Lab 06-03.exe – Malware Analysis Report

Table of Contents

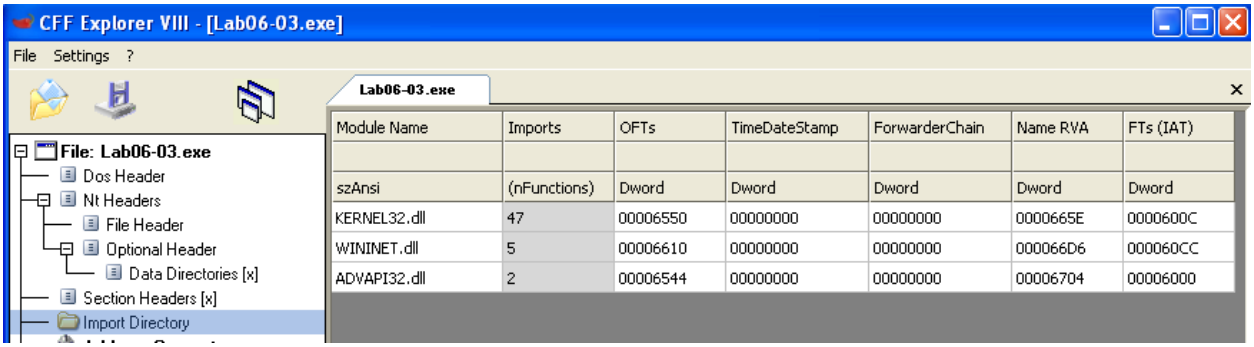
1. Static Analysis

1.1. Preparation

Before conducting the static analysis, this being the first malware sample I have investigated in this course, I needed to download and push all of the necessary tools (and malwares samples themselves) to the VM network. The VM was created in such a way that it was isolated from the host machine and local area network as to not risk contamination from the malware.

1.2. CFF Explorer

The initial findings that were made for static analysis was through a tool called CFF Explorer. I found some imported .dll's (see screenshot):



Upon further research, these DLL's were responsible for the following:

- KERNEL32.dll - Used for file manipulation, memory allocation and the creation of processes and threads
- WININET.dll - Used for establishing HTTP or FTP connections with web servers
- ADVAPI32.dll - Used for modifying Windows registry. Can be used in escalating privileges and adjusting other security settings.

