Tranalyzer2

telegram

Telegram

Tranalyzer Development Team

Contents

1 telegram

1.1 Description

The telegram plugin detects Telegram UDP and TCP traffic using heuristics and the IP labeling of basicFlow. Moreover it can extract L7 content of flows for further deobfuscation experiments. It is a rudimentary version, lots to improve.

1.2 Configuration Flags

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

Name	Default	Description
TG_SAVE	0	1: save telegram flows
TG_DEOBFUSCATE	0	1: deobfuscate telegram flows
TG_4_9_OR_NEWER	1	1: reduce deobfuscation false positives for Telegram >= 4.9.0 0: needed when deobfuscating traffic generated by Telegram < 4.9.0
TG_DEBUG_MESSAGES	0	1: print debug messages

1.3 Flow File Output

The telegram plugin outputs the following columns:

Column	Type	Description	Flags
tgStat	H16	Status	
tgAuthKeyId	H64	Authentication key ID	TG_DEOBFUSCATE!=0

1.3.1 tgStat

The tgStat column is to be interpreted as follows:

tgStat	Description
2^0 (=0x0001)	Telegram detected by heuristics
2^1 (=0x0002)	Control channel
2^1 (=0x0004)	Voice
2^3 (=0x0008)	Telegram detected by IP
2^4 (=0x0010)	File save
2^5 (=0x0020)	Bot app
2^6 (=0x0040)	—
2^7 (=0x0080)	—
2^8 (=0x0100)	Write error
2^9 (=0x0200)	—
2^{10} (=0x0400)	—
2^{11} (=0x0800)	—
2^{12} (=0x1000)	Internal state machine
2^{13} (=0x2000)	Internal state machine

tgStat	Description
2^{14} (=0x4000)	Internal state machine
2^{15} (=0x8000)	Internal state machine init

1.4 Packet File Output

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

Column	Type	Description	Flags
tgStat	H16	Status	

1.5 Plugin Report Output

The following information is reported:

- Aggregated tgStat
- Number of Telegram packets

1.6 TODO

- Shift IP labeling to on flow generated in basicFlow