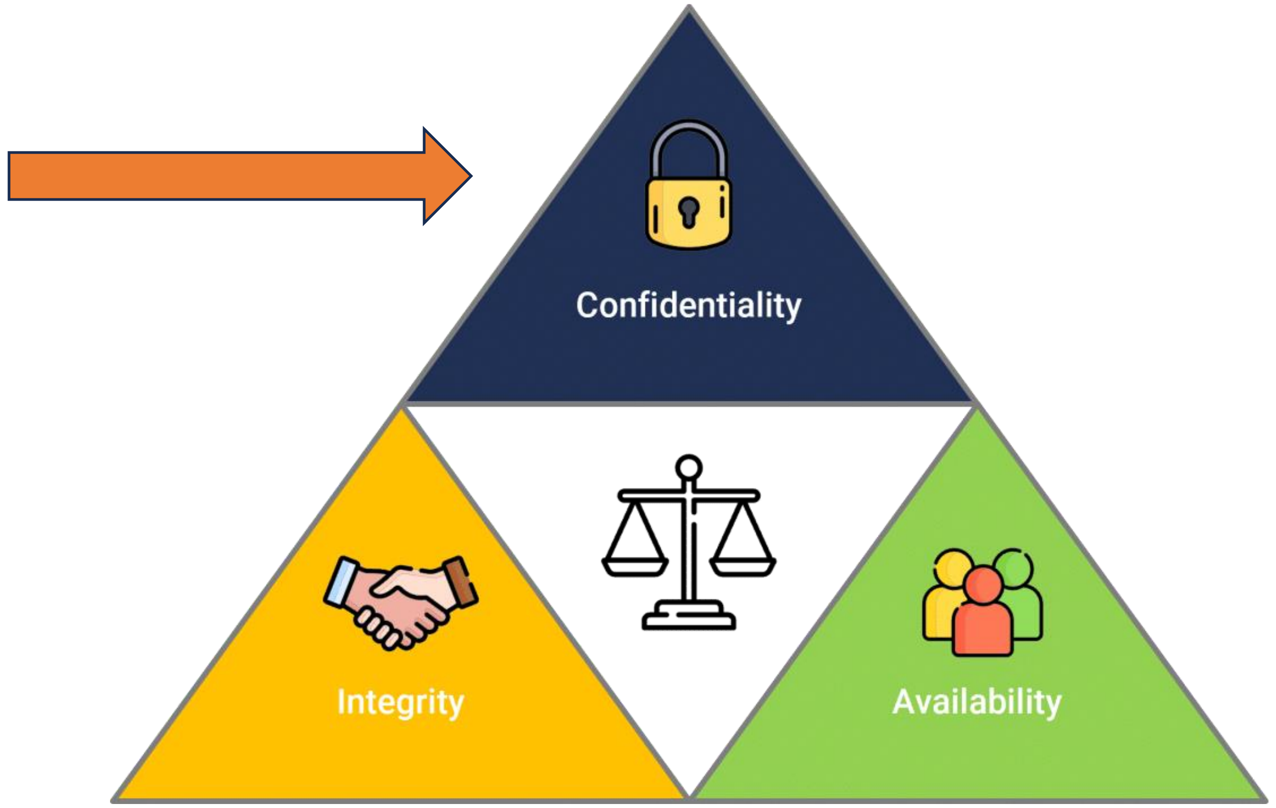
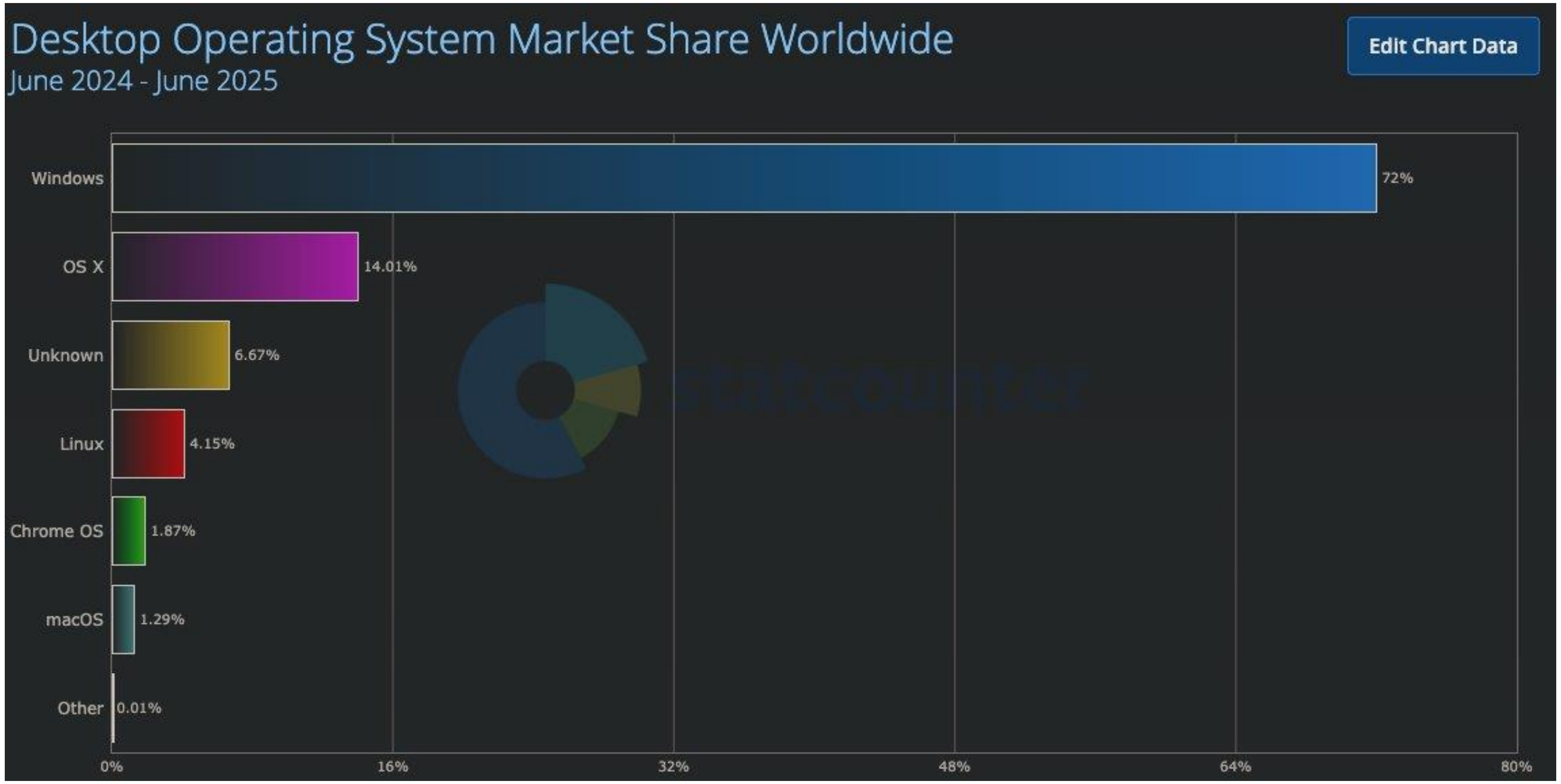
Keylogger

A type of **spyware** that record keyboard strokes made on device.

