Attacco a reti Air Gap, tra mito e realtà

Author : Francesco Arruzzoli

Date : 5 novembre 2018

La protezione di ambienti classificati da attacchi non convenzionali

Air Gap, termine che in italiano significa “vuoto d’aria”, “intercapedine”, è una parola spesso utilizzata in ambito edile per definire un spazio divisorio tra due o più ambienti, uno spazio spesso utilizzato come isolante termico, tra due stanze.

In sicurezza informatica con il termine “Air Gap” si intende una misura di sicurezza che isola fisicamente un’infrastruttura critica (computer, reti private con dati altamente sensibili) da qualsiasi altro collegamento con il mondo esterno, come ad esempio Internet.

Quando si adottano misure di sicurezza di questo tipo, normalmente il livello di riservatezza delle informazioni gestite (all’interno del sistema ICT) è altamente confidenziale e classificato. Nella mia esperienza professionale, l’applicazione di una misura “Air Gap” ad una infrastruttura ICT ha il suo vantaggio nella sicurezza informatica dei governi ed in settori critici quali ad es. reti militari classificate o centrali nucleari, ma soffre anche di svantaggi significativi, come ad esempio: costi di implementazione, manutenzione, limitazione nella produttività e paradossalmente il degrado di alcuni aspetti chiave della sicurezza (ad es. l’aggiornamento tempestivo dei sistemi).

Un "Air Gap" crea barriere, molti servizi e sistemi governativi che hanno lo scopo di interagire direttamente con i cittadini rischiano di essere rallentati e resi più macchinosi dai protocolli di separazione. I vantaggi delle città intelligenti (Smart Cities) e delle nazioni intelligenti rischiano di essere significativamente ridotti se non possono sfruttare tecnologie come il cloud e le Internet of Things. L’isolamento fisico da qualsiasi tipo di contatto umano o tecnologico diminuisce drasticamente le probabilità che i dati protetti possano essere “portati fuori” accidentalmente o trafugati, perché gli attacchi informatici non possono attraversare il "vuoto d'aria" per raggiungere il loro obiettivo. Eppure esiste sempre una remota possibilità che questo accada, un ambiente difficilmente può essere isolato completamente dal mondo esterno, esistono forze elettriche, magnetiche, termiche, acustiche e la natura “fallibile” dell’essere

umano che possono creare canali di comunicazione segreta in grado di superare queste barriere fisiche.

Attacchi a sistemi di protezione “Air Gap” sono studiati da anni e nel corso del tempo sono state realizzate varie soluzioni di attacco che sfruttano spesso ambiti e approcci completamente diversi, di seguito vi illustrerò alcune delle tecniche più note anche in considerazione delle loro caratteristiche e limitazioni.

La rilevanza di queste minacce è sempre proporzionale all’interesse dei dati, poi l’evoluzione tecnologica unita alla “creatività” dell’uomo permettono di sviluppare tecniche di attacco più o meno sofisticate e non convenzionali. L’attacco in ogni caso prevede normalmente sempre tre fasi (Fig.1):

Fig.1

Tralasciando per il momento la fase di “infiltration” che vi illustrerò nel mio prossimo articolo, per entrare maggiormente nel “mood” dell’argomento, una tecnica di attacco che è possibile provare anche a casa senza particolari requisiti è quella basata sulle frequenze ad ultrasuoni. Questo attacco prevede la possibilità di creare un canale di comunicazione segreto attraverso la trasmissione con frequenze a ultrasuoni.

Gli ultrasuoni sono onde sonore con frequenza superiore a 20.000 hz. Il limite superiore di frequenza nell'uomo (circa 20 kHz) è dovuto alle limitazioni dell'orecchio medio (Fig.2). Le onde sono troppo piccole e veloci perché l'orecchio interno trasmetta le vibrazioni. Se il suono è troppo basso o troppo alto, le nostre orecchie non sono in grado di percepirlo.

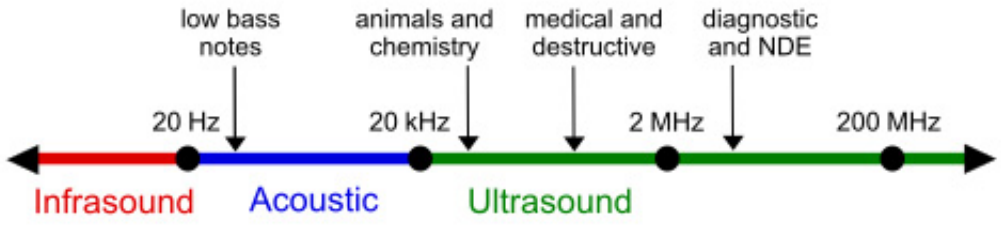

Fig.2

In queste tipologie di attacco mediamente la distanza max di comunicazione può arrivare mediamente a 4/5 metri che può sembrare poca ma in certi ambiti può essere più che sufficiente.

