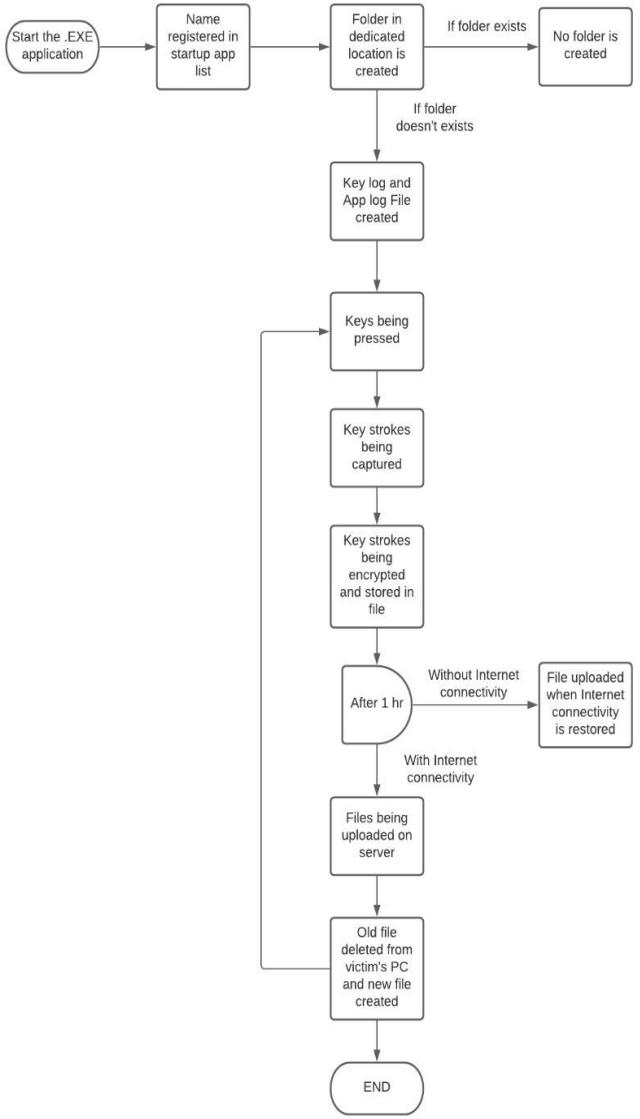
Features

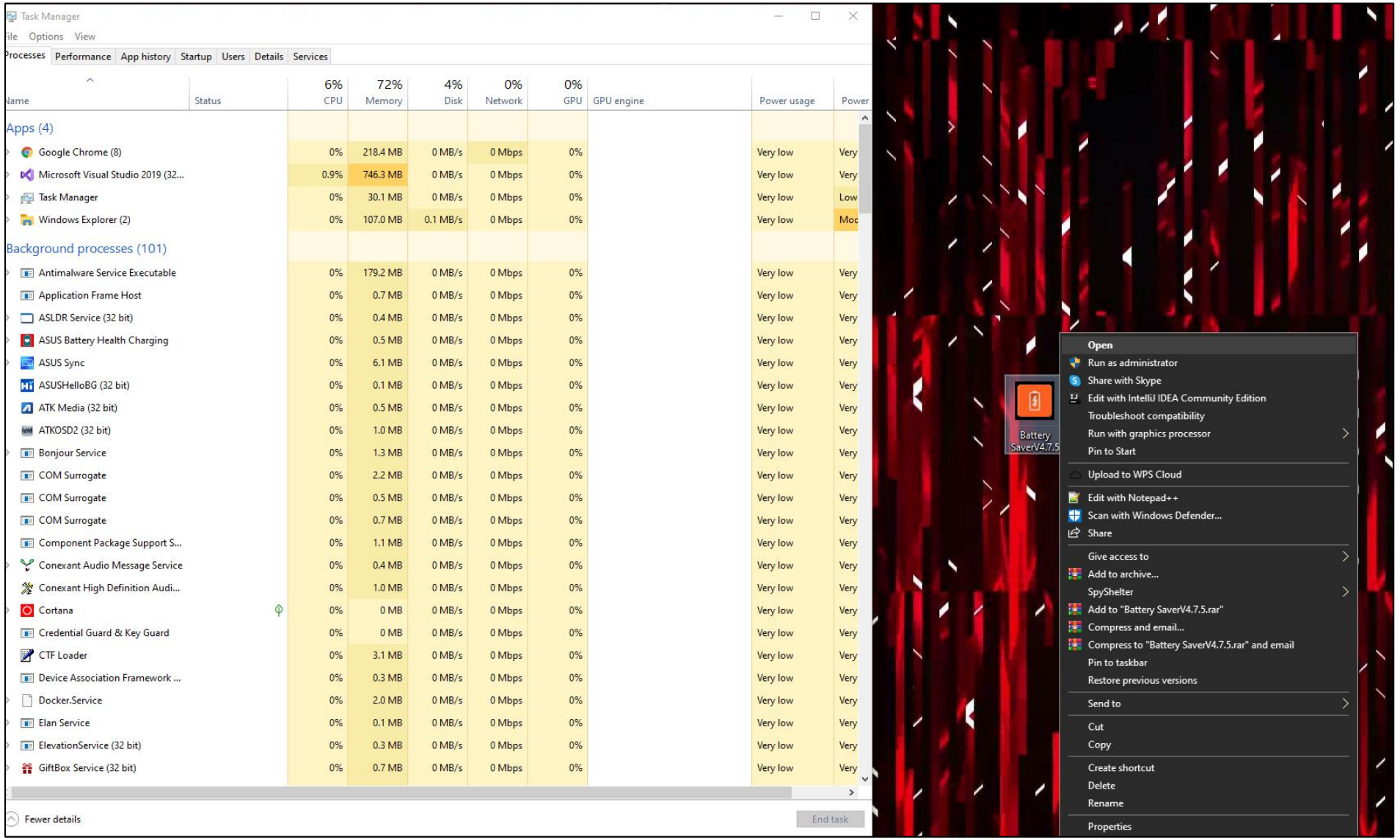
1. Key Logger acts like a legitimate software(Trojan Horse)
2. Encrypted Key Log files.
3. Keystroke Log files are uploaded to a server.
4. Gathers data about the users running application.
5. Gathers some additional information about the user.
6. Automatically runs at startup.