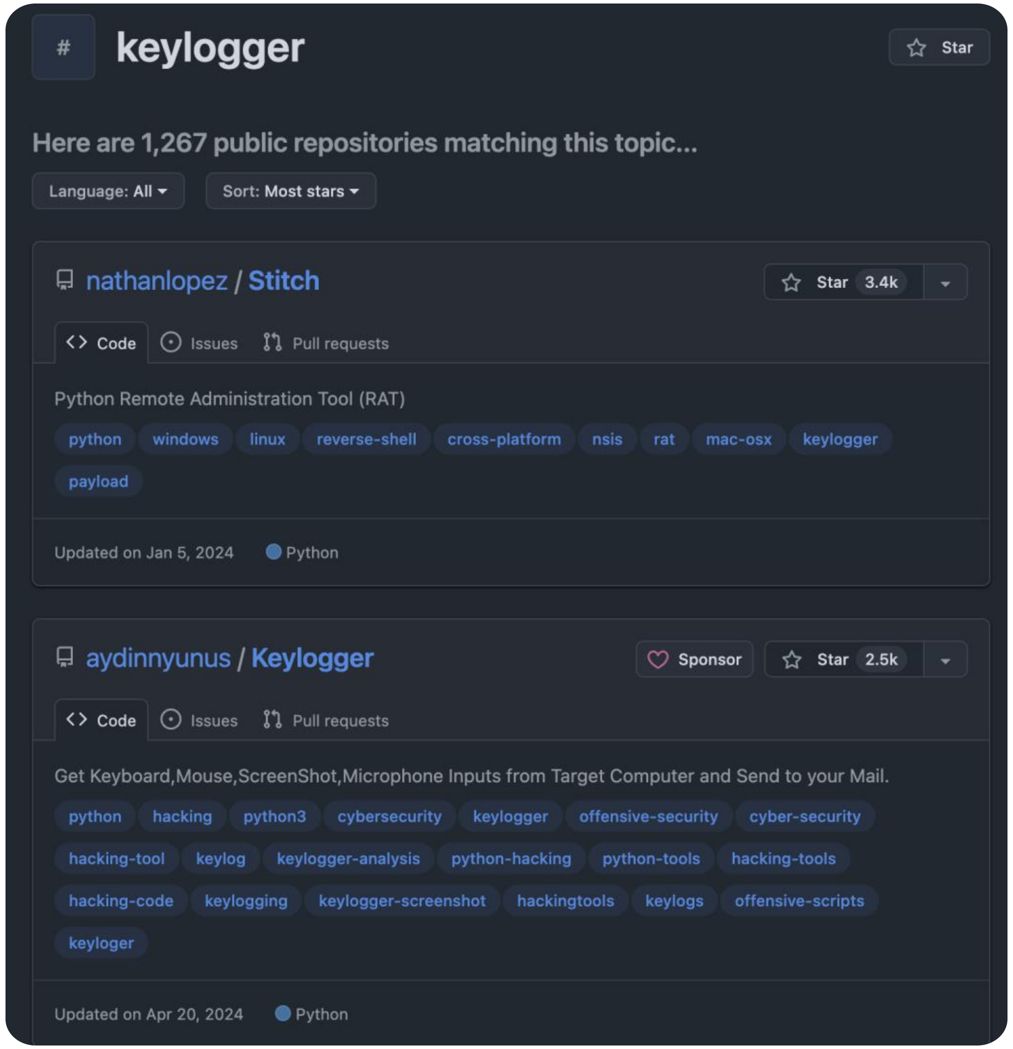
Encryption protects confidentiality, but not against keyloggers.



Target: Windows OS Device



Language: C++



keylogger

Star

Here are 1,267 public repositories matching this topic...

Language: All

Sort: Most stars

nathanlopez / Stitch

Star 3.4k

Code Issues Pull requests

Python Remote Administration Tool (RAT)

python windows linux reverse-shell cross-platform nsis rat mac-osx keylogger payload

Updated on Jan 5, 2024 ● Python

aydinnyunus / Keylogger

Sponsor Star 2.5k

Code Issues Pull requests

Get Keyboard,Mouse,ScreenShot,Microphone Inputs from Target Computer and Send to your Mail.

python hacking python3 cybersecurity keylogger offensive-security cyber-security hacking-tool keylog keylogger-analysis python-hacking python-tools hacking-tools hacking-code keylogging keylogger-screenshot hackingtools keylogs offensive-scripts keyloger

Updated on Apr 20, 2024 ● Python

Python

- Interpreted on runtime
- My top preference language

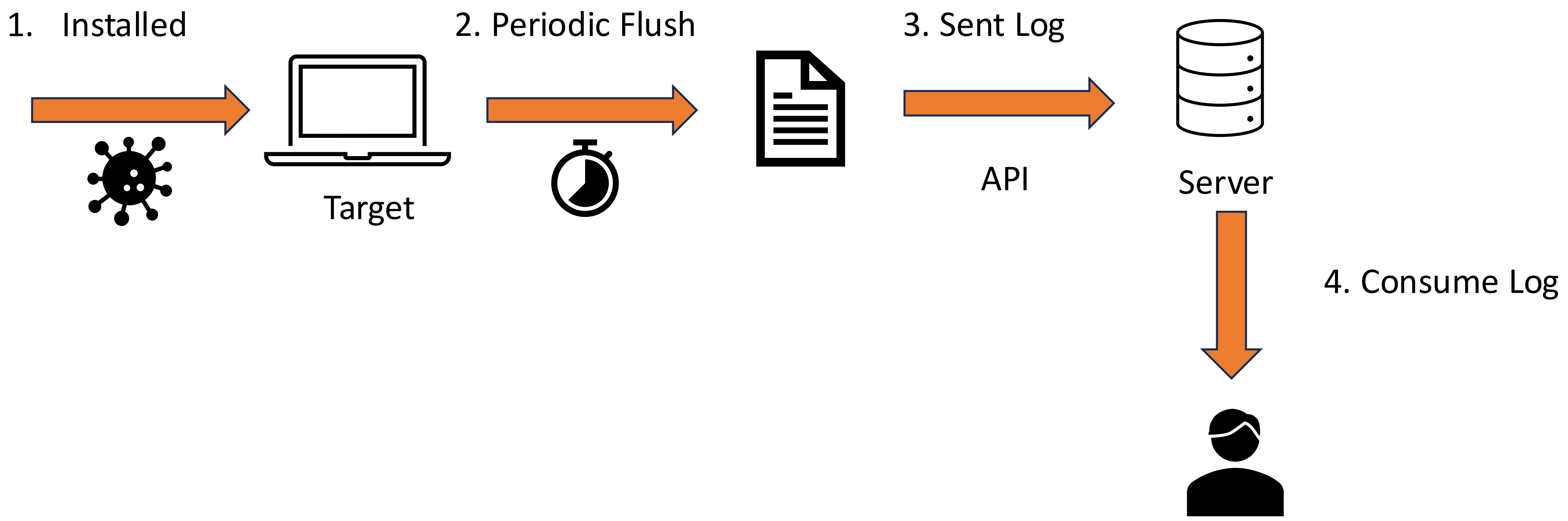
C++

- Compiled language
- Haven't used it in some years

Key Features

- Key stroke log
    - Filtering keystroke
    - Periodic flush
- Auto Launch
- Run in Background
- Log deliver to Server via API

Flowchart


1. Installed
Target
2. Periodic Flush
3. Sent Log
API
Server
4. Consume Log

Design Consideration

- Why periodic flush keystroke?

