

CommunityWatch: The Swiss-Army Knife of BGP Anomaly Detection

Vasileios Giotsas
Lancaster University
v.giotsas@lancaster.ac.uk

ABSTRACT

We present CommunityWatch, an open-source system that enables timely and accurate detection of BGP routing anomalies. CommunityWatch leverages meta-data encoded by AS operators on their advertised routes through the BGP Communities attribute. The BGP Communities values lack standardized semantics, offering the flexibility to attach a wide range of information, including AS relationships, location data, and route redistribution policies. Therefore, parsing and correlating Community values and their dynamics enables the detection and tracking of a variety of routing anomalies. We exhibit the efficacy of CommunityWatch through the detection of three different types of anomalies: infrastructure outages, route leaks, and traffic blackholing.

CCS CONCEPTS

• **Networks** → **Network measurement**; **Network dynamics**; **Network monitoring**; *Denial-of-service attacks*; *Network manageability*;

KEYWORDS

BGP; Network Monitoring; Outage Detection; DDoS; Routing; BGP Communities.

ACM Reference Format:

Vasileios Giotsas. 2018. CommunityWatch: The Swiss-Army Knife of BGP Anomaly Detection. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada*. ACM, New York, NY, USA, 1 page. <https://doi.org/10.1145/3232755.3232858>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

ANRW '18, July 16, 2018, Montreal, QC, Canada

© 2018 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-5585-8/18/07.

<https://doi.org/10.1145/3232755.3232858>