# Metasploit Payload Injection By using Raspberry Pico Pi

Dr. T. Arumuga Maria Devi
Associate Professor,
Centre for Information Technology
and Engineering,
Manonmaniam Sundaranar
University

K. Rooban Prakash
PG Scholar,
Centre for Information Technology
and Engineering,
Manonmaniam Sundaranar
University

M. Arunima
PG Scholar,
Centre for Information Technology
and Engineering,
Manonmaniam Sundaranar
University

***Abstract*:- By leaving our computer system unlocked Hackers can get access to your computer system by using the BAD USB such as USB rubber ducky or some other tools like Raspberry Pico pi. The purpose of this work is to describe the necessary research and development of a raspberry Pico pi to use as a rubber ducky and this paper laid out in section discussing Ducky scripts to disable the window Defender and inject the metasploit payload in the target system (Windows Operating System)**

***Keywords: Raspberry Pico Pi, USB Rubber Ducky, Hacking, scripting, and duck tool kit.***

## 1.INTRODUCTION

Nearly every computer including desktops, laptops, tablets and smartphone take input from humans via keyboards. This is possible because there is a specification with every ubiquitous USB standard known as Human Interface Device (HID). Practically, this means that any USB device claiming to be a Keyboard HID will be automatically detected and accepted by most modern operating systems including Windows, Mac OS, Linux or Android.

Usually USB is generally a dangerous medium for attack. This is why many organization banned the usage of USB in their office Computer systems. USB storage utilizations to serve as a malware delivery component insidious form of

USB-based attack has emerged known as Bad USB. This devices register themself as a input devices to take actions on the computer system. For example a USB device could project itself as a device or a keyboard enabling the ability to inject the malicious scripts. This technology is available in the rubber ducky penetration testing tool. The advantage in this tool is that this tool cannot be scanned by any antivirus software or Operating System detect or defend against this attack. Any device that communicates over USB is susceptible to this kind of Attack. Moreover, existing USB security solutions, such as whitelisting individual devices by their serial number, to make sure the device is not spurious

There are several methods to penetrate a machine as a social engineering or a penetration tester. This can be using a USB device detected by a victim's by a victim's computer as a bad USB device and run the code without the knowledge of the victims.

In this paper I use the Raspberry pico pi for the replacement of the Rubber Ducky.

independent document. Please do not revise any of the current designations.

## 2.2USB Keylogging

Keyloggers are activity-monitoring software programs that give hackers access to your personal data. The keylogging software has the capability of capturing the keystrokes, may contain User id, passwords, emails, instant messages.

This USB key includes a 133MHz programmable microcontroller and a SD slot. It behaves like a keyboard and it looks like USB

flash drives. It can be easily hidden on a computer port. Another feature of this device is that it may be hidden in the task manager.

And there are some python scripts needs to be upload as a payload and inject to the target system by using the raspberry pico pi and use it as a key logger. All we need is a physical access to the victims device and need a key logging malware.

The USB rubber ducky is a keyboard emulator disguised within a USB thumb drive case. It has been used by IT professionals, pen testers and hackers, since 2010 and has become the most used commercial keystroke injection attack platform in the business. Combined with its scripting language, payloads can be written and deployed. It is not uncommon for the users who does not leave their system unlocked only for just few minutes. This time was enough for getting the user name and password of the Microsoft account or other accounts using the ducky scripts and these passwords can be extracted by the software named "**LAZagne**"

This tool was designed to extract the saved passwords in the computer whether it is Windows or Linux or MAC. The next section was the important section of this paper named **Metasploit**.

*A*

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

## 2.TOOLS AND TECHNOLOGIES

### *2.1 Metasploit*

Metasploit is a penetration testing platform that enables you to find, exploit, and validate vulnerabilities. The platform includes the Metasploit Pro and Metasploit Framework.