Reduce Disk I/O, Performance and Stealth Consideration

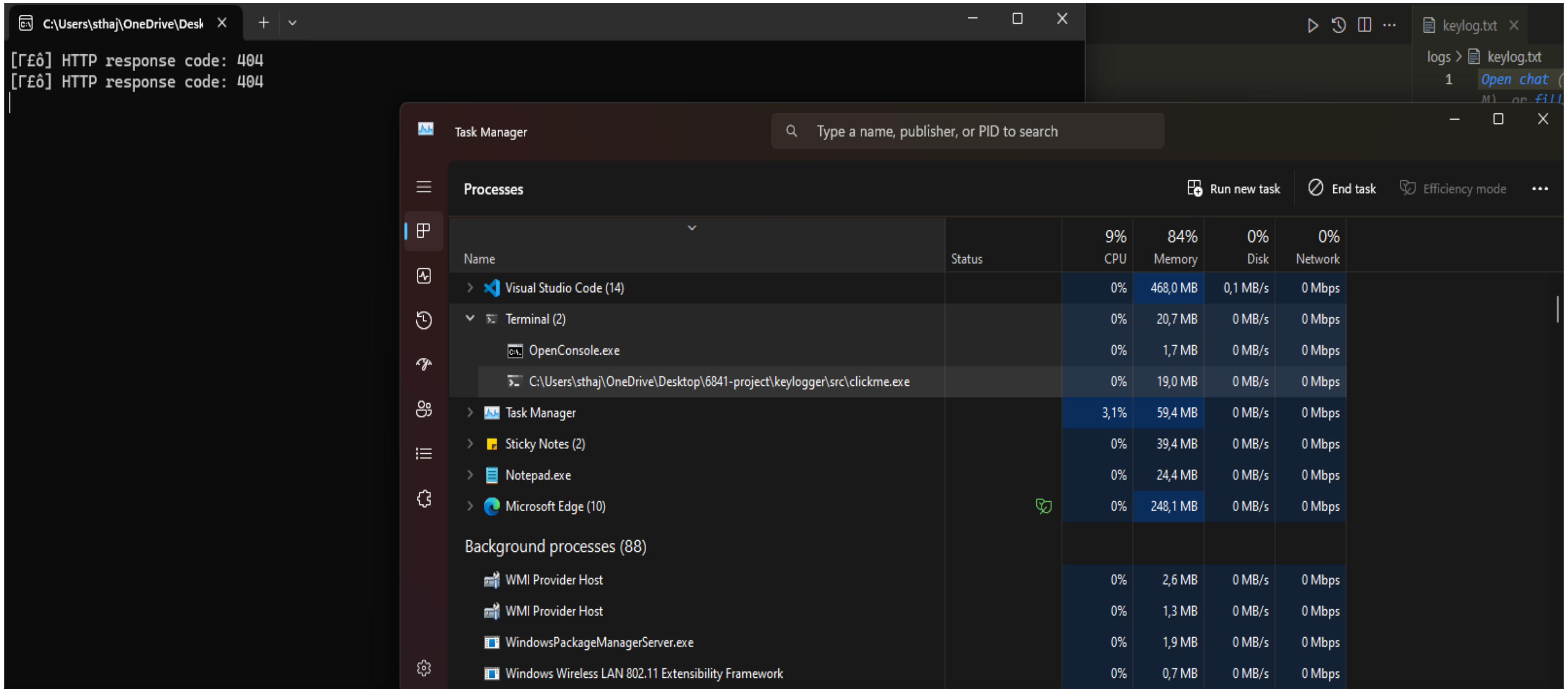
- Why filtering keystroke?

Keep only relevant keystroke (alphanumeric + symbols. The one commonly used in password)

- Why deliver over API ?

APIs outgoing request can blend with browsing https traffic. Increase stealth.
API request do not need creds unlike email.

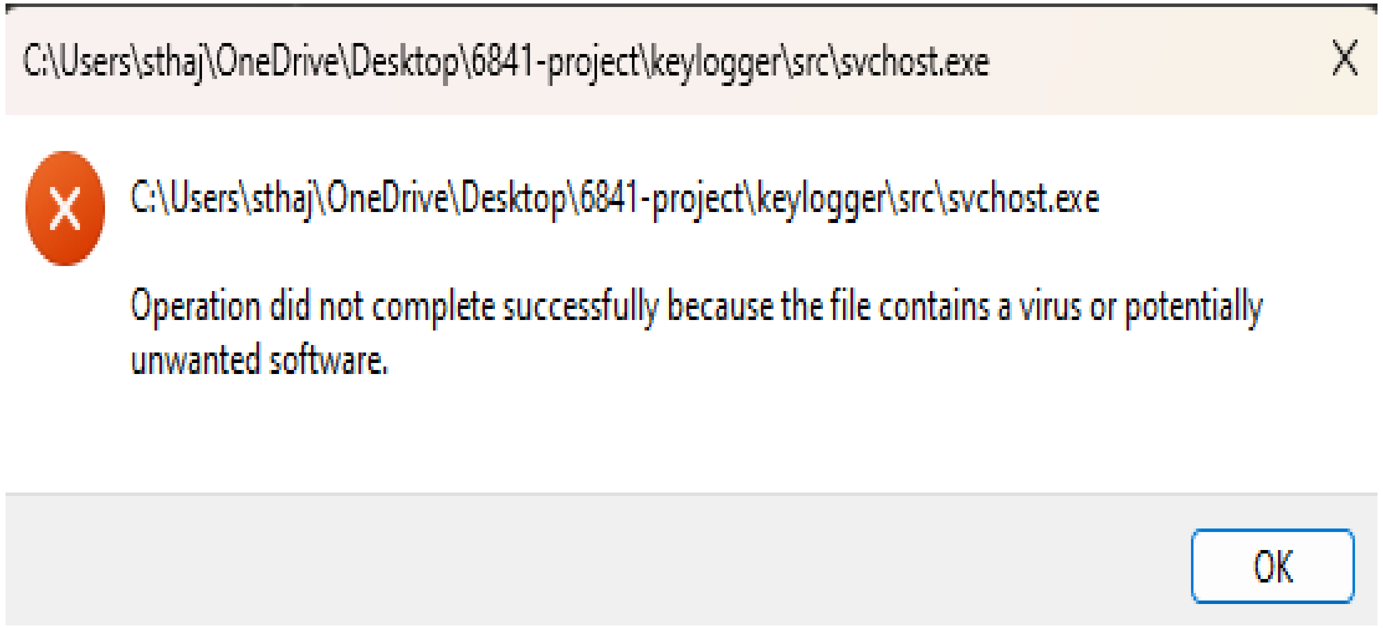
Discovery Attempt: Program Console



```
[Γ£ô] HTTP response code: 404
[Γ£ô] HTTP response code: 404
```

Name	Status	9% CPU	84% Memory	0% Disk	0% Network
Visual Studio Code (14)		0%	468,0 MB	0,1 MB/s	0 Mbps
Terminal (2)		0%	20,7 MB	0 MB/s	0 Mbps
OpenConsole.exe		0%	1,7 MB	0 MB/s	0 Mbps
C:\Users\sthaj\OneDrive\Desktop\6841-project\keylogger\src\clickme.exe		0%	19,0 MB	0 MB/s	0 Mbps
Task Manager		3,1%	59,4 MB	0 MB/s	0 Mbps
Sticky Notes (2)		0%	39,4 MB	0 MB/s	0 Mbps
Notepad.exe		0%	24,4 MB	0 MB/s	0 Mbps
Microsoft Edge (10)		0%	248,1 MB	0 MB/s	0 Mbps
Background processes (88)					
WMI Provider Host		0%	2,6 MB	0 MB/s	0 Mbps
WMI Provider Host		0%	1,3 MB	0 MB/s	0 Mbps
WindowsPackageManagerServer.exe		0%	1,9 MB	0 MB/s	0 Mbps
Windows Wireless LAN 802.11 Extensibility Framework		0%	0,7 MB	0 MB/s	0 Mbps

