2014

# Transport Traffic Analysis

## NAME

*ttad* − Transport Traffic Analysis daemon

## SYNOPSIS

**ttad** [options]

## DESCRIPTION

*ttad* passively listens to network traffic on the specified interface and accumulates fine-grained per-flow traffic characteristics and features. These features include packet timing (jitter, three-way handshake RTT, etc), loss and retransmissions, flow control, and other detailed features that have been shown useful in identifying traffic flows to or from abusive hosts. *ttad* normally runs as a daemon and accepts XML-RPC queries for a flow identifier and returns that flow's traffic features. However, *ttad* can also read a pcap savefile for interactive use. *ttad* supports the SpamFlow and ttadclass plugins.

## OPTIONS

*−b* Include byte counts in addition to packet counts.

*−c count*
Number of packets to accept. Default is unlimited.

*−D* Do not detach and daemonize. Useful for debugging.

*−e host:port*
Specify a host to export flows via XML-RPC.

*−h* Help.

*−i int* Traffic interface name (e.g., eth0). If not specified, ttad attempts to auto-detect. When run in promiscuous mode, *ttad* must be run as root.

*−m ip:port*
Specify the server IP:port on which to filter. Defaults to auto-detect.

*−p w.x.y.z/mask*
Specify an IP prefix (w.x.y.z/mask) on which to filter. Defaults to auto-detect.

*−r file* Read from a pcap savefile rather than a live interface.

*−s* Switch perspective so that we expect to initiate an active open (i.e. send SYNs rather than receive SYNs). Default is to expect incoming SYNs to MTA.

*−t* Include timestamps.

*−v* Increase verbosity by one level. Four verbosity levels exist (in increasing order): Off, Low, High, Debug.

## SPAMFLOW

*ttad* is not generally useful alone. Rather, applications can issue XML-RPC queries to *ttad* in order to receive traffic statistics for a particular IP or IP:port tuple. One specific example is the *spamflow* plugin for spamassassin.

Likewise, *ttad* can export flow features to an XML-RPC collector for classification. One specific example is the *ttadclass* plugin.

Those wishing to experiment with *ttad* for other purposes are encouraged to look at the source code, run *ttad* in the foreground with high verbosity, etc. Many options are not documented in this manpage for clarity and usage reasons.

## SEE ALSO

spamflow(1), ttadclass(1)

## VERSION

This manual page documents ttad version 0.4

The current version is available from The Center for Measurement and Analysis of Network Data:

*http://www.cmand.org/ttad*

## AUTHOR



## BUGS

Please send problems, bugs, questions, desirable enhancements, etc. to:

spamflow@lists.cmand.org