Windows Mini KeyLogger - Daniel Ayzenshteyn

The key logger uses global hooks to detect every single one of the keystrokes made in the current desktop in which the keylogger is running.
It stores each key press in a memory buffer thus avoiding writing to the hard drive.
The keylogger is planned to exfiltrate the data with a usb stick - on usb insertion the keylogger detects it and writes to it an encrypted version of the buffer with a randomly generated log file name.
The MiniKeyLogger.exe can be started from quickly from the command line and on start it executes the main part of the keylogger which is called MiniKeyLoggerDaemon - It runs on background and is listening for keystrokes and usb insertion - for data exfiltration.

Command line:

```
MiniKeyLogger.exe start
```

Starts the daemon keylogger in the background.

```
MiniKeyLogger.exe stop
```

Stop the daemon keylogger, every thing in the buffer is deleted - the buffer is volatile.

```
MiniKeyLogger.exe decrypt <path to encrypted log file>
```

Decrypts the file with all the keylogging and displayes it.

The keylogger has millisecond precision ability to document when the key was pressed, and in which application window it happened. Giving the ability to quickly search for credentials in RDP, SSH, Web applications, etc… or interesting conversations in Gmail, ,Discord ,Whatsapp…

The keylogger doesn't write anything to the computer hard drive to avoid detection and only stores the logs in memory.
The keylogger has the ability to write swiftly to the inserted usb stick and exfiltrate all the data from memory.

**Encryption key is hardcoded.