Malware Analysis Write-Up

Introduction - Setting up the Virtual Machine

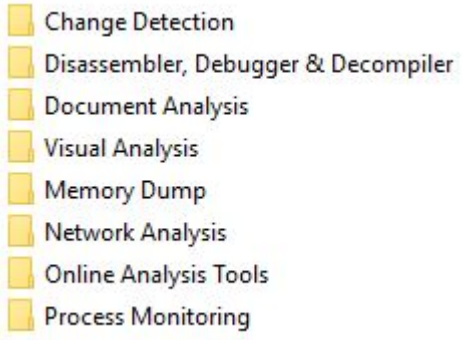
I'm beginning to research Malware Analysis and thought I would make a write-up based on everything I've been doing and the problems I have come across with hopefully the solution.

For my 'Malware Analysis Lab', I will be using Windows 10 Professional N, thanks to Sheffield Hallam University for Supplying the Licences. I chose Windows 10 Professional N because Windows 10, at the minute, is the most secure Windows OS which allows some flexibility with what the malware can actually do to my Lab VM i.e WannaCry – Could encrypt the OS if the user clicked the executable but couldn't be infected over SMB.

You may ask, "what's Professional N and what's the difference?". For Microsoft to get licensing in the EU, they had to create a version of Windows, from Windows XP N, that doesn't include some Microsoft packages like Microsoft Media Player, Movie Maker, Live Essentials etc. The Idea of Windows N was for Governments and Companies that don't require these packages. After this, you may also ask, "So why are you using it?". I'm using this version of Windows just for the pure fact that I won't need the other packages that comes with Windows. This Virtual Machine is purely just for malware analysis so I won't need the extra applications wasting space. It is very rare if a piece of malware exploit windows media player or live essentials.

For my virtual machine, I'm using VMware Workstation, again thank you SHU, because it allows me to use Snapshots. Snapshots are going to be crucial with malware analysis, as it allows me to restore my virtual machine back to stock before the malware was executed. I also know that VirtualBox allows Snapshots and doesn't cost a thing. But this shows after trying to install 3 versions of Windows 10 and not even getting past the installation boot screen.

I have setup some basic malware analysis tools which will be included in the snapshot (Saves me having to download the same files over and over again). These applications cover different ranges of analysis. These include



Change Detection

For change detection I have a few applications. One application, flypaper, recommended by a brilliant malware analyst called Collin Hardy(@Cybercdh). Flypaper stops applications trying to close or delete files which allows you to dig deeper into potential unencrypted

applications and even more processes. My second application, is RegShot. RegShot monitors any changes in in the registry.

Disassembly, Debugging & Decompiling

My disassembler of choice is IDA5 Pro (Freeware). This version of IDA is old and is a legacy version of IDA but it's free, if Sheffield Hallam had a licence for IDA, I'd be all over it but unfortunately, I don't have the money to fork out just for IDA. If I believe it is too old to use I will use an Open-Source solution.

For Debugging, I'm using OllyDB again because it's free but I've used it before when reverse engineering so I feel comfortable using it.

Decompiling, the decompiler I'm using is called ILSpy; again free and open source *(You can find it here at http://ilspy.net/)*. I believe is important because given the correct application with very little to absolutely no obfuscation, a decompiler will give you far more information than any Disassembler will because you have the raw code. You can recreate the code, find vulnerabilities and maybe find basic actions to stop or sinkhole the malware. This can be found in a disassembler but it's in plain text in a decompiler.

Alongside these applications I use Easy-Identify. This is used to identify application wrapping/obfuscation on an application. This will allow me to have a chance unwrapping the application which will allow me to disassemble or decompile the malware.

Document Analysis

At the minute, the only document analysis application I have is PdfStreamDumper, this dumps all the data in a PDF, if a file has a hidden script, the script will be dumped allowing you to do further analysis.

Visual Analysis

As a visual way of viewing malware, I'm using procDot. procDot is both a process manager and wireshark but displays the output as a graph giving you a visual representation of timing for each process, injection detection etc.

Memory Dump

Memory dumping is important for malware analysis. This is because, like DRM on games, malware will run some processes in memory unencrypted. If you dump that information you're given an encrypted, unwrapped and potentially source code (e.g. batch file, powershell or command prompt script etc).

Network Analysis

Network Analysis is a little simpler than disassembly, debugging & decompiling. I only have 2 applications for networking which are Wireshark. No brainer, right? It's free and it allows me to filter through all the network traffic coming in and out of my virtual machine while looking pretty and not having to deal with terminals like TCPDump, not that there is anything wrong with terminals just easier to read.

The second application I have is called GlassWire, this application does cost a small charge but I use this on my personal computer anyway. GlassWire monitors network changes and will give you a description telling you what application has established a new connection and where, DNS changes and also monitors the Windows Host file. If the Host file has changed it will alert you immediately telling you which program has changed the host file. All this information comes with a timestamp and labelled with a colour depending on if its normal activity, questionable activity and suspicious activity.

Online Analysis

This section is just some helpful links that can be used. The websites are listed below:
Anubis
EUREKA
Malwr
ThreatExpert

Process Monitoring

Because applications can run multiple 'hidden' processes, I have chosen ProcessHacker because it is my preferred process monitor; It allows you to see far more information compared to windows process manager and it allows you to force kill an application if needed.

My introduction post has been a very long post but anyone can just have tools without knowing how to use them and a good starting point for my malware analysis journey is to understand my 'weapons' and tools. Any feedback is appreciated and any pointers to help me along the way is greatly appreciated too :)