Basic Executable Analysis

This section contains information obtained from a variety of tools and services that helped me form a preliminary hypothesis about the nature of this binary.

MD5: **E95998D23233476FCC61A1FECA6D02A2**
SHA1: **A5847314E89A0B335F583803D29D4BF753EB9174**
Created: **Tuesday, November 10, 2015 4:07:28 AM**
Size: **82944**

VirusTotal Most of the engine hits seemingly came from AV engines that equate a packed binary with malware (names reported like *Gen.Packer.PESpin* and *Pascked.Win32.MNSP.Gen*).

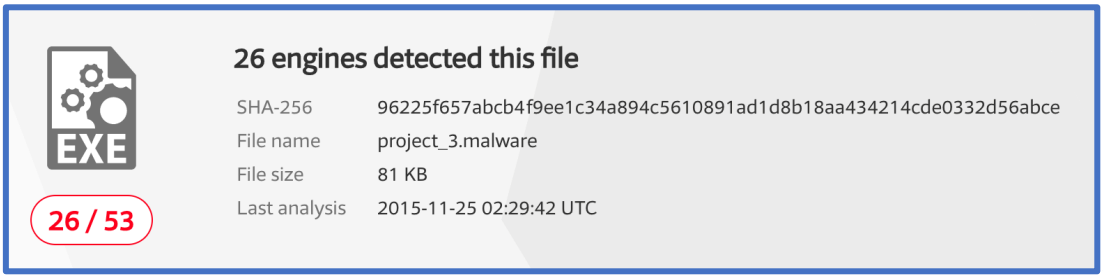

Figure 1 VirusTotal report for the original project_3.malware binary.

PEiD The binary is packed with a version of PESpin ranging from 0.3 to 1.x. Not much could be found about PESpin online except for the programs website and a few manual unpacking tutorials.

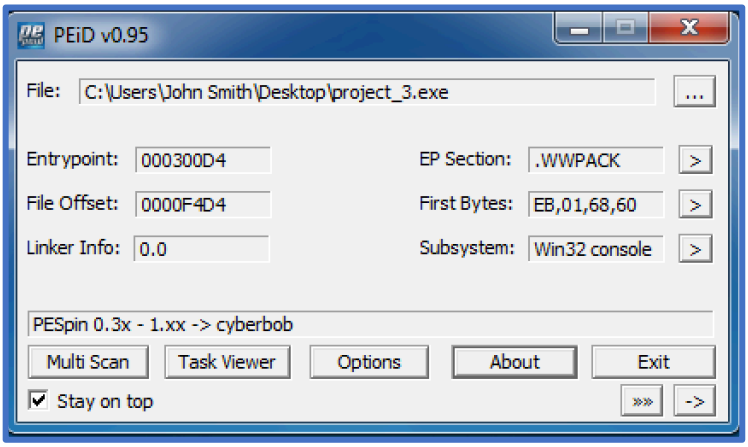

Figure 2 PEiD scan of the original project_3.malware binary.

ProcMon Since the imports for this PE are not evident through static analysis, we must use dynamic analysis tools like Process Monitor to see what libraries the binary needs.