7th Lab - Windows malware

Rodrigo Castillo and Juan Esteban Murcia

20 de septiembre de 2020

1. Read the introduction to the Section .ªnalyzing Malicious Windows Programs.ªnd explain why is it important to know the details of Windows OS (Windows API, user/kernel mode, execution of code outside a file)?

As a computer science student, is important to know details about Windows OS because is the most used operating system , as a forensics investigator, is important because most of the malware works for windows, somethimes, malware will use those libraries and services making the aknowledgment of those libraries really important for understanding and studyng malware and how it works.

2. Read the section "The Windows API.ªnd identify which are the Windows API Types

.

types of windows api:

- WORD: is a unsigned 16bit value .
- DWORD: is a unsigned 32bit value .
- HANDLES: is a reference to an object , is not documented so it should only be managed by windows APIs.
- Long Pointer is a pointer to another type of variable.
- Callback represents a function that is going to be called by a windows API.

3. Read the section "File System Functions.ªnd explain the difference between shared files and files accesible via namespaces

shared files are special files which paths looks like $//nameserver/share$ **or** $//?/nameserver/share$. the symbol tells the operating system to not parse the string, in order to access longer filenames.

Files accesible via namespaces: namespaces can be understood as the number of a folder, each one store different type of objects.
lowest namespace is called **NT** and it has access to all devices and all namespaces exist inside **NT** .