Discovery Attempt: Installation Warning



C:\Users\sthaj\OneDrive\Desktop\6841-project\keylogger\src\svchost.exe

C:\Users\sthaj\OneDrive\Desktop\6841-project\keylogger\src\svchost.exe

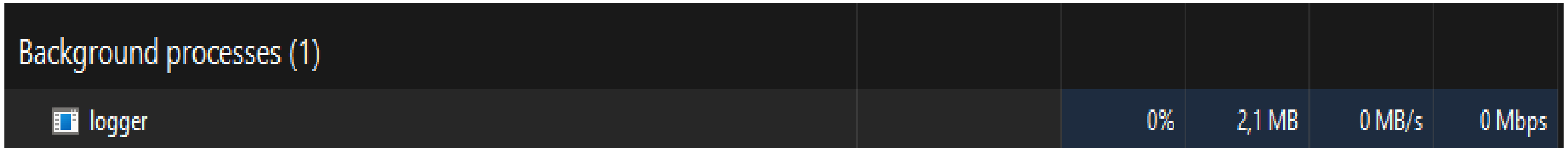
Operation did not complete successfully because the file contains a virus or potentially unwanted software.

Reverse Psychology from Windows Defender

Svchost.exe, also known as the Service Host process, is a crucial system process in Windows that hosts and manages various services

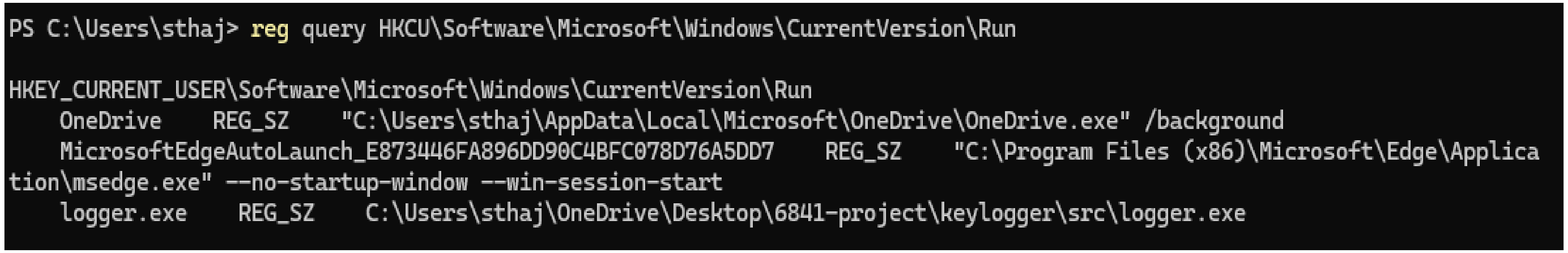
Hiding Attempt: Program Execution

Execute in Background without any obviously noticable window



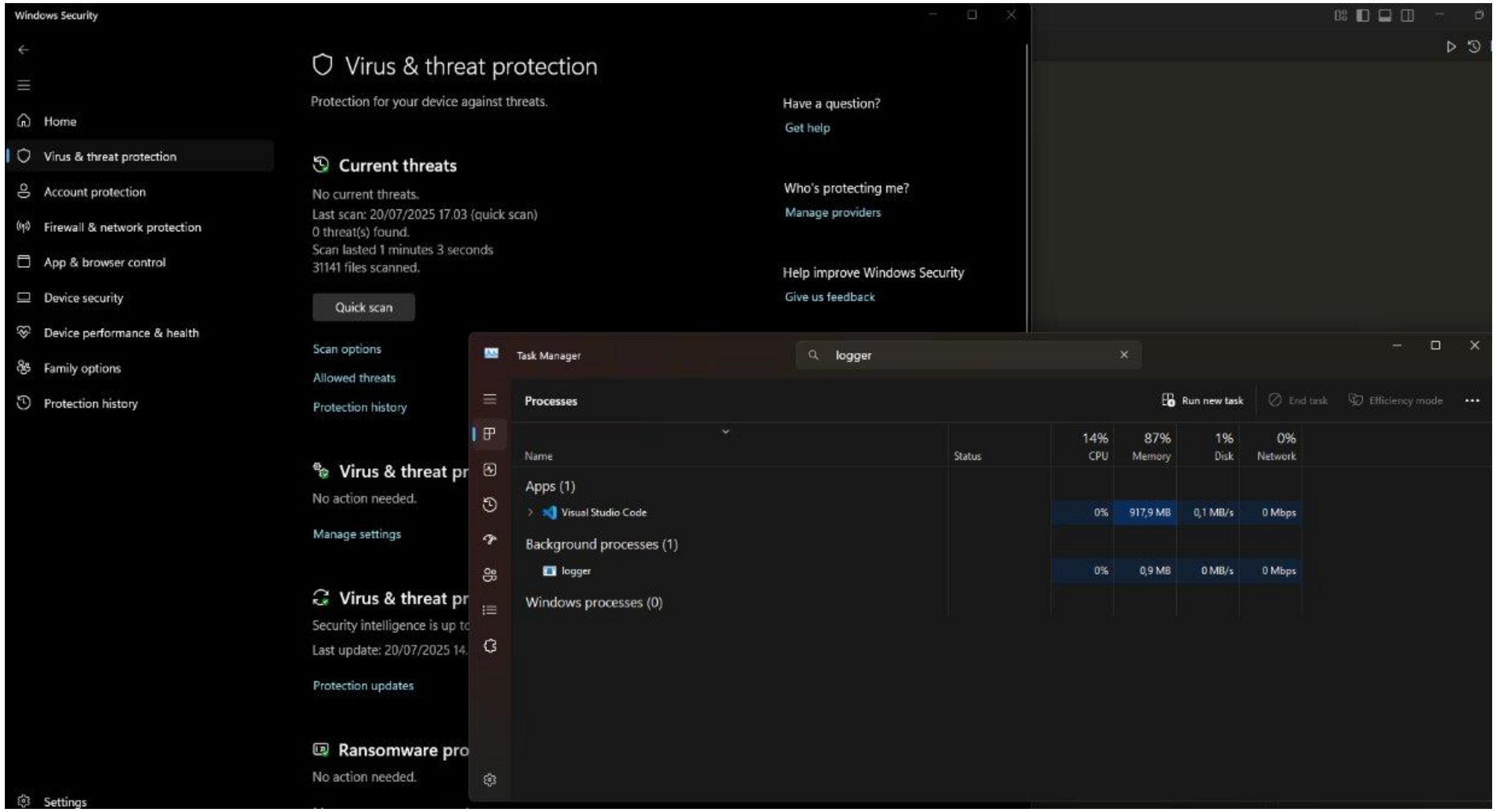
```
Background processes (1)
    logger                                  0%    2,1 MB    0 MB/s    0 Mbps
```

Execute in Background so program can Autolaunch



```
PS C:\Users\sthaj> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    OneDrive    REG_SZ    "C:\Users\sthaj\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
    MicrosoftEdgeAutoLaunch_E873446FA896DD90C4BFC078D76A5DD7    REG_SZ    "C:\Program Files (x86)\Microsoft\Edge\Applica
tion\msedge.exe" --no-startup-window --win-session-start
    logger.exe    REG_SZ    C:\Users\sthaj\OneDrive\Desktop\6841-project\keylogger\src\logger.exe
```

Discovery Attempt: Windows Defender Scan



Windows Security

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 20/07/2025 17.03 (quick scan)
0 threat(s) found.
Scan lasted 1 minutes 3 seconds
31141 files scanned.

