# Gaining Insight into AS-level Outages through Analysis of Internet Background Radiation

*Karyn Benson, Alberto Dainotti, kc claffy*
*{karyn,alberto,kc}@caida.org*
*CAIDA/UCSD*

*Emile Aben*
*emile.aben@ripe.net*
*RIPE NCC*

## abstract

Unsolicited traffic, such as malware, can be used to make opportunistic measurements providing insights into a remote network [1, 2, 3]. In this work, we examine Conficker-like traffic reaching the UCSD Network Telescope, a /8 darknet which receives but does not respond to traffic. Each TCP connection attempt thus generates unidirectional traffic - a sequence of SYN retransmits - which is expected to follow a consistent pattern based on the sender's operating system and/or application. Changes in this pattern across hosts located in the same autonomous system (AS) enable to make inferences about a remote network. In particular, fewer packets per flow reaching the darknet from hosts in a particular AS may indicate packet loss (e.g., congestion) along the path. We propose a metric, γ, that captures this type of change.

## signal and metric

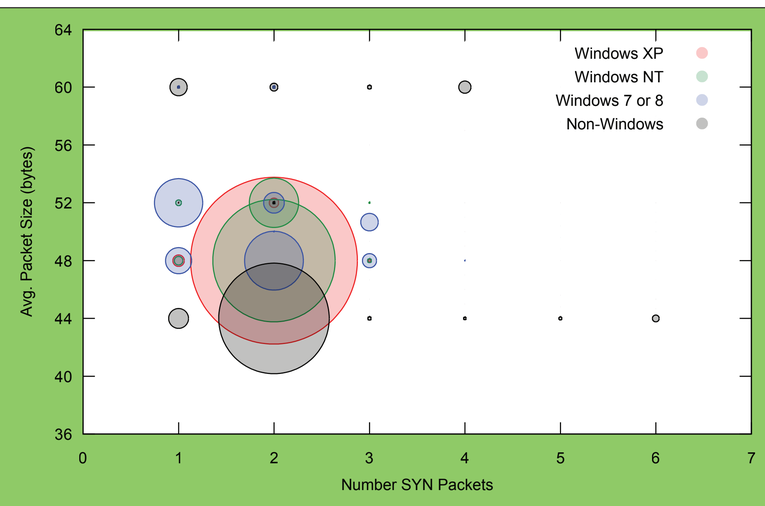
### signal

We extract a strong (statistically significant), stable (low noise), and globally pervasive (seen in most networks) signal. We use Conficker-like traffic from Windows XP and Windows NT hosts with packet sizes of 48 or 52. This traffic satisfies our criteria:

- strong: traffic to port 445 makes up ~40% traffic to the darknet and most senders use Windows XP or NT
- stable: sending two packets per flow of size 48 or 52 is the norm for XP and NT hosts
- globally pervasive: Conficker-like IBR is sent by hosts distributed worldwide.

| | |
|---|---|
| BSD | < 0.01% |
| HP-UX | < 0.01% |
| Solaris | < 0.01% |
| Mac OS | < 0.01% |
| Nmap | < 0.01% |
| Linux | 0.125% |
| Windows 7 or 8 | 2.07% |
| Windows NT | 8.89% |
| Windows XP | 88.9% |

Breakdown by OS of TCP port 445 IBR reaching the UCSD Network Telescope (Jan 2012).



