Table of Contents

1. Introduction

Definition of keyloggers.

A keylogger is a form of surveillance technology that can monitor and record each keystroke made on a particular computer. It is sometimes referred to as a keystroke logger or keyboard capture, depending on the context. It is also possible to install keylogger software on mobile devices like the Apple iPhone and Android-based gadgets, among others. In order for hackers to obtain personally identifiable information (PII), login passwords, and sensitive organisational data, keyloggers are frequently employed as a spyware weapon. There are a few applications for keyloggers that may, to differing degrees, be seen as ethical or appropriate. Keylogger recorders can also be used by employers to monitor the computer activities of their employees, parents to monitor the internet usage of their children, device owners to monitor any potentially unauthorised activity on their devices, law enforcement agencies to investigate incidents involving computer use, and so on. (Gillis*, What is a keylogger? definition from searchsecurity* 2021)

A keylogger's primary purpose is to monitor and record your keystrokes before sending those logs in some form or another to the person who installed the keylogger on your computer. The fact that most of your interactions with your computer and with the people you communicate with via your computer are mediated through your keyboard means that the range of potential information that a snooper can acquire by using this method is truly vast. This range of information includes everything from passwords and banking information to private correspondence.

Some keyloggers not only record the text that is typed but also spy in a variety of different ways in addition to capturing the keystrokes that are typed. It is possible for more sophisticated keyloggers to Log clipboard text, which records information that you cut and paste from other documents; Track activity, such as opening folders, documents, and applications; Take and record randomly timed screenshots; and even Request the text value of certain on-screen controls, which can be helpful for grabbing passwords. (Fruhlinger, *Keyloggers explained: How attackers record computer inputs* 2022)

Types of Keyloggers

Keyloggers can be either hardware- or software-based, depending on how they collect data. Keylogger tools are all essentially built for the same thing. However, they are fundamentally different in terms of both their methodologies and physical design.

A hardware-based keylogger is a small hardware device that plugs into the keyboard and steals data. It is easy for someone who wants to monitor your activity to hide this device

because it appears like a regular PS/2 keyboard connection, computer cable, or USB adapter.

Keylogger software may be installed on a computer even if the attacker does not have physical access to the machine. A person who wishes to keep tabs on a computer can download it on deliberately, or it might be installed secretly as part of a rootkit or a remote administration Trojan (RAT). (Popovici, *What is a keylogger? definition, types, examples and prevention* 2022)

Hardware Based Keyloggers

A Hardware-Based keylogger has to be physically inserted into a computer or installed nearby the targeted machine. Due to this, direct access is required, which is a difficult task that is often accomplished using social engineering tactics or a compromised insider.

A keylogger that is based on hardware can include recording devices that can be inserted in the wiring of the keyboard itself. Alternatively, a keylogger might be designed to look like a USB thumb drive and slid into a port on a laptop or a computer. There are additional devices on the market that are capable of recording the Bluetooth conversation that takes place between a wireless keyboard and a computer.

An acoustic keylogger is a particularly exotic type of keylogger that has been tested in the lab. This type of keylogger is able to discern with amazing precision what you are typing only solely on the sounds that your fingers create while they are on the keys. The concept of third-party recording, which simply consists of a camera being covertly aimed at your screen and keyboard, which is one of the simpler form of Hardware based Keyloggers. (Fruhlinger, *Keyloggers explained: How attackers record computer inputs* 2022)

It's possible for a hardware keylogger to appear in the shape of a module that's meant to be put right inside the keyboard itself. When the user writes on the keyboard, the keylogger records each keystroke and stores it as text on its own hard drive. The memory capacity of the keylogger's hard drive might be as high as several gigabytes. There is another type of wireless keylogger known as a wireless keylogger sniffer. This type of wireless keylogger sniffer is able to capture and decode data packets that are sent between a wireless keyboard and its receiver. (Gillis, *What is a keylogger? definition from searchsecurity* 2021)

Software Based Keyloggers

These are programmes that are installed on your device and record everything you do, including the keystrokes you type.

A user mode keylogger, often known as an API-level keylogger, is perhaps the most popular variety of keylogger software. Although these programmes do not have administrator capabilities, they are nonetheless able to intercept information that is being broadcast via the application programming interfaces (APIs) that are responsible for allowing various apps to accept input from the keyboard. These keyloggers monitor GetAsyncKeyState or GetKeyState API methods on Microsoft Windows and utilise a DLL to capture the data that they gather.

Once they are installed, kernel-level keyloggers get their hooks into the operating system itself, making it more difficult to detect and remove them. However, creating and installing these keyloggers is more complex than other types of keyloggers. On the other end of the spectrum are screen scrapers and browser-level keyloggers. Screen scrapers do not log keystrokes but rather use the computer's screenshot capabilities to record onscreen text. Browser-level keyloggers can only detect text entered into a browser form; however, given how much of our online life takes place within a web browser, this is still a pretty dangerous. (Fruhlinger, *Keyloggers explained: How attackers record computer inputs* 2022)

The files that make up a standard software keylogger are a dynamic link library (DLL) file that actually accomplishes the recording and an executable file that both installs the DLL file and prompts it to start recording. These files are typically installed in the same directory together. The keylogger software keeps a track of every keystroke that is typed by the user and sends the information to the person who originally installed the programme through the internet at regular intervals. Hackers are able to develop software that logs keystrokes by employing keyboard application programme interfaces (APIs) from one application to another, malicious script injection, or memory injection. (Gillis, *What is a keylogger? definition from searchsecurity* 2021)

History of Keyloggers

The usage of keyloggers may be traced back to the 1970s, when the Soviet Union created a hardware keylogging device for electric typewriters. This marked the beginning of the widespread use of keyloggers. By analysing the changes in magnetic field strength caused by the motion of the printer, the keylogger, also known as the Selectric bug, was able to monitor and record the location of the printhead. The IBM Selectric typewriters were the subject of the Selectric bug, which spied on United States diplomats working in the United States embassy and consulate facilities in Moscow and St. Petersburg. Keyloggers made by Selectric were discovered in 16 different typewriters. These keyloggers had been in use until 1984, when they were discovered by a U.S. ally who was a distinct target of this operation.

A software keylogger that was built by Perry Kivolowitz in 1983 is an example of another early keylogger. The character list dumps were found and dumped by the user mode keylogger that was in a Unix kernel.

The usage of keyloggers has been increasingly widespread, particularly during the 1990s. The development of additional keylogger software meant that attackers no longer needed to install hardware keyloggers. This made it possible for attackers to obtain confidential data, such as credit card information, from victims who were unaware of the attack and were located in a remote location. The usage of keyloggers began to target home users for the goal of fraud, in addition to users in a variety of businesses for the purpose of phishing.

After an incident in which a keylogger was discovered at hotels in Dallas, Texas, the United States Department of Homeland Security started issuing warnings to hotel owners regarding keyloggers in 2014. This was in 2014. Computers that are open to the public or that are located in communal spaces are prime locations for keyloggers.

A keylogger was smuggled inside a modification for the video game Grand Theft Auto V in the year 2015. It was also discovered in 2017 that HP laptops included a keylogger, which the company patched out after stating that the keyloggers were employed as a tool for troubleshooting the software. (Gillis, *What is a keylogger? definition from searchsecurity* 2021)

Keylogger Detection

Since there are numerous types of keyloggers, each of which employ a unique mechanism, there is no one detection or eradication method that is universally acknowledged as being the most efficient. Due to the fact that keyloggers are able to make changes to the kernel of an operating system, checking the Task Manager of a computer is not always sufficient to identify a keylogger.

By comparing the files on a computer with a keylogger signature base or a checklist of common keylogger attributes, security software, such as an anti-keylogger software programme, is designed specifically to scan for software-based keyloggers. This is accomplished by scanning for software-based keyloggers. It's possible that using a programme that stops keyloggers will be more successful than using an antivirus or antispyware tool. It is possible for the latter to mistakenly recognise a keylogger as a normal software rather than malware.

It is possible that an antispyware application, depending on the method that it employs, will be able to discover and deactivate keylogger malware that possesses lesser privileges than it does. The usage of a network monitor will guarantee that the user is

warned each time an application tries to create a network connection, allowing a security team the opportunity to block any potential keylogger activity that may be taking place. (Gillis, *What is a keylogger? definition from searchsecurity* 2021)

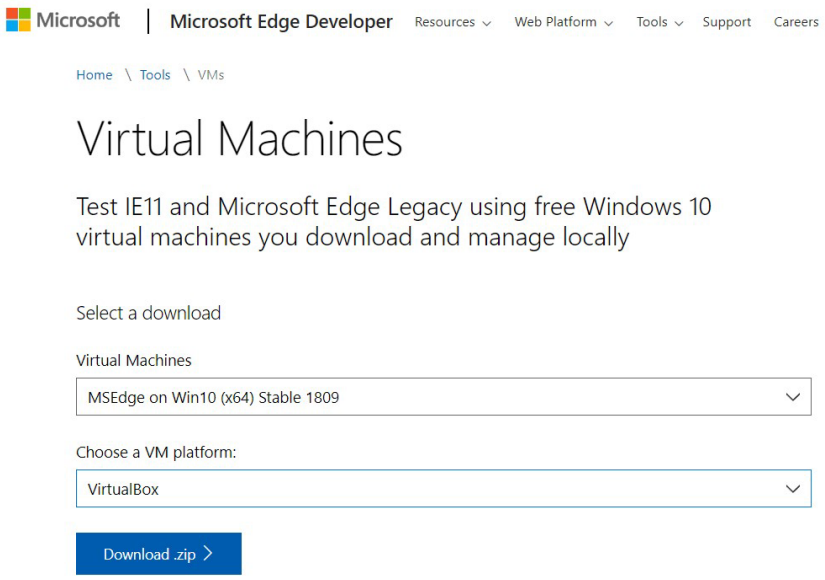
if a keylogger is hardware-based, you should look for the hardware itself. If there's a strange-looking flash drive or other device hooked into your computer, you should remove it immediately. From time to time, it's a good idea to peek behind your workplace desktop and see if anything unusual has been added. (Fruhlinger, *Keyloggers explained: How attackers record computer inputs* 2022)