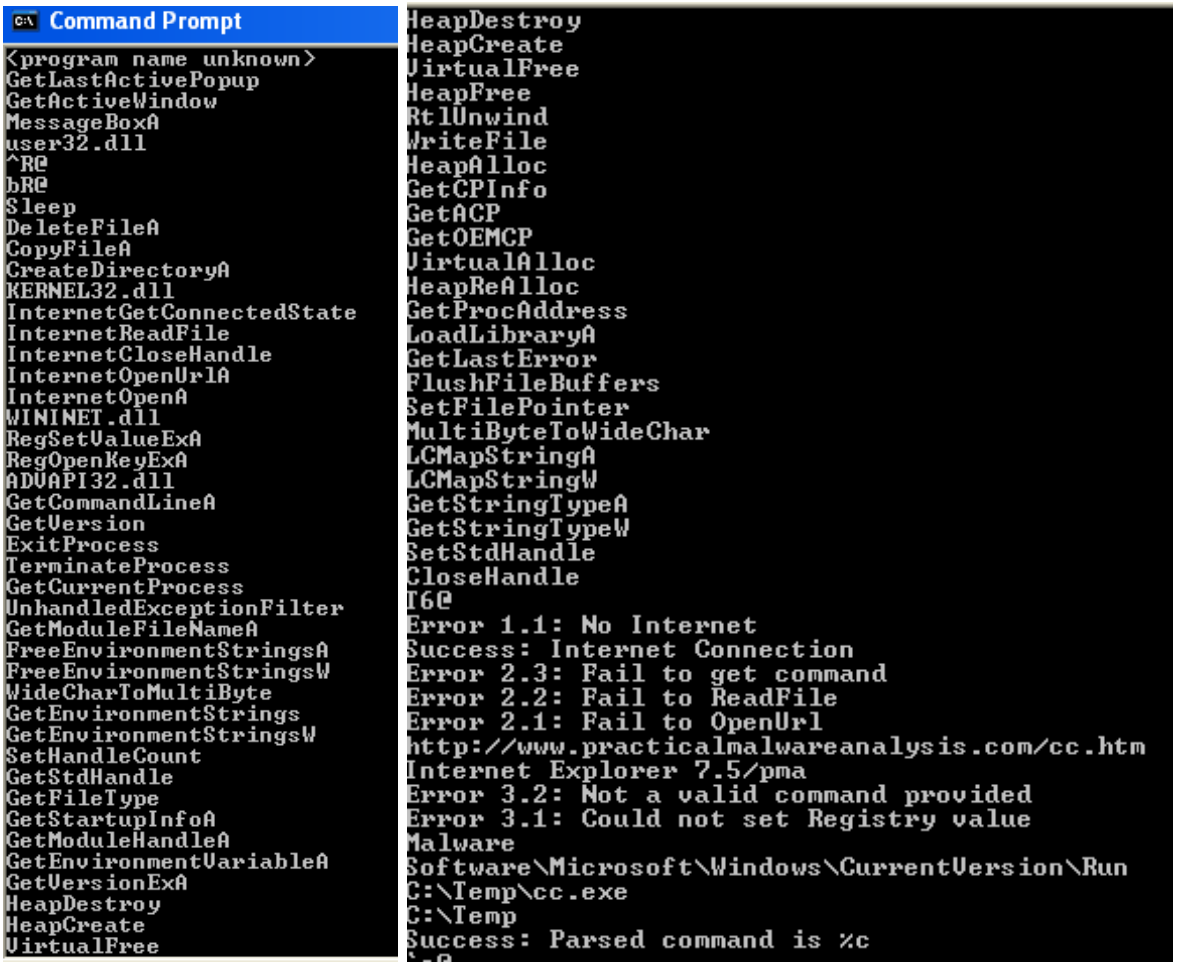
From looking over the libraries which are imported by this malware sample, I have some initial ideas for what the malware may be intending to utilize from them:

- Modifies Windows registry (via ADVAPI32.dll) to enable execution at startup and hide itself from the user.
- Establishes HTTP/FTP connections to remote servers (via WININET.dll) for:
    - Downloading additional payloads.
    - Exfiltrating data.
    - Receiving attacker commands.
- Performs file and memory operations (via KERNEL32.dll) to:
    - Modify system files.

- Launch processes or threads for malicious payloads.

1.3. SysInternals Strings

The next tool I utilized was Strings from Microsoft SysInternals. When running strings into Lab06-03 we make some more interesting findings:
File Operations: There are many function calls that are noteworthy and indicate file manipulation. A few are:
DeleteFileA, CopyFileA, CreateDirectoryA, RegSetValueExA, InternetOpenUrlA, InternetReadFile, InternetCloseHandle. Particularly of note the RegSetValueExA could be indicative of the malware or the changes its making attempting to persist within the system. The internet calls are strong indicator of the malware communicating through a command-and-control server, which is further proven in the next finding.
URL - http://www.practicalmalwareanalysis.com. This URL points to what we could assume to be the potential command-and-control server.



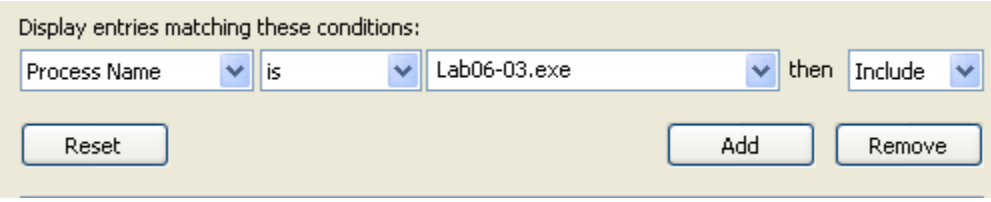
2. Dynamic Analysis

2.1. Preparation

Before running the malware, I took a snapshot of the current VM state to return to after analysis. This ensures that no malware functions will linger on the virtual machine after testing has concluded. I also installed multiple tools, such as Wireshark and FakeNet which are crucial for capturing any network activity, which from the static analysis is to be expected.