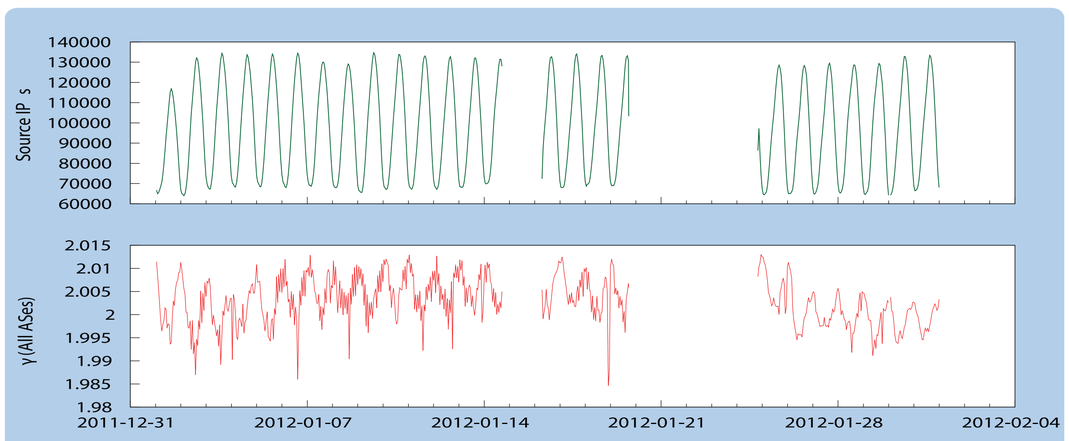

The radius of each circle is proportional to the percentage of SYN flows having that packet size and number of packets in the month of January 2012 from the given OS. Windows 7 or 8 and Non-Windows hosts send a variety of packets per flow and packet sizes - making it hard to extract a stable signal. Conversely, Windows XP and NT consistently send flows with 2 packets of size 48 or 52, creating a stable signal. Flows with more than 7 packets (very infrequent) are omitted.

### metric

The metric γ attempts to capture sudden changes in packets per flow (flows are made of only TCP SYN packets in this context). For example, if routers between the source and the darknet are dropping packets (e.g., there is congestion) γ will decrease.

$$\gamma = \frac{1}{|S|} \sum_{s \in S} \frac{\sum_{f \in F_s} \text{packets}(f)}{|F_s|}$$

S is the set of all source IPs, $F_S$ denotes the set of flows matching our criteria for a source IPs, and the function packets(f) returns the number of packets in a flow f.



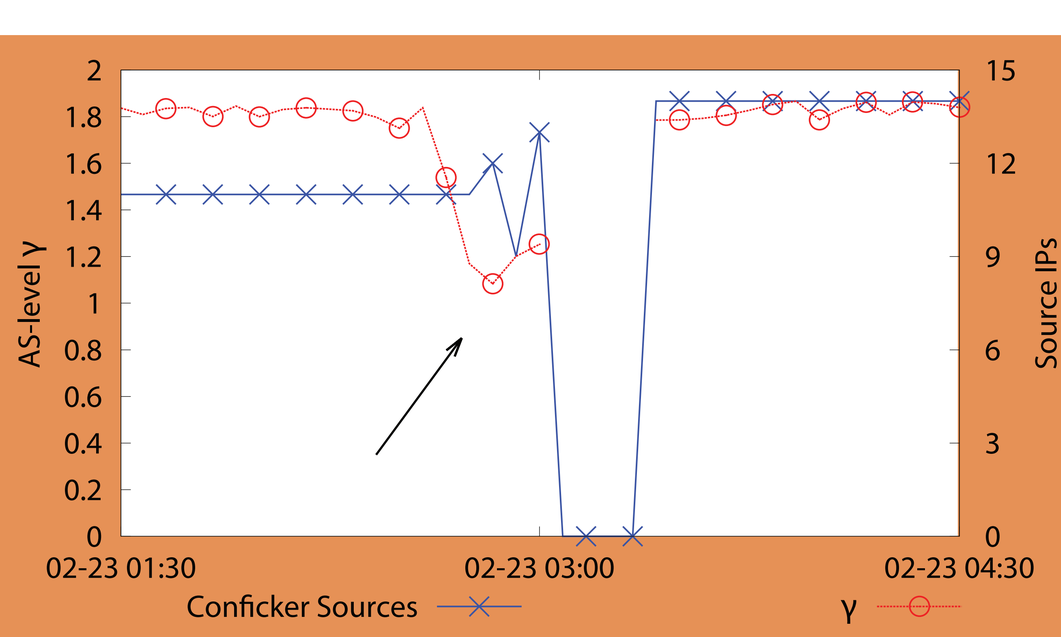

Number of source IPs and γ for all ASes (Jan. 2012) with time bins of 1 hour. Under normal circumstances, γ has a small range - which is necessary to identify deviations associated with outages. *Note: The telescope was down for about 40 hours starting on 2012-01-14 and for about 120 hours starting on 2012-01-19.*

## case studies

We apply our metric to two case studies: the first one is an outage in which network-induced packet loss is involved; the other is the result of packet filtering.