2. Experiment Setup

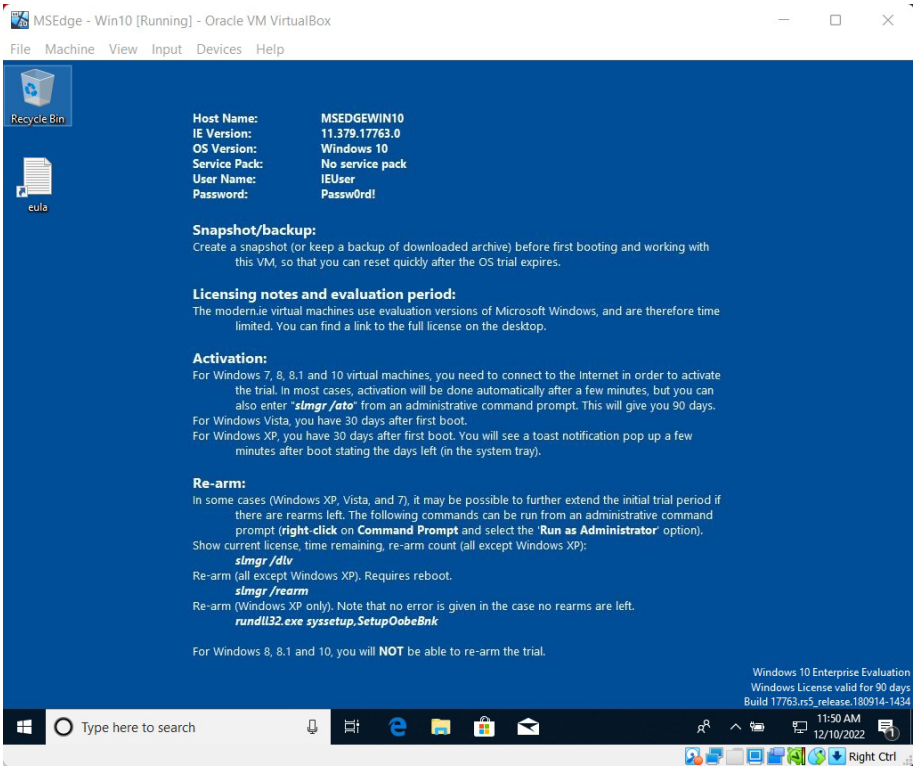
The VirtualBox was used as the virtualization software and as for the operating system, MSEdge on Win 10 (x64) was utilized. The operating system consumed 4096MB of Ram and 38.5GB of storage space after installing all the required tools for malware analysis and creating snapshot as well in Virtual Box so that we are able to revert back if things go wrong or anything becomes corrupt when we are analyzing the malware. The Windows defender and security protection had to be disabled prior to our analysis. There were numerous tools used in this analysis, majority of them were taken from the labs we did. Additionally 4 other tools were utilized as well which were not part of this units lab tutorials which was required for the completion of Advanced Task 1. The Keylogger Executable required GIT and Python inorder to be executed. GIT was used to Clone the Keylogger Executable from the GIthub page and Python which required inorder to execute the Keylogger Executable. We had to create an Outlook Email as well inorder to receive the Keylogger's result.

Setting Up of the New VM

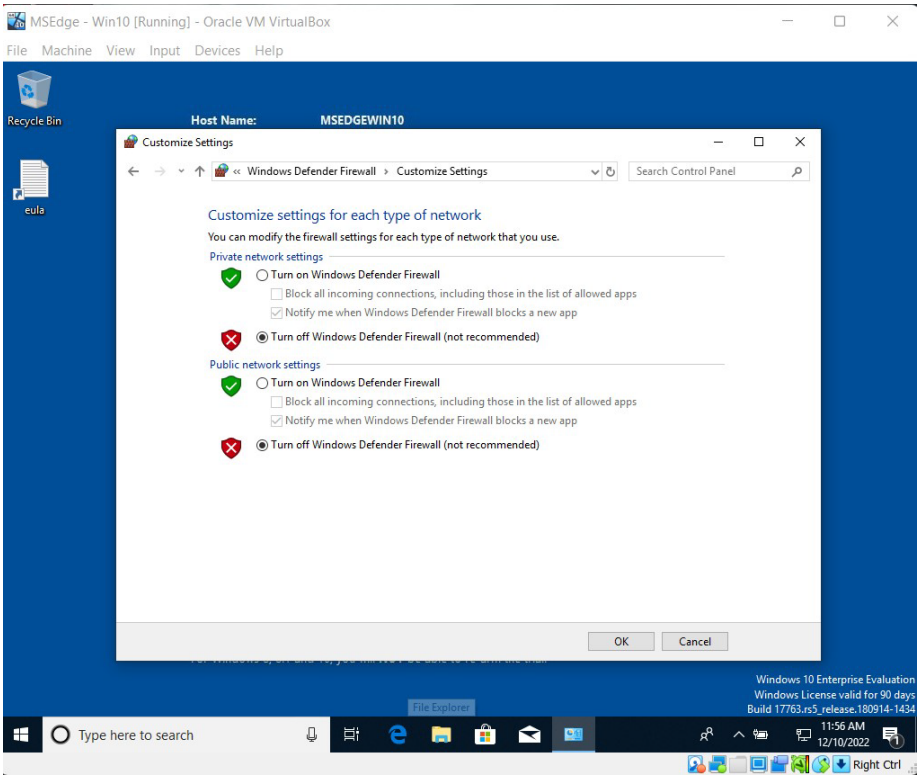
1. The Virtual Machine was sourced from https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/. MSEdge on Win10 (x64) Stable 1809 was installed for VirtualBox.



2. Snippet after successful installation of the Virtual Machine.



3. Disabling Windows Defender and Virus and Threat Protection Settings.



Now the Virtual Machine was ready for Malware Analysis.

Description of Analysis Tools used

1. PEview

PE Viewer is a convenient and easy-to-use tool for viewing PE structures. It offers editing capabilities to change PE headers to correct corrupt PE files. To see imported DLLs and functions of any Windows 32- or 64-bit files, use the utility. Identify the exported functions and the offset at which they begin to run. Beginners who wish to learn about PE file structure may find this to be a useful tool. It is also a fantastic tool for analysing viruses and malware. (Viewer, Pe Viewer)

2. PEiD

PEiD is a lightweight programme used to identify popular compilers, packers, and cryptors. Virus authors frequently make an effort to pack or obfuscate their malware to make it more difficult to detect and analyse. When loaded from a text file named userdb, the current version of PEiD can identify over 470 distinct signatures in PE files. (Hacking Tutorials, 2017)

3. BinText

BinText is a text extractor and file scanner that aids in locating character strings hidden within binary files. The application can extract text from any type of file and display Resource strings, plain ASCII text, and Unicode (double byte ANSI) text. In the "Advanced" mode, each item has additional helpful information. The application will, in a novel way, display both the file offset and the memory offset of each string discovered. (Tpr, Bintext)

4. Dependency Walker

Any 32-bit or 64-bit Windows module (exe, dll, ocx, sys, etc.) may be scanned by the Dependency Walker, which creates a hierarchical tree diagram of all dependant modules. It shows all the functions that are exported by each module it finds, along with which of those functions other modules have actually called. Detailed information about each file, including its entire path, base address, version numbers, machine type, debug information, and more, is also shown in another view along with the minimal set of files that are necessary. (Dependency walker (depends.exe) Home Page)

5. Process Explorer

You may see information about the handles and DLLs that processes have opened or loaded in Process Explorer. There are two sub-windows in the Process Explorer display. The information displayed in the bottom window depends on the mode that Process Explorer is in; if it is in DLL mode, you will see the DLLs and memory-mapped files that the process has loaded. The top window always displays a list of the currently active processes, along with the names of their owning accounts. Powerful search features in Process Explorer allow you to easily identify processes that have specific handles opened or DLLs loaded. (Markruss, Process explorer - sysinternals)

6.Process Monitor

Process Monitor is a sophisticated Windows monitoring programme that displays process/thread activity, file system activity, and registry activity in real time. It combines the capabilities of two venerable Sysinternals tools, Filemon and Regmon, and adds a long list of upgrades, such as comprehensive event properties like session IDs and user names, trustworthy process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. (Markruss, Process Monitor - Sysinternals)

7. HashCalc

A quick and simple calculator that makes it possible to calculate message digests, checksums, and HMACs for files, text, and hex strings. It provides a selection of 13 of

the most widely used hash and checksum methods. (HashCalc - hash, CRC, and HMAC Calculator)

8.PEstudio

PeStudio's objective is to identify executable file artefacts in order to facilitate and quicken malware initial assessment. Globally, Digital-Forensic Labs, Security Operations Centers, and Computer Emergency Response Teams (CERT) use the technology. PeStudio is totally portable and works on any Windows platform; no installation is necessary. The system is not altered by PeStudio, and nothing is left behind. (PeStudio 2022)

9. WireShark

Wireshark is an open-source packet analyzer that is free to use. It is employed in education, analysis, software development, and the design of communications protocols for networks. Cross-platform Wireshark uses pcap to capture packets and the Qt widget toolkit for its user interface in more recent releases, which also make it cross-platform. With the exception of its graphical user interface and integrated sorting and filtering functionality, Wireshark and tcpdump are comparable programmes. (Wireshark 2022)

Description of 4 Additional Analysis Tools used

1. Fiddler

The Fiddler tool records network traffic between the Internet and test PCs to assist with web application debugging. With the help of the tool, you can look at both incoming and outgoing data to keep track of and alter requests and answers before the browser sees them. A robust event-based scripting subsystem is also included in Fiddler, which you may expand using any.NET Framework language.

