Tranalyzer2

regex_re2

Traffic pattern matching using the RE2 library.

Tranalyzer Development Team

Contents

1 regex_re2

1.1 Description

This plugin applies regexes on the network traffic using the RE2 library: https://github.com/google/re2. The regexes are applied per packet from the layer 7.

1.2 Dependencies

1.2.1 External Libraries

This plugin depends on the RE2 library.

Ubuntu 15.10+:	`sudo apt-get install`	`g++ libre2-dev`
Arch:	`sudo pacman -S`	`re2`
Gentoo:	`sudo emerge`	`re2`
openSUSE:	`sudo zypper install`	`re2-devel`
Red Hat/Fedora[1]:	`sudo dnf install`	`gcc-c++ re2-devel`
macOS[2]:	`brew install`	`re2`

Alternatively (or for older Ubuntu versions), compile it from source:

```
sudo apt-get install git g++
git clone https://github.com/google/re2.git
cd re2
make
sudo make install
sudo ldconfig
```

1.2.2 Required Files

The file `re2file.txt` contains the regexes and their corresponding ID. The lines starting with `%` are comments. The other lines must contain two columns:

Column	Description
1	A string ID which will appear in the flow output if the flow matches the regex in column 2.
2	A regex in the RE2 syntax: https://github.com/google/re2/wiki/Syntax

When the regex file located in the plugin folder is modified, it is automatically reloaded by tranalyzer.

1.3 Configuration Flags

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

[1] If the `dnf` command could not be found, try with `yum` instead

[2] Brew is a packet manager for macOS that can be found here: https://brew.sh

Name	Default	Description
RE2_DEBUG_MESSAGES	0	Activate debug output
RE2_REGEX_FILE	"re2file.txt"	The name of the file described in Section 1.2.2.
RE2_MAX_MEMORY	2^{31} (= 2GB)	Max. memory RE2 can use to build the regex automaton.
RE2_MERGE	1	0: Compiles each regex separately → slower, less memory. 1: Merge all regexes into one automaton → faster, more memory.
RE2_RELOADING	1	Automatically reload regex file when modified. (disabled for macOS, refer to Section 1.6)
RE2_MAX_MATCH_PER_PACKET	8	Max. number of regexes which can match on a single packet.
RE2_MAX_MATCH_PER_FLOW	32	Max. number of regexes which can match on a single flow.

1.4 Flow File Output

The regex_re2 plugin outputs the following columns:

Column	Type	Description	Flags
re2match	RS	IDs of all regexes matching this flow	

1.5 Plugin Report Output

The following information is reported:

- Number of signatures matched
- Number of flows with matched signatures

1.6 Known Bugs and Limitations

- macOS does not provide the inotify library, therefore modified regex files cannot be automatically reloaded.