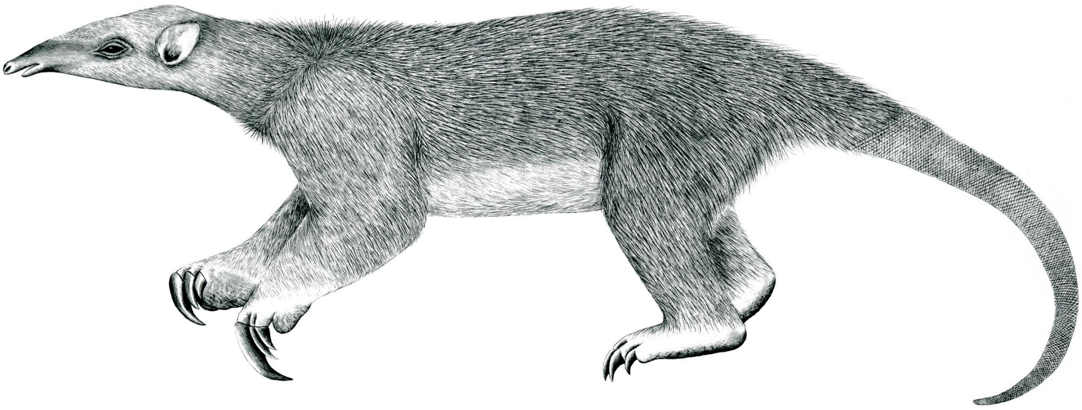
Tranalyzer2

ftpDecode

File Transfer Protocol (FTP)



Tranalyzer Development Team

Contents

1 ftpDecode

1.1 Description

The ftpDecode plugin analyzes FTP traffic. The plugin identifies the client FTP flows automatically and links them via the ftpCDFindex, identifying the findex of the associated flows.

1.2 Configuration Flags

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

Name	Default	Description	Flags
FTP_SAVE	0	Save content to FTP_F_PATH	
FTP_RMDIR	1	Empty FTP_F_PATH before starting	FTP_SAVE=1
FTP_CMD_AGGR	1	Aggregate FTP commands/response codes	
FTP_BTFLD	0	Bitfield coding of FTP commands	
FTP_UXNMLN	10	maximal username length	
FTP_PXNMLN	15	maximal password length	
FTP_MXNMLN	50	maximal name length	
FTP_MAXCPFI	10	maximal number of parent findex	
FTP_MAXUNM	5	maximal number of users	
FTP_MAXPNM	5	maximal number of passwords	
FTP_MAXCNM	20	maximal number of parameters	
FTP_F_PATH	"/tmp/FTPFILES/"	Path for extracted content	
FTP_NONAME	"nudel"	Filename to use when none available	

1.2.1 Environment Variable Configuration Flags

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

- FTP_F_PATH
- FTP_NONAME

1.3 Flow File Output

The ftpDecode plugin outputs the following columns:

Column	Type	Description	Flags
ftpStat	H8	Status bit field	
ftpCDFindex	R(U64)	Command/data findex link	
ftpCBF	H64	Command bitfield	FTP_BTFLD=1
ftpCC	R(SC)	Command codes	
ftpRC	R(U16)	Response codes	
ftpNumUser	U8	Number of users	
ftpUser	R(S)	Users	
ftpNumPass	U8	Number of passwords	

Column	Type	Description	Flags
`ftpPass`	R(S)	Passwords	
`ftpNumCP`	U8	Number of command parameters	
`ftpCP`	R(S)	Command parameters	

1.3.1 ftpStat

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

ftpStat	Description
2^0 `(=0x01)`	FTP control port found
2^1 `(=0x02)`	FTP passive parent flow
2^2 `(=0x04)`	FTP passive parent flow length overrun, possibly by dupACK/retransmits
2^3 `(=0x08)`	FTP active parent flow
2^4 `(=0x10)`	FTP hash map full
2^5 `(=0x20)`	File error (`FTP_SAVE=1`)
2^6 `(=0x40)`	Data flow not detected
2^7 `(=0x80)`	Array, string or filename overflow