Specifications

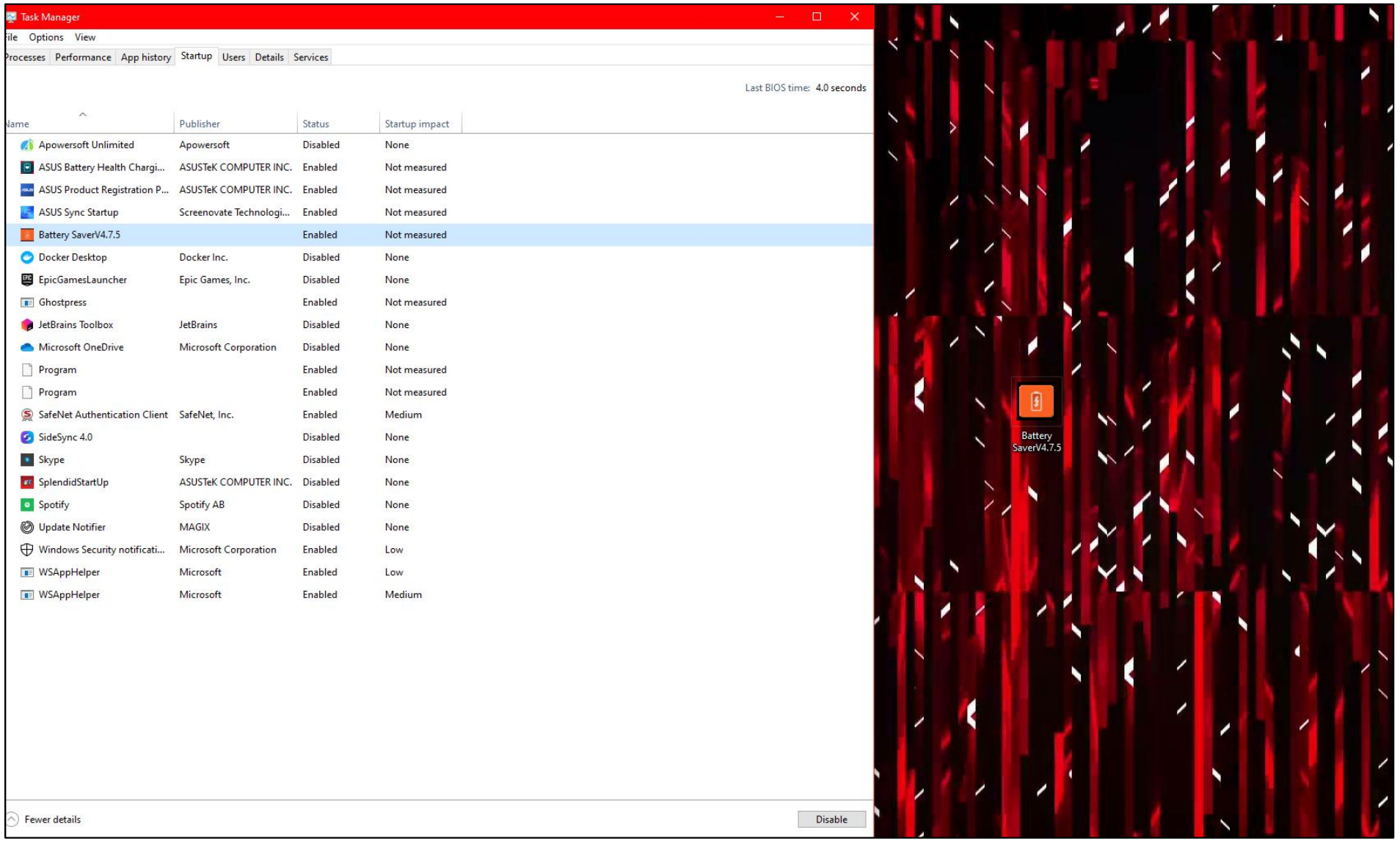
1. Programming Language Used - C#(C Sharp).
2. 2 Encryption Algorithm Used: White Space (Self Made)
3. Server Used - www.000webhost.com
4. Server Side Language Used - PHP
5. OS Platform - Windows.