Un volta attivato, il malware all'interno del computer target, invierà all'attaccante le informazioni richieste attraverso una trasmissione ad ultrasuoni generata con le casse audio ed il microfono del computer target, e se pensiamo a pc portatili e notebook parliamo del 99% di essi.

A scopo didattico un buon esempio pratico per comprendere il "proof of concept" di funzionamento di un canale di comunicazione ad ultrasuoni è il progetto QuietNet (https://github.com/Katee/quietnet), un semplice programma di chat che utilizza frequenze vicine agli ultrasuoni (19100 Hz) per comunicare.

Una volta scaricato da github il file zip contenente il progetto e decompressi i file in una cartella, si troveranno due principali script in python:

- **send.py**
- **listen.py**

Il file **send.py** trasmette il testo digitato mentre il file listen.py riceve il testo. Nella mia prova ho utilizzato due pc portatili ed ho eseguito su uno **send.py** (trasmettitore) e sull'altro il file **listen.py** (ricevente).

Usando sistemi Microsoft Windows ho installato su entrambi i pc il linguaggio di programmazione python ver. 2.7.x e successivamente ho installato due librerie (pyaudio e numpy) necessarie al funzionamento di QuietNet attraverso i seguenti comandi:

```
python -m pip install pyaudio  python -m pip install numpy
```

A questo punto ho avviato il file listen.py (Ricevitore Fig.3) sul primo pc e send.py sul secondo pc (Trasmettitore Fig.4).

Dal secondo pc (trasmettitore) ho scritto una frase e con invio ho iniziato la trasmissione (Fig.4).

Sul primo PC (ricevente) dopo alcuni secondi di ritardo è apparso il testo. Prima di riuscire a trasmettere correttamente il testo ho dovuto però effettuare diverse prove, modificare il volume del trasmettitore sotto il 50% e posizionare i due pc ad una distanza di 70 cm tra loro, questo pur essendo un semplice esempio la dice lunga sulla difficoltà nel mettere a punto un attacco che sfrutta questa tecnologia.

