# Advanced Methods for Infiltrating Isolated Systems: A Case Study of Extracting Information Without Network Access

**Introduction:**

In the realm of information security, one of the significant challenges is infiltrating systems that are entirely isolated. These systems lack internet access, have blocked USB ports, and do not allow the use of physical media like CDs/DVDs. This article presents a creative and advanced method for stealing information from such systems using mouse and keyboard dongles and leveraging a webcam.

**The Story Begins:**

The story starts with an attempt to infiltrate a system in an isolated environment. This system had no internet access, and only mouse and keyboard dongles were allowed to be connected. Additionally, the only software installed was Microsoft Word.

**First Step:**

Initially, a Wi-Fi dongle was connected to the system. Although the dongle was recognized, network access was restricted. This led to the idea of using a webcam.

**Utilizing the Webcam:**

A webcam was connected to the system and recognized by the Windows Camera application. This was the starting point for the infiltration. A script was written to perform the following tasks sequentially:

- Receive the file path as input.
- Convert the file content to base64.
- Convert the base64 output to QRCode.
- Save the QRCode outputs as PNG files.
- Save the base64 output in a text file.

**Running the Script:**

The script was saved as transfer.exe and executed with the following command:

```
transfer.exe c:\users\hojat\desktop\transfer.exe .\output\qr.png
```

The input file path could be any file, such as malware, but in this example, the goal was to transfer the script itself to the target system.

**Transferring the Information:**

After running the script, several QRCode files and a text file containing the base64 content were generated. I printed the base64.txt file using a printer and then used the webcam to capture images of the printed codes. These images were added to a Word document on the target system. The document was then saved as a PDF and reopened in Word, which automatically converted the images to text. Using the following command, the base64 content was converted back to the original file:

```
certutil -decode base64.txt decoded_output
```

**Retrieving the File:**

Now, the original malware was restored and executed. To steal the backup.zip file, the file path was provided to the script, resulting in multiple QRCode outputs. These QRCodes were filmed using a smartphone and later converted to images, then to base64, and finally to the backup.zip file.

**Conclusion:**

This method demonstrates that even in conditions without network and physical media access, creativity and the use of available tools can still allow for the infiltration of isolated systems. If the attacker has enough time, they can manually input the base64 code of the malware into the system and perform any desired operations.

**Personal Opinions:**

This experience highlights that complete isolation of systems poses significant challenges for attackers, but with creativity and unconventional methods, there are still ways to infiltrate. I hope this experience contributes to improving security measures and identifying weaknesses.

https://www.linkedin.com/in/seyedhojjathosseini