# Malware Analysis Report

1. Overview

1.1 File Information

|  |  |
| --- | --- |
| File Name | Keylogger.exe |
| File Size | 65 KB |
| Detection Name | Software-Based Keylogger/ Hookup Keylogger |
| Malicious Activities | * Tracks user’s keyboard with the scope of stealing data such as bank account information or any type of valuable information |
| Features | * Stores users input from keyboard in a specific text file * Is not detectable by most free antivirus software |

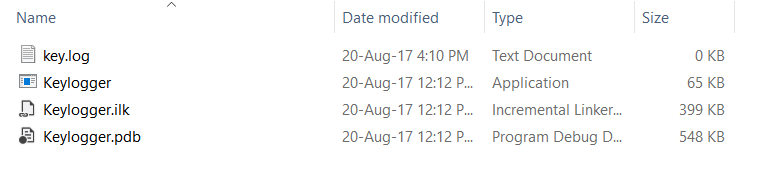
1. Analysis Result

2.1 Simple Analysis

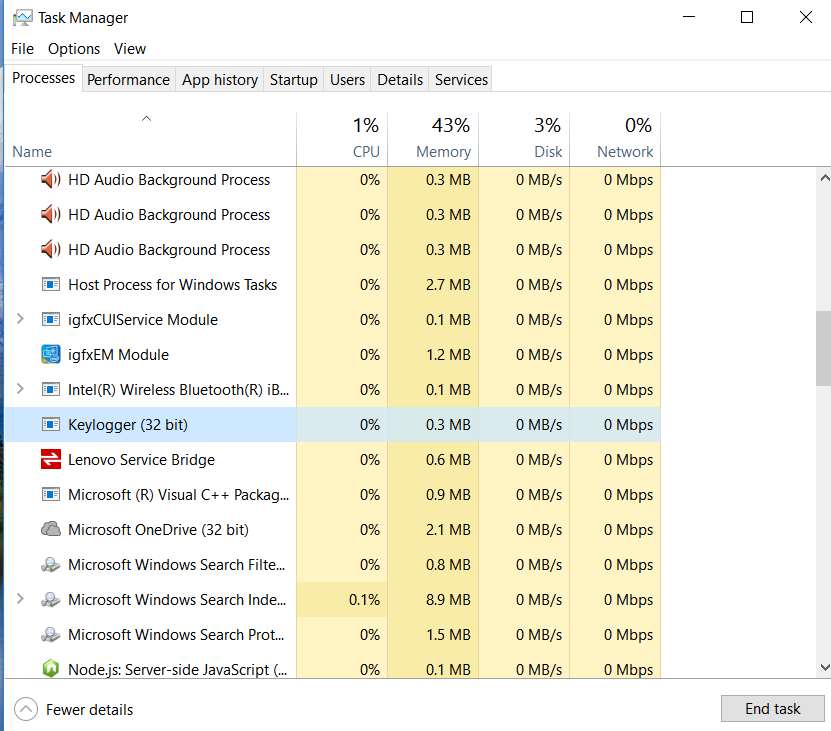
Keylogger.exe is classified with Hookup vulnerability of the Windows Operating System and allows the attacker to steal the keyboard input of the user and store it locally in a text file. In this report, the analysis was focused on the internal operation of the malicious code with his weakness of storing the data locally instead of making a DLL injection or to create a connection to the attacker’s server in order to send him the information that is stolen.

2.2.1 Deep Analysis of the Keylogger.exe

As I already mentioned the Keylogger.exe doesn’t make a DLL injection so the malicious activities are performed by the executable file itself. At this time, the text file where or the keyboard input is stored is created in the D drive with the name keys.log and if the D drive does not exist then the text file will be created on the C drive or at the same location as the executable file is located.