By creating an offline replica of the test site, Fiddler and the HTTP replay features can assist you in troubleshooting client-side problems with web applications. With the help of these tools, you may capture offline photos of the browsing session, package them, and do further analysis to get more in-depth diagnostic data. (QuinnRadich, Fiddler web debugger tool for internet explorer - win32 apps)

2. RegShot

Regshot is an open-source (LGPL) registry comparison tool that enables you to rapidly take a snapshot of your registry and then compare it with a second one—done after making system modifications or installing new software—in order to identify any registry changes. (Regshot)

3.ApateDNS

A simple-to-use GUI is provided by ApateDNS, an utility for managing DNS answers. By listening on UDP port 53 on the local system, ApateDNS acts as a false DNS server by forging DNS replies sent to a user-specified IP address. Additionally, ApateDNS instantly configures localhost as the DNS server. It restores the initial local DNS settings when the tool is closed. (ApateDNS)

4.AutoRuns

This tool, which has the most thorough understanding of auto-starting locations of any startup monitor, displays the programmes that are set to launch at system bootup or login as well as when you launch other built-in Windows programmes like Internet Explorer, Explorer, and media players. Ones in your starting folder, Run, RunOnce, and other Registry entries are examples of these applications and drivers. Auto-start services, toolbars, browser assistance objects, Winlogon alerts, and many other things are reported by Autoruns. Other autostart tools can't compare to Autoruns in any manner. (Markruss, Autoruns for windows - sysinternals)

Steps Taken to Generate the Keylogger Executable

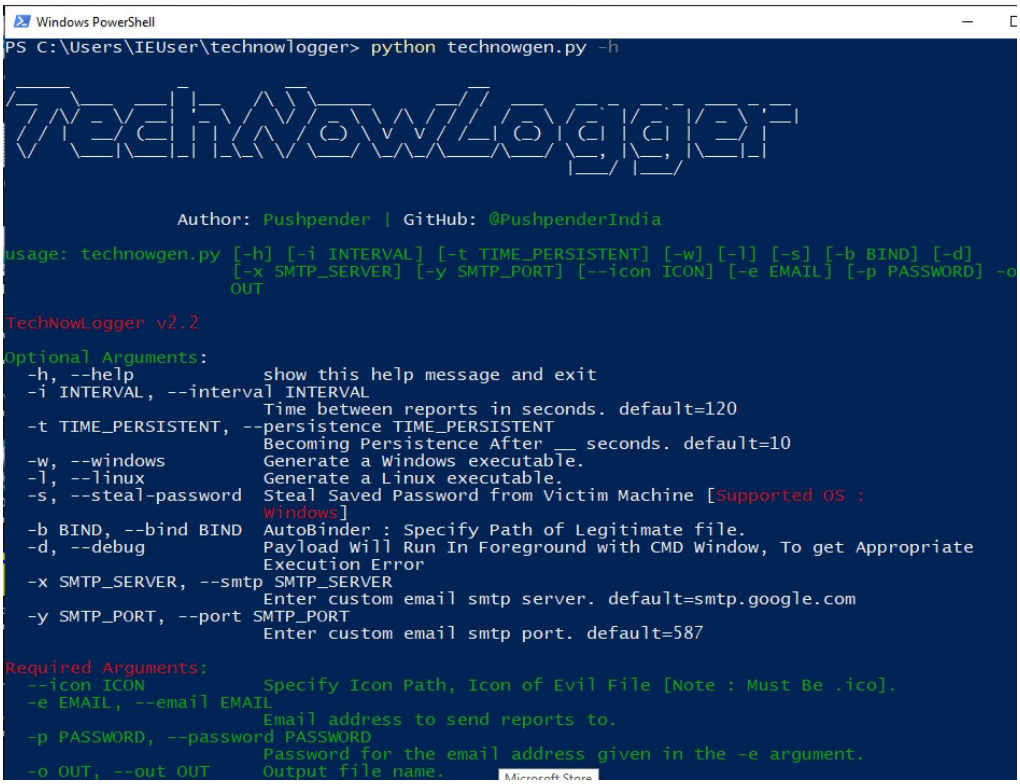
1. Git Clone

```
C:\Users\IEUser>git clone https://github.com/PushpenderIndia/technowlogger.git
Cloning into 'technowlogger'...
remote: Enumerating objects: 616, done.
remote: Counting objects: 100% (138/138), done.
remote: Compressing objects: 100% (90/90), done.
remote: Total 616 (delta 69), reused 84 (delta 43), pack-reused 478
Receiving objects: 100% (616/616), 15.90 MiB | 1.09 MiB/s, done.
Resolving deltas: 100% (319/319), done.
```

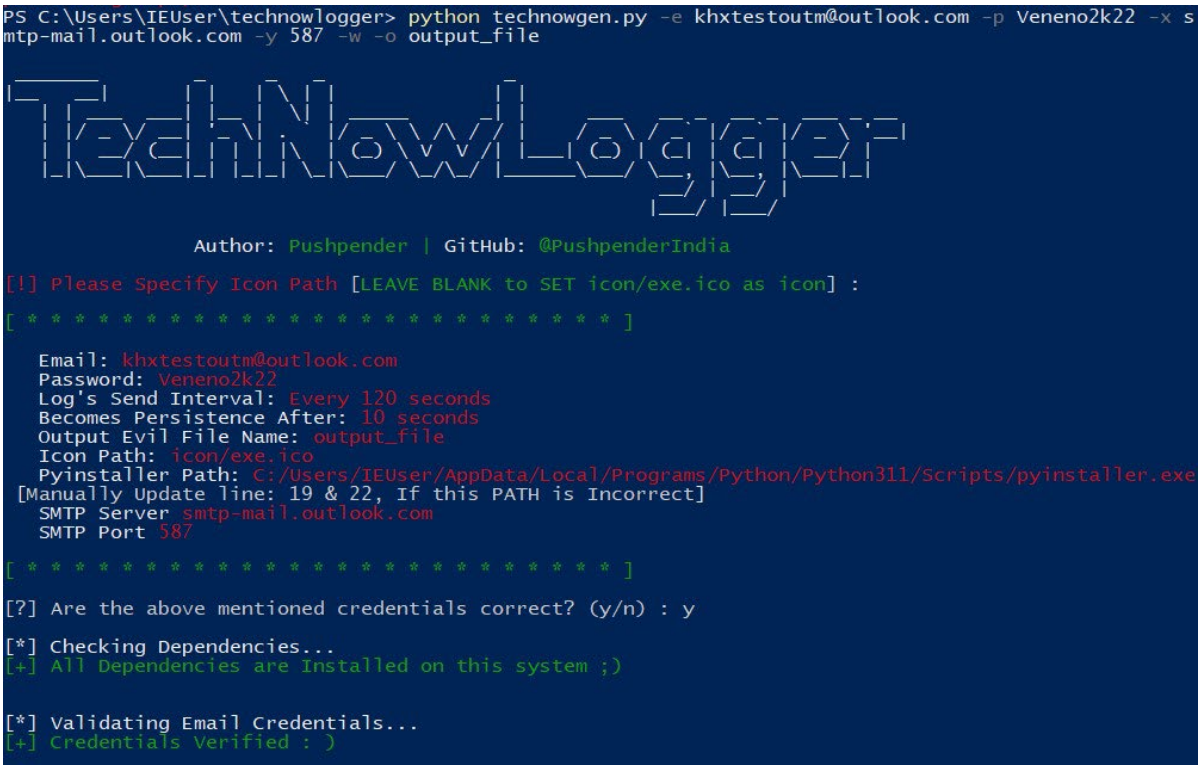
2. Installing all the Requirements through Python

```
Command Prompt
C:\Users\IEUser>python --version
Python 3.11.1

C:\Users\IEUser>cd technowlogger

C:\Users\IEUser\technowlogger>python -m pip install -r requirements.txt
Collecting mss==4.0.3
  Downloading mss-4.0.3-py2.py3-none-any.whl (19 kB)
Collecting essential_generators==0.9.2
  Downloading essential_generators-0.9.2-py3-none-any.whl (9.5 MB)
     ---------------------------------------- 9.5/9.5 MB 2.2 MB/s eta 0:00:00
Collecting PyInstaller
  Downloading pyinstaller-5.7.0-py3-none-win_amd64.whl (1.3 MB)
     ---------------------------------------- 1.3/1.3 MB 1.8 MB/s eta 0:00:00
Collecting pynput==1.4.4
  Downloading pynput-1.4.4-py2.py3-none-any.whl (84 kB)
     ---------------------------------------- 84.1/84.1 kB 1.6 MB/s eta 0:00:00
Collecting six==1.12.0
  Downloading six-1.12.0-py2.py3-none-any.whl (10 kB)
Collecting python-xlib==0.25
  Downloading python_xlib-0.25-py2.py3-none-any.whl (165 kB)
     ---------------------------------------- 165.7/165.7 kB 903.8 kB/s eta 0:00:00
Collecting pywin32
  Downloading pywin32-305-cp311-cp311-win_amd64.whl (12.1 MB)
     ---------------------------------------- 12.1/12.1 MB 2.1 MB/s eta 0:00:00
Collecting colorama
  Downloading colorama-0.4.6-py2.py3-none-any.whl (25 kB)
Requirement already satisfied: setuptools>=42.0.0 in c:\users\ieuser\appdata\local\programs\python\python311\lib\site-package
s (from PyInstaller->-r requirements.txt (line 3)) (65.5.0)
Collecting altgraph
  Downloading altgraph-0.17.3-py2.py3-none-any.whl (21 kB)
Collecting pyinstaller-hooks-contrib>=2021.4
  Downloading pyinstaller_hooks_contrib-2022.14-py2.py3-none-any.whl (252 kB)
     ---------------------------------------- 252.6/252.6 kB 2.6 MB/s eta 0:00:00
Collecting pefile>=2022.5.30
  Downloading pefile-2022.5.30.tar.gz (72 kB)
     ---------------------------------------- 72.9/72.9 kB 3.9 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting pywin32-ctypes>=0.2.0
  Downloading pywin32_ctypes-0.2.0-py2.py3-none-any.whl (28 kB)
Collecting future
  Downloading future-0.18.2.tar.gz (829 kB)
     ---------------------------------------- 829.2/829.2 kB 2.9 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
```