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems. Some Common Mistakes.
Due to its wide range of applications and open-source availability, Metasploit is used by everyone from the evolving field of Dev Sec Ops pros to hackers. It's helpful to anyone who needs an easy to install, reliable tool that gets the job done regardless of which platform or language is used Metasploit now includes more than 1677 exploits organized over 25 platforms, including Android, PHP, Python, Java, Cisco, and more. The framework also carries nearly 500 payloads, some of which include:

Fig 1. Metasploit

- Command shell payloads that enable users to run scripts or random commands against a host
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
- Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files
- Static payloads that enable port forwarding and communications between networks

### 2.2 Metasploit Modules

Metasploit provides you with modules for:

**Exploits**: Tools used to take advantage of system weaknesses
**Payloads**: Sets of malicious code.
**Auxiliary functions:** Supplementary tools and commands.
**Encoders:** Used to convert code or information.
**Listeners:** Malicious software that hides in order to gain access
**Shell code:** code that in programmed to activate once inside the target
**Post Exploitation code:** Helps test deeper penetration once inside
**Nops:** An instruction to keep that payload from crashing.

### 2.3. **Payload creation**

I created the payload using this command:

```
#Msfvenom –p windows/x64/metrepreter/reverse_tcp lhost=192.168.43.200 lport=2343 –f exe > payload.exe
```

This command will create the payload for windows, we create this payload in Kali Linux Now we need to inject the payload to the targeted system in order to get the victims pc's access To inject the payload to the target we need a USB rubber ducky, in our case I use Rasberry pico pi and configure it and it will works like a Rubber Ducky USB.

## 3.HARDWARE CONFIGURATION

### 3.1.Rasberry Pico Pi

Raspberry Pi Pico W is a microcontroller board based on the Raspberry Pi RP2040 microcontroller chip.
It has been designed to be a low cost yet flexible development platform for RP2040, with a 2.4GHz wireless interface and many features. RP2040 chip which provides ample power for embedded projects and enables users of any age or ability to learn coding and electronics. The Pico and third-party RP2040 boards can use a variety of programming languages, include Micro Python, Circuit Python, C/C++ and Arduino language. There's even Piper Play, a block-based version of Python for the Pico.
Micro Python and C/C++ are the officially supported languages from the Pi Foundation, but Circuit Python, which is similar, has certain advantages such as its built-in support for USB **HID,** which means that you can turn your Pico into a **keyboard, mouse or joystick** that's recognized by a PC.

### 3.2 To make raspberry pico pi to rubber ducky we need to make changes to it

We need to make a python script to run to work a raspberry pico pi as a rubber ducky

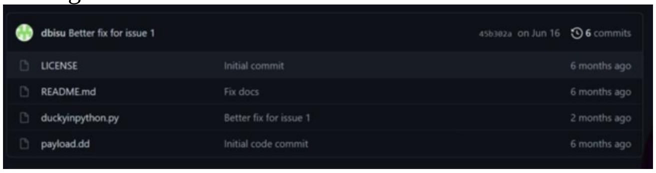
- First we need to download the adafruit-circuit-python-raspberry-pi-pico.uf2 file .
- **Push and hold the BOOTSEL button** on the Pico, then connect to your computer using a micro USB cable. Release BOOTSEL once the drive RPI-RP2 appears on your computer
- And we need to copy the flashnuke uf2 to the RPI-RP2

In order to make the raspberry pico pi pretend to be a HID device we need a HID Library

- And we need to copy the adafruit_hid and paste in the lib folder in the Circuit Python
- Download the pico ducky Python file and replace the code.py to this pico ducky python file and rename to code.py
- Now its all set, our raspberry pico pi is going to work as a Rubber Ducky

Now lets see how to configure it

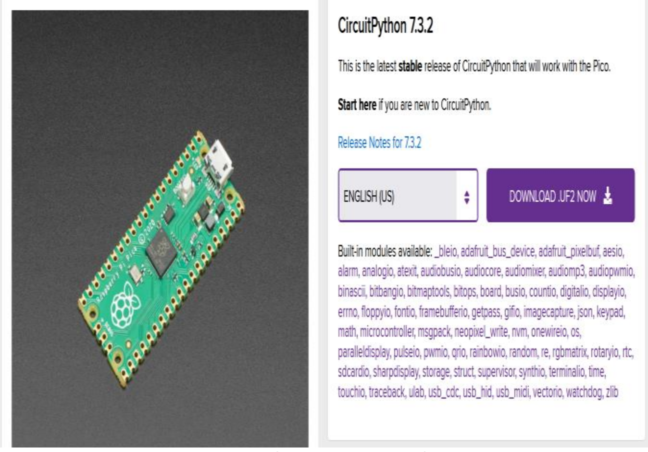
Step 1: Download the duck in python payload files from the git hub.



| | | |
|---|---|---|
| dbisu Better fix for issue 1 | 45b302a on Jun 16 | 6 commits |
| LICENSE | Initial commit | 6 months ago |
| README.md | Fix docs | 6 months ago |
| duckyinpython.py | Better fix for issue 1 | 2 months ago |
| payload.dd | Initial code commit | 6 months ago |

Fig 2. Git hub repository

Step 2: Download the circuit python .uf2 file from circuit python website



CircuitPython 7.3.2

This is the latest **stable** release of CircuitPython that will work with the Pico.

