**Memo – Infection**

**Group 3: Fnu Abdullah & Ahmed Hussain**

**Rubber Ducky USB**

We are going to use a Rubber Ducky which is a USB device that emulates a keyboard and can deliver scripted keystrokes to a host. For this project, we are going to utilize it to download an online script that will be run to attack the host.

**Process**

The Rubber Ducky USB is configured with a payload that, upon insertion, opens a terminal, downloads a malicious script, executes it, and closes the terminal in almost 8 seconds. The script runs invisibly in the background, downloads and installs required packages, sets, runs the program and unsets the edge shared key, and displays a window prompting for a password to decrypt files. The attack is irreversible after the terminal is closed/after 8 seconds. A desktop icon named "Files" with a locked icon is created, allowing the user to reopen the password prompt if the initial window is closed.

**Detailed Overview**

**Rubber Ducky USB Payload Configuration**:

* **Upon Insertion**:
  + Opens a terminal.
  + Downloads a malicious script.
  + Executes the script.
  + Closes the terminal in almost 8 seconds.
* **Malicious Script Actions** (runs invisibly in the background):
  + Downloads and installs required packages.
  + Sets the edge shared key.
  + Runs the malicious program.
  + Unsets the edge shared key.
* **Post-Execution Effects**:
  + Displays a window prompting for a password to decrypt files.
  + Attack becomes irreversible after the terminal closes (after 3 seconds).
* **Additional Features**:
  + Creates a desktop icon named "Files" with a locked icon.
  + Allows the user to reopen the password prompt if the initial window is closed.