2.2. Process Monitor (ProcMon)

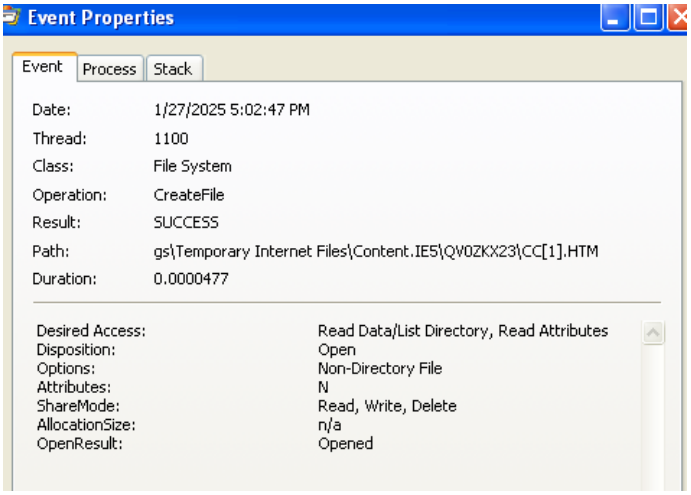
The primary tool used in discovery of the functionality of this malware was Process Monitor or ProcMon. I began a capture of the processes and then ran the lab06-03.exe file, after giving some time for the program to run, I stopped the capture and filtered for only captures with the Process Name of the malware:



This yielded many results that I sifted through, there were a few that I found particularly noteworthy. The first was the Image Loads of many .DLL's, some of which were mentioned in the static analysis:

12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\wininet.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\advapi32.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\rpcrt4.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\secur32.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\crypt32.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\msasn1.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\msvcrt.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\user32.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\gdi32.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\oleaut32.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\ole32.dll
12:33:...	Lab06-03.exe	1268	Load Image	C:\WINDOWS\system32\shlwapi.dll

We also see the creation of the cc.htm file which was references when we ran Strings.

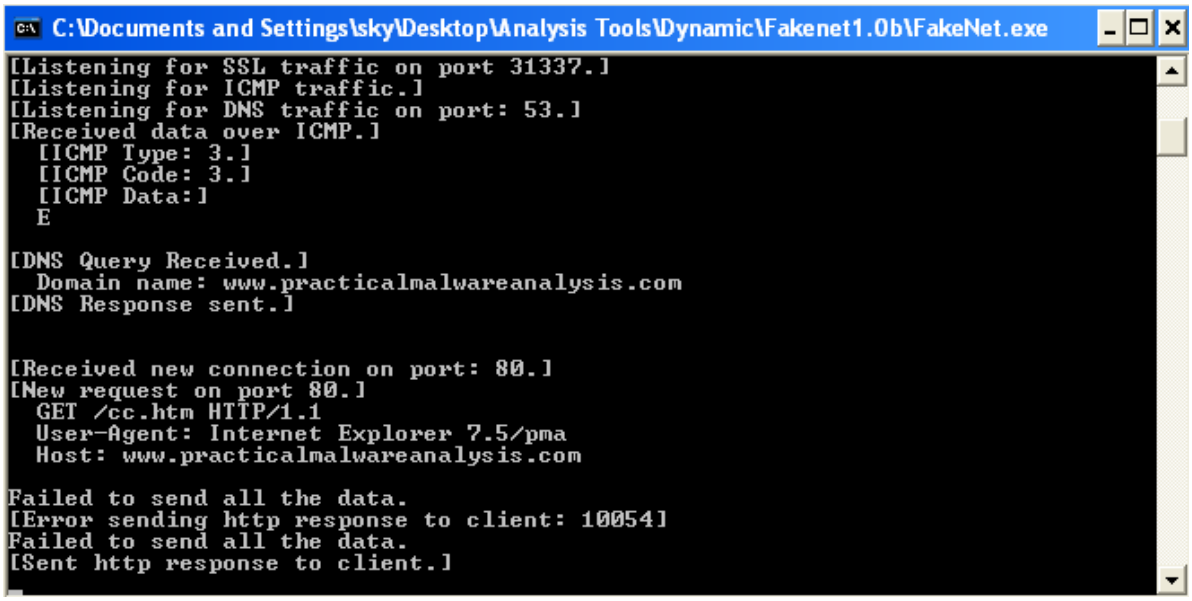


2.3. FakeNet

FakeNet intercepted malware communication attempts with www.practicalmalwareanalysis.com, confirming C2 behavior.