**Start here** if you are new to CircuitPython.

Release Notes for 7.3.2

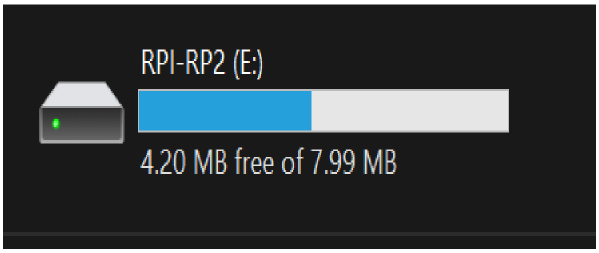
ENGLISH (US)

DOWNLOAD .UF2 NOW

Built-in modules available: _bleio, adafruit_bus_device, adafruit_pixelbuf, aesio, alarm, analogio, atexit, audiobusio, audiocore, audiomixer, audiomp3, audiopwmio, binascii, bitbangio, bitmaptools, bitops, board, busio, countio, digitalio, displayio, errno, floppyio, fontio, framebufferio, getpass, gifio, imagecapture, json, keypad, math, microcontroller, msgpack, neopixel_write, nvm, onewireio, os, paralleldisplay, pulseio, pwmio, qrio, rainbowio, random, re, rgbmatrix, rotaryio, rtc, sdcardio, sharpdisplay, storage, struct, supervisor, synthio, terminalio, time, touchio, traceback, ulab, usb_cdc, usb_hid, usb_midi, vectorio, watchdog, zlib

Fig 3. Uf2 Micro-python file

Step 3:Insert the Rasberry pico pi by pressing the boot button and the RPI – PR2 folder was appears on the disk

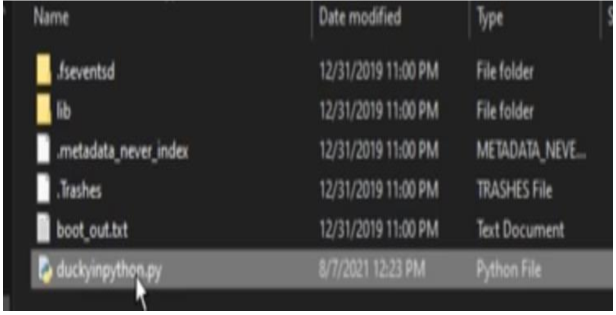


RPI-RP2 (E:)

4.20 MB free of 7.99 MB

Fig4. Pico pi storage media

Copy the Files that we download from git hub and rename the code.py

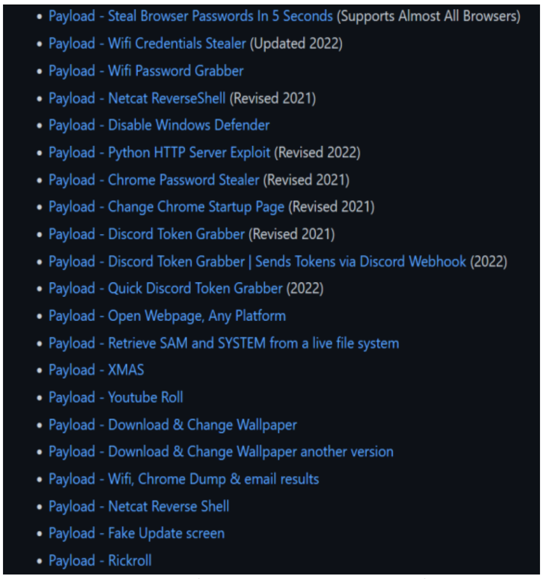


| Name | Date modified | Type |
|---|---|---|
| .fseventsd | 12/31/2019 11:00 PM | File folder |
| lib | 12/31/2019 11:00 PM | File folder |
| .metadata_never_index | 12/31/2019 11:00 PM | METADATA_NEVE... |
| .Trashes | 12/31/2019 11:00 PM | TRASHES File |
| boot_out.txt | 12/31/2019 11:00 PM | Text Document |
| duckyinpython.py | 8/7/2021 12:23 PM | Python File |

Fig 5. Ducky-in Python

Now download the payload for disabling the Windows Defender from git hub

This payload will disable the Windows defender and ready to inject the payload to our targeted system.



