Manual Unpacking

Azlan Mukhtar

F-Secure

Introduction

- Why Pack?
  - Reduce executable file size with compression (faster program loading)
  - Obfuscation
  - Protection from debugging/disassembling
  - Evading Anti-Virus detection

The Basics

- PE format revisits – Import table, VA, RVA, Disk Offset
- Manual Unpacking flow
  - Bypassing Anti-debug (if any)
  - Finding OEP
  - Dump
  - Fix Import Table (IT)

The Tools

- PE Tools and Dumper
  - LordPE, Stud_PE, Ollydump or OllydumpEx
- IAT fixing tools
  - Imprec (Import Reconstructor) or Scylla, and UIF

- Where to get the tools?
  - http://www.woodmann.com/collaborative/tools/index.php/Category:Unpacking_Tools
  - http://forum.tuts4you.com/files/file/576-scylla-imports-reconstruction/
  - http://www.cgsoftlabs.ro/studpe.html

Import Table

- **IMAGE_IMPORT_DESCRIPTOR Structure *** http://msdn.microsoft.com/en-us/magazine/bb985996.aspx

Member	Description
OriginalFirstThunk	This field is badly named. It contains the RVA of the Import Name Table (INT). This is an array of IMAGE_THUNK_DATA structures. This field is set to 0 to indicate the end of the array of IMAGE_IMPORT_DESCRIPTORs
TimeDateStamp	This is 0 if this executable is not bound against the imported DLL. When binding in the old style (see the section on Binding), this field contains the time/date stamp (number of seconds since 1/1/1970 GMT) when the binding occurred. When binding in the new style, this field is set to -1.
ForwarderChain	This is the Index of the first forwarded API. Set to -1 if no forwarders. Only used for old-style binding, which could not handle forwarded APIs efficiently.
Name	The RVA of the ASCII string with the name of the imported DLL.
FirstThunk	Contains the RVA of the Import Address Table (IAT). This is array of IMAGE_THUNK_DATA structures. ** This array is part of the import address table and will change*

The Demo

- UPX
- Xpack
- Spack
- Packman
- PESpin

Further Reading

- Anti-debug - http://pferrie.host22.com/papers/unp2011.htm
- Import Table - http://www.reverse-engineering.info/PE_Information/Understanding_ImportTables.pdf
- An In-Depth Look into the Win32 Portable Executable File Format, Part 2 - http://msdn.microsoft.com/en-us/magazine/cc301808.aspx
- http://www.codeproject.com/Articles/30815/An-Anti-Reverse-Engineering-Guide
- LUEVELSMEYER's The PE file format tutorial - http://net.pku.edu.cn/~course/cs201/2003/mirrorWebster.cs.ucr.edu/Page_TechDocs/pe.txt
- The art of unpacking - http://www.blackhat.com/presentations/bh-usa-07/Yason/Whitepaper/bh-usa-07-yason-WP.pdf

Thank you...

Contact Info:

Email: azlan.mukhtar@gmail.com

LinkedIn: http://my.linkedin.com/in/azlanmukhtar

F-Secure

Protecting the irreplaceable

F-Secure