Virus & threat pr
No action needed.

Virus & threat pr
Security intelligence is up to
Last update: 20/07/2025 14.

Ransomware pro
No action needed.

Have a question?
Get help

Who's protecting me?
Manage providers

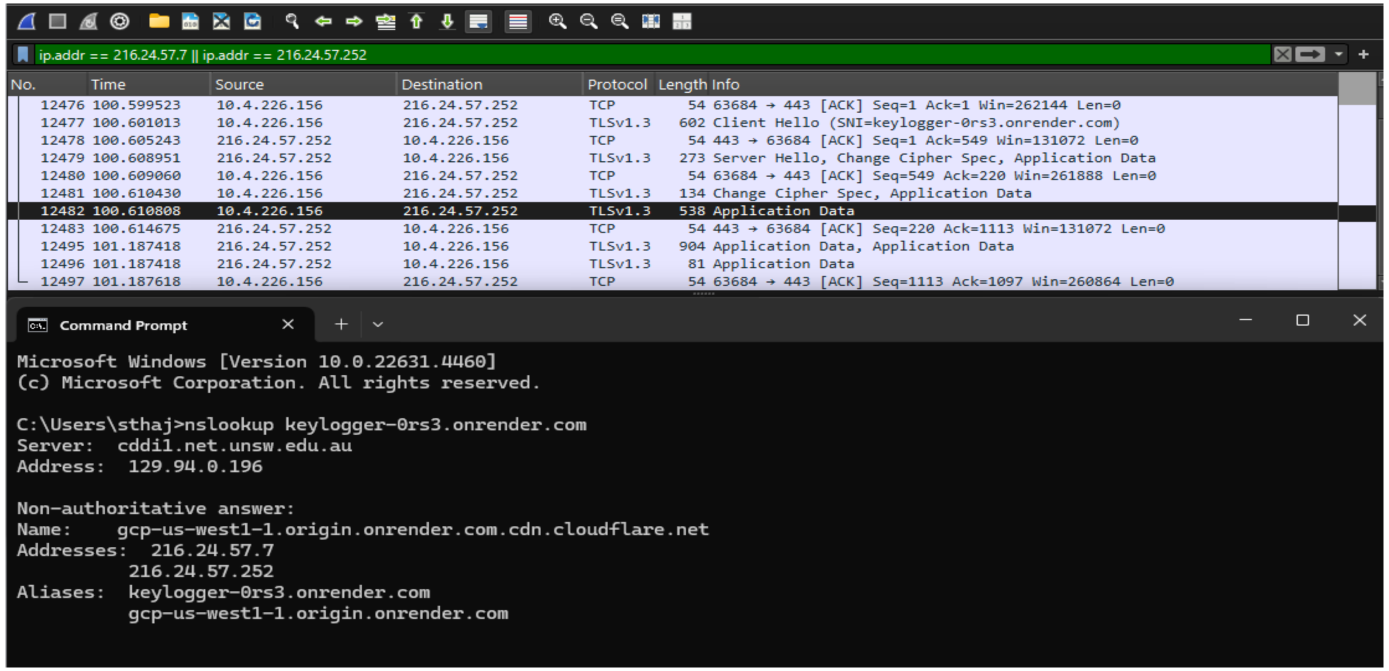
Help improve Windows Security
Give us feedback

Task Manager — search: logger

Processes

```
Name                        Status   14%   87%       1%        0%
                                     CPU   Memory    Disk      Network
Apps (1)
  Visual Studio Code                 0%    917,9 MB  0,1 MB/s  0 Mbps
Background processes (1)
  logger                             0%    0,9 MB    0 MB/s    0 Mbps
Windows processes (0)
```

Discovery Attempt: Wireshark Trace



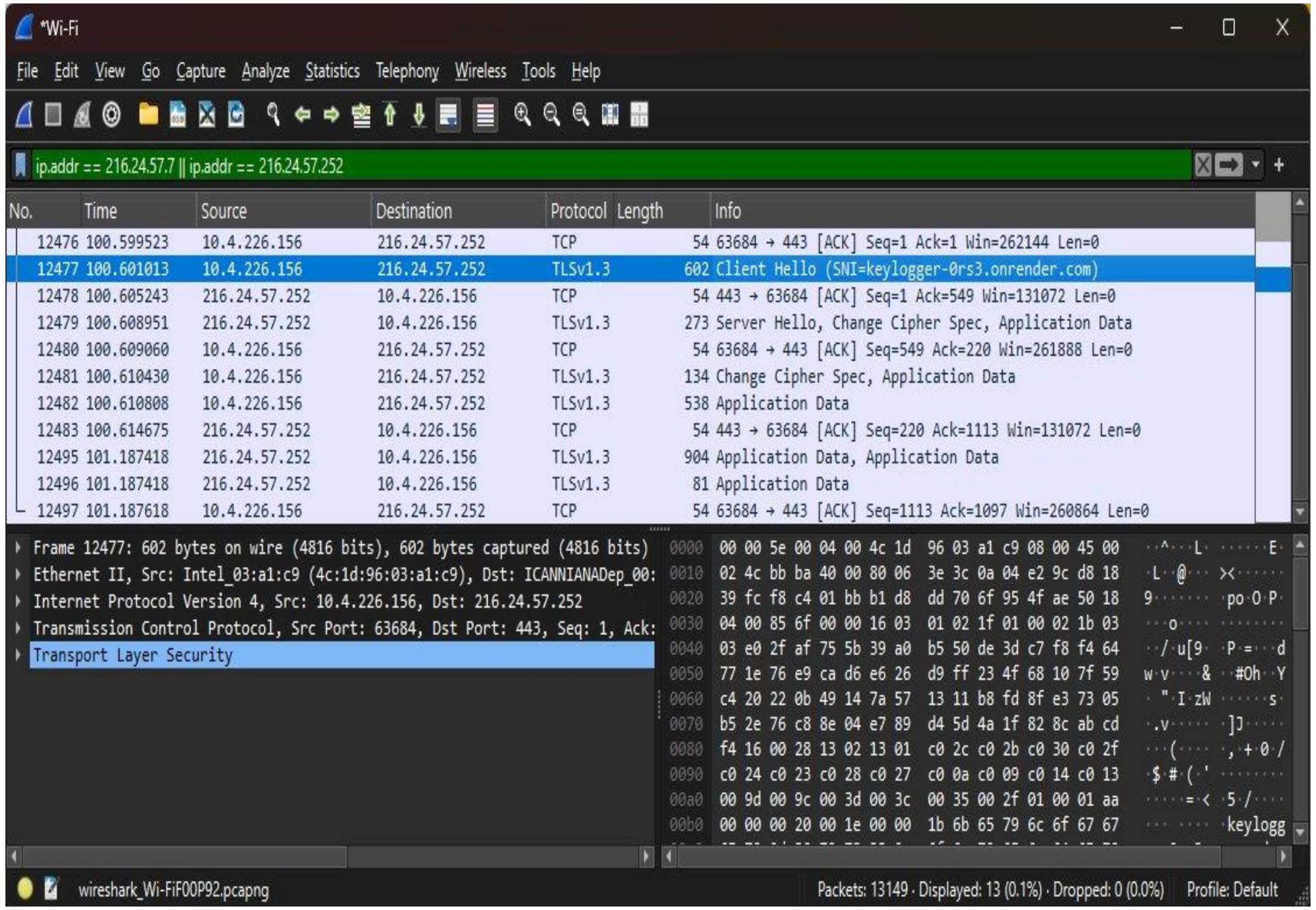
```
ip.addr == 216.24.57.7 || ip.addr == 216.24.57.252
```

```
No.    Time        Source           Destination      Protocol  Length Info
12476 100.599523  10.4.226.156     216.24.57.252    TCP         54 63684 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
12477 100.601013  10.4.226.156     216.24.57.252    TLSv1.3    602 Client Hello (SNI=keylogger-0rs3.onrender.com)
12478 100.605243  216.24.57.252    10.4.226.156     TCP         54 443 → 63684 [ACK] Seq=1 Ack=549 Win=131072 Len=0
12479 100.608951  216.24.57.252    10.4.226.156     TLSv1.3    273 Server Hello, Change Cipher Spec, Application Data
12480 100.609060  10.4.226.156     216.24.57.252    TCP         54 63684 → 443 [ACK] Seq=549 Ack=220 Win=261888 Len=0
12481 100.610430  10.4.226.156     216.24.57.252    TLSv1.3    134 Change Cipher Spec, Application Data
12482 100.610808  10.4.226.156     216.24.57.252    TLSv1.3    538 Application Data
12483 100.614675  216.24.57.252    10.4.226.156     TCP         54 443 → 63684 [ACK] Seq=220 Ack=1113 Win=131072 Len=0
12495 101.187418  216.24.57.252    10.4.226.156     TLSv1.3    904 Application Data, Application Data
12496 101.187418  216.24.57.252    10.4.226.156     TLSv1.3     81 Application Data
12497 101.187618  10.4.226.156     216.24.57.252    TCP         54 63684 → 443 [ACK] Seq=1113 Ack=1097 Win=260864 Len=0
```

