MALWARE ANALYSIS

Windows analysis enviroment

I've conducted a basic **static** analysis on 3 malicious PE samples. The files are stored on a windows machine accessible via the THM learning platform. The same windows enviroment is set up with some specific tools that I've used in different stages.
I firstly analysed the **MD5 checksum** to see if they have been recorded on VirusTotal. After that, I identified if the PE samples have been obfuscated or packed with known softwares using **PE ID**. I have then proceed attempting to disassemble the files and veiw the imports with **IDA Freeware**. I finally analysed the strings and, once more, the imports with **PE explorer**.

Outcome
Upon completion of this introductory module I fully understood the importance of malware analysis and the impact that malware campaigns have on the current Cyber Security scenario. I therefore understoond the ultimate process of a malware attack and malware campaigns targeting. I have studied and understood the difference between static and dynamic analysis, and ultimately, I have gained a brief knowledge of some techniques and tools used throughout malware analysis.

1. Introduction

1.1 Purpose of Malware analysis

Not only is malware analysis a form of incidence response but it is al useful to gain an understanding of how a specific piece of malware functions so that defenses can be built to protect an organization's network.
When analysing malware it is important to take to consider the followig

- Point of Entry
- Indicators that the malware has been executed
- How does the malware perform
- Can we prevent/detect further infection?

1.2 Malware Campaigns

Despite the many variants of malware, attacks can generally be classified into two types: Targeted and Mass Campaign.

Targeted
A "Targeted" attack is just that - targeted. In most cases, malware attacks that occur this way are created for a specific purpose against a specific target. A great

example of this type of purpose could be the DarkHotel malware, whom is designed to steal information such as authentication details from government officials.

Mass Campaigns
On the other hand, the "Mass Campaign" classification can be akin to many real life examples, and is the most common type of attacks. The entire purpose of this type of Malware is to infect as many devices as possible and perform whatever it may - regardless of target.

1.3 2022 Ukraine Cyber attacks

On 14 January 202, a cyberattack took down a dozen of Ukraine's government websites during the 2021-2022 Russo-Ukrainian crisis. According to Ukranian officials, around 70 government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers, and Security and Defense council, were attacked. A month later, another attack took down multiple government and bank services.

1.4 Malware attack process

The ultimate process of a malware attack can be broken down into a few broad steps and these steps will generate lots of data!

- ***Delivery***: This could be of many methods, to name a few: USB (Stuxnet!), PDF attachments through "Phising" campaigns or vulnerability enumeration.

- ***Execution***: Here's the main part of how we classify Malware. What does it actually do? If it encrypts files - it's Ransomware! If it records information like keystroke or displays adware - we can classify it as Spyware

- ***Mantaining persistence***: It wouldn't make much sense for Malware authors to go through all the trouble of developing a piece of code that is capable of execution - just for it to execute and that's it...Gone

- ***Propagation:*** If you can infect one device, why not trying to infect more?

In Summary, there are two categories of fingerprints that malware may leave behind on a Host after an attack:

- ***Host based Signatures:*** These are generally speaking the results of execution and any persistence performed by the Malware. For example, has a file been encrypted? Has any additional software been installed

- ***Network-based Signature:*** At an overview, this classification of signatures are the observation of any networking communication taking place during delivery, execution and propagation.

1.4 Static vs Dinamic Analysis

- ***Static Analysis:*** At its core, this method is of the analysis of the sample at the state it presents itself as, without executing the code.

- ***Dinamic Analysis:*** "Dynamic Analysis" essentially involves executing the sample and observing what happens.