Flowchart

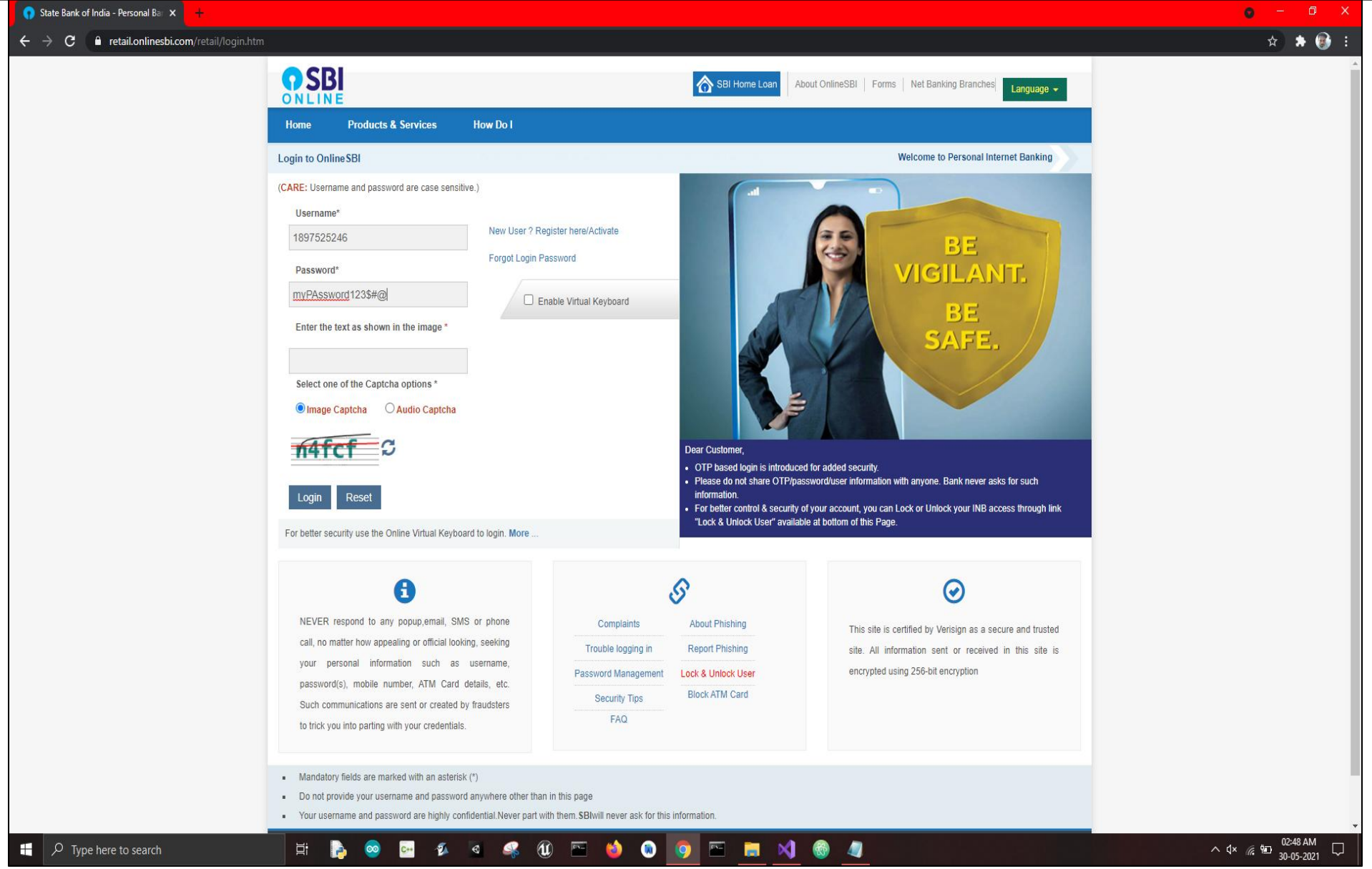

Start the .EXE application
Name registered in startup app list
Folder in dedicated location is created
If folder exists
No folder is created
If folder doesn't exists
Key log and App log File created
Keys being pressed
Key strokes being captured
Key strokes being encrypted and stored in file
