# Malduino

## Research

Malduino intro <https://malduino.com/wiki/doku.php?id=start>

DuckyScript <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript>

Duckencoder <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckencoder>

## Hoe schrijf ik scripts?

De syntax is gebaseerd op **DuckyScript**: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript> . Hier is een klein script om al eens te zien hoe de syntax is:

DELAY 3000

\*\*

Wacht 3 seconden voor hij iets uitvoert, dit wordt gedaan zodat het script nog niet meteen wordt uitgevoerd omdat de pc eerst de usb moet initialiseren.

\*\*

GUI r

\*\*

Houdt de windows knop ingedrukt en tegelijkertijd ‘r’. Dit opent het prompt venster

\*\*

DELAY 200

\*\*

Vertraging van 200ms. Het wacht zodat het prompt venster open gaat.

\*\*

STRING https://www.youtube.com/watch?v=UAzNXbutRHw

\*\*

Schrijft een youtube url

\*\*

ENTER

\*\*

Drukt op de enter toets.

\*\*

DELAY 2000

\*\*

Het script watch 2 seconden zodat de video kan worden geopend.

\*\*

STRING f

\*\*

Drukt ‘f’ om de video te zien in fullscreen modus.

\*\*

## DuckyScript Syntax

Elke commando wordt op een aparte lijn geschreven. Commandos worden geschreven in kapitaal.

REM: wordt gebruikt om commentaar te schrijven bij een commando

DEFAULTDELAY of DEFAULT\_DELAY

Wordt gebruikt om te definieren hoe lang het moet wachten voor het volgende commando. Het moet gedeclareerd worden in het begin van het DuckyScript als je dit wilt gebruiken. Wordt vaak gebuikt voor debugging.

DEFAULTDELAY 100

declaratie van een vertraging tussen commando’s van 100ms

STRING text

Een commando dat het script moet schrijven.

Voorbeeldscript:

GUI r

DELAY 500

STRING notepad.exe

ENTER

DELAY 1000

STRING Hello Word!

WINDOWS of GUI

Windos key

MENU of APP

Is de app key, menu key of context menu key.

Voorbeeldscript:

GUI d

MENU

STRING v

STRING d

Veranderd naar desktop en brengt het menu. V en d krijg je windows desktop icons te zien.

SHIFT

Voor het navigeren in velden om tekst te selecteren of andere functies.

Optionele parameters bij SHIFT:

DELETE, HOME, INSERT, PAGEUP, PAGEDOWN, WINDOWS, GUI, UPARROW, DOWNARROW, LEFTARROW, RIGHTARROW, TAB

ALT

Wordt vaak gebruikt bij commando’s.

Optionele parameters bij ALT:

END, ESC, ESCAPE, F1-F12, Single Char, SPACE, TAB

Voorbeeldscript:

GUI r

DELAY 50

STRING notepad.exe

ENTER

DELAY 100

STRING Hello World

ALT f

STRING s

‘Alt f’ opent het bestandenmenu en ‘s’ slaagt het bestand op.

CONTROL of CTRL

Wordt vaak gebruikt bij commando’s.

Optionele parameters bij CTRL:

BREAK, PAUSE, F1-F12, ESCAPE, ESC, Single Char

Arrow keys:

DOWNARROW of DOWN

LEFTARROW of LEFT

RIGHTARROW of RIGHT

UPARROW of UP

Uitgebreide Commando’s:

BREAK of PAUSE

CAPSLOCK

DELETE

END

ESC of ESCAPE

HOME

INSERT

NUMLOCK

PAGEUP

PAGEDOWN

SCROLLLOCK

SPACE

TAB

REPEAT

Herhaal het commando x aantal keer.

Voorbeeldscript:

DOWN

REPEAT 100

Het vorige commando wordt 100 keer uitgevoerd. (dus 101keer).

Compiling:

DuckyScripts worden gecompiled naar hex files klaar om genaamd te worden inject.bin en naar de root van de microsd kaart te gaan om uitgevoerd te kunnen worden door een USB Rubber Ducky. Dit kan gedaan worden door de tool Duckencoder: <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckencoder> . Duckencoder is een cross-platform commandline java programma dat de code converteerd van Ducky Script syntax naar hex files.

Gebruiksmethode:

duckencode –i [filenaam] \*\* encode specifieke file\*\*

duckencode –i [filenaam] –o [filenaam] \*\*encode naar een specifieke file\*\*

voorbeeld bij een linux system:

java –jar duckencoder.jar –i exploit.txt –o /media/microsdcard/inject.bin