1.3.2 ftpCBF

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

ftpCBF	Description
2^{0} (=0x0000.0000.0000.0001)	ABOR
2^{1} (=0x0000.0000.0000.0002)	ACCT
2^{2} (=0x0000.0000.0000.0004)	ADAT
2^{3} (=0x0000.0000.0000.0008)	ALLO
2^{4} (=0x0000.0000.0000.0010)	APPE
2^{5} (=0x0000.0000.0000.0020)	AUTH
2^{6} (=0x0000.0000.0000.0040)	CCC
2^{7} (=0x0000.0000.0000.0080)	CDUP
2^{8} (=0x0000.0000.0000.0100)	CONF
2^{9} (=0x0000.0000.0000.0200)	CWD
2^{10} (=0x0000.0000.0000.0400)	DELE
2^{11} (=0x0000.0000.0000.0800)	ENC
2^{12} (=0x0000.0000.0000.1000)	EPRT
2^{13} (=0x0000.0000.0000.2000)	EPSV
2^{14} (=0x0000.0000.0000.4000)	FEAT
2^{15} (=0x0000.0000.0000.8000)	HELP
2^{16} (=0x0000.0000.0001.0000)	LANG
2^{17} (=0x0000.0000.0002.0000)	LIST
2^{18} (=0x0000.0000.0004.0000)	LPRT
2^{19} (=0x0000.0000.0008.0000)	LPSV
2^{20} (=0x0000.0000.0010.0000)	MDTM
2^{21} (=0x0000.0000.0020.0000)	MIC
2^{22} (=0x0000.0000.0040.0000)	MKD
2^{23} (=0x0000.0000.0080.0000)	MLSD
2^{24} (=0x0000.0000.0100.0000)	MLST
2^{25} (=0x0000.0000.0200.0000)	MODE
2^{26} (=0x0000.0000.0400.0000)	NLST
2^{27} (=0x0000.0000.0800.0000)	NOOP
2^{28} (=0x0000.0000.1000.0000)	OPTS
2^{29} (=0x0000.0000.2000.0000)	PASS
2^{30} (=0x0000.0000.4000.0000)	PASV
2^{31} (=0x0000.0000.8000.0000)	PBSZ
2^{32} (=0x0000.0001.0000.0000)	PORT
2^{33} (=0x0000.0002.0000.0000)	PROT
2^{34} (=0x0000.0004.0000.0000)	PWD
2^{35} (=0x0000.0008.0000.0000)	QUIT
2^{36} (=0x0000.0010.0000.0000)	REIN
2^{37} (=0x0000.0020.0000.0000)	REST
2^{38} (=0x0000.0040.0000.0000)	RETR
2^{39} (=0x0000.0080.0000.0000)	RMD
2^{40} (=0x0000.0100.0000.0000)	RNFR
2^{41} (=0x0000.0200.0000.0000)	RNTO
2^{42} (=0x0000.0400.0000.0000)	SITE
2^{43} (=0x0000.0800.0000.0000)	SIZE
2^{44} (=0x0000.1000.0000.0000)	SMNT
2^{45} (=0x0000.2000.0000.0000)	STAT
2^{46} (=0x0000.4000.0000.0000)	STOR
2^{47} (=0x0000.8000.0000.0000)	STOU
2^{48} (=0x0001.0000.0000.0000)	STRU
2^{49} (=0x0002.0000.0000.0000)	SYST
2^{50} (=0x0004.0000.0000.0000)	TYPE
2^{51} (=0x0008.0000.0000.0000)	USER
2^{52} (=0x0010.0000.0000.0000)	XCUP
2^{53} (=0x0020.0000.0000.0000)	XMKD
2^{54} (=0x0040.0000.0000.0000)	XPWD
2^{55} (=0x0080.0000.0000.0000)	XRCP
2^{56} (=0x0100.0000.0000.0000)	XRMD
2^{57} (=0x0200.0000.0000.0000)	XRSQ
2^{58} (=0x0400.0000.0000.0000)	XSEM
2^{59} (=0x0800.0000.0000.0000)	XSEN
2^{60} (=0x1000.0000.0000.0000)	CLNT

1.4 Packet File Output

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

Column	Type	Description	Flags
ftpStat	H8	Status	

1.5 Monitoring Output

In monitoring mode, the ftpDecode plugin outputs the following columns:

Column	Type	Description	Flags
ftpPkts	U64	Number of FTP control packets	
ftpDataPkts	U64	Number of FTP-DATA packets	

1.6 Plugin Report Output

The following information is reported:

- Aggregated ftpStat
- Number of FTP control packets
- Number of FTP-DATA packets
- Number of files extracted (FTP_SAVE=1)