Lab 1

*Lab01-01.dll and Lab01-01.exe*

* 32 engines detected the DLL file as being malicious.
* 40 out of 70 engines detected the EXE as being malicious.
* The DLL file was compiled at: 2010-12-19 at 16:16:38.
* The EXE file was compiled at: 2010-12-19 16:16:19.
* Both compiled within less than a minute from each other.

DLL Table:

|  |  |  |
| --- | --- | --- |
| **Name** | **Virtual Data** | **Raw Data** |
| .text | 926 | 4096 |
| .rdata | 147398 | 147398 |
| .data | 108 | 4096 |
| .reloc | 516 | 4096 |

* Usually the virtual size is smaller than the raw data.
* This is due to the file section being padded out to the next boundary, containing unnecessary data.
* Seeing as we can see the raw data size is larger, there are no indications that the file is packed or obfuscated.

EXE Table:

|  |  |  |
| --- | --- | --- |
| **Name** | **Virtual Data** | **Raw Data** |
| .text | 2416 | 4096 |
| .rdata | 690 | 4096 |
| .data | 252 | 4096 |

* There are no signs that the EXE is obfuscated or packed.
* The DLL file contains imports: KERNEL32.dll, MSVCRT.dll and WS2\_32.dll.
  + The KERNEL32.dll informs us that this DLL can open and manipulate processes.
  + MSVCRT.dll contains standard C library functions such as printf, memcpy and cos.
  + The MS2\_32.dll is a network DLL which carries out network-related tasks. This malware could be some type of backdoor / information-stealing malware as the imports indicate that this DLL has the ability to send data over a network.
* The EXE file contains imports: KERNEL32.dll and MSVCRT.dll.
  + FindFirstFileA, FindNextFileA, CopyFileA and CreateFileA are functions that allow the malware to find files, along with copying and creating new files.
  + THE MSVCRT.dll indicates that this malware has the ability to perform network-related tasks and could allow a user backdoor access to the system.

1. Examine C:\Windows\System32\kerne132.dll for additional malicious activity. Note that the file kerne132.dll, with the number 1 instead of the letter l, is meant to look like the system file kernel32.dll. This file can be used as a host indicator to search for the malware.
2. The .dll file contains a reference to local IP address 127.26.152.13. This address is an artefact of this program having been created for educational and not malicious purposes. If this was real malware, the IP address should be routable, and it would be a good network-based indicator for use in identifying this malware.
3. The DLL is most likely a backdoor, the EXE file is used to install or run the DLL as DLLs are unable to run on their own.