- Payload - Steal Browser Passwords In 5 Seconds (Supports Almost All Browsers)
- Payload - Wifi Credentials Stealer (Updated 2022)
- Payload - Wifi Password Grabber
- Payload - Netcat ReverseShell (Revised 2021)
- Payload - Disable Windows Defender
- Payload - Python HTTP Server Exploit (Revised 2022)
- Payload - Chrome Password Stealer (Revised 2021)
- Payload - Change Chrome Startup Page (Revised 2021)
- Payload - Discord Token Grabber (Revised 2021)
- Payload - Discord Token Grabber | Sends Tokens via Discord Webhook (2022)
- Payload - Quick Discord Token Grabber (2022)
- Payload - Open Webpage, Any Platform
- Payload - Retrieve SAM and SYSTEM from a live file system
- Payload - XMAS
- Payload - Youtube Roll
- Payload - Download & Change Wallpaper
- Payload - Download & Change Wallpaper another version
- Payload - Wifi, Chrome Dump & email results
- Payload - Netcat Reverse Shell
- Payload - Fake Update screen
- Payload - Rickroll

Fig 6. Payload for disabling Windows Defender.

Copy the script and make a file and copy it to lib folder in our raspberry pico pi

Now see How it going to work

In the first time we insert the raspberry pico pi to the target system it will run the payload.dd file

It will run the code.py python file, it will disable the Windows Defender

And we inject the payload file by using the power shell script that we embed into the python scripts

```
STRING power shell -window style hidden
(new-object
System.Net.WebClient).DownloadFile('http:
//*kaliIP*/payload.exe','%TEMP%\payload.e
xe'); Start-Process "%TEMP%\payload.exe"
```

The payload will create the reverse shell to the Kali linux that we created this payload.

## CONCLUSION:

This paper shows that the working of Raspberry pico pi as a rubber ducky, we can use this ducky scripts to perform a offensive attack as well as penetration testing. Within organizations, a preventative measure such as a USB blocking software is a necessity because Bad USB attacks, if undetected or stopped, could result in the unauthorized execution of commands that instigate security bypass incidents, privilege.

**Physical protection**: By blocking the USB ports in the BIOS and authorize only the devices escalation, DDoS attacks or malware infections of the host computers which could then spread to target entire networks.

Accessing only the authorized USB by allowing only the selected serial number in the Device.

**Less Privilege**: This was the common technique that limit the permission of the user that they can't run the untrusted programs.

## REFERENCES

[1] https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---WIN10-Disable-Windows-Defender
[2] https://micropython.org/download/rp2-pico-w/
[3] https://gainsec.com/2020/04/27/generating-a-msf-reverse-shell-kali-tips-9/
[4] https://github.com/dbisu/pico-ducky/blob/main/duckyinpython.py

## AUTHOR'S PROFILE

**Dr. T. Arumuga Maria Devi** Received B.E. degree in Electronics & Communication Engineering from Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India, in 2003, M.Tech degree in Computer & Information Technology from Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India, in 2005, also received Ph.D degree in Information Technology—Computer Science and Engineering, from Manonma niam Sundaranar University, Tirunelveli, Tamil Nadu, India, in 2012 and also the Associate Professor of Centre for Informa tion Technology and Engineering of Manonmaniam Sundaranar University since November 2005 onwards. Her research includes Signal Processing, Remote Communication, Multimedia and Mobile Computing .

**K. Rooban Prakash,** M.sc.Cyber Security II year, Centre for Information Technology & Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli - 627012, Tamilnadu, India. He received his Bachelor of Networking in Madurai Kamaraj University. His research interests include USB rubber ducky, raspberry pico pi, and Metasploit, Web app vulnerability, Digital forensics, Ethical hacking

**M.Arunima**, M.sc. Cyber Security II year, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli - 627012, Tamilnadu, India. She received her Bachelor of Information Technology in Manonmaniam Sundaranar University. Her research interests include USB rubber ducky, raspberry pico pi, and Metasploit, Ddos tool, Digital forensics, Ethical hacking.