2. Static Analysis
MD5 Checksum

The md5 Checksum analysis is the first step I took with 3 samples. MD5 "Checksums" are cryptographic "fingerprints" of the files. This allows a uniformed identification throughout the community - especially with automated Sandboxes. The 3 files in question are:

- **aws.exe**
- **NetLog.exe**
- **vlc.exe**

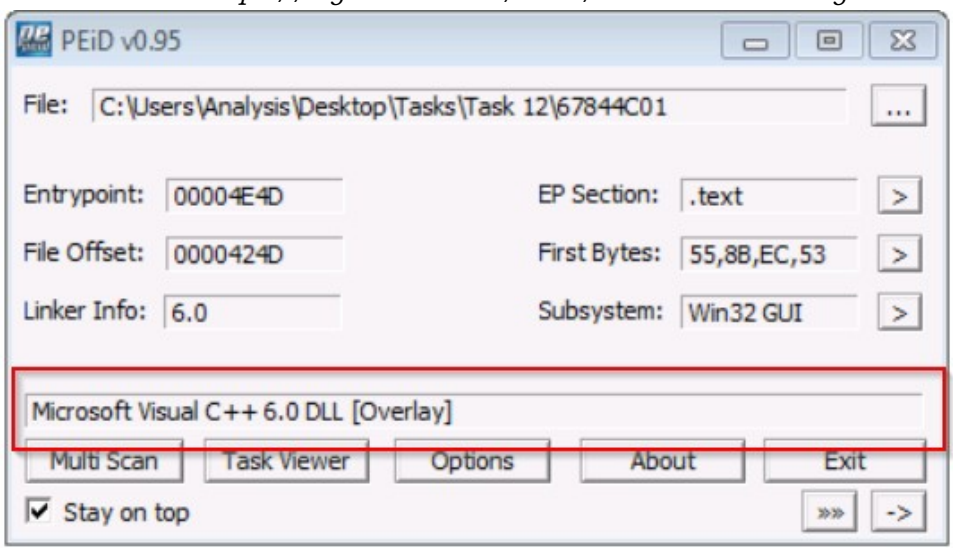
Anyone can rename an executable and give it a well-known and safe software name. For this reason we need to analyse the genuinity of the files by analysing the checksum.
An **Hash Tab** application has been installed and we can see the checksum by simply right-clicking the file and select **Properties**.
We open the **File Hashes** tab and we copy and paste the checksum in VirusTotal to see if they have been reported previously within the community. The reserach would eventually give us a negative result.

3. Identify the compiler/packer
PEID

3.1 What is obfuscation/packing?
Packing is one form of obfuscation that malware Authors employ to prevent the analysis of programmes. There are both legitimaten (protection of intellectual property) and malicious reasons (Preventing analysts to revert and understand the program) as to why the Author of a program will want to prevent the decompiling of their program.

3.2 Compiler analysis
This operation is pretty easy and it only envolve the use of a software called PEID. If drag and drop the file into the software we'll be able to see what compiler or packer has been used.

Source: https://tryhackme.com/room/malmalintroductory



4. Visualise a packed code
IDA Freeware

Whilst PeID is capable of detecting the possibility of packers being used, it is not able to automatically de-obfuscate them.
It's time to make use of a disassebler called Ida Freeware. The operation is the same as we did with PEID, we select the file we want to analyse and then we open the TAB we interested on. In this case we'll look at the **Imports** tab.

4.1 Disassembler

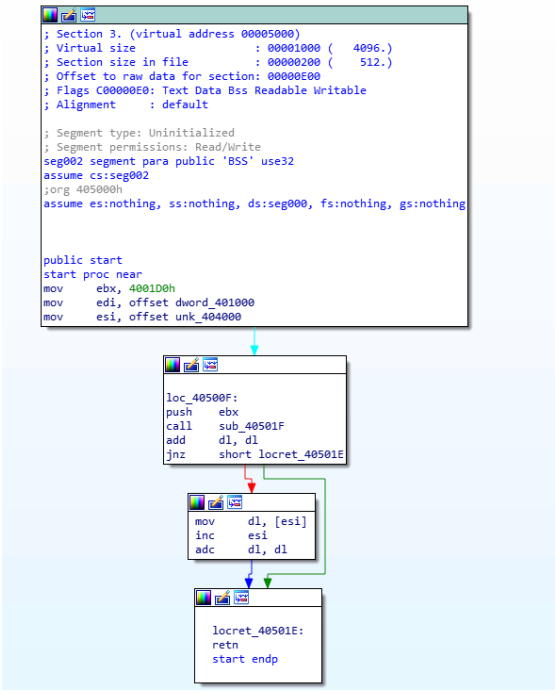
Disassemblers reverse the compiled code of a program from machine code to human-readable instructions (assembly). This is limited to how the program represents itself in its current state! I.e. If the contents of an executable changes during execution - "Disassemblers" will not reflect this

4.2 Imports

Imports are the functions that a piece of software (in this case, the backdoor) calls from other files (typically various DLLs that provide functionality to the Windows operating system).