After 1 hr
Without Internet connectivity
File uploaded when Internet connectivity is restored
With Internet connectivity
Files being uploaded on server
Old file deleted from victim's PC and new file created
END



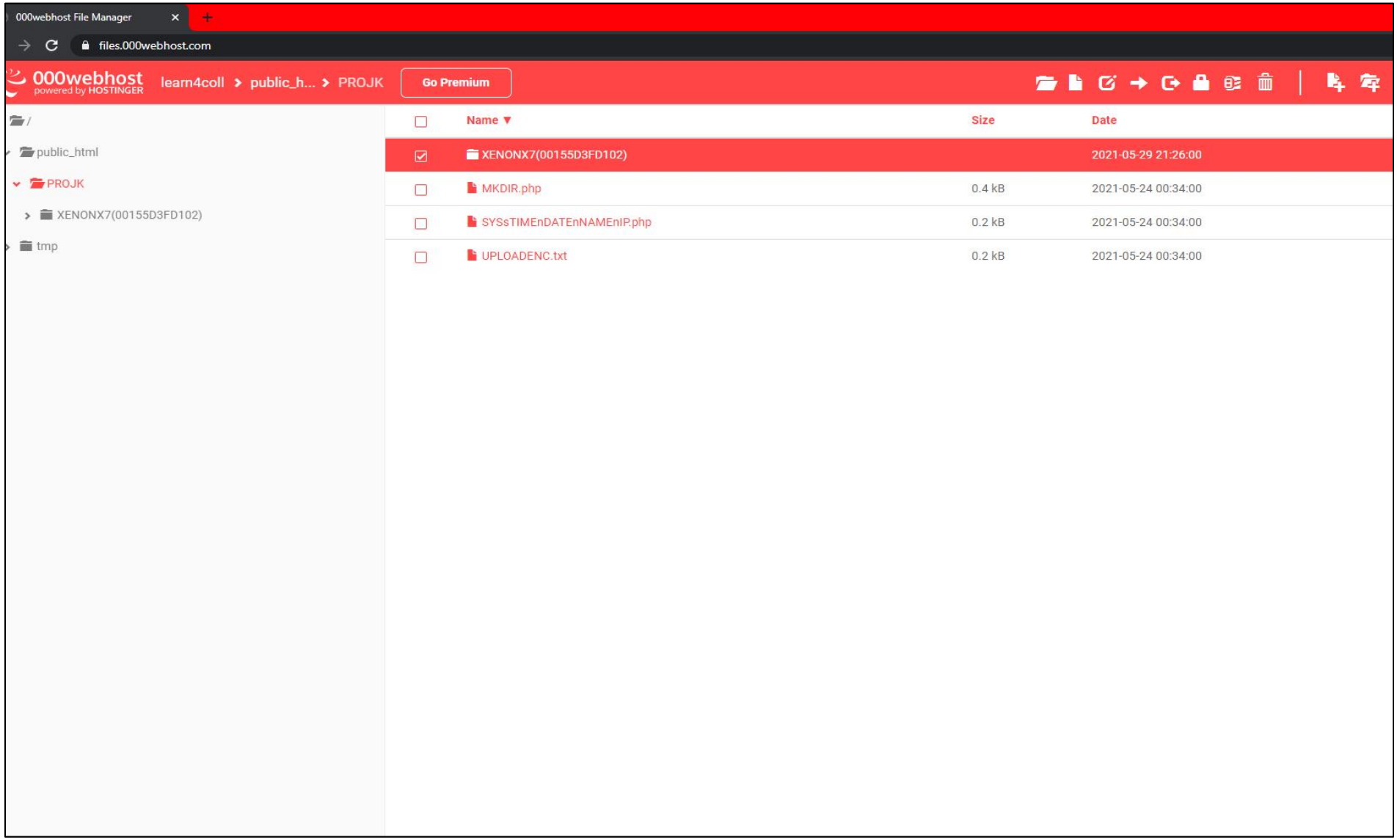
Our keylogger appears as a legitimate software to the target.



