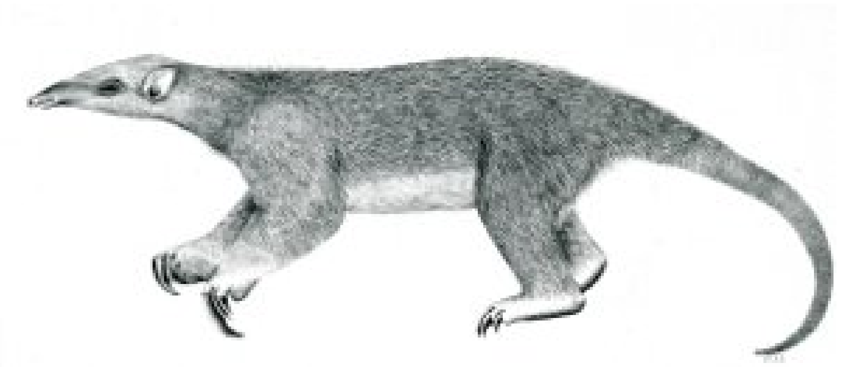
Tranalyzer2

sctpDecode

Stream Control Transmission Protocol (SCTP)



Tranalyzer Development Team

Contents

1 sctpDecode

1.1 Description

The sctpDecode plugin produces a flow based view of SCTP operations between computers for anomaly detection and troubleshooting purposes.

1.2 Configuration Flags

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

Name	Default	Description	Flags
SCTP_CRC32CHK	0	1: CRC32 check	
SCTP_ADL32CHK	0	1: Adler32 check	
SCTP_CHNKVAL	0	1: chunk type value, 0: chunk type field	
SCTP_CHNKSTR	0	1: chunk types as string	SCTP_CHNKVAL=1
SCTP_MAXCTYPE	15	1: maximum chunk types to store/flow	SCTP_CHNKVAL=1

1.3 Flow File Output

The sctpDecode plugin outputs the following columns:

Column	Type	Description	Flags
sctpStat	H8	SCTP status	
sctpNumS	U16	SCTP max Number of streams/stream number	
sctpPID	U32	SCTP Payload ID	
sctpVTag	H32	SCTP verification tag	
sctpTypeBf	H16	SCTP aggregated type bit field	SCTP_CHNKVAL=0
sctpType	H8R	SCTP uniq type value	SCTP_CHNKVAL=1&&SCTP_CHNKSTR=0
sctpTypeN	SCR	SCTP uniq type name	SCTP_CHNKVAL=1&&SCTP_CHNKSTR=1
sctpCntD_I_A	3U16	SCTP Data_Init_Abort count	
sctpCFlgs	H8	SCTP aggregated chunk flag	
sctpCCBF	H16	SCTP aggregated error cause code bit field	
sctpIS	U16	SCTP inbound streams	
sctpOS	U16	SCTP outbound streams	
sctpIARW	U32	SCTP Initial Advertised Receiver Window	
sctpIARWMin	U32	SCTP Initial Advertised Receiver Window Minimum	
sctpIARWMax	U32	SCTP Initial Advertised Receiver Window Maximum	
sctpARW	F	SCTP Advertised Receiver Window	

1.3.1 sctpStat

The sctpStat column is to be interpreted as follows:

sctpStat	Description
2^0 (=0x01)	Adler32 error

sctpStat	Description
2^1 (=0x02)	CRC32 error
2^2 (=0x04)	—
2^3 (=0x08)	Chunk truncated
2^6 (=0x10)	—
2^7 (=0x20)	Type Field overflow
2^4 (=0x40)	Type BF: Do not report
2^5 (=0x80)	Type BF: Stop processing of the packet

1.3.2 sctpCFlgs

The `sctpCFlgs` column is to be interpreted as follows:

sctpCFlgs	Description
2^0 (=0x01)	Last segment
2^1 (=0x02)	First segment
2^2 (=0x04)	Ordered delivery
2^3 (=0x08)	Possibly delay SACK
2^6 (=0x10)	—
2^7 (=0x20)	—
2^4 (=0x40)	—
2^5 (=0x80)	—

1.4 Packet File Output

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

Column	Type	Description
`sctpVerifTag`	H32	Verification tag
`sctpChunkType_Sid_Flags_Len`	U8/S_H8_U16(R)	Chunk type, flags and length
`sctpNChunks`	U8	Number of chunks