3. Initializing Keylogger



4. Generation of Keylogger

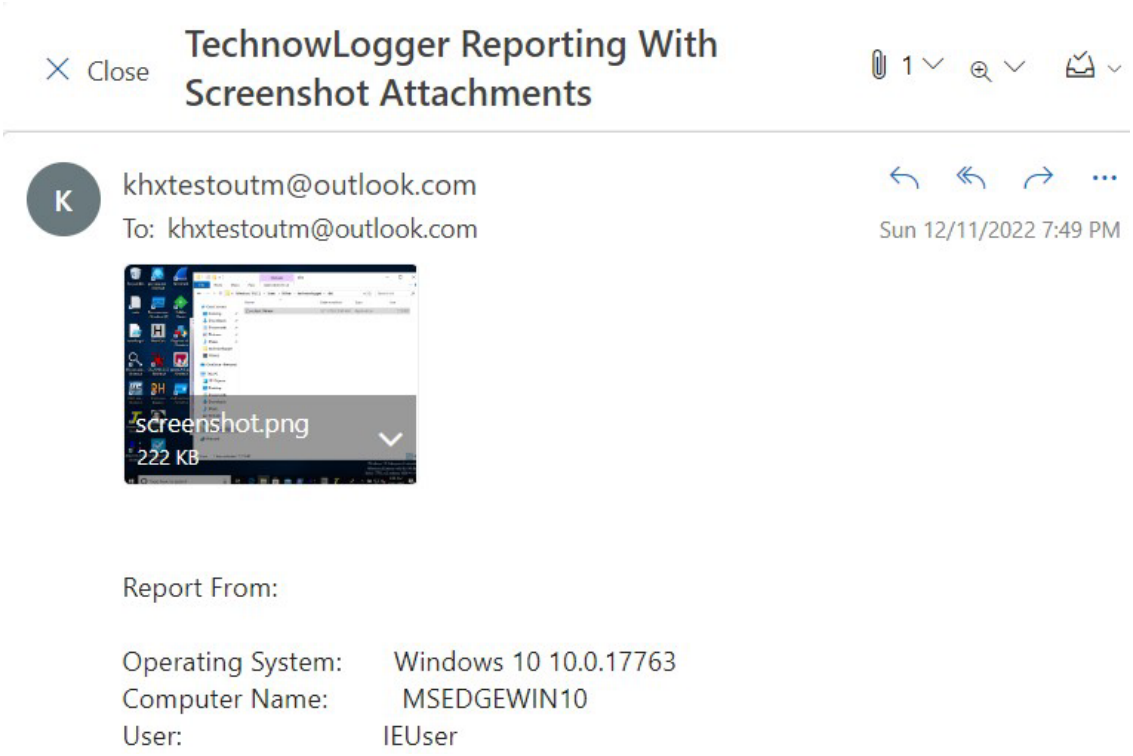


```
[*] Validating Email Credentials...
[+] Credentials Verified : )


[*] Generating Please wait for a while...


[*] Encrypting Source Codes...
[+] Operation Completed Successfully!


715 INFO: PyInstaller: 5.7.0
715 INFO: Python: 3.11.1
734 INFO: Platform: Windows-10-10.0.17763-SP0
734 INFO: wrote C:\Users\IEUser\technowlogger\output_file.spec
747 INFO: UPX is not available.
747 INFO: Extending PYTHONPATH with paths
['C:\\Users\\IEUser\\technowlogger']
1266 INFO: checking Analysis
1266 INFO: Building Analysis because Analysis-00.toc is non existent
1266 INFO: Initializing module dependency graph...
1314 INFO: Caching module graph hooks...
1353 INFO: Analyzing base_library.zip ...
4005 INFO: Loading module hook 'hook-heapq.py' from 'C:\\Users\\IEUser\\AppData\\Local\\Programs\\Py
thon\\Python311\\Lib\\site-packages\\PyInstaller\\hooks'...
4301 INFO: Loading module hook 'hook-encodings.py' from 'C:\\Users\\IEUser\\AppData\\Local\\Programs
\\Python\\Python311\\Lib\\site-packages\\PyInstaller\\hooks'...
6508 INFO: Loading module hook 'hook-pickle.py' from 'C:\\Users\\IEUser\\AppData\\Local\\Programs\\P
ython\\Python311\\Lib\\site-packages\\PyInstaller\\hooks'...
9438 INFO: Caching module dependency graph...
9544 INFO: running Analysis Analysis-00.toc
9599 INFO: Adding Microsoft.Windows.Common-Controls to dependent assemblies of final executable
  required by C:\Users\IEUser\AppData\Local\Programs\Python\Python311\python.exe
9660 INFO: Analyzing C:\Users\IEUser\technowlogger\output_file
9660 INFO: Analyzing hidden import 'win32event'
9706 INFO: Analyzing hidden import 'winerror'
9706 INFO: Analyzing hidden import 'win32api'
9706 INFO: Analyzing hidden import 'pynput.keyboard'
9821 INFO: Loading module hook 'hook-pynput.py' from 'C:\\Users\\IEUser\\AppData\\Local\\Programs\\P
```

```
14209 INFO: Found binding redirects:
[]
14209 INFO: Warnings written to C:\Users\IEUser\technowlogger\build\output_file\warn-output_file.txt
14209 INFO: Graph cross-reference written to C:\Users\IEUser\technowlogger\build\output_file\xref-ou
tput_file.html
14303 INFO: checking PYZ
14303 INFO: Building PYZ because PYZ-00.toc is non existent
14303 INFO: Building PYZ (ZlibArchive) C:\Users\IEUser\technowlogger\build\output_file\PYZ-00.pyz
14597 INFO: Building PYZ (ZlibArchive) C:\Users\IEUser\technowlogger\build\output_file\PYZ-00.pyz co
mpleted successfully.
14718 INFO: checking PKG
14718 INFO: Building PKG because PKG-00.toc is non existent
14718 INFO: Building PKG (CArchive) output_file.pkg
17342 INFO: Building PKG (CArchive) output_file.pkg completed successfully.
17342 INFO: Bootloader C:\Users\IEUser\AppData\Local\Programs\Python\Python311\Lib\site-packages\PyI
nstaller\bootloader\Windows-64bit-intel\runw.exe
17342 INFO: checking EXE
17353 INFO: Building EXE because EXE-00.toc is non existent
17353 INFO: Building EXE from EXE-00.toc
17353 INFO: Copying bootloader EXE to C:\Users\IEUser\technowlogger\dist\output_file.exe.notanexecut
able
17529 INFO: Copying icon to EXE
17535 INFO: Copying icons from ['C:\\Users\\IEUser\\technowlogger\\icon\\exe.ico']
17551 INFO: Writing RT_GROUP_ICON 0 resource with 90 bytes
17551 INFO: Writing RT_ICON 1 resource with 744 bytes
17551 INFO: Writing RT_ICON 2 resource with 2216 bytes
17551 INFO: Writing RT_ICON 3 resource with 1384 bytes
17551 INFO: Writing RT_ICON 4 resource with 9640 bytes
17620 INFO: Writing RT_ICON 5 resource with 4264 bytes
17620 INFO: Writing RT_ICON 6 resource with 1128 bytes
17620 INFO: Copying 0 resources to EXE
17636 INFO: Embedding manifest in EXE
17636 INFO: Updating manifest in C:\Users\IEUser\technowlogger\dist\output_file.exe.notanexecutable
17636 INFO: Updating resource type 24 name 1 language 0
17636 INFO: Appending PKG archive to EXE
17874 INFO: Fixing EXE headers
18454 INFO: Building EXE from EXE-00.toc completed successfully.

[*] Deleting Junk Files...
[+] Junk Files Removed Successfully!

[+] Generated Successfully!
```

3. Results and Discussion

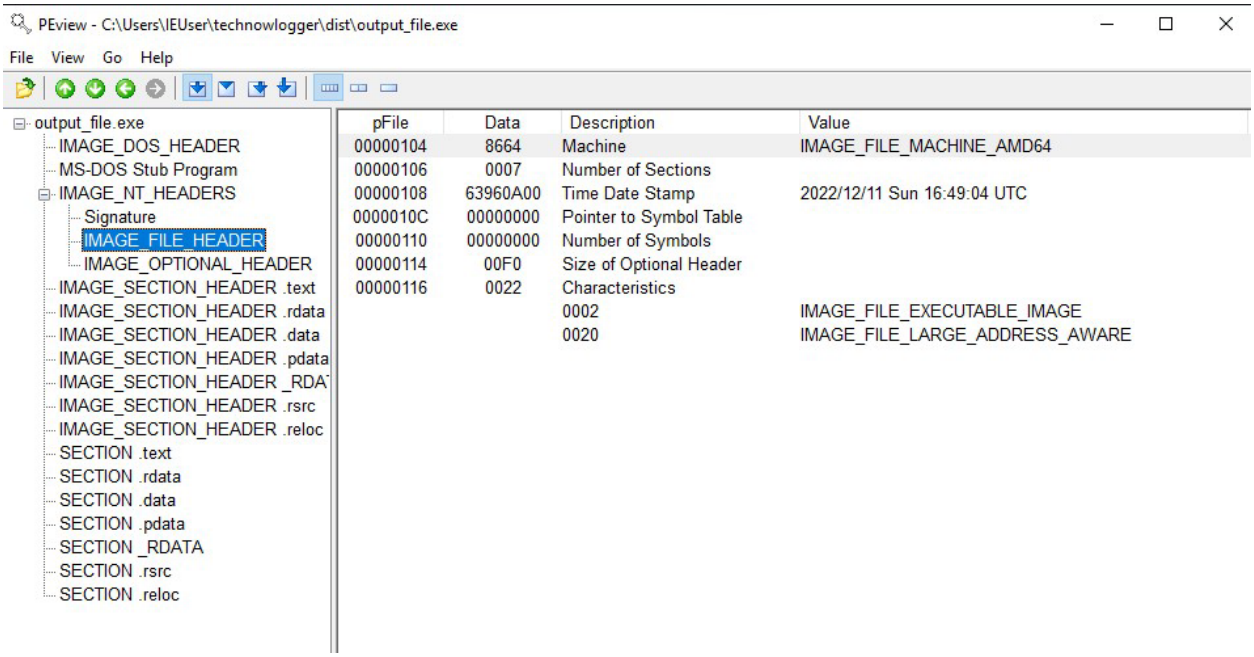
Keylogger confirming that the target computer is successfully connected.



