

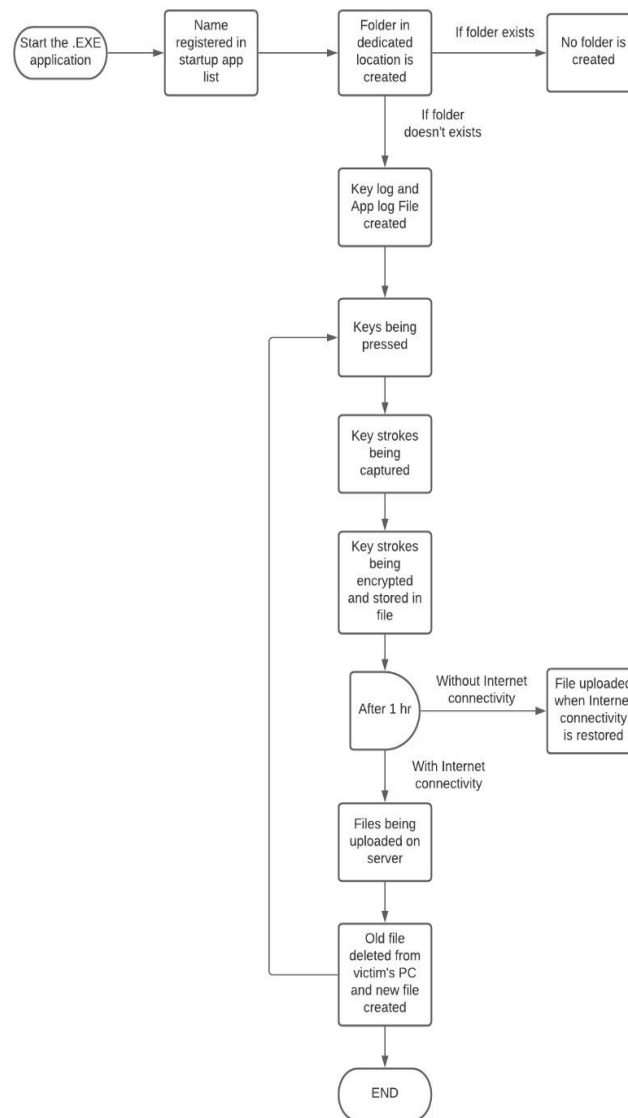
# Features

- 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. Encryption Algorithm Used: White Space (Self Made)**
- 3. Server Used - [www.000webhost.com](http://www.000webhost.com)**
- 4. Server Side Language Used - PHP**
- 5. OS Platform - Windows.**

