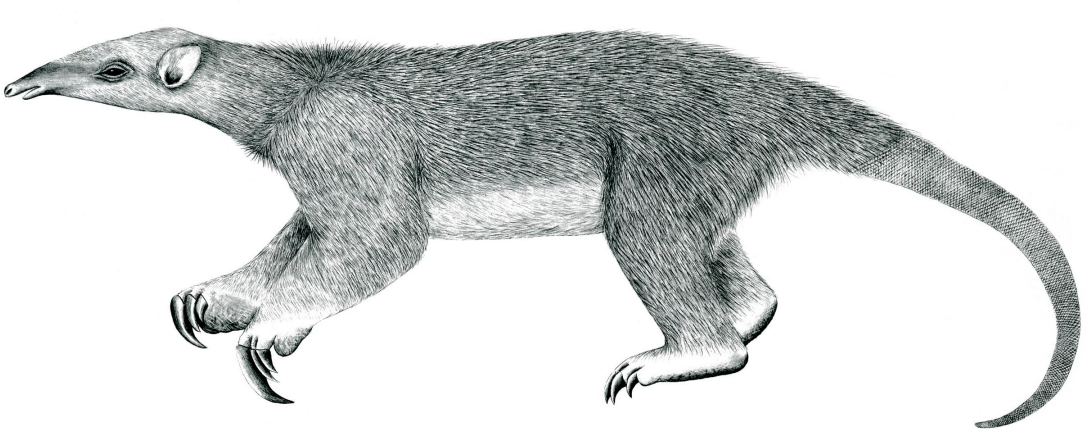
Tranalyzer2

payloadDumper

Dump the payload of layer 2, TCP, UDP or SCTP flows to files



Tranalyzer Development Team

Contents

1 payloadDumper

1.1 Description

The payloadDumper plugin dumps the payload of layer 2, TCP, UDP or SCTP flows to files. It provides features similar to tcpflow.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
PLDUMP_L2	0	Extract payload for layer 2 flows	ETH_ACTIVATE>0
PLDUMP_ETHERTYPES	{}	Only extract L2 payloads for those ethertypes e.g., {0x2000,0x2003}	PLDUMP_L2=1
PLDUMP_TCP	1	Extract payload for TCP flows	
PLDUMP_TCP_PORTS	{}	Only extract TCP payloads on those ports, e.g., {80,8080}	PLDUMP_TCP=1
PLDUMP_UDP	1	Extract payload for UDP flows	
PLDUMP_UDP_PORTS	{}	Only extract UDP payloads on those ports, e.g., {80,8080}	PLDUMP_UDP=1
PLDUMP_SCTP	0	Extract payload for TCP flows	SCTP_ACTIVATE=1
PLDUMP_SCTP_PORTS	{}	Only extract SCTP payloads on those ports, e.g., {80,8080}	PLDUMP_SCTP=1&& SCTP_ACTIVATE=1
PLDUMP_MAX_BYTES	0	Max. number of bytes per flow to dump (use 0 for no limits)	
PLDUMP_START_OFF	0	Start dumping bytes at a specific offset (Layer 2 and UDP only)	PLDUMP_L2=1|| PLDUMP_UDP=1
PLDUMP_RMDIR	1	Empty PLDUMP_FOLDER before starting	
PLDUMP_NAMES	0	Format for filenames: 0: flowInd_[AB] 1: srcIP.srcPort-dstIP.dstPort-l4Proto Extra suffix for SCTP: _sctpStream For L2: srcMac-dstMac-etherType 2: Same as 1, but prefixed with timestampT	
PLDUMP_FOLDER	"/tmp/payloadDumper/"	Output folder for saved files	
PLDUMP_PREFIX	""	Prefix for output files	
PLDUMP_SUFFIX	""	Suffix for output files	

1.2.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- PLDUMP_RMDIR
- PLDUMP_FOLDER
- PLDUMP_PREFIX
- PLDUMP_SUFFIX

1.3 Flow File Output

The payloadDumper plugin outputs the following columns:

Column	Type	Description	Flags
pldStat	H8	Status	

1.3.1 pldStat

The pldStat column is to be interpreted as follows:

	pldStat	Description
2^0	(=0x01)	Match for this flow
2^1	(=0x02)	Dump payload for this flow
2^2	(=0x04)	SCTP init TSN diff engine
2^3	(=0x08)	SCTP payload truncated
2^4	(=0x10)	TCP sequence numbers out of order or roll-over or TCP keep-alive
2^5	(=0x20)	SCTP TSN out of order or roll-over
2^6	(=0x40)	Filename truncated
2^7	(=0x80)	Failed to open file

1.4 Packet File Output

In packet mode (-s option), the payloadDumper plugin outputs the following columns:

Column	Type	Description	Flags
pldStat	H8	Status	

1.5 Plugin Report Output

The following information is reported:

- Aggregated pldStat
- Number of non zero content dumped flows

1.6 Additional Output

The payload of the layer 2, TCP, UDP and/or SCTP flows is extracted in `PLDUMP_FOLDER`. Each file is named according to the value of `PLDUMP_NAMES`, `PLDUMP_SUFFIX` and `PLDUMP_SUFFIX`.