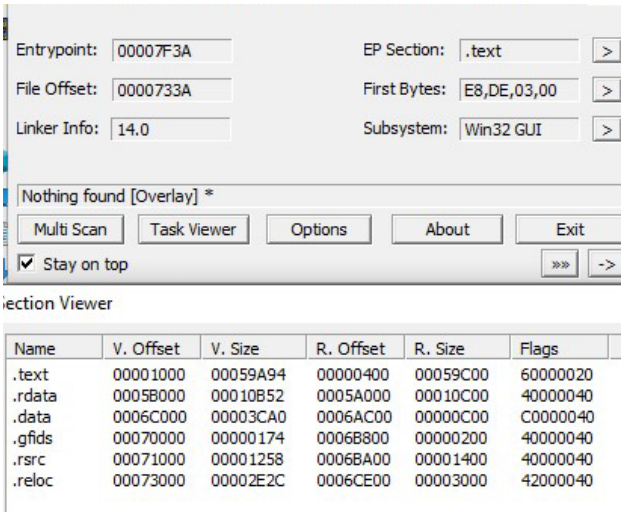
Keylogger sending screenshot of Victims computer at regular intervals which might potentially contain private information such as the Victims Account Passwords, Bank Details etc.

Static Analysis

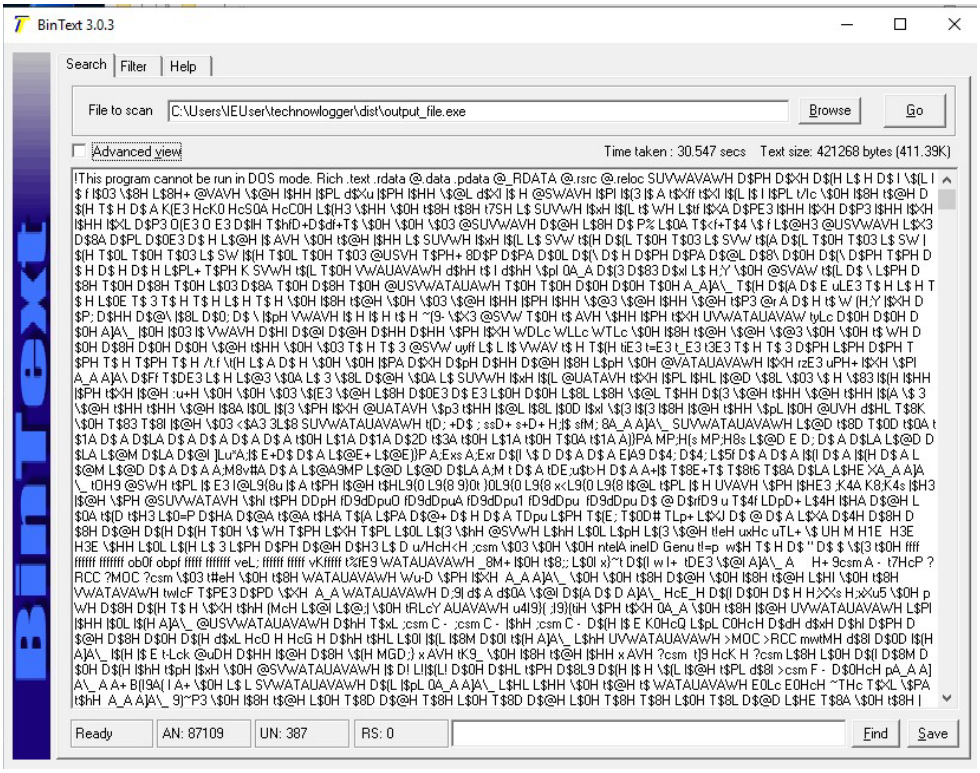
1.Through PEview we can see the time and date when the keylogger was packed.



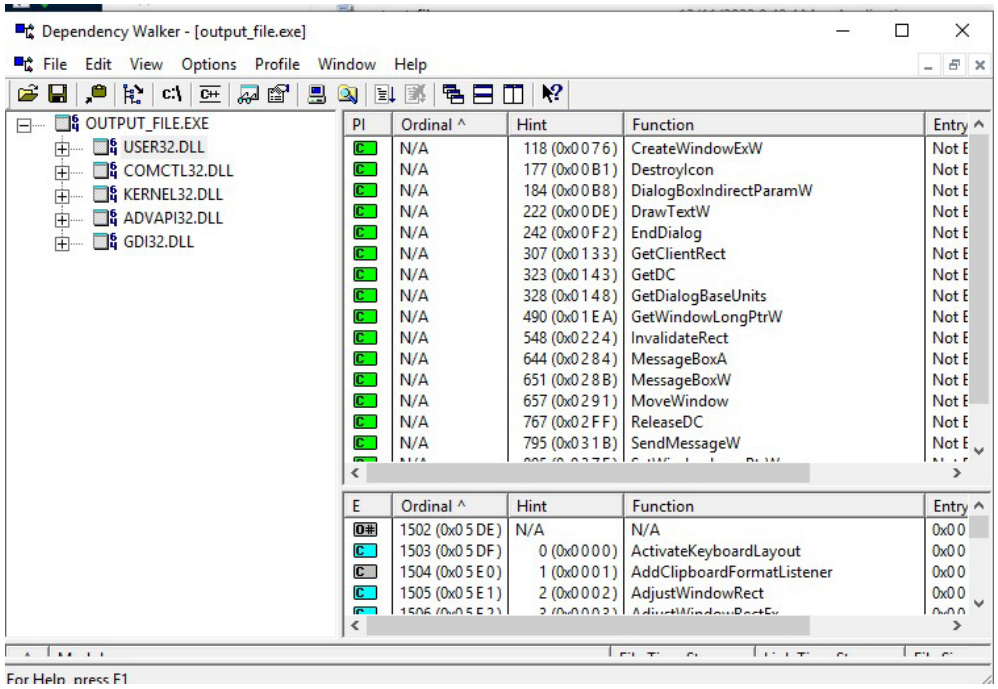
2. PEiD was able to identify 6 types of signature of the Keylogger



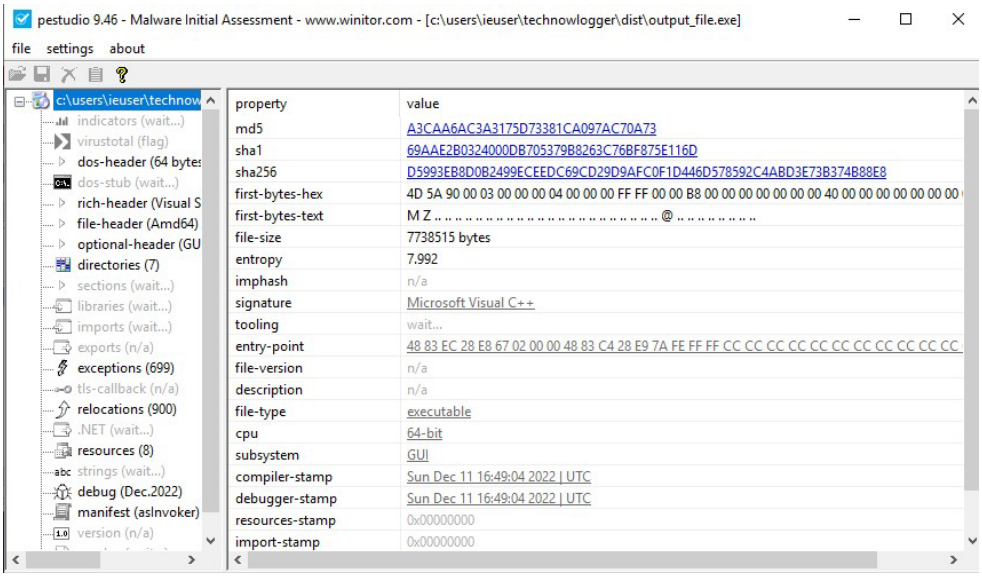
3.The BinText returns jumbled letters, numbers and symbols which indicate that the file is packed.



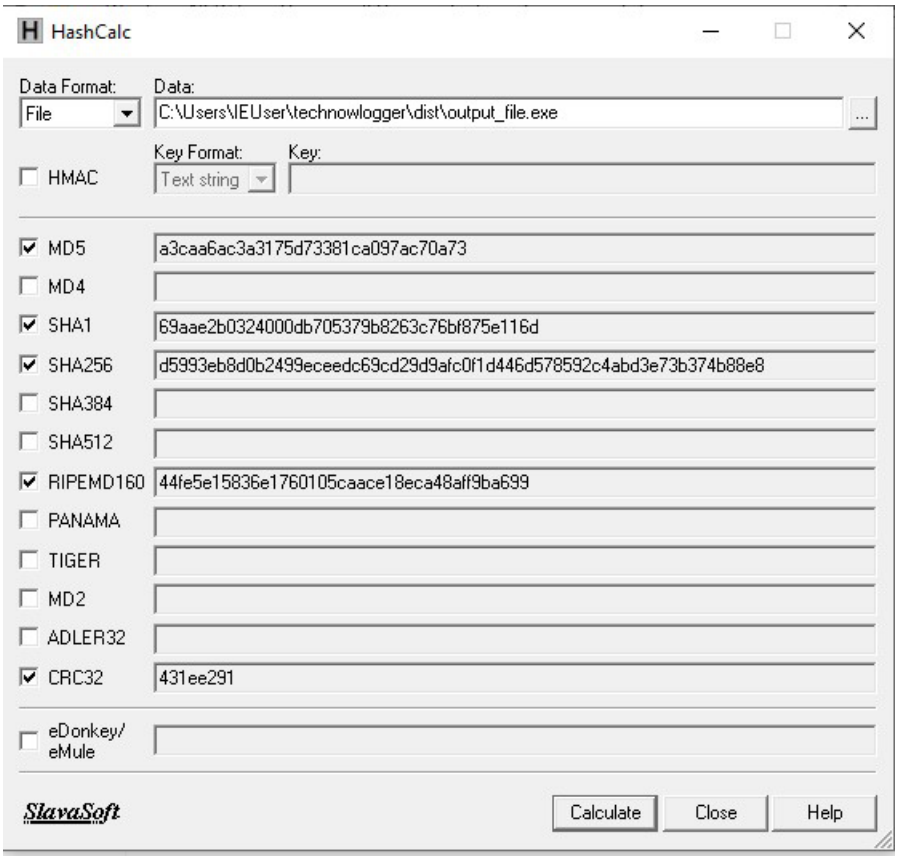
4. Dependency Walker shows us the Five type of DLLs which is used by the Keylogger. Namely USER32.DLL, COMCTL32.DLL, KERNEL32.DLL, ADVAPI32.DLL and GDI32.DLL



