

Forum:[Hack Forums](#)

Thread: [\[HOW TO\] Create BAD USB's \(USB Rubber Ducks\) for FREE](#)

SplloitEXE - June 30, 2018, 11:06 am

PS. Sorry for the bad Layout Its my first thread so give me a break ?

Sup fellow Hackers, Welcome to:
How to create USB BAD USB's (Rubber Duckies) for Absolutely FREE!

So lets begin ?

Warning: <!--><!--><!--> Run all of this software in a sandbox or a VM I am NOT responsible for what happens to your USB's or PC! <!--><!--><!-->

Chapter 1: Re imaging a existing USB stick with custom ducky firmware

1. Gather all of your existing USB sticks (Anything you can find that your not going to use ever again)

2. Download a "USB Firmware/Hardware Information" Tool (I personally use [ChipGenius](#))

3. Open Your USB Firmware tool or ChipGenius in this example and click your your USB drive that's plugged into your PC and look for,

" Controller Vendor: "
and
" Controller Part-Number: "

Then see if your USB Stick Controller Vendor is "Phison"
and your Controller Part-Number is "2303"

If not then either its not compatible or you need to find the .BIN (Burner Image) file for your USB Stick on google or some other website!

The .BIN is usually easily searchable though google, For Example: "Phison 2200 Burner Image" straight into google!

Now IF you have a Phison 2303 USB stick then well done your USB is compatible! ?
if you don't have a Phison 2303 but have another and have found a .BIN (Burner Image) online and have it downloaded then its compatible! ?

and if you don't have a Phison 2303 OR another usb with a burner image downloaded then just say in this thread something on the lines of

"I dont have a Compatible USB :(" and if I get 10 or more reply's I will make another tutorial on how to make a USB Ducky with a \$1 Attiny85 board!

Soo now you have a compatible USB head over to Phychson on [GitHub](#)
and download the latest version of Phychson and "Download as ZIP"

If your bored of reading my thread just go over to the Github and Simply follow there tutorial but for all of you new hackers follow mine ?

MAKE SURE TO HAVE VISUAL STUDIO INSTALLED OTHERWISE THE PROGRAM WONT WORK! (For devs all you need is stuff like MSBuild and all included VS Tools)

Ok so download Visual Studio Community and just install it!

Then download [SDCC](#) from Source Forge (I'm not going into detail on installing its a simple installer exe)

Then CD into the directory of your Phychson Download then in the tools folder! EG. "cd C:\Downloads\Phychson\tools"

and if you want to 100% make sure you have a Phison 2303 then just run: (Change the "E" to your drive letter)

Code DriveCom.exe /drive=E /action=GetInfo

Now if you have the Burner Image already just continue forward to the big "JUMP HERE IF YOU ALREADY HAVE A BURNER IMAGE" ?

If not just follow this tutorial from the Phychson Github:

<https://github.com/brandonlw/Pyichson/wiki/Obtaining-a-Burner-Image>

<!><!><!>JUMP HERE IF YOU ALREADY HAVE A BURNER IMAGE<!><!><!>

Now finally after all of that your nearly there! So feel free to go get a drink if your tired ?

Now back to it.

So in the tools directory of your download run this command replacing the "E" with your USB Drive letter again!

Code DriveCom.exe /drive=E /action=DumpFirmware /burner=<Burner Image Path>.bin

/firmware=<Call it whatever as long as you know its the original (This is the output)>.bin

Then run to reset drive back to its default state if you want a normal USB Drive for storage:

Code DriveCom.exe /drive=<Drive Letter> /action=SendFirmware /burner=<Original Burner

Image>.bin /firmware=<Whatever you called it above>.bin If you want to use it for a Ducky which is this whole tutorial just follow along!

Now to the gucci stuff!

Make your own Ducky Script or use one from an expanding library: [Hak5 Ducky Scripts](#)

Save that to a txt file and then download [DuckEncoder](#)

Again CD to the DuckEncoder Directory and find duckencoder.jar

and type:

Code java -jar duckencoder.java -i <Your Ducky Script>.txt -o inject.binto make a inject.bin

Now to inject your code into the original USB Firmware!