4.3 Visualization

Essentially, we can see the flow of how the program executes - indicated by the arrows. The problem? There's very little here! And we can also see there are 2 imports only!



Source:
https://tryhackme.com/room/malmalintroductory

5. Further Imports Analysis
PE Explorer

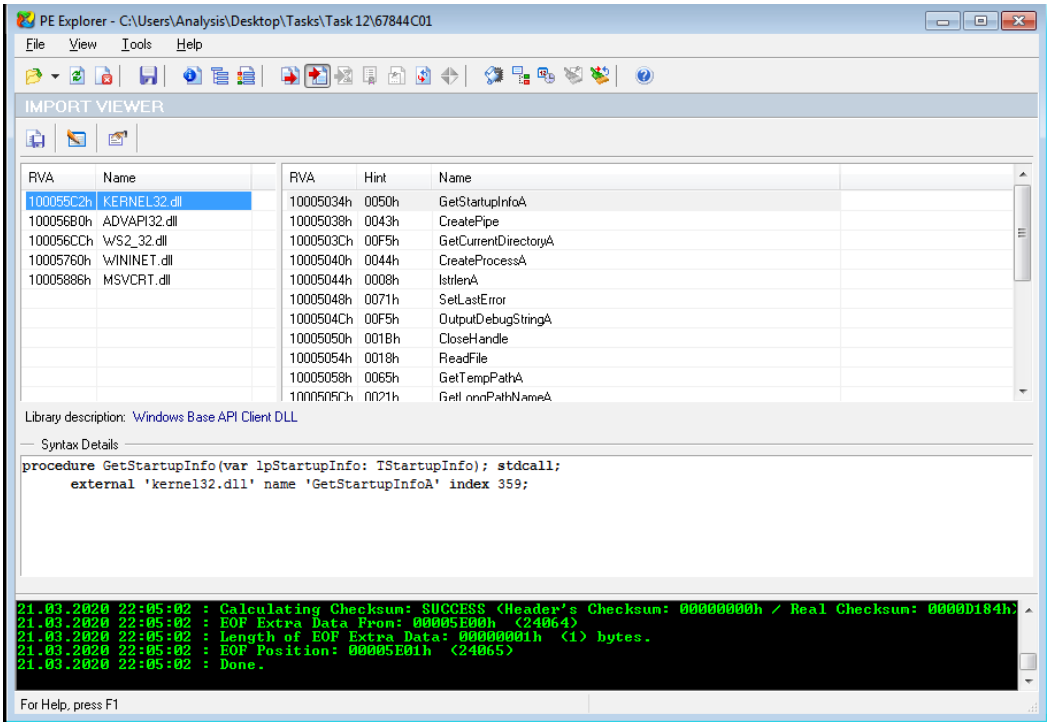
5.1 What are strings?

"Strings" are essentially the ASCII / Text contents of a program...this could be anything from passwords for self-extracting zips, to bitcoin addresses in ransomware samples. when analysing the contents of these strings, we can sometimes paint a fairly indicative picture of the behaviours of the programme - bitcoin wallets being used in ransomware.

5.2 Visualize strings/imports

Making use of an application called PE explorer we can easily see the strings and imports contained in the files. Once again we can see that only few imports are shown.

Source: https://tryhackme.com/room/malmalintroductory



6. Resources

Kaspersky – Malware Campaigns
https://www.kaspersky.co.uk/resource-center
Mandiant - Imports
https://www.mandiant.com/resources
Malwaretips – Imports
https://malwaretips.com/threads/malware-analysis-2-pe-imports-static-analysis.62135/
Tryhackme
https://tryhackme.com/room/malmalintroductory

BrightTALK – Russia cyber activity
https://www.brighttalk.com/webcast/7451/527124?utm_source=Mandiant.com&utm_medium=web

Credit
Alessio Ragazzi,
London