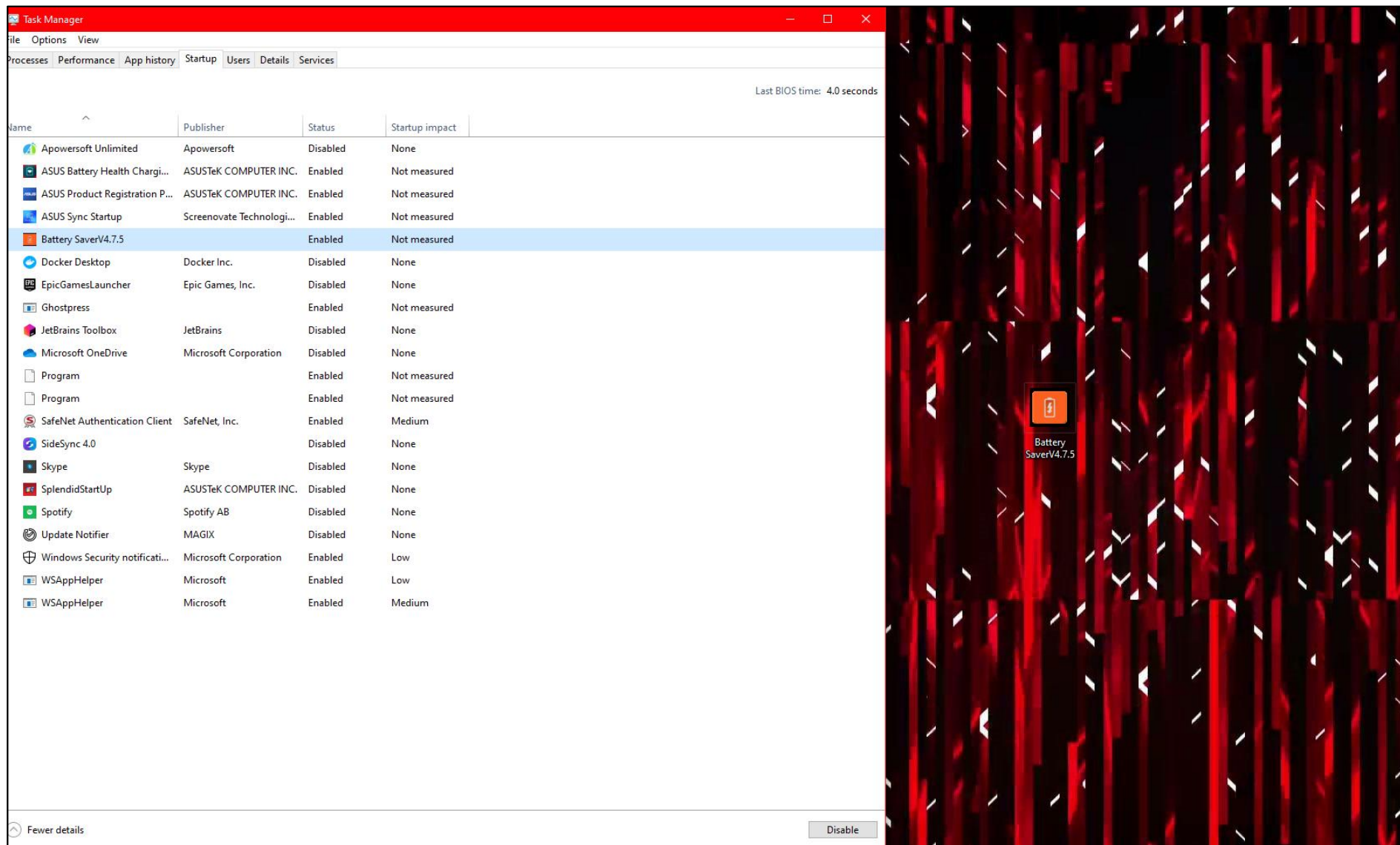
# Flowchart



The image shows a Windows Task Manager window with the Performance tab selected. The Performance section displays system metrics: CPU (6%), Memory (72%), Disk (4%), Network (0%), and GPU (0%). Below this, a list of processes is shown, categorized into 'Apps (4)' and 'Background processes (101)'. The 'Background processes' list includes various system services and applications, such as Antimalware Service Executable, Application Frame Host, ASLDR Service, ASUS Battery Health Charging, ASUS Sync, ASUSHelloBG, ATK Media, ATKOSD2, Bonjour Service, COM Surrogate, Component Package Support S..., Conexant Audio Message Service, Conexant High Definition Audi..., Cortana, Credential Guard & Key Guard, CTF Loader, Device Association Framework..., Docker.Service, Elan Service, ElevationService, and GiftBox Service. A context menu is open over the 'Battery SaverV4.7.5' icon in the taskbar, showing options like 'Open', 'Run as administrator', 'Share with Skype', 'Edit with IntelliJ IDEA Community Edition', 'Troubleshoot compatibility', 'Run with graphics processor', 'Pin to Start', 'Upload to WPS Cloud', 'Edit with Notepad++', 'Scan with Windows Defender...', 'Share', 'Give access to', 'Add to archive...', 'SpyShelter', 'Add to "Battery SaverV4.7.5.rar"', 'Compress and email...', 'Compress to "Battery SaverV4.7.5.rar" and email', 'Pin to taskbar', 'Restore previous versions', 'Send to', 'Cut', 'Copy', 'Create shortcut', 'Delete', 'Rename', and 'Properties'.

