Ducky Script

Ducky Script is the language of the USB Rubber Ducky. Writing scripts for can be done from any common ascii text editor such as Notepad, vi, emacs, nano, gedit, kedit, TextEdit, etc.

Syntax

Ducky Script syntax is simple. Each command resides on a new line and may have options follow. Commands are written in ALL CAPS, because ducks are loud and like to quack with pride. Most commands invoke keystrokes, key-combos or strings of text, while some offer delays or pauses. Below is a list of commands and their function, followed by some example usage.

Note: In the tables below //n// represents a number and //Char// represents characters A-Z, a-z.

REM

Similar to the REM command in Basic and other languages, lines beginning with REM will not be processed. REM is a comment.

Command
REM

```
REM The next three lines execute a command prompt in Windows
GUI r
STRING cmd
ENTER
```

DEFAULT_DELAY or DEFAULTDELAY

DEFAULT_DELAY or DEFAULTDELAY is used to define how long (milliseconds) to wait between each subsequent command. DEFAULT_DELAY must be issued at the beginning of the ducky script and is optional. Not specifying the DEFAULT_DELAY will result in faster execution of ducky scripts. This command is mostly useful when debugging.

Command	Parameters
DEFAULT_DELAY	0..->
DEFAULTDELAY	0..->

```
DEFAULT_DELAY 100
REM delays 100ms between each subsequent command sequence
```

DELAY

DELAY creates a momentary pause in the ducky script. It is quite handy for creating a moment of pause between sequential commands that may take the target computer some time to process. DELAY time is specified in milliseconds from 1 to 10000. Multiple DELAY commands can be used to create longer delays.

Command	Parameters
DELAY	0..->

```
DELAY 500
REM will wait 500ms before continuing to the next command.
```

STRING

STRING processes the text following taking special care to auto-shift. STRING can accept a single or multiple characters.

Command	Parameters
STRING	a...z A...Z 0..9 !...) `~ += _- "' :; <, >. ?/ \ and pipe

```
GUI r
DELAY 500
STRING notepad.exe
ENTER
DELAY 1000
STRING Hello World!
```

WINDOWS or GUI

Emulates the Windows-Key, sometimes referred to as the Super-key.

Command	Optional Parameters
GUI	Single Char
WINDOWS	Single Char

```
GUI r
REM will hold the Windows-key and press r, on windows systems resulting in the Run menu.
```

MENU or APP

Emulates the App key, sometimes referred to as the menu key or context menu key. On Windows systems this is similar to the SHIFT F10 key combo, producing the menu similar to a right-click.

Command
APP
MENU

```
GUI d
MENU
STRING v
STRING d
```

//Switch to desktop, pull up context menu and choose actions v, then d toggles displaying Windows desktop icons//

SHIFT

Unlike CAPSLOCK, cruise control for cool, the SHIFT command can be used when navigating fields to select text, among other functions.

Command	Optional Parameter
SHIFT	DELETE, HOME, INSERT, PAGEUP, PAGEDOWN, WINDOWS, GUI, UPARROW, DOWNARROW, LEFTARROW, RIGHTARROW, TAB

```
SHIFT INSERT
REM this is paste for most operating systems
```

ALT

Found to the left of the space key on most keyboards, the ALT key is instrumental in many automation operations. ALT is envious of CONTROL

Command	**Optional Parameter**
ALT	END, ESC, ESCAPE, F1...F12, Single Char, SPACE, TAB

```
GUI r
DELAY 50
STRING notepad.exe
ENTER
DELAY 100
STRING Hello World
ALT f
STRING s
REM alt-f pulls up the File menu and s saves. This two keystroke combo is why ALT is
jealous of CONTROL's leetness and CTRL+S
```

CONTROL or CTRL

The king of key-combos, CONTROL is all mighty.

Command	**Optional Parameters**
CONTROL	BREAK, PAUSE, F1...F12, ESCAPE, ESC, Single Char
CTRL	BREAK, PAUSE, F1...F12, ESCAPE, ESC, Single Char

```
CONTROL ESCAPE
REM this is equivalent to the GUI key in Windows
```

Arrow Keys

Command
DOWNARROW or DOWN
LEFTARROW or LEFT

Command
RIGHTARROW or RIGHT
UPARROW or UP

Extended Commands

Command	Notes
BREAK or PAUSE	For the infamous combo CTRL BREAK
CAPSLOCK	Cruise control for cool. Toggles
DELETE	
END	When will it ever
ESC or ESCAPE	You can never
HOME	There's no place like
INSERT	
NUMLOCK	Toggles number lock
PAGEUP	
PAGEDOWN	
PRINTSCREEN	Typically takes screenshots
SCROLLLOCK	Hasn't been nearly as useful since the GUI was invented
SPACE	the final frontier

Command	Notes
TAB	not just a cola
FN	another modifier key

REPEAT

Repeats the last command n times

Command	n
REPEAT	number of times to repeat

```
DOWN
REPEAT 100
REM The previous command is repeated 100 times (thus performed 101 times total)
```

Compiling

Ducky Scripts are compiled into hex files ready to be named inject.bin and moved to the root of a microSD card for execution by the USB Rubber Ducky. This is done with the tool duckencoder.

duckencoder is a cross-platform command-line Java program which converts the Ducky Script syntax into hex files. Usage is:

As of duckencoder 1.X usage is:

```
usage: duckencode -i [file ..]                    encode specified file
or: duckencode -i [file ..] -o [file ..]  encode to specified file
```

For example on a Linux system:

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

REM This is for Windows 10 DELAY 2000 GUI r DELAY 300 STRING cmd ENTER DELAY 800 STRING del %tmp%\dvloptical.vbs ENTER DELAY 200 STRING cd %tmp% && copy con dvloptical.vbs ENTER STRING Set oWMP = CreateObject("WMPlayer.OCX.7") ENTER STRING Set colCDROMs = oWMP.cdromCollection ENTER STRING do ENTER STRING if colCDROMs.Count >= 1 then ENTER STRING For i = 0 to colCDROMs.Count -1 ENTER STRING colCDROMs.Item(i).Eject ENTER STRING Next ENTER STRING For i = 0 to colCDROMs.Count -1 ENTER STRING colCDROMs.Item(i).Eject ENTER STRING Next ENTER STRING End If

ENTER STRING wscript.sleep 5000 ENTER STRING loop ENTER DELAY 100 CTRL z ENTER STRING start dvloptical.vbs ENTER STRING exit ENTER REM Written by Emil Simec