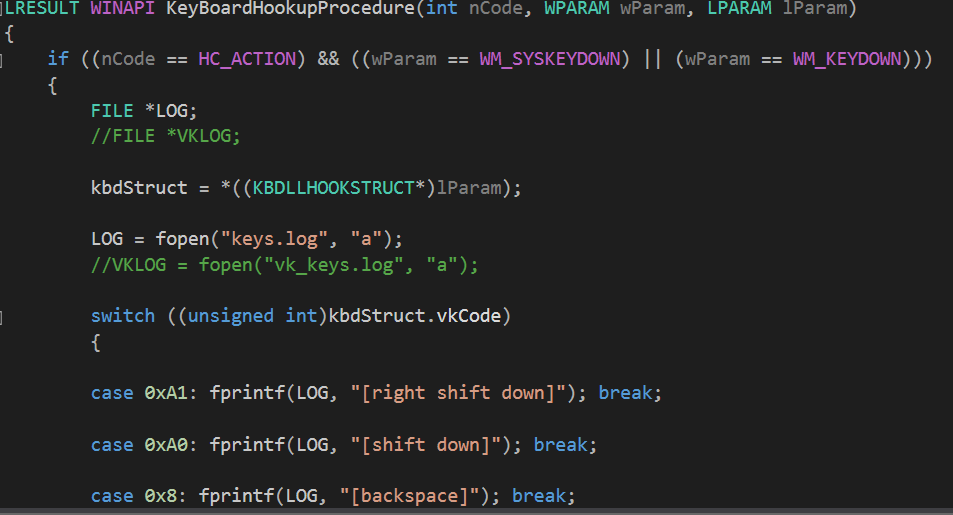


After the Keylogger.exe is executed a process called Keylogger is created and is visible in the task manager with the name Keylogger and the resource consumption is minimal so the user will not notify any change in the performance of their computer by any means.



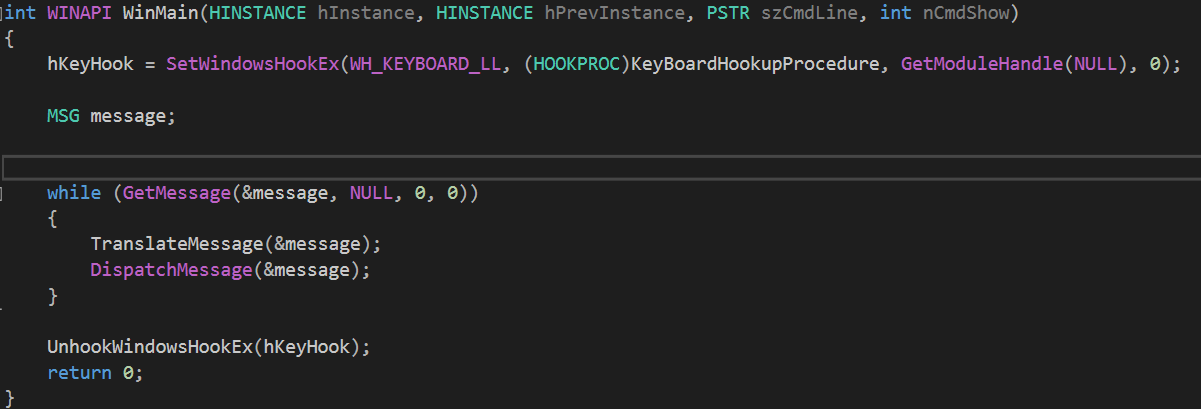
2.2.2 Deep analysis for the Hookup function

The function takes as parameters an int parameter of the keyboard code and the wParamater and lParameter that we already know that provide additional information in the message-handling mechanism of the window. The function checks whenever a key is pressed and determines the exact key by checking the code of the respective key to be equal or not to it’s ASCII Code in Hex. At the end of the function the next hook will be invoked.



After that, the function “WinMain” ensures that the user won’t notify then the malicious program starts by launching an invisible console window that takes as arguments the Hook-Procedure showed previously and the Module-Handler, witch is running all the time the computer is working but will not automatically start after a restart or a boot, which is another weakness of this malware.