### Dodo-Telstra

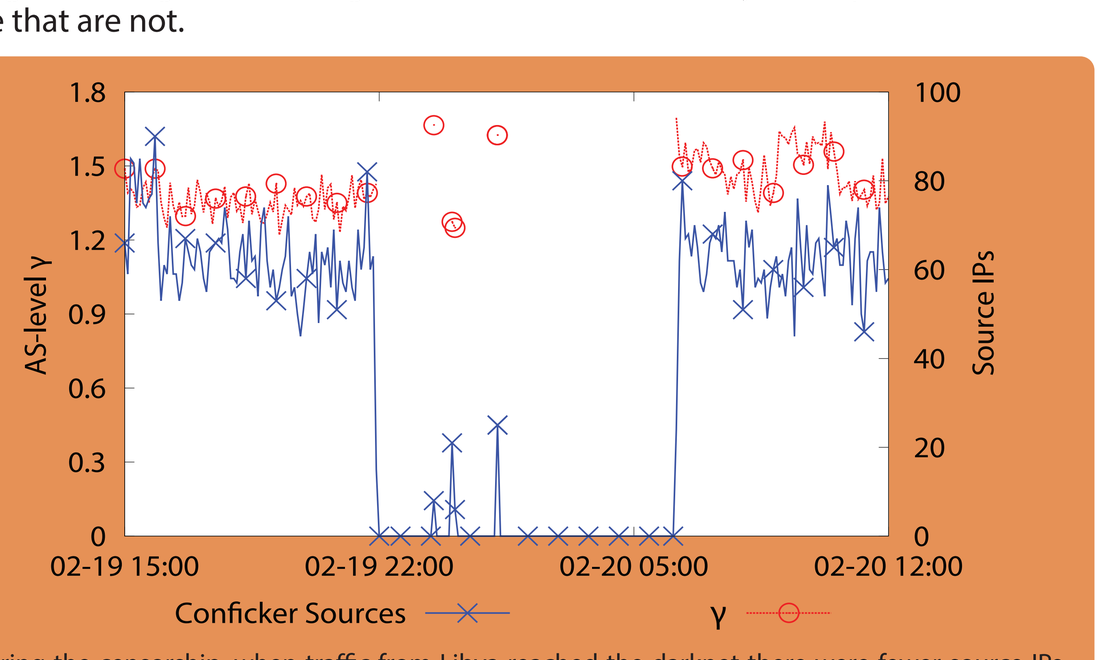
On February 23, 2012, around 2:40 UTC, the multi-homed network operator Dodo announced internal BGP routes to its provider Telstra, a major ISP in Australia, which erroneously accepted them. As a result, Telstra sent all of its traffic to the small network, Dodo, instead of a large transit provider, inducing a bottleneck leading to a complete outage [4, 5]. Our metric γ reflects this packet loss.




Our packet-loss metric is plotted in 5-min. bins for traffic originating from AS1221 during the Dodo-Telstra routing leak in February 2012. In the outage's first phase, the decrease in γ indicates a packet loss (e.g., a bottleneck). Although γ decreased, the number of IPs sending Conficker traffic remained about the same.

### Libya Internet Blackout

The Libyan Internet blackout occurred in February and March 2011, when the Libyan government used BGP disconnection, and later packet filtering, to implement nationwide censorship [2]. We examine the second of three outages, when the state telecom isolated most of the country through packet filtering [2] for approximately 7 hours. This case study illustrates that our metric effectively distinguishes large-scale outages that are characterized by some packet loss from those that are not.




During the censorship, when traffic from Libya reached the darknet there were fewer source IPs. However, the hosts that did send Conficker-like flows during the censorship, sent approximately the same number of packets per flow as prior to the outage, indicated by the similar values of γ (calculated in 5 minute time bins). This implies there was not network-induced packet loss.

1: M. Casado, T. Garfinkel, W. Cui, V. Paxson, and S. Savage. Opportunistic Measurement: Spurious Network Events as a Light in the Darkness. In ACM Fourth Workshop on Hot Topics in Networks (HotNets-IV), New York, NY, USA, 2005.
2: A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescape´. Analysis of Country-wide Internet Outages Caused by Censorship. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement, IMC '11, pages 1–18, New York, NY, USA, 2011.
3: 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 Comput. Commun. Rev., 42(1):31–39, 2012.
4: How the Internet in Australia went down under. http://bgpmon.net/blog/?p=554, Feb. 2012.
5: G. Huston. Leaking Routes. www.potaroo.net/ispcol/2012-03/leaks.html, 2012.

**sponsored by**
Funding source:
NSF CNS-1228994.