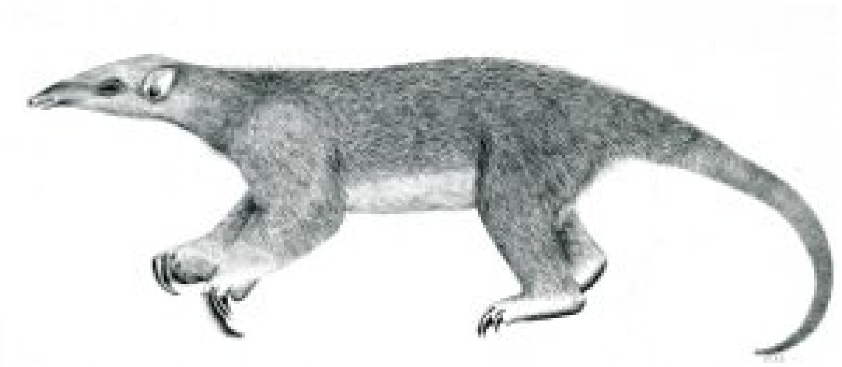
Tranalyzer2

entropy

Entropy



Tranalyzer Development Team

Contents

Copyright © 2008–2019 by Tranalyzer Development Team

1 entropy

1.1 Description

The entropy plugin calculates the entropy of the snapped IP payload distribution. The calculation of the entropy demands a number elements equal to the SQR(alphabet) = 16 in the default case. The size of the alphabet is variable. By default, one byte = 256 characters. Two other key parameters, a binary and text based ratio, in combination with the entropy serve as input for AI for content and application classification. The character and binary ratio denote the degree of text or binary content respectively.

The entropy plugin operates in two modes:

- entropy payload
- entropy payload + time series

and for production purposes by default deactivated. The parameter `ENT_MAXPBIN` controls the size of the alphabet and `ENT_ALPHA_D` the output of the payload character distribution per flow.

1.1.1 Entropy Time Series (Experimental)

The reason for this flow file addition is the exploration of entropy chunks calculated over the whole payload as a series.

1.2 Configuration Flags

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

Name	Default	Description
`ENT_THRES`	1	calc entropy only if number of payload bytes >
`ENT_ALPHA_D`	0	1: print Alphabet distribution in flow file
`ENT_D_OFFSET`	0	start of entropy calc in payload
The following flags are experimental for the MAC anomaly detection end report:		
`ENT_FLOW`	0	global flow entropy: 1: entropy, 0 output; 2: + distribution
`ENT_NTUPLE`	55	

1.3 Flow File Output

The entropy plugin outputs the following columns:

Column	Type	Description	Flags
`PyldEntropy`	F	Payload entropy: no entropy calculated:-1.0	
`PyldChRatio`	F	Payload Character ratio	
`PyldBinRatio`	F	Payload Binary ratio	
`Pyldlen`	U32	Payload length	`ENT_ALPHA_D=1`
`PyldHisto`	RU32	Payload histogram	`ENT_ALPHA_D=1`

Copyright © 2008–2019 by Tranalyzer Development Team