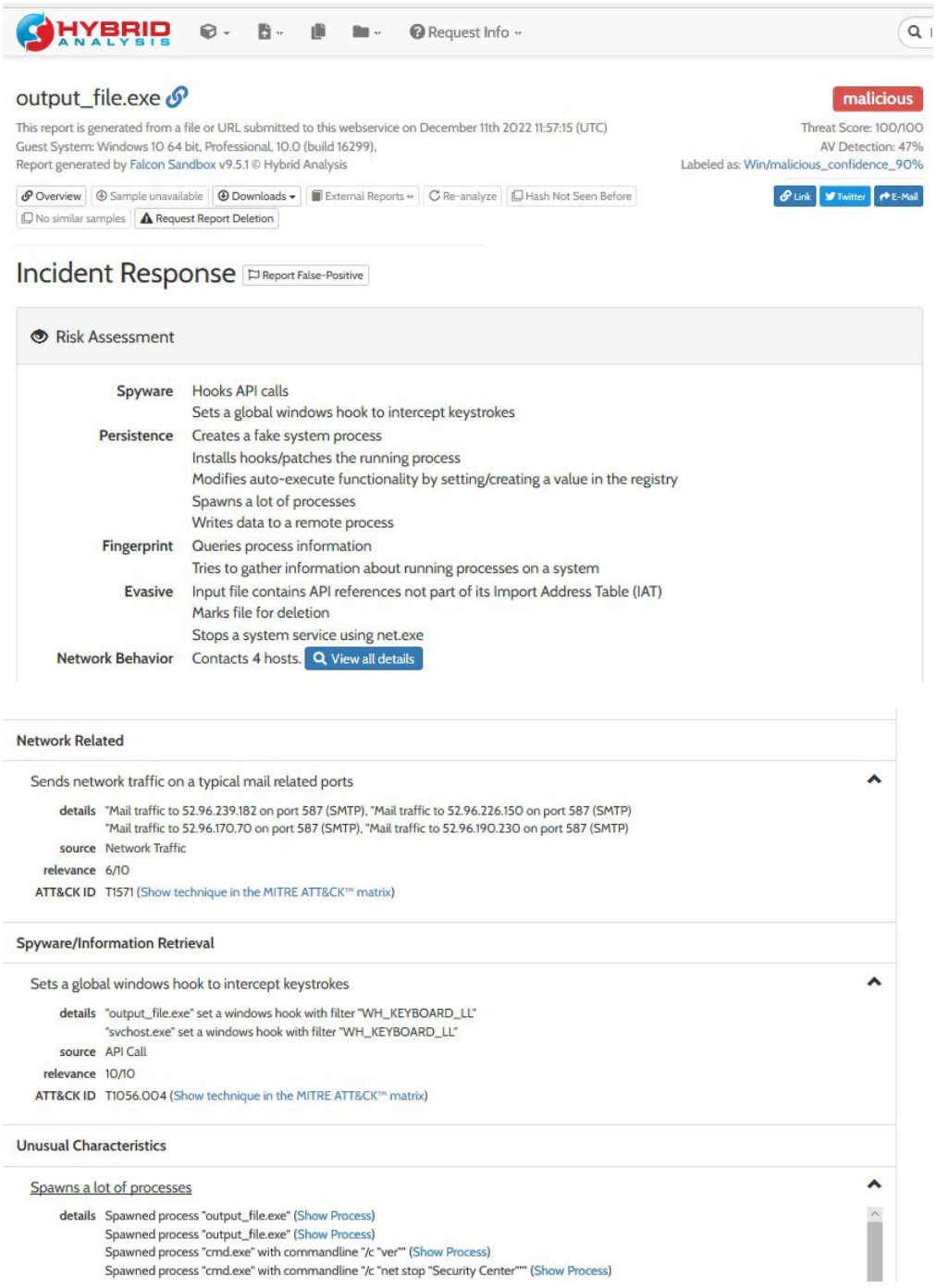
5. PEStudio returns some specifications of the Keylogger such as MD5, sha1 and Sha 256 among other general specifications, nothing precise we can use.



6. HashCalc returns the Keylogger's MD5, SHA1, SHA256, RIPEMD160 and CRC32 which can be used to further analyze the Keylogger through VirusTotal, Hybrid Analysis etc.



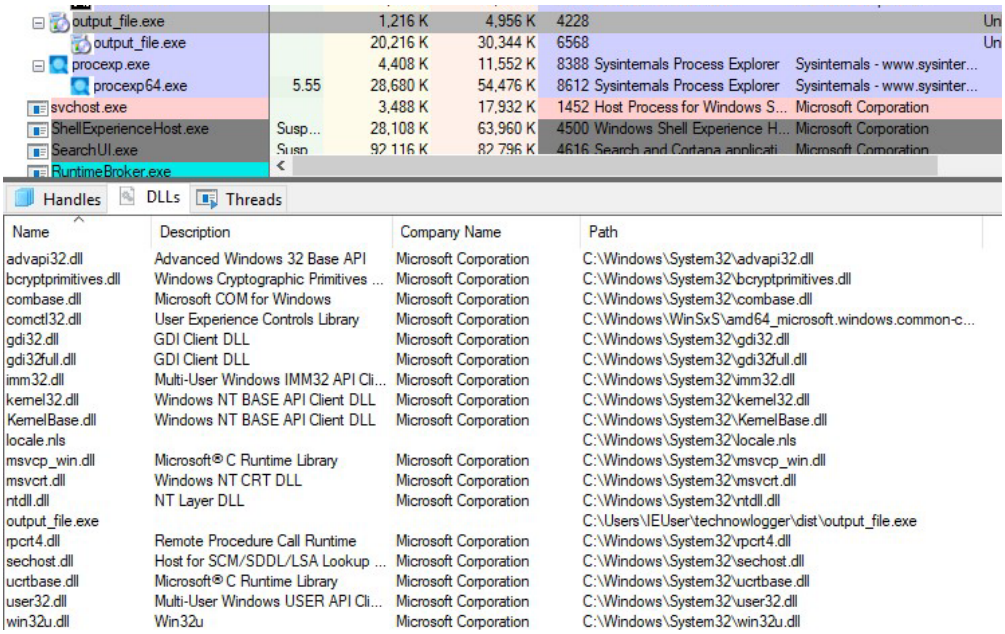
7. Hybrid Analysis returns us the following output:



Hybrid Analysis shows us that the Keylogger is a network based Malware and that it's a type of Spyware.

Dynamic Analysis

1. The Process Monitor Lists out all the DLLs utilized by the Keylogger while its being executed in the background. One of the DLLs called by the Keylogger is rpcrt4.dll which is a network based dll. This indicates that the Keylogger has some networking functionality.

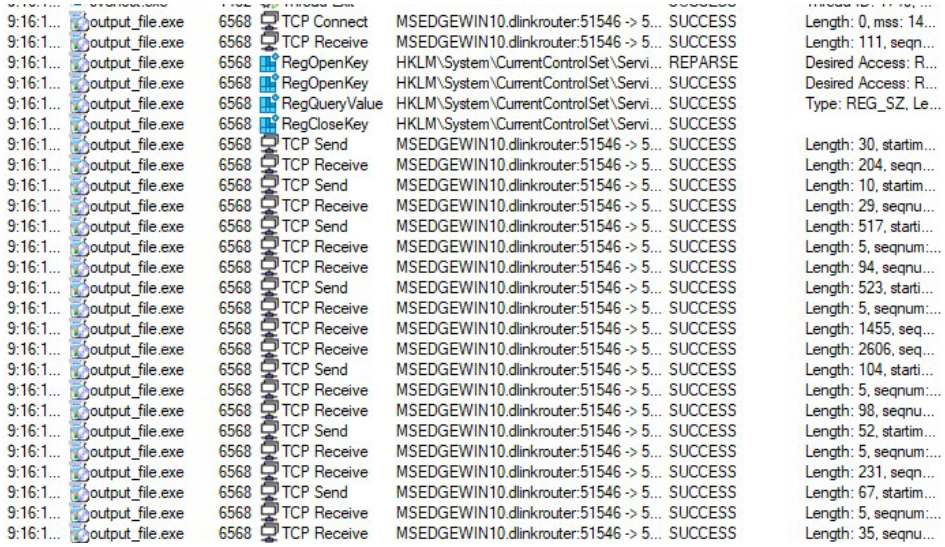


output_file.exe		1,216 K	4,956 K	4228		Un
output_file.exe		20,216 K	30,344 K	6568		Un
procexp.exe		4,408 K	11,552 K	8388	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	5.55	28,680 K	54,476 K	8612	Sysinternals Process Explorer	Sysinternals - www.sysinter...
svchost.exe		3,488 K	17,932 K	1452	Host Process for Windows S...	Microsoft Corporation
ShellExperienceHost.exe	Susp...	28,108 K	63,960 K	4500	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	92,116 K	82,796 K	4616	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe						