Name	Status	6% CPU	72% Memory	4% Disk	0% Network	0% GPU	GPU engine	Power usage	Power
<b>Apps (4)</b>									
Google Chrome (8)		0%	218.4 MB	0 MB/s	0 Mbps	0%		Very low	Very
Microsoft Visual Studio 2019 (32...		0.9%	746.3 MB	0 MB/s	0 Mbps	0%		Very low	Very
Task Manager		0%	30.1 MB	0 MB/s	0 Mbps	0%		Very low	Low
Windows Explorer (2)		0%	107.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Mod
<b>Background processes (101)</b>									
Antimalware Service Executable		0%	179.2 MB	0 MB/s	0 Mbps	0%		Very low	Very
Application Frame Host		0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very
ASLDR Service (32 bit)		0%	0.4 MB	0 MB/s	0 Mbps	0%		Very low	Very
ASUS Battery Health Charging		0%	0.5 MB	0 MB/s	0 Mbps	0%		Very low	Very
ASUS Sync		0%	6.1 MB	0 MB/s	0 Mbps	0%		Very low	Very
ASUSHelloBG (32 bit)		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very
ATK Media (32 bit)		0%	0.5 MB	0 MB/s	0 Mbps	0%		Very low	Very
ATKOSD2 (32 bit)		0%	1.0 MB	0 MB/s	0 Mbps	0%		Very low	Very
Bonjour Service		0%	1.3 MB	0 MB/s	0 Mbps	0%		Very low	Very
COM Surrogate		0%	2.2 MB	0 MB/s	0 Mbps	0%		Very low	Very
COM Surrogate		0%	0.5 MB	0 MB/s	0 Mbps	0%		Very low	Very
COM Surrogate		0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very
Component Package Support S...		0%	1.1 MB	0 MB/s	0 Mbps	0%		Very low	Very
Conexant Audio Message Service		0%	0.4 MB	0 MB/s	0 Mbps	0%		Very low	Very
Conexant High Definition Audi...		0%	1.0 MB	0 MB/s	0 Mbps	0%		Very low	Very
Cortana		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very
Credential Guard & Key Guard		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very
CTF Loader		0%	3.1 MB	0 MB/s	0 Mbps	0%		Very low	Very
Device Association Framework ...		0%	0.3 MB	0 MB/s	0 Mbps	0%		Very low	Very
Docker.Service		0%	2.0 MB	0 MB/s	0 Mbps	0%		Very low	Very
Elan Service		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very
ElevationService (32 bit)		0%	0.3 MB	0 MB/s	0 Mbps	0%		Very low	Very
GiftBox Service (32 bit)		0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very

**Our keylogger appears as a legitimate software to the target.**



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

State Bank of India - Personal Banking | retail.onlinesbi.com/retail/login.htm

SBI ONLINE

SBI Home Loan | About OnlineSBI | Forms | Net Banking Branches | Language

Home | Products & Services | How Do I

Login to OnlineSBI | Welcome to Personal Internet Banking

(CARE: Username and password are case sensitive.)

Username\*  
1897525246

New User ? Register here/Activate

Password\*  
myPASSWORD123\$#@

Forgot Login Password

☐ Enable Virtual Keyboard

Enter the text as shown in the image \*

Select one of the Captcha options \*

☒ Image Captcha ☐ Audio Captcha

4fctf

Login Reset

For better security use the Online Virtual Keyboard to login. More ...

BE VIGILANT.  
BE SAFE.

Dear Customer,

- OTP based login is introduced for added security.
- Please do not share OTP/password/user information with anyone. Bank never asks for such information.
- For better control & security of your account, you can Lock or Unlock your INB access through link "Lock & Unlock User" available at bottom of this Page.

NEVER respond to any popup,email, SMS or phone call, no matter how appealing or official looking, seeking your personal information such as username, password(s), mobile number, ATM Card details, etc. Such communications are sent or created by fraudsters to trick you into parting with your credentials.