Command Prompt

```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sthaj>nslookup keylogger-0rs3.onrender.com
Server:  cddi1.net.unsw.edu.au
Address:  129.94.0.196

Non-authoritative answer:
Name:    gcp-us-west1-1.origin.onrender.com.cdn.cloudflare.net
Addresses:  216.24.57.7
          216.24.57.252
Aliases:  keylogger-0rs3.onrender.com
          gcp-us-west1-1.origin.onrender.com
```

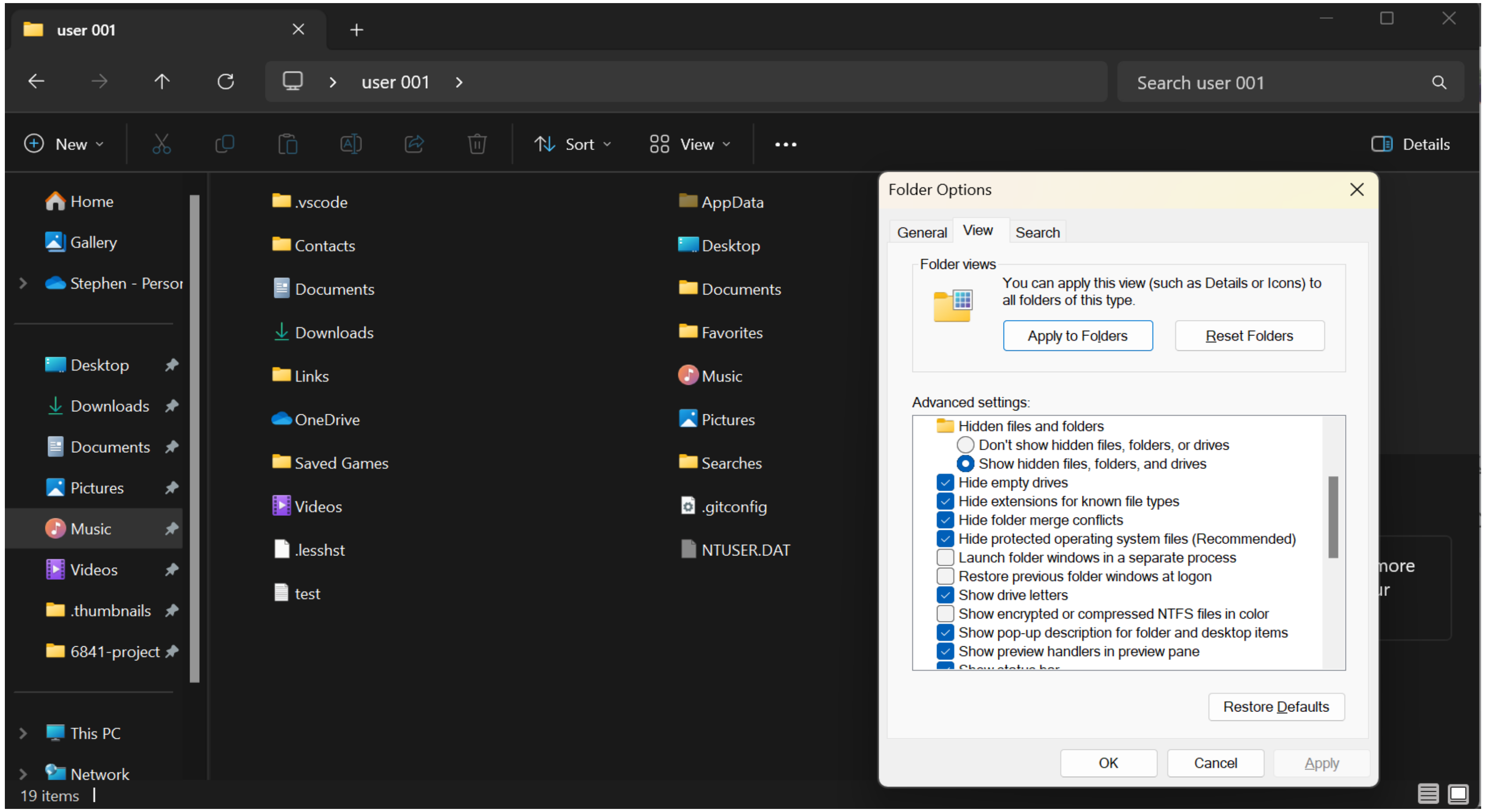
Trace Outgoing POST


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 216.24.57.7 || ip.addr == 216.24.57.252

