Malware Reverse Engineering Basic Knowledge

Andrea Mambretti (mambro007@gmail.com)

Politecnico di Milano

October 3, 2012

List of Tool

- Tool for Windows
- Linux Tool

(1) Tools Windows

- Dependency Walker http://www.dependencywalker.com
- LordPE http://www.woodmann.com/collaborative/tools/index.php/LordPE
- OllyDbg http://www.ollydbg.de
- PDF Tools http://blog.didierstevens.com/programs/pdf-tools/
- PE Explorer https://www.heaventools.com/
- PEiD http://www.peid.info/
- PE view www.magma.ca/~wjr/
- Process Explorer http://www.sysinternals.com/
- Process Hacker http://processhacker.sourceforge.net/

(2) Tools Windos

- Process Monitor `http://www.sysinternal.com`
- Regshot `http://sourceforge.net/projects/regshot/`
- Resource Hacker
  `http://www.angusj.com/resourcehacker/`
- Snort `http://www.snort.org/`
- Strings `http://www.sysinternals.com/`
- TCPView `http://www.sysinternals.com/`
- Tor `http://torproject.org`
- WinDbg `http://msdn.microsoft.com/`
- Wireshark `http://www.wireshark.org/`
- UPX `http://upx.sourceforge.net/`
- netcat `http://joncraton.org/media/files/nc111nt.zip`
- CFF Explorer `www.ntcore.com`

Linux Tool

- string
- Assemblatore : **as -a -o nome_oggetto.o nome_sorgente.s**
- Linker: **ld -o nome_eseguibile nome_oggetto.o**
- objdump
- file
- gcc
- gdb

Other Tool

- VirusTotal `http://www.virustotal.com/`
- VMware Workstation `http://www.vmware.com/`
- Some Test Malware
  `http://www.malwareanalysisbook.com`