Handles | DLLs | Threads

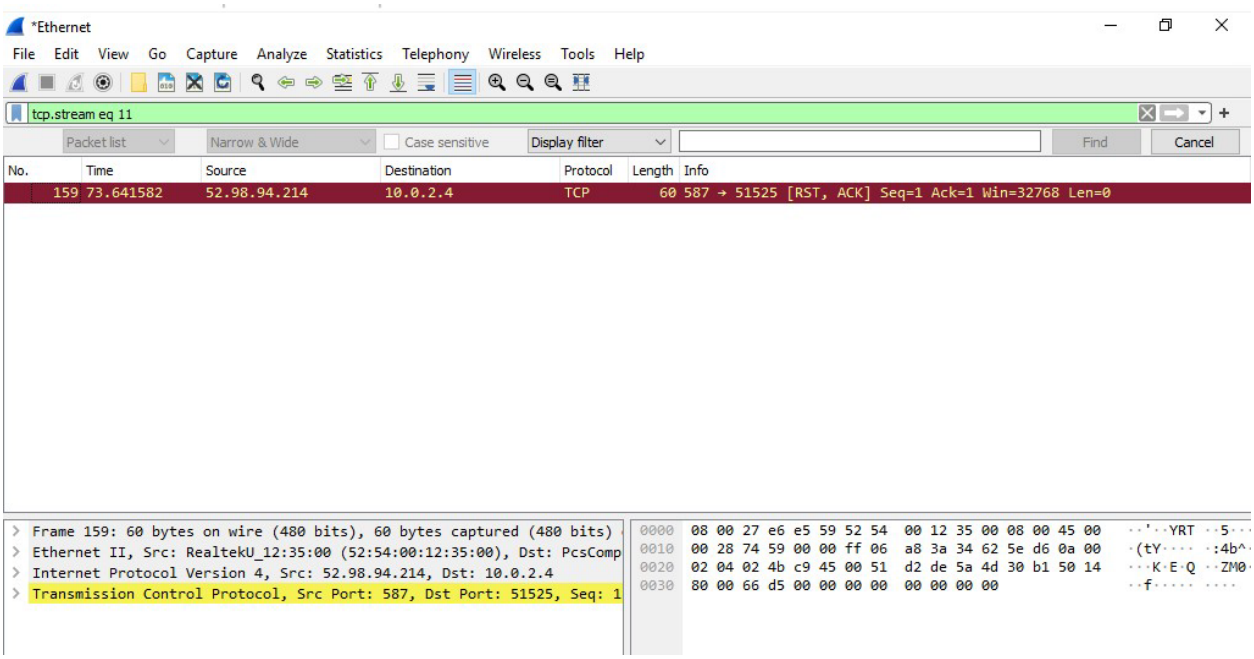
Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\WinSxS\amd64_microsoft.windows.common-c...
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\System32\imm32.dll
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
locale.nls			C:\Windows\System32\locale.nls
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcrt.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
output_file.exe			C:\Users\IEUser\technowlogger\dist\output_file.exe
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll
sechost.dll	Host for SCM/SDDL/LSA Lookup ...	Microsoft Corporation	C:\Windows\System32\sechost.dll
ucrtbase.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\ucrtbase.dll
user32.dll	Multi-User Windows USER API Cli...	Microsoft Corporation	C:\Windows\System32\user32.dll
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\System32\win32u.dll

2. The Process Explorer shows that the Keylogger is Sending and Receiving TCP which indicates that there is a network conversation taking place by the application, and the data is being exchanged by the application and the internet.

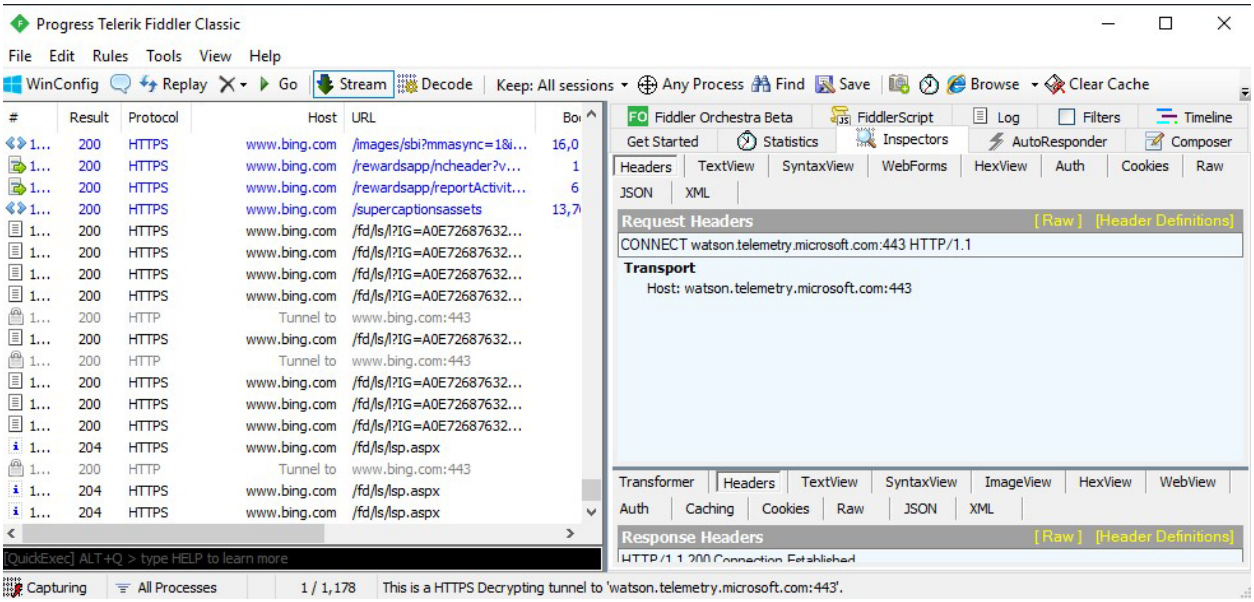


9:16:1...	output_file.exe	6568	TCP Connect	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 0, mss: 14...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 111, seqn...
9:16:1...	output_file.exe	6568	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	REPARSE	Desired Access: R...
9:16:1...	output_file.exe	6568	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Desired Access: R...
9:16:1...	output_file.exe	6568	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Type: REG_SZ, Le...
9:16:1...	output_file.exe	6568	RegCloseKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	
9:16:1...	output_file.exe	6568	TCP Send	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 30, startim...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 204, seqn...
9:16:1...	output_file.exe	6568	TCP Send	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 10, startim...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 29, seqnu...
9:16:1...	output_file.exe	6568	TCP Send	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 517, starti...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 5, seqnum:...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 94, seqnu...
9:16:1...	output_file.exe	6568	TCP Send	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 523, starti...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 5, seqnum:...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 1455, seq...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 2606, seq...
9:16:1...	output_file.exe	6568	TCP Send	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 104, starti...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 5, seqnum:...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 98, seqnu...
9:16:1...	output_file.exe	6568	TCP Send	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 52, startim...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 5, seqnum:...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 231, seqn...
9:16:1...	output_file.exe	6568	TCP Send	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 67, startim...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 5, seqnum:...
9:16:1...	output_file.exe	6568	TCP Receive	MSEDGEWIN10.dlinkrouter:51546 -> 5...	SUCCESS	Length: 35, seqnu...

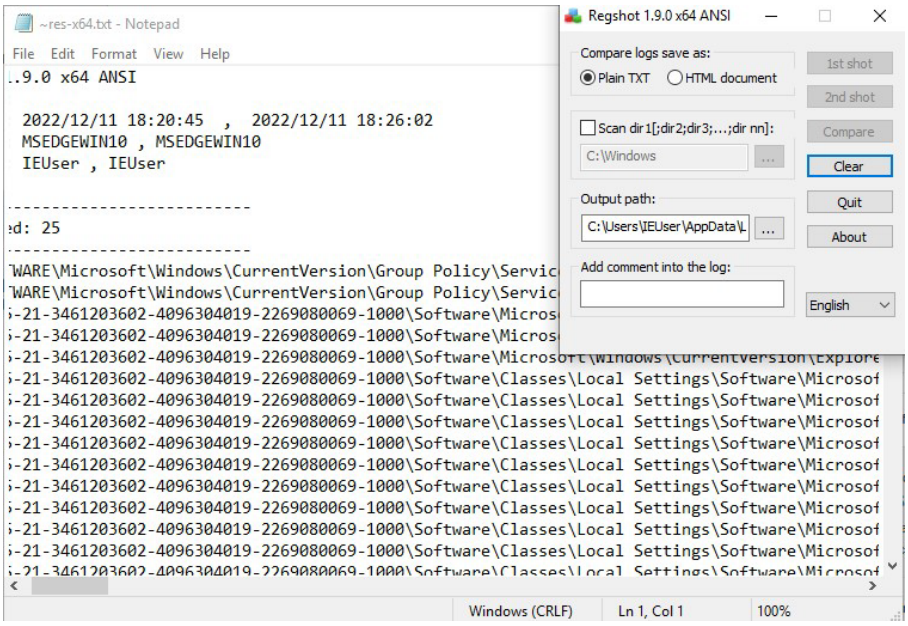
3. WireShark shows us that the Keylogger is communicating with Port 587, which is the default SMTP(Simple Mail Transfer Protocol). This indicates the Keylogger is communicating with a third party through mails using port 587.