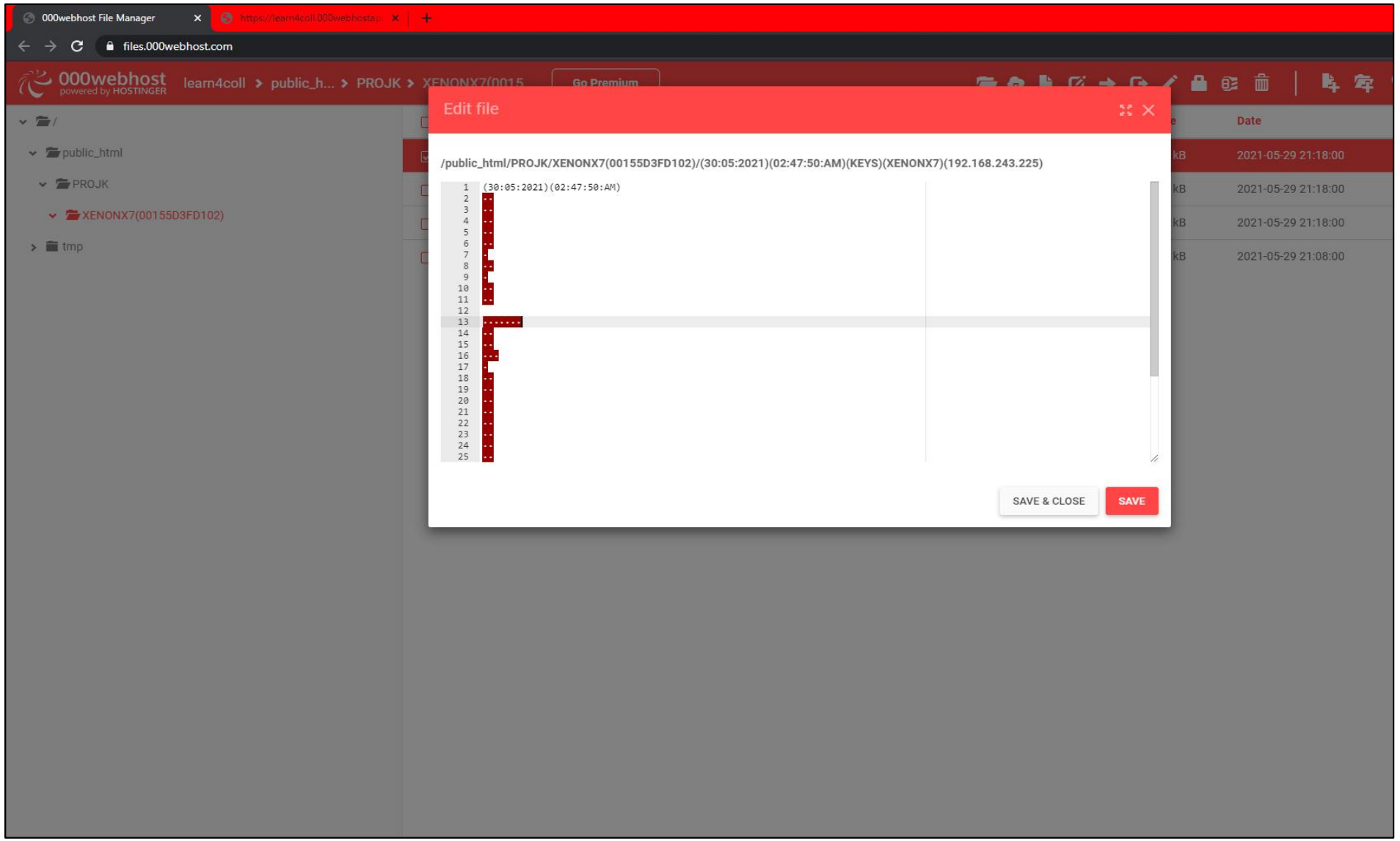
It registers itself in the startup app list. So that it runs contuniously 24x7.



