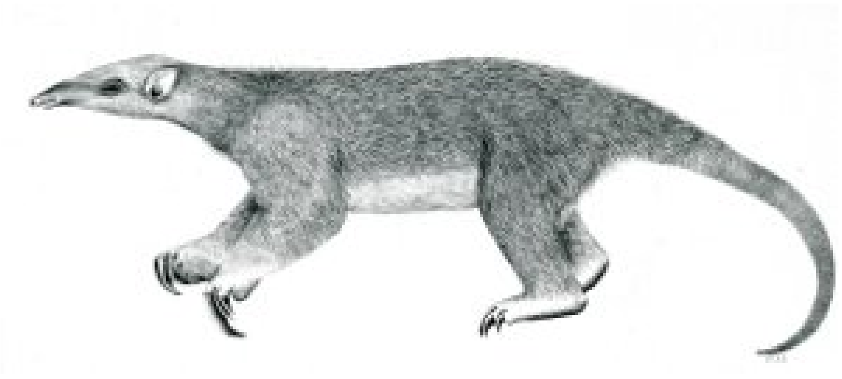
Tranalyzer2

ircDecode

Internet Relay Chat (IRC)



Tranalyzer Development Team

Contents

1 ircDecode

1.1 Description

The ircDecode plugin analyses IRC traffic. User defined compiler switches are in *ircDecode.h*.

1.2 Configuration Flags

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

Name	Default	Description
IRC_SAVE	0	Save content to IRC_F_PATH
IRC_BITFIELD	0	Bitfield coding of IRC commands
IRC_UXNMLN	10	maximal USER length
IRC_PXNMLN	10	maximal PW length
IRC_MXNMLN	50	maximal name length
IRC_MAXUNM	5	Maximal number of users
IRC_MAXPNM	5	Maximal number of passwords
IRC_MAXCNM	20	Maximal number of parameters

1.3 Flow File Output

The ircDecode plugin outputs the following columns:

Column	Type	Description	Flags
ircStat	H8	Status	
ircCBF	H64	Commands	BITFIELD=1
ircCC	RSC	Command codes	
ircRC	RU16	Response codes	
ircUsrNum	U8	Number of users	
ircPwNum	U8	Number of passwords	
ircCNum	U8	Number of parameters	
ircUsr	RS	Users	
ircPw	RS	Passwords	
ircC	RS	Content	

1.3.1 ircStat

The ircStat column is to be interpreted as follows:

ircStat	Description
2^0 (=0x01)	IRC port found
2^1 (=0x02)	IRC passive parent flow
2^2 (=0x04)	IRC passive write finished
2^3 (=0x08)	IRC active parent flow
2^4 (=0x10)	—

ircStat	Description
2^{5} (=0x20)	File error
2^{6} (=0x40)	—
2^{7} (=0x80)	Array overflow

1.3.2 ircCBF

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

ircCBF	Description
2^{0} (=`0x0000.0000.0000.0001`)	`ADMIN`
2^{1} (=`0x0000.0000.0000.0002`)	`AWAY`
2^{2} (=`0x0000.0000.0000.0004`)	`CONNECT`
2^{3} (=`0x0000.0000.0000.0008`)	`DIE`
2^{4} (=`0x0000.0000.0000.0010`)	`ERROR`
2^{5} (=`0x0000.0000.0000.0020`)	`INFO`
2^{6} (=`0x0000.0000.0000.0040`)	`INVITE`
2^{7} (=`0x0000.0000.0000.0080`)	`ISON`
2^{8} (=`0x0000.0000.0000.0100`)	`JOIN`
2^{9} (=`0x0000.0000.0000.0200`)	`KICK`
2^{10} (=`0x0000.0000.0000.0400`)	`KILL`
2^{11} (=`0x0000.0000.0000.0800`)	`LINKS`
2^{12} (=`0x0000.0000.0000.1000`)	`LIST`
2^{13} (=`0x0000.0000.0000.2000`)	`LUSERS`
2^{14} (=`0x0000.0000.0000.4000`)	`MODE`
2^{15} (=`0x0000.0000.0000.8000`)	`MOTD`
2^{16} (=`0x0000.0000.0001.0000`)	`NAMES`
2^{17} (=`0x0000.0000.0002.0000`)	`NICK`
2^{18} (=`0x0000.0000.0004.0000`)	`NJOIN`
2^{19} (=`0x0000.0000.0008.0000`)	`NOTICE`
2^{20} (=`0x0000.0000.0010.0000`)	`OPER`
2^{21} (=`0x0000.0000.0020.0000`)	`PART`
2^{22} (=`0x0000.0000.0040.0000`)	`PASS`
2^{23} (=`0x0000.0000.0080.0000`)	`PING`
2^{24} (=`0x0000.0000.0100.0000`)	`PONG`
2^{25} (=`0x0000.0000.0200.0000`)	`PRIVMSG`
2^{26} (=`0x0000.0000.0400.0000`)	`QUIT`
2^{27} (=`0x0000.0000.0800.0000`)	`REHASH`
2^{28} (=`0x0000.0000.1000.0000`)	`RESTART`
2^{29} (=`0x0000.0000.2000.0000`)	`SERVER`
2^{30} (=`0x0000.0000.4000.0000`)	`SERVICE`
2^{31} (=`0x0000.0000.8000.0000`)	`SERVLIST`
2^{32} (=`0x0000.0001.0000.0000`)	`SQUERY`
2^{33} (=`0x0000.0002.0000.0000`)	`SQUIRT`
2^{34} (=`0x0000.0004.0000.0000`)	`SQUIT`
2^{35} (=`0x0000.0008.0000.0000`)	`STATS`
2^{36} (=`0x0000.0010.0000.0000`)	`SUMMON`
2^{37} (=`0x0000.0020.0000.0000`)	`TIME`
2^{38} (=`0x0000.0040.0000.0000`)	`TOPIC`
2^{39} (=`0x0000.0080.0000.0000`)	`TRACE`
2^{40} (=`0x0000.0100.0000.0000`)	`USER`
2^{41} (=`0x0000.0200.0000.0000`)	`USERHOST`
2^{42} (=`0x0000.0400.0000.0000`)	`USERS`
2^{43} (=`0x0000.0800.0000.0000`)	`VERSION`
2^{44} (=`0x0000.1000.0000.0000`)	`WALLOPS`
2^{45} (=`0x0000.2000.0000.0000`)	`WHO`
2^{46} (=`0x0000.4000.0000.0000`)	`WHOIS`
2^{47} (=`0x0000.8000.0000.0000`)	`WHOWAS`
2^{48} (=`0x0001.0000.0000.0000`)	`-`
2^{49} (=`0x0002.0000.0000.0000`)	`-`
2^{50} (=`0x0004.0000.0000.0000`)	`-`
2^{51} (=`0x0008.0000.0000.0000`)	`-`
2^{52} (=`0x0010.0000.0000.0000`)	`-`
2^{53} (=`0x0020.0000.0000.0000`)	`-`
2^{54} (=`0x0040.0000.0000.0000`)	`-`
2^{55} (=`0x0080.0000.0000.0000`)	`-`
2^{56} (=`0x0100.0000.0000.0000`)	`-`
2^{57} (=`0x0200.0000.0000.0000`)	`-`
2^{58} (=`0x0400.0000.0000.0000`)	`-`
2^{59} (=`0x0800.0000.0000.0000`)	`-`
2^{60} (=`0x1000.0000.0000.0000`)	`-`