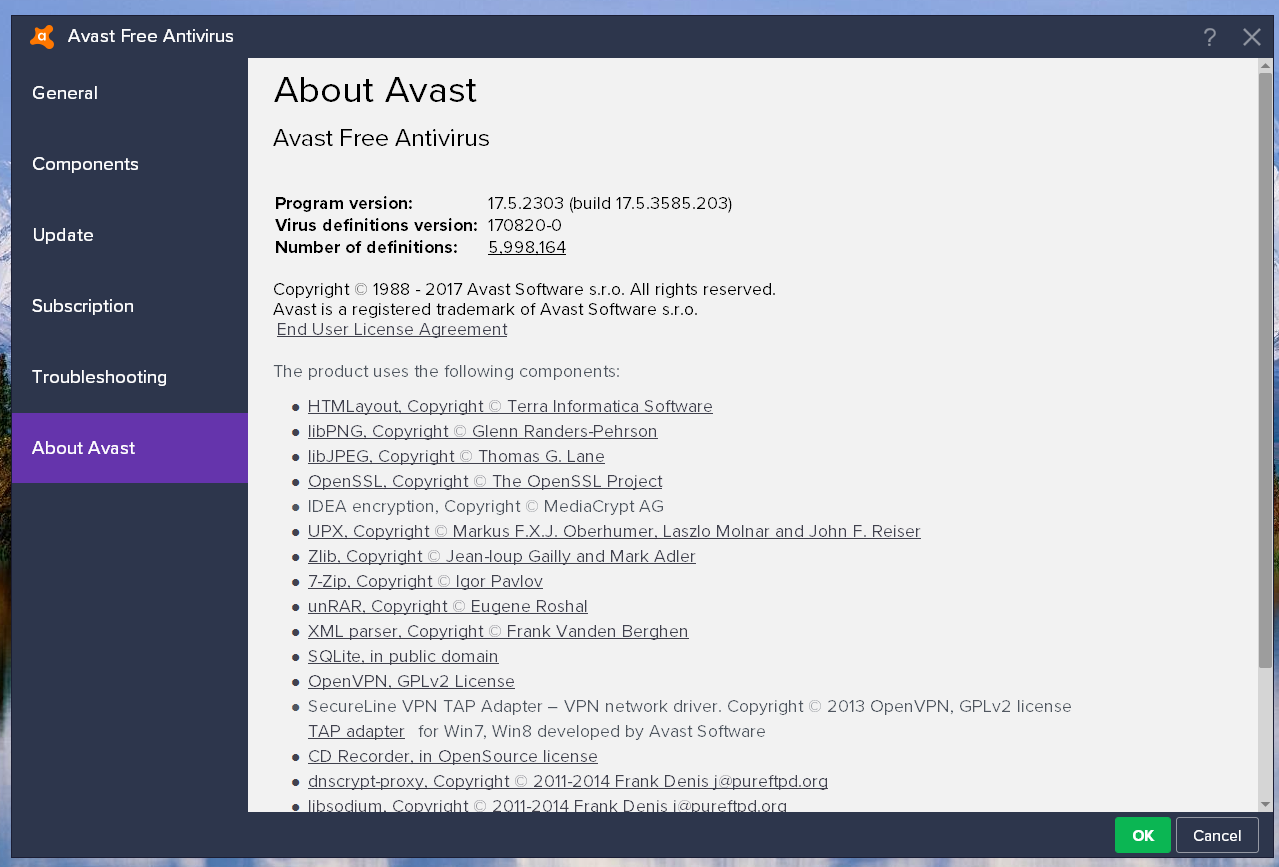
Also, the messages will be translated and dispatched in the log file.