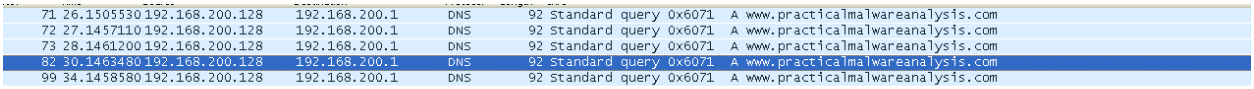
Analysis suggests:

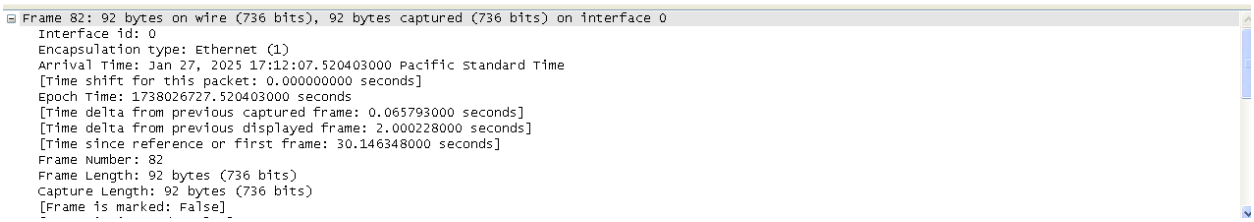
- Possible periodic beaconing.
- Attempted retrieval of commands or payloads.
- Exfiltration of data through HTTP requests.



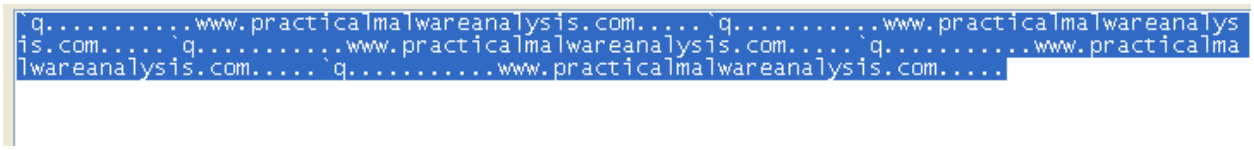
2.4. Wireshark

On top of the communication intercepted by FakeNet. We can view the packets in Wireshark which show further information about the Command and Control Communication:





With a followed UDP stream yielding the following:



3. Conclusion of Analysis

The executable **Lab 06-03.exe** is a piece of malware with multiple functionalities aimed at system persistence, network communication, and potential data exfiltration. Through static analysis it was determined that Windows libraries, such as ADVAPI3.dll, WININET.dll and KERNEL.dll were utilized. The use of these libraries, which contain registry modification functions suggest that the malware will continue it's execution even upon system restart.

Our earlier hypothesis of a C2-network and directory manipulation were also confirmed through the findings of Strings from SysInternals (see function calls such as InternetOpenUrlA and DeleteFileA). The URL that is to be utilized by this malware was also snagged by Strings, which we found to be http://www.practicalmalwareanalysis.com.

Dynamic analysis later confirmed that this C2 server was attempted to be connected to upon running the malware. Furthermore, this malware sent a GET request for the file cc.htm in it's connection with the C2 server. This cc.htm file was later found, using ProcMon to be created by the malware itself. In summary, malware analysis confirmed the following functionalities of the lab06-03.exe sample:

- Modifying the registry for persistence.
- Connecting to an external C2 server for command execution.

- Creating and deleting system files to manipulate its presence.
- Exfiltrating potentially sensitive data over the network.