Title: Advanced Methods for Extracting Information from Isolated Systems

Authors:

Seyed Hojat Hosseini

Corresponding Author:

Seyed Hojat Hosseini

Email: seyedhojjathosseini@gmail.com

Article Type: Original Article

Keywords: Isolated Systems, Data Extraction, Cybersecurity, Air-Gapped Networks, Information Security

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 repository 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 attempt to infiltrate an isolated system started with:

- No internet access
- Only mouse and keyboard dongles allowed
- Microsoft Word as the only installed software

First Step: Connecting a WiFi Dongle

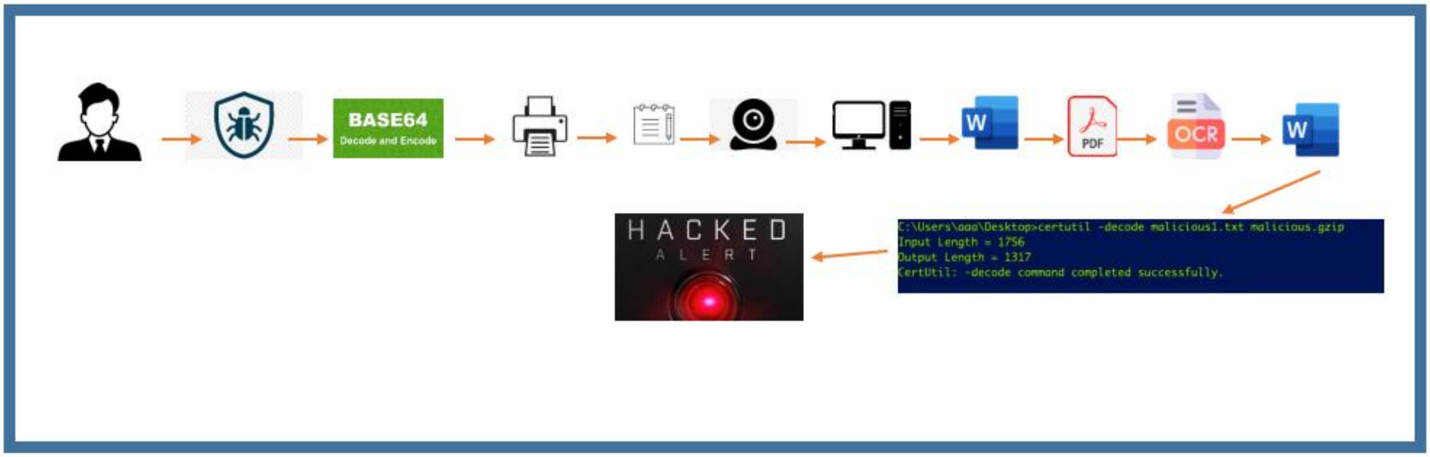
Initially, a WiFi dongle was connected to the system. Although the dongle was recognized, network access was restricted. This led to the idea of using a webcam.

Utilizing the Webcam

A webcam was connected and recognized by the Windows Camera application. This was the starting point for the infiltration.

Malware Infiltration Steps

- The attacker writes the malware.
- The malware executable is converted to base64.
- The generated base64 code is printed on paper.
- The printed codes are photographed using the connected webcam.
- The photos are inserted into a Word document and saved as a PDF.
- The PDF is reopened with Word, using OCR to convert images to text.
- The base64 text is saved as a file and decoded with **certutil** to restore the malware executable.



```
C:\Users\aaa\Desktop>certutil -decode malicious1.txt malicious.gzip
Input Length = 1756
Output Length = 1317
CertUtil: -decode command completed successfully.
```

Script Overview

A script was written to perform the following tasks:

- 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

File Conversion

Using the following command, the base64 content was converted back to the original file:

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

Running the Script

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

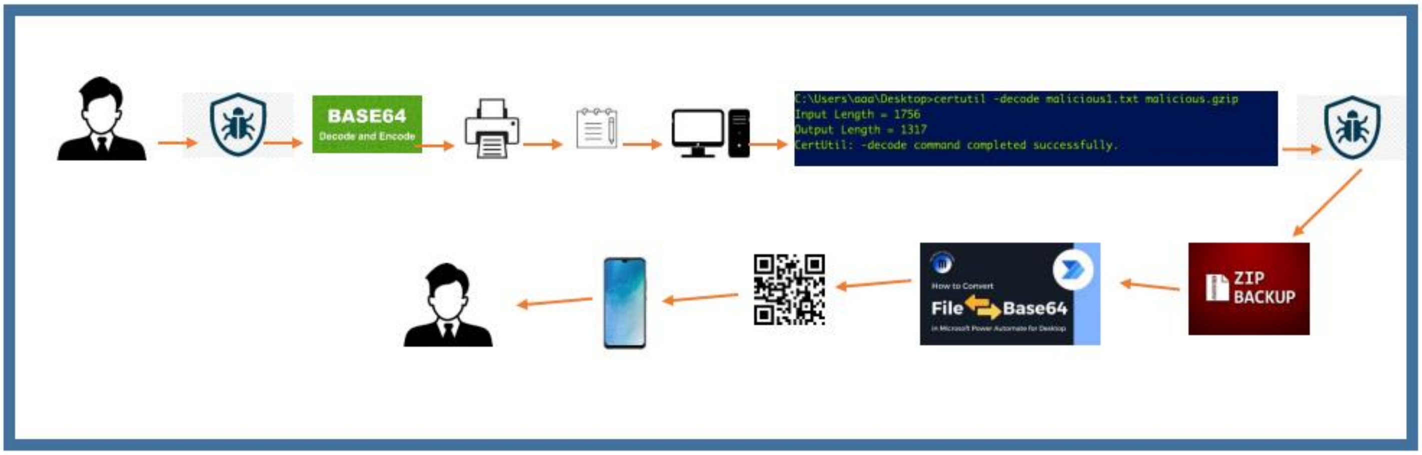
```
.transfer.exe c:\backup.zip .\output\qr.png
```

Transferring the Information

When the malware enters the system through any method (whether via webcam or manually typing base64 codes):

- Execute the malware.
- Input the file backup.zip to the malware.
- The malware converts backup.zip to base64.
- The base64 codes are converted to QRCodes.
- The attacker films all QRCodes with a smartphone.
- The attacker performs file recovery on their own system.

The following image illustrates this process:



```
C:\Users\aaa\Desktop>certutil -decode malicious1.txt malicious.gzip
Input Length = 1756
Output Length = 1317
CertUtil: -decode command completed successfully.
```

Transferring the Information

- 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.

Contributions and Feedback

Feel free to contribute or provide feedback. If you have any questions or suggestions, please open an issue or submit a pull request.

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