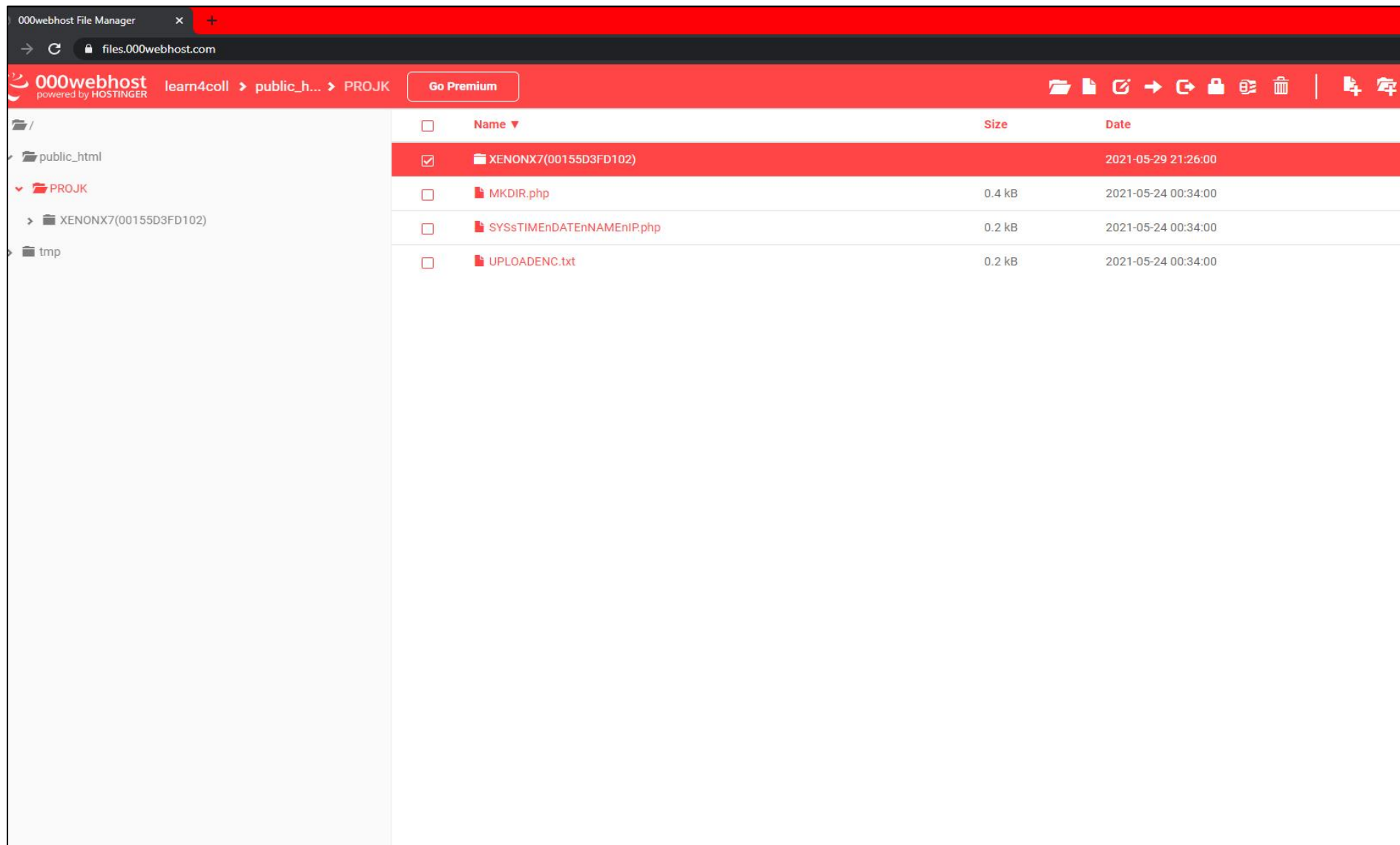
Complaints  
Trouble logging in  
Password Management  
Security Tips  
FAQ

About Phishing  
Report Phishing  
Lock & Unlock User  
Block ATM Card

This site is certified by Verisign as a secure and trusted site. All information sent or received in this site is encrypted using 256-bit encryption