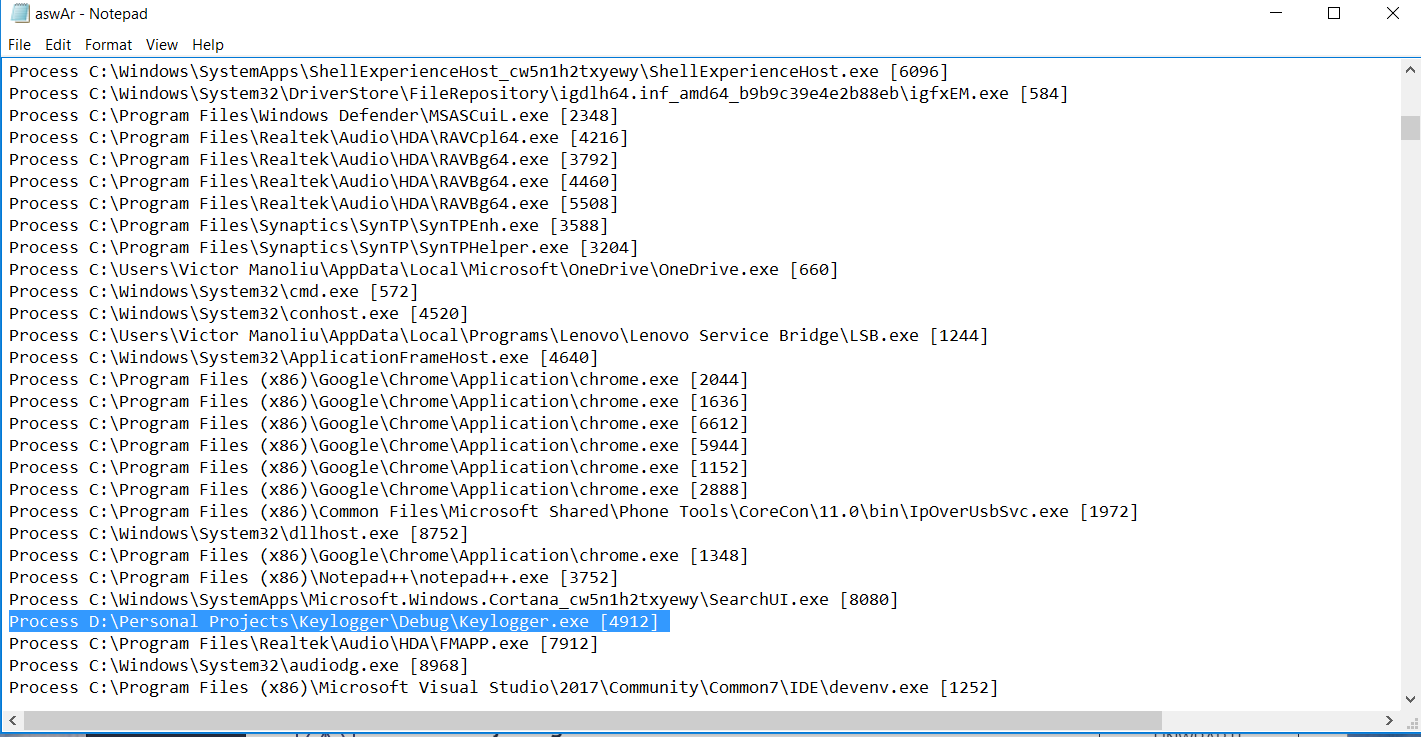
2.2.3 Antivirus Software Anti-Detection Software