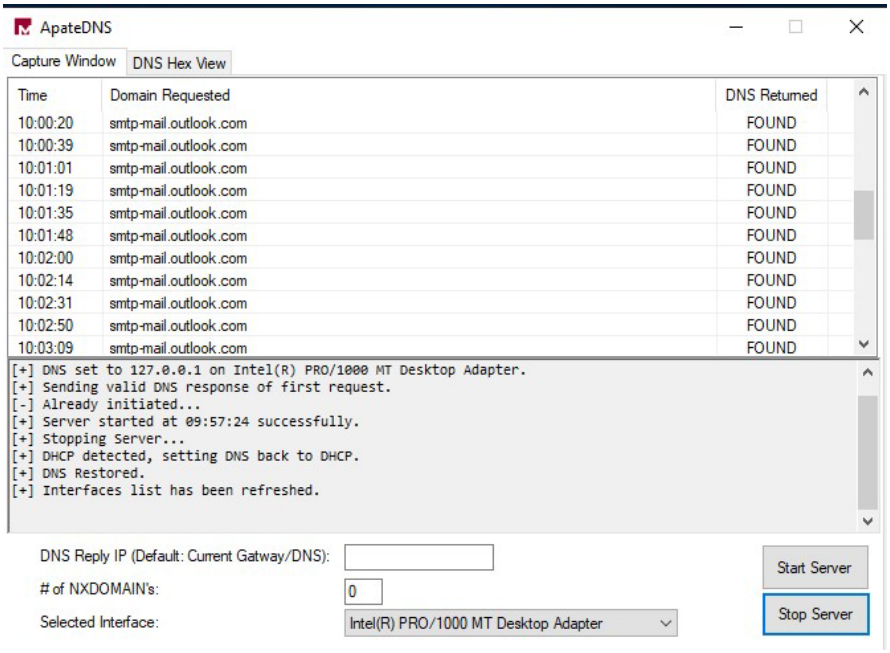
4. Fiddler does not show any activity of the Keylogger which means that the Keylogger is very well hidden and cannot be discovered by all the applications.



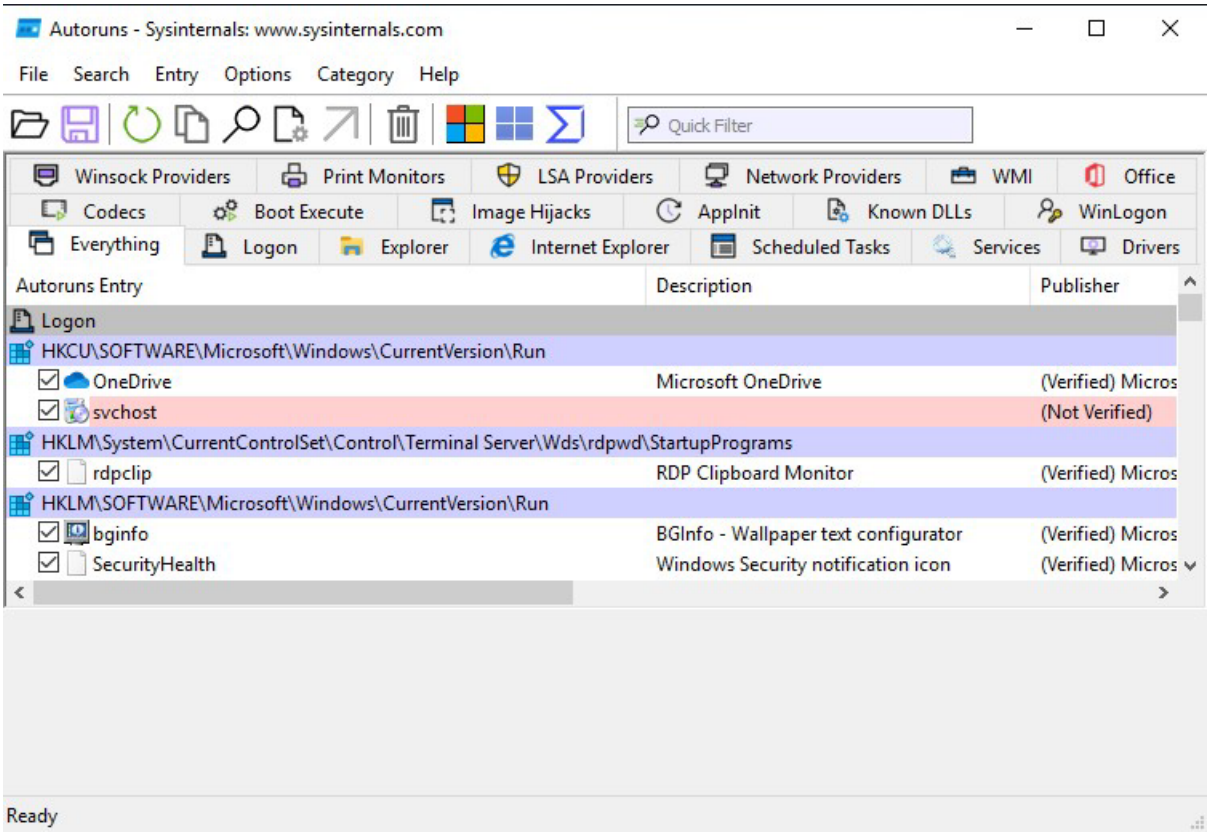
5. RegShot compared the Number of Registries used by the Computer before and after execution of Keylogger. As we can see from the screenshot below, 25 Additional Registries were used by the Keylogger.



6. ApateDNS shows us that there is a clear communication between the Computer and Outlook. From the analysis we have gathered until now, we can conclude that the Keylogger is communicating with a third party through sending mail to the third party's outlook account.



7. AutoRun was not able to detect the Keylogger which implies how hard it is to detect Keyloggers.



4. Conclusion

In this research project, we discovered that the keylogger is a highly effective tool used to spy on the target computer and record all keyboard inputs as well as screenshot the target computers activities without informing the target computers user, which may contain the victim's personal information like a password or bank account information. We discovered that the Keylogger is a network-based spyware that logs the victim's activities and sends them over Port 587, the standard SMTP(Simple Mail Transfer Protocol), to a third party's mail account.

Recommendations on how to guard against potential keyloggers:

1. Install Anti-Virus software on each device you own. Typically, malicious keyloggers infiltrate machines using software based techniques. An active barrier to protect against viruses will be present if you use an Anti-Virus Software.
2. Maintain software updates for all other devices. The most recent security updates for your operating system, applications, and web browsers should all be installed. Be careful to download and install updates as soon as they are available.
3. By using 2-Step verification, keylogging attacks may be avoided. To confirm identification, a pin code must be entered into a cell phone by text message. Even if a hacker manages to get your login and password using a keylogger, it prohibits them from accessing your account.
4. if you don't download cracked software, you will be saved from potential Keyloggers. Malware is frequently present in cracked software. Although they are free, they could be harmful to your PC. Unintentionally installing a keylogger that poses as computer software is possible.
5. To stop keyloggers from recording the precise keys you press on the keyboard, key encryption software encrypts those keys as you press them. As soon as users go to the programme, they hide the keystrokes. Therefore, a keylogger will only be able to record the characters that were used to encrypt the sensitive data.
6. Unknown external hard discs and USB devices should never be used. In order to persuade you to grab and use them, many crooks leave these devices in public areas. Once connected, they can penetrate and plant a keylogger in your computer as well.
7. Keep an eye on your computer and mobile devices. Your smartphone could be all that a thief needs if they can take it or even just get their hands on it briefly, they can plant a keylogger in it. Keep your gadgets close by to help stop keyloggers from being planted.

8. Install a password manager since keyloggers can't record your inputs if you don't enter them in. You can protect your passwords and personal information by using programmes that automatically fill out forms.
9. Changing your passwords often is another strategy to reduce the potential impact from keylogging. This is not only a suggested data security practise, but it could also make the data that a keylogger has taken unusable.

5. References

Gillis, A.S. (2021) *What is a keylogger? definition from searchsecurity*, *Security*. TechTarget. Available at: https://www.techtarget.com/searchsecurity/definition/keylogger (Accessed: December 2, 2022).

Fruhlinger, J. (2022) *Keyloggers explained: How attackers record computer inputs*, *CSO Online*. CSO. Available at: https://www.csoonline.com/article/3326304/keyloggers-explained-how-attackers-record-computer-inputs.html#:~:text=A%20keylogger%20is%20a%20tool,type%20as%20you%20type%20it. (Accessed: December 2, 2022).

Popovici, M. (2022) *What is a keylogger? definition, types, examples and prevention*, *Heimdal Security Blog*. Heimdal Security. Available at: https://heimdalsecurity.com/blog/what-is-a-keylogger/ (Accessed: December 2, 2022).

Viewer, P.E. (no date) Pe Viewer, Download.com. Download.com. Available at: https://download.cnet.com/PE-Viewer/3000-2352_4-10966763.html (Accessed: December 8, 2022).

Hacking Tutorials (2017) Basic malware analysis tools, Hacking Tutorials. Available at: https://www.hackingtutorials.org/malware-analysis-tutorials/basic-malware-analysis-tools/ (Accessed: December 8, 2022).

Tpr (no date) Bintext, The Portable Freeware Collection. Available at: https://www.portablefreeware.com/index.php?id=2506 (Accessed: December 8, 2022).

Dependency walker (depends.exe) Home Page (no date) Dependency Walker (depends.exe) Home Page. Available at: https://www.dependencywalker.com/ (Accessed: December 8, 2022).

Markruss (no date) Process explorer - sysinternals, Process Explorer - Sysinternals | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer (Accessed: December 8, 2022).

Markruss (no date) Process Monitor - Sysinternals, Process Monitor - Sysinternals | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon (Accessed: December 8, 2022).

HashCalc - hash, CRC, and HMAC Calculator (no date) Slavasoft HashCalc - hash, CRC, and HMAC Calculator. Available at: https://www.slavasoft.com/hashcalc/ (Accessed: December 8, 2022).

PeStudio (2022) TechSpot. Marc Ochsenmeier. Available at: https://www.techspot.com/downloads/6350-pestudio.html (Accessed: December 8, 2022).

Wireshark (2022) Wikipedia. Wikimedia Foundation. Available at: https://en.wikipedia.org/wiki/Wireshark (Accessed: December 8, 2022).

QuinnRadich (no date) Fiddler web debugger tool for internet explorer - win32 apps, Fiddler web debugger tool for Internet Explorer - Win32 apps | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows/win32/win7appqual/fiddler-web-debugger-tool (Accessed: December 8, 2022).

Regshot (no date) SourceForge. Available at: https://sourceforge.net/projects/regshot/ (Accessed: December 9, 2022).

ApateDNS (no date) FireEye Market. Available at: https://fireeye.market/apps/211380 (Accessed: December 9, 2022).

Markruss (no date) Autoruns for windows - sysinternals, Autoruns for Windows - Sysinternals | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns (Accessed: December 9, 2022).