We are entering our username and password on the official website of SBI on our browser.

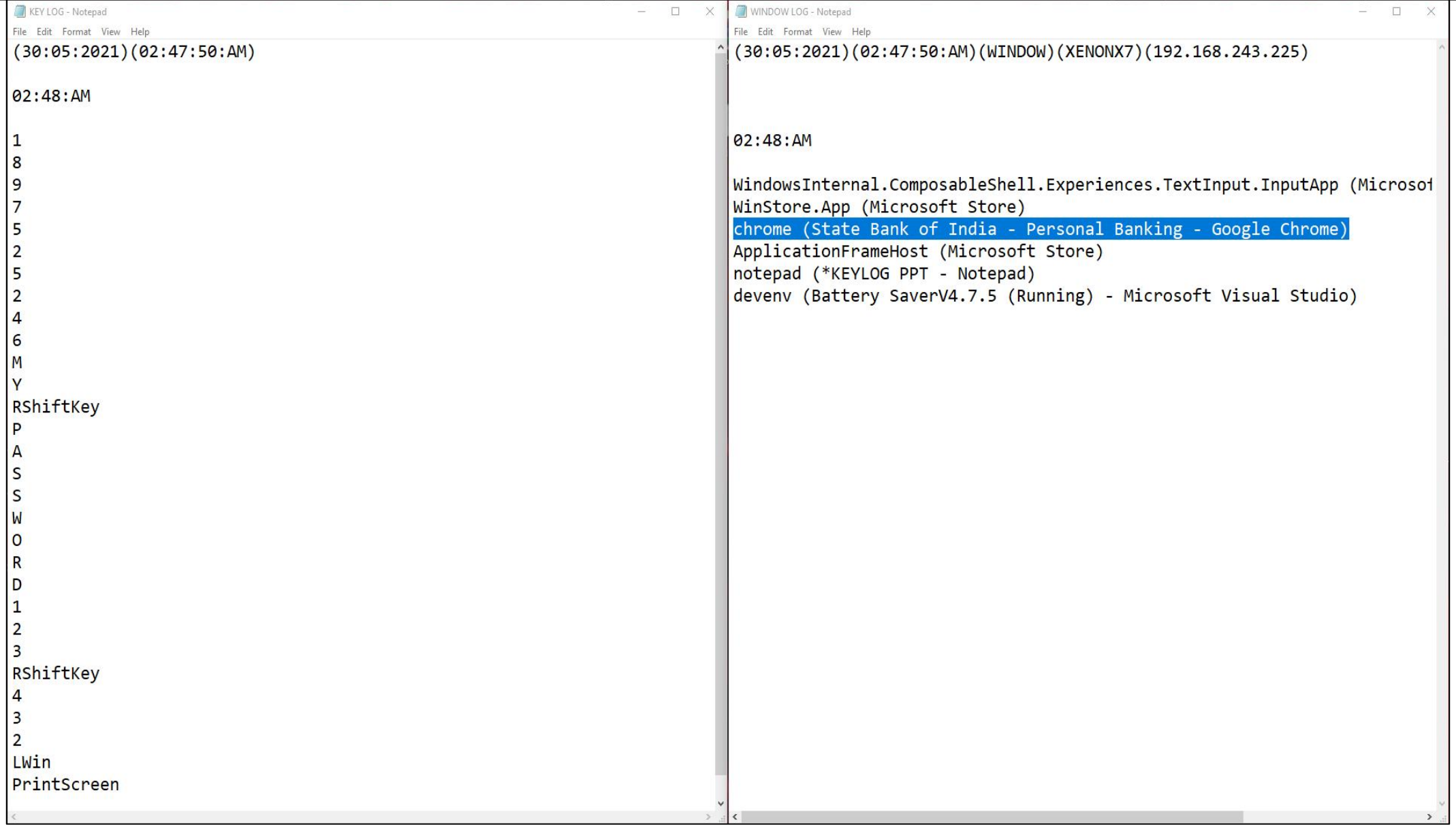


On our private server, a folder is created named after target's [System Name and (MAC address)].



The file containing the captured keystroke is encrypted. So, we can only see some dots.

Now we Paste the copied URL on the Decryptor Application window and click "Download and Decrypt" Button.



Now both the files are decrypted and with the help of these we can find the username and password of the SBI account.