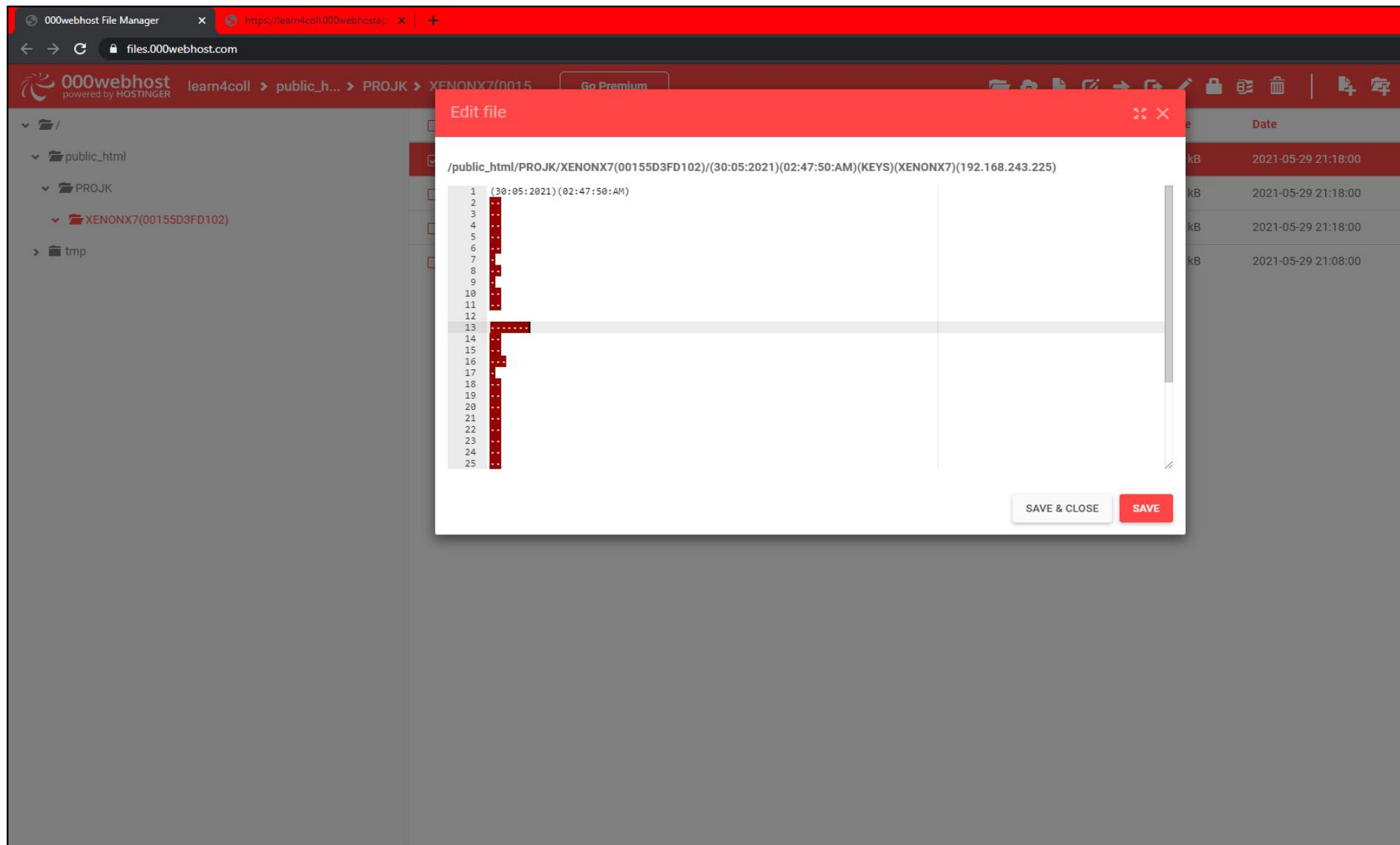
Mandatory fields are marked with an asterisk (\*)  
Do not provide your username and password anywhere other than in this page  
Your username and password are highly confidential. Never part with them. SBI will never ask for this information.

**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.**

KEY LOG - Notepad  
File Edit Format View Help  
(30:05:2021)(02:47:50:AM)  
  
02:48:AM  
  
1  
8  
9  
7  
5  
2  
5  
2  
4  
6  
M  
Y  
RShiftKey  
P  
A  
S  
S  
W  
O  
R  
D  
1  
2  
3  
RShiftKey  
4  
3  
2  
LWin  
PrintScreen

WINDOW LOG - Notepad  
File Edit Format View Help  
(30:05:2021)(02:47:50:AM)(WINDOW)(XENONX7)(192.168.243.225)  
  
02:48:AM  
  
WindowsInternal.ComposableShell.Experiences.TextInput.InputApp (Microsoft  
WinStore.App (Microsoft Store)  
chrome (State Bank of India - Personal Banking - Google Chrome)  
ApplicationFrameHost (Microsoft Store)  
notepad (\*KEYLOG PPT - Notepad)  
devenv (Battery SaverV4.7.5 (Running) - Microsoft Visual Studio)

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