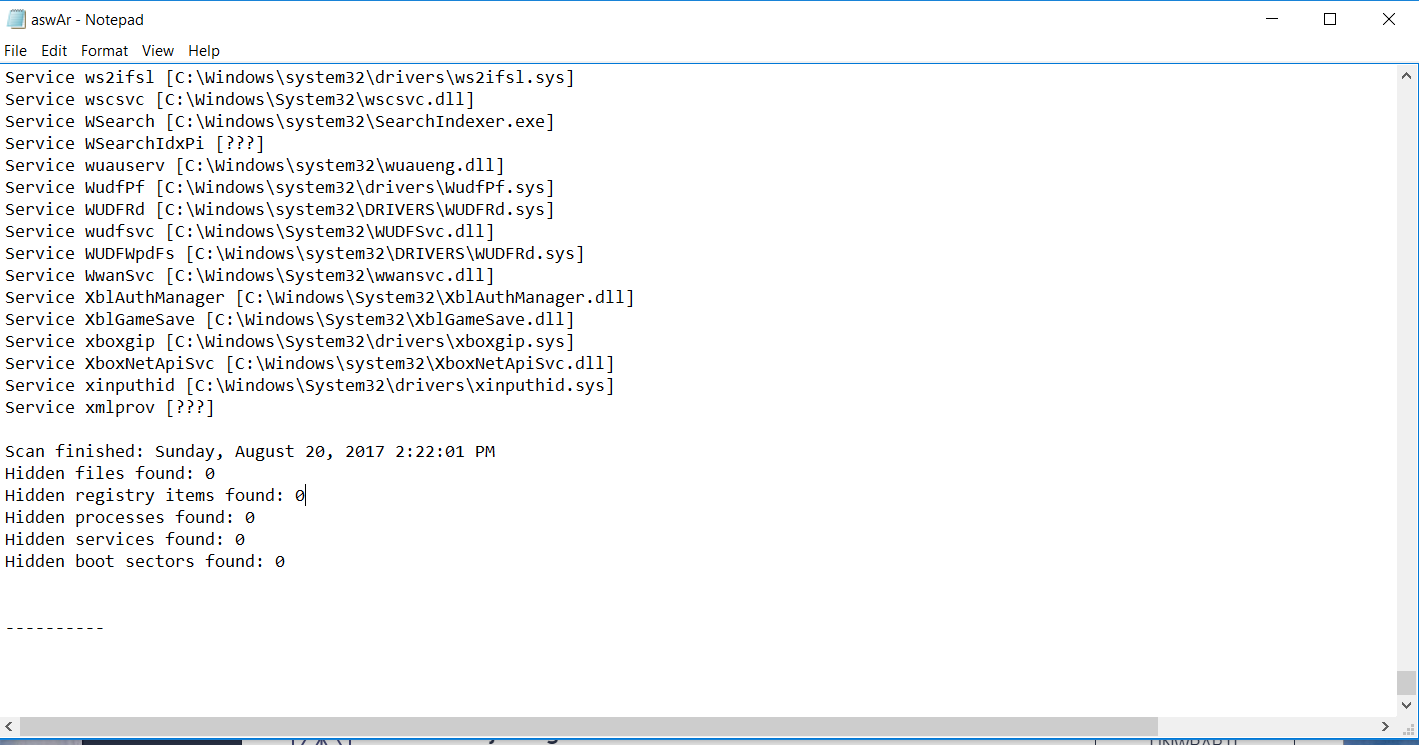
Even thought the Hookup functions will be the first to be detected by the antivirus software even the free version ones , this malware won’t be detected by even after the process has been created and running.

1. Avast Free Version



We can see in the picture below of the detailed raport of the scan that even thought we ran a Smart-Scan and the process was still running and tracking our keyboard input it was not detected as a malware or even potential infected or harm file and no action was taken by the software





1. Conclusion

Keylogger.exe is just a simple keylloger malware created with the C++ language with the purpose of learning and is not harmful for the user or the computer itself by any means because it doesn’t have a DLL injection or the ability to connect to an external concurrent server to actually transfer the data that the user is typing even thought it can be used as part of such mechanism.

4. Things to improve

Such mechanism would require this malware and another one to establish the connection between the user’s computers and the concurrent server and to search the location of the log file but that require a very good optimization in such way that the program that is responsible of establishing the connection to not be detected by the antivirus software and also to not use many resources. That would require an injection of a DLL file in the firefox.exe or chrome.exe process and after is loaded to intercept the “GetMessage()” API and log the key presses to a temporary file that will be uploaded to the attacker’s server using the pipe communication.

For more information or feedback, please contact me using the details below:

Victor Manoliu

Tel : 0752094300

Email : [victormanoliu97@gmail.com](mailto:victormanoliu97@gmail.com)