No.    Time        Source          Destination     Protocol Length Info
 12476 100.599523  10.4.226.156    216.24.57.252   TCP         54 63684 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 12477 100.601013  10.4.226.156    216.24.57.252   TLSv1.3    602 Client Hello (SNI=keylogger-0rs3.onrender.com)
 12478 100.605243  216.24.57.252   10.4.226.156    TCP         54 443 → 63684 [ACK] Seq=1 Ack=549 Win=131072 Len=0
 12479 100.608951  216.24.57.252   10.4.226.156    TLSv1.3    273 Server Hello, Change Cipher Spec, Application Data
 12480 100.609060  10.4.226.156    216.24.57.252   TCP         54 63684 → 443 [ACK] Seq=549 Ack=220 Win=261888 Len=0
 12481 100.610430  10.4.226.156    216.24.57.252   TLSv1.3    134 Change Cipher Spec, Application Data
 12482 100.610808  10.4.226.156    216.24.57.252   TLSv1.3    538 Application Data
 12483 100.614675  216.24.57.252   10.4.226.156    TCP         54 443 → 63684 [ACK] Seq=220 Ack=1113 Win=131072 Len=0
 12495 101.187418  216.24.57.252   10.4.226.156    TLSv1.3    904 Application Data, Application Data
 12496 101.187418  216.24.57.252   10.4.226.156    TLSv1.3     81 Application Data
 12497 101.187618  10.4.226.156    216.24.57.252   TCP         54 63684 → 443 [ACK] Seq=1113 Ack=1097 Win=260864 Len=0

› Frame 12477: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits)
› Ethernet II, Src: Intel_03:a1:c9 (4c:1d:96:03:a1:c9), Dst: ICANNIANADep_00:
› Internet Protocol Version 4, Src: 10.4.226.156, Dst: 216.24.57.252
› Transmission Control Protocol, Src Port: 63684, Dst Port: 443, Seq: 1, Ack:
› Transport Layer Security

0000  00 00 5e 00 04 00 4c 1d  96 03 a1 c9 08 00 45 00   ··^···L· ······E·
0010  02 4c bb ba 40 00 80 06  3e 3c 0a 04 e2 9c d8 18   ·L··@··· ><······
0020  39 fc f8 c4 01 bb b1 d8  dd 70 6f 95 4f ae 50 18   9······· ·po·O·P·
0030  04 00 85 6f 00 00 16 03  01 02 1f 01 00 02 1b 03   ···o···· ········
0040  03 e0 2f af 75 5b 39 a0  b5 50 de 3d c7 f8 f4 64   ··/·u[9· ·P·=···d
0050  77 1e 76 e9 ca d6 e6 26  d9 ff 23 4f 68 10 7f 59   w·v····& ··#Oh··Y
0060  c4 20 22 0b 49 14 7a 57  13 11 b8 fd 8f e3 73 05   · "·I·zW ······s·
0070  b5 2e 76 c8 8e 04 e7 89  d4 5d 4a 1f 82 8c ab cd   ·.v····· ·]J·····
0080  f4 16 00 28 13 02 13 01  c0 2c c0 2b c0 30 c0 2f   ···(···· ·,·+·0·/
0090  c0 24 c0 23 c0 28 c0 27  c0 0a c0 09 c0 14 c0 13   ·$·#·(·' ········
00a0  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 01 00 01 aa   ·····=·< ·5·/····
00b0  00 00 00 20 00 1e 00 00  1b 6b 65 79 6c 6f 67 67   ··· ···· ·keylogg

