shedding light into botnets [1], [2], detecting network outages [3], [4], understanding randomly-spoofed denial of service attacks [5], [6], [7], examining the behavior of IoT devices [8], detecting Internet misconfigurations [9], [10], detecting the presence of aggressive-scanners in the Internet [12], etc.

A network telescope or "darknet" consists of networking infrastructure that records unsolicited Internet-wide activities destined to an *unused* but *routed* IP space. Since this "dark IP space" serves no network services (e.g., Web servers), any traffic arriving to the darknet is inherently suspicious. However, extracting meaningful information from the vast amount of "noisy" data collected in large network telescopes can be a challenge. We will discuss how we attempted to address some of these challenges and some lessons learned by operating Merit's ORION (Observatory for cyber-Risk Insights and Outages of Networks) network telescope [11]. We will review ORION's near-real-time data pipeline that extracts darknet events of interest (such as scanning activities and "backscatter-based" denial of service attacks) and uploads the extracted events into Google's BigQuery for further processing and analysis. We will also showcase ORION's labeling efforts to enrich the identified darknet events with several useful meta-data (such as routing, DNS and geolocation information) along with useful fingerprints that can be extracted from packet headers (i.e., the Mirai, Masscan and ZMap fingerprints).

We will also highlight some innate limitations that monolithic network telescopes exhibit. First, it is well-known that sophisticated attackers may avoid scanning the address space of large darknets or engage into more targeted activities such as directing their efforts into "cloud-providers" or specific geographic locations [13, 14]. Further, "passive" darknets lack the ability to collect useful payload information from protocols that require a protocol handshake (such as TCP). This fact frequently hinders their ability to discover details about the specific vulnerabilities that bad actors are trying to exploit; on the other hand, "interactive/reactive network telescopes" [15] do allow the extraction of additional insights. We will discuss efforts made under the auspices of the ORION telescope to overcome these limitations by operating a "reactive and distributed" network telescope component, and offer some thoughts for future research directions.

[1] The author is currently with Akamai Technologies. The work described in this abstract does not represent Akamai, and is based solely on the author's prior work at Merit Network, Inc.

References

[1] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, Yi Zhou, “Understanding the mirai botnet,” in 26th USENIX Security Symposium (USENIX Security 17), 2017.

[2] A. Dainotti, A. King, K. Claffy, F. Papale, and A. Pescap´e, “Analysis of a /0; stealth scan from a botnet,” IEEE/ACM Transactions on Networking, vol. 23, no. 2, pp. 341–354, April 2015

[3] K. Benson, A. Dainotti, k. Claffy, and E. Aben, “Gaining insight into as-level outages through analysis of internet background radiation,” ser. CoNEXT Student 2012, 2012.

[4] A. Dainotti, R. Amman, E. Aben, and K. C. Claffy, “Extracting benefit from harm: Using malware pollution to analyze the impact of political and geophysical events on the internet,” SIGCOMM CCR 2012

[5] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, “Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks,” in Proceedings of the 2014 Conference on Internet Measurement Conference, 2014

[6] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, “Inferring internet denial-of-service activity,” ACM Trans. Comput. Syst.

[7] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, and A. Dainotti, “Millions of targets under attack: A macroscopic characterization of the dos ecosystem,” in Proceedings of the 2017 IMC, 2017

[8] F. Shaikh, E. Bou-Harb, J. Crichigno, and N. Ghani, “A machine learning model for classifying unsolicited iot devices by observing network telescopes,” in 2018 14th International Wireless Communications and Mobile Computing Conference (IWCMC), 2018, pp. 938–943.

[9] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, “Internet background radiation revisited,” 10th ACM SIGCOMM Conference on Internet Measurement, 2010

[10] J. Czyz, K. Lady, S. G. Miller, M. Bailey, M. Kallitsis, and M. Karir, “Understanding IPv6 Internet background radiation,” in IMC 2013, 2013.

[11] Merit Network, Inc., ORION Network Telescope: Observatory for cyber-Risk Insights and Outages of Networks, https://www.merit.edu/initiatives/orion-network-telescope/. Note: An NSF-funded project with PIs Michalis Kallitsis, Zakir Durumeric and Stilian Stoev.

[12] Aniket Anand, Michalis Kallitsis, Jackson Sippe, and Alberto Dainotti. 2023. Aggressive Internet-Wide Scanners: Network Impact and Longitudinal Characterization. In Companion of the 19th International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2023). Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3624354.3630583

[13] Liz Izhikevich, Manda Tran, Michalis Kallitsis, Aurore Fass, and Zakir Durumeric. 2023. Cloud Watching: Understanding Attacks Against Cloud-Hosted Services. In Proceedings of the 2023 ACM on Internet Measurement Conference (IMC '23). Association for Computing Machinery, New York, NY, USA, 313–327. https://doi.org/10.1145/3618257.3624818

[14] Daniel Wagner, Sahil Ashish Ranadive, Harm Griffioen, Michalis Kallitsis, Alberto Dainotti, Georgios Smaragdakis, and Anja Feldmann. 2023. How to Operate a Meta-Telescope in your Spare Time. In Proceedings of the 2023 ACM on Internet Measurement Conference (IMC '23). Association for Computing Machinery, New York, NY, USA, 328–343. https://doi.org/10.1145/3618257.3624831

[15] Raphael Hiesgen, Marcin Nawrocki, Alistair King, Alberto Dainotti, Thomas C. Schmidt, Matthias Wählisch, Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope, 31st USENIX Security Symposium (USENIX Security 22), Boston, MA