Go back to your Tools folder in the download from the Phychson folder!

copy the inject.bin to the tools folder and type:

Code EmbedPayload.exe inject.bin <Your Firmware>.bin YES now finnaly your done you have your

firmware, just type the same command as above just like this (Make sure to backup the Original Firmware):

Code DriveCom.exe /drive=<Drive Letter of USB> /action=SendFirmware /burner=<Original Burner Image>.bin /firmware=<Your Original Firmware>.bin And bang you have a fully functioning USB Rubber Ducky for absolutely free!! Just plug it into any computer you like and it will just run the script the second the PC loads the drive! Even if its locked!

Thanks for reading my HUGE First ever tutorial! Hope you all enjoyed and if anything in here is bothering you just send me a PM in HF ?

Chapter 2: Coming Soon! Including Botnet Setup with Ducky Script!

Chapter 3: Coming Soon! DigiSpark Attiny 85 \$1 boards and USB cases for a Bad USB replica for only \$1.50 each!

Chapter 4: Coming Soon! Including Self Sustaining Raspberry PI Zero's and 3G/4G Connectivity to your PI from home!

Feel free to add me on Skype if you have any problems! It might take a while for me to get back to you though... Anyways here you go: live:sploit.exe

Seany - June 30, 2018, 11:10 am

Haha lovely how pleasant this tutorial is. Have a good day OP and thanks spending the time creating this.

D?ceived - June 30, 2018, 11:10 am

Really nice tutorial you have here, I will come back to it later!

Condescend - June 30, 2018, 11:32 am

Nice tutorial, OP. This'll definitely help people! ?

HangMansheart - June 30, 2018, 2:41 pm

Got damn, lookin good. Will definitely try this this out and report back when I get a chance.

pomwtin - June 30, 2018, 3:28 pm

Nice job OP, but sadly this tutorial is useless. It would be useful about 5 years ago :P

Phison patched affected chips long time ago and there are no new products today that have it installed.

I'd reccomend one to simply use a board with USB A interface and 32U4 chip on it. Cheap, easy to get and effective.

SploitEXE - July 1, 2018, 2:25 am

(Jun 30, 2018 03:28 PM)pomwtin Wrote: [\[CITE\]](#) Nice job OP, but sadly this tutorial is useless. It would be useful about 5 years ago :P

Phison patched affected chips long time ago and there are no new products today that have it installed.

I'd reccomend one to simply use a board with USB A interface and 32U4 chip on it. Cheap, easy to get and effective.

Srsly!??? I tried it about a month ago on a USB but it was a really old one, In the UK we have a shop called "Cex" its like a gadget shop with second hand tech and the USB was from there and it was quite old... So yeah thanks for the heads up, in Chapter 2 I'm going to finish that one up the in Chapter 3 I'm going to speak about some private methods I use like using a Raspberry PI Zero as a

HID and other stuff like the kickstarter boards for \$1, the Digispark Attiny85 + using the Raspberry Pi Zero as a self sustaining stick that you can put into a computer anywhere to use as a kinda base station that you can connect to from home, to MITM and exploit the networks/computer with all of the kali tools like armitarge or John the ripper for cracking the PC hash! So there is quite alot coming up!

ScarletRosee04 - *July 19, 2018, 10:49 am*

This looks dope, thanks for sharing that lol

ÇdnîS Lu?i? - *July 30, 2018, 4:28 pm*

I will be testing this soon, thanks for the TUT!

v3rtices - *July 30, 2018, 10:00 pm*

I remember this from a while back, sadly it no longer works due to Phison.

zeliatania - *September 10, 2018, 1:14 pm*

Nice tutorial, thank you very much.

Hacker_Mun - *February 13, 2019, 11:19 am*

Im pretty late to this post but im trying to make a Bad_usb to further my own knowledge rather than buy a ducky I bought a compatible usb but it doesn't arrive for a while. I have plenty of usb 2.0 but how would ik what image would let it be a bad_usb. I would love some tips or something thanks