wireshark_Wi-FiF00P92.pcapng     Packets: 13149 · Displayed: 13 (0.1%) · Dropped: 0 (0.0%)     Profile: Default
```

API request made with **HTTPS** protocol, payload are encrypted.
Nothing particular suspicious found

Hiding Attempt: Log File Location



.vscode
Contacts
Documents
Downloads
Links
OneDrive
Saved Games
Videos
.lesshst
test
AppData
Desktop
Documents
Favorites
Music
Pictures
Searches
.gitconfig
NTUSER.DAT

Folder Options

General | View | Search

Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Apply to Folders | Reset Folders

Advanced settings:

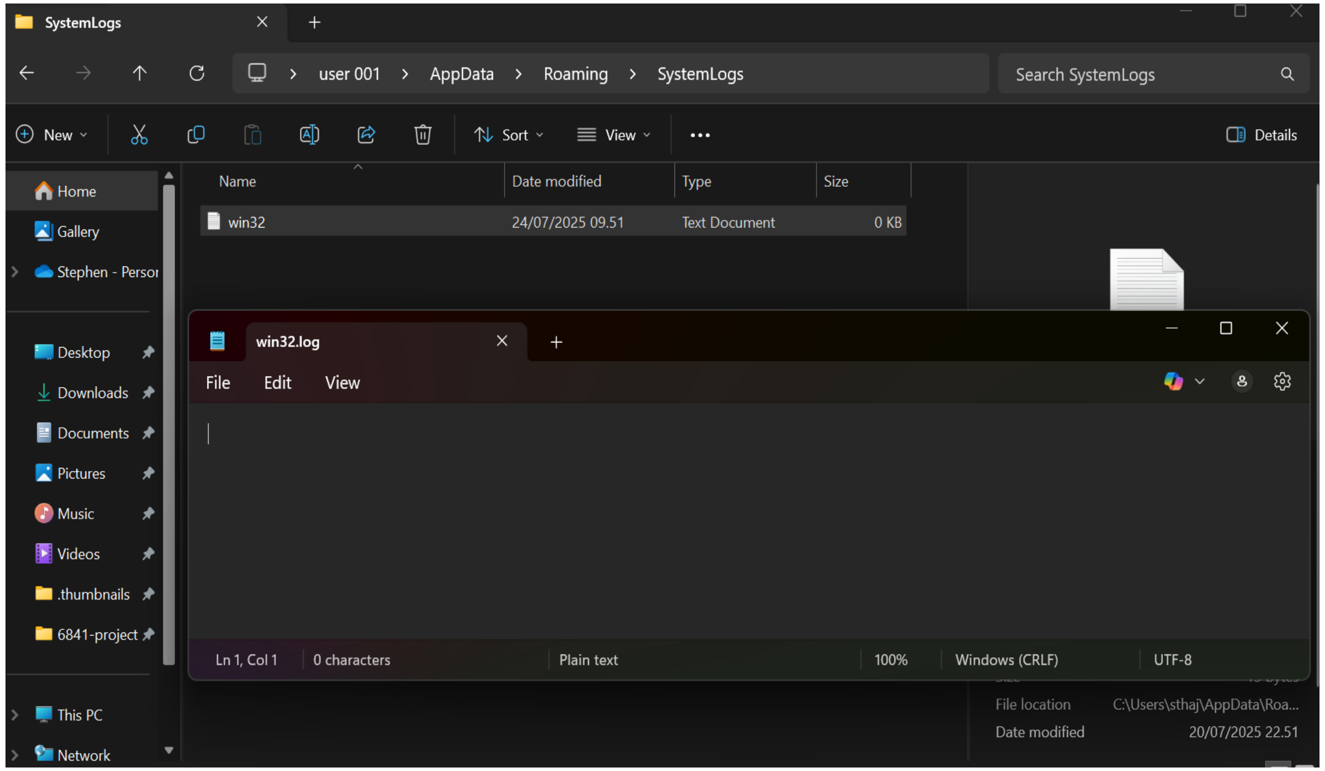
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ✓ Hide empty drives
- ✓ Hide extensions for known file types
- ✓ Hide folder merge conflicts
- ✓ Hide protected operating system files (Recommended)
- ☐ Launch folder windows in a separate process
- ☐ Restore previous folder windows at logon
- ✓ Show drive letters
- ☐ Show encrypted or compressed NTFS files in color
- ✓ Show pop-up description for folder and desktop items
- ✓ Show preview handlers in preview pane

Restore Defaults

OK | Cancel | Apply

AppData folder is **by default hidden**

Hiding Attempt: Log File Location



Name	Date modified	Type	Size
win32	24/07/2025 09.51	Text Document	0 KB

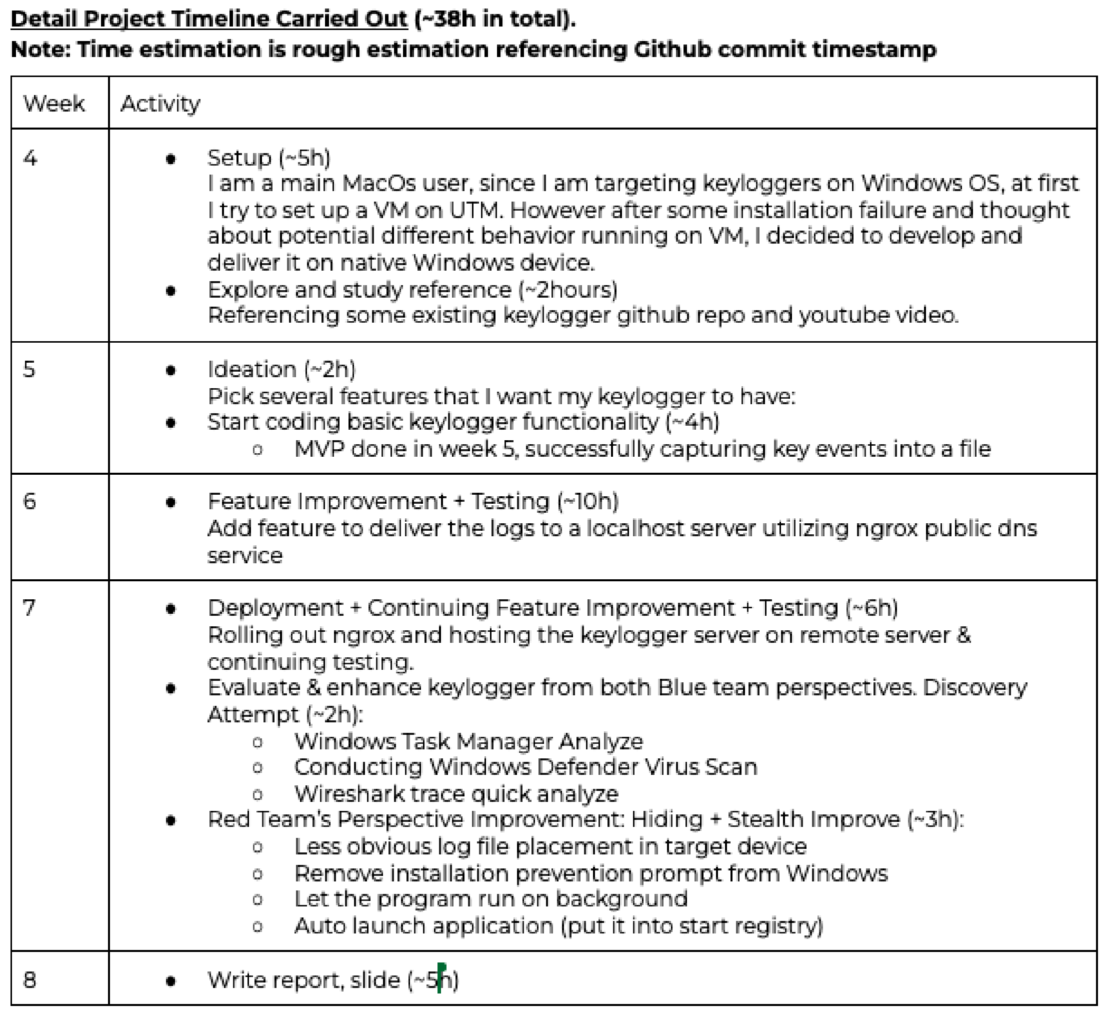
Ln 1, Col 1 | 0 characters | Plain text | 100% | Windows (CRLF) | UTF-8

File location	C:\Users\sthaj\AppData\Roa...
Date modified	20/07/2025 22.51

Key strokes are buffered and logged into the file.

- Can consider encryption content (NOT for demo)
- Log content are periodically clear after sending to server

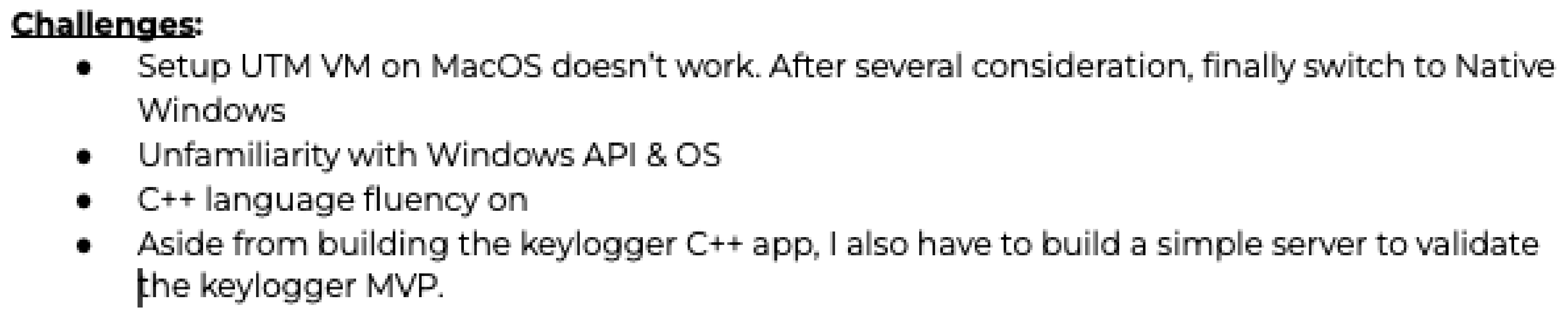
Timeline Carried Out



<u>Detail Project Timeline Carried Out</u> (~38h in total).
Note: Time estimation is rough estimation referencing Github commit timestamp

Week	Activity
4	• Setup (~5h) I am a main MacOs user, since I am targeting keyloggers on Windows OS, at first I try to set up a VM on UTM. However after some installation failure and thought about potential different behavior running on VM, I decided to develop and deliver it on native Windows device. • Explore and study reference (~2hours) Referencing some existing keylogger github repo and youtube video.
5	• Ideation (~2h) Pick several features that I want my keylogger to have: • Start coding basic keylogger functionality (~4h) 　○ MVP done in week 5, successfully capturing key events into a file
6	• Feature Improvement + Testing (~10h) Add feature to deliver the logs to a localhost server utilizing ngrox public dns service
7	• Deployment + Continuing Feature Improvement + Testing (~6h) Rolling out ngrox and hosting the keylogger server on remote server & continuing testing. • Evaluate & enhance keylogger from both Blue team perspectives. Discovery Attempt (~2h): 　○ Windows Task Manager Analyze 　○ Conducting Windows Defender Virus Scan 　○ Wireshark trace quick analyze • Red Team's Perspective Improvement: Hiding + Stealth Improve (~3h): 　○ Less obvious log file placement in target device 　○ Remove installation prevention prompt from Windows 　○ Let the program run on background 　○ Auto launch application (put it into start registry)
8	• Write report, slide (~5h)

Challenges



Challenges:

- Setup UTM VM on MacOS doesn't work. After several consideration, finally switch to Native Windows
- Unfamiliarity with Windows API & OS
- C++ language fluency on
- Aside from building the keylogger C++ app, I also have to build a simple server to validate the keylogger MVP.

DEMO