pev documentation

Release 0.80

pev authors

December 10, 2015

Contents

1 Building and installing pev 3

Since version 0.50, `pev` is a multiplatform toolkit to work with PE (Portable Executable) binaries. Its main goal is to provide feature-rich tool for proper analyze binaries, specially suspicious ones. pev has born in 2010 from a simple need: a program to find out the version (File Version) of a PE32 file and that could be run in Linux. This version number is stored in Resources (.rsrc) section but at the time we've decided to simply search for the string in the whole binary, without any optimization.

Later on we've decided to parse the PE32 file until reach .rsrc section and get the File Version field. In order to do that, we realized we must parse the entire file and we thought if we could print out all the fields and values as well...

Until version 0.40, pev was an unique program for parse the PE headers and sections (now readpe is responsible for this). In version 0.50 we focused on malware analysis and splitted pev into various programs beyond a library, called libpe. Currently all pev programs use libpe.

CHAPTER 1

Building and installing `pev`

You can download the ready for use binaries for pev that we call pre-compiled binaries. This is the easiest way to start using pev, although you may want to compile it in your environment if you feel comfortable but that will require you to install dependencies, some libraries headers and some programs to do the job.

If you choose to use the pre-compiled binaries (recommended for beginners), you only need to download it from our download page. There pre-compiled binaries for Windows, Linux packages in DEB and RPM format and Mac OS X. Linux users can also use their packaging manager to install pev. Look for it in your repository but make sure you have the latest pev version available first. ;)