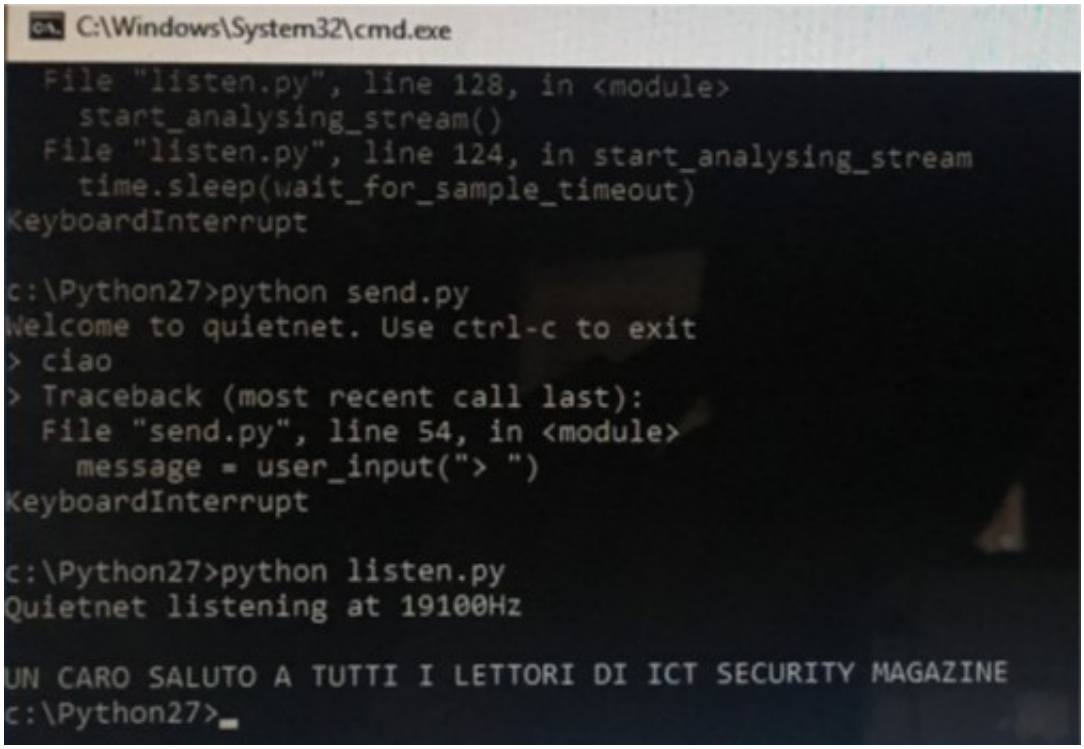

Fig.3

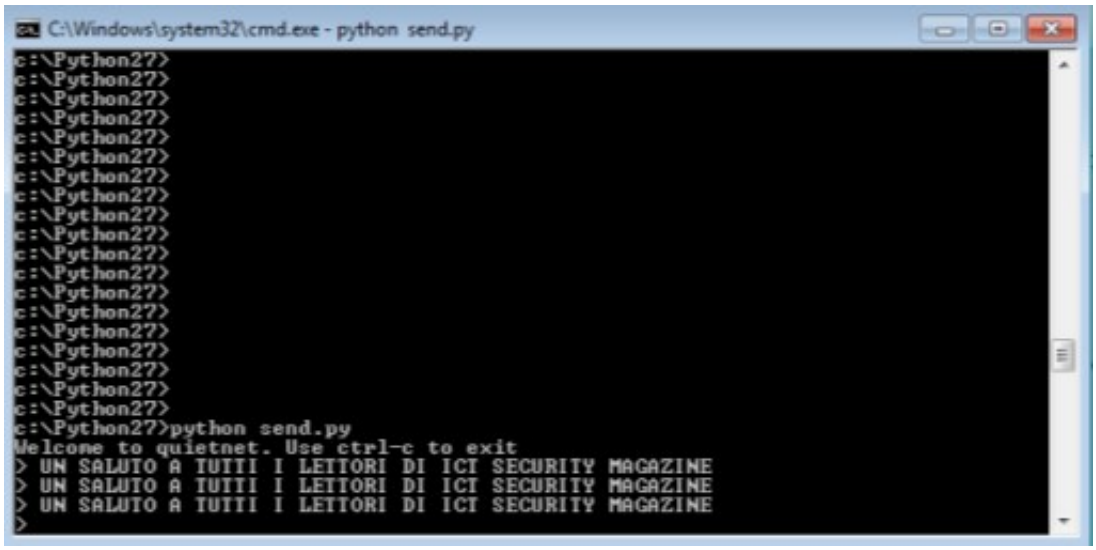

Fig.4

AirHopper è un attacco che sfrutta i campi elettromagnetici, si basa sul principio che la corrente elettrica in un conduttore produce un campo elettromagnetico, il campo elettromagnetico dipende quindi dal passaggio di corrente che attraversa il conduttore. Se si controlla la corrente nel conduttore, si controlla l'emissione elettromagnetica (frequenza ed ampiezza). I cavi dello schermo emanano radiazioni elettromagnetiche, dipende dall'immagine trasmessa nel cavo. E' possibile controllare la radiazione elettromagnetica trasmettendo immagini appositamente predisposte regolando la radiazione elettromagnetica su una frequenza ricevibile da una radio FM (88 Mhz-108 MHz), Il malware utilizza il display video come trasmettitore FM per trasmettere i dati ed il cavo dello schermo come un'antenna.

Maggiori dettagli potete trovarli in questo articolo: https://ieeexplore.ieee.org/document/6999418 mentre ecco un video dimostrativo:

https://www.youtube.com/watch?v=2OzTWiGl1rM

Se AirHopper vi ha stupito, il metodo **ODINI** lo farà di più. Si basa sullo sfruttamento dei campi magnetici a bassa frequenza generati dalla CPU del computer, la radiazione magnetica a bassa frequenza emessa si propaga attraverso l'aria, riuscendo a penetrare anche schermature metalliche come la gabbia di Faraday. Anche in questo caso il malware installato controlla la frequenza della CPU facendogli eseguire specifici calcoli che convertono i dati da trasmettere in onde magnetiche. L'attaccante dal di fuori con un ricevitore di onde magnetiche riconvertirà le radiazioni in dati.

Per maggiori dettagli potete consultare la seguente documentazione: https://arxiv.org/abs/1802.02700 mentre di seguito un video dimostrativo:

https://www.youtube.com/watch?v=h07iXD-aSCA

Concludo questo breve viaggio tra le connessioni segrete non convenzionali dette “Air Gap Jumpers” riportandovi due metodologie di attacco che sfruttano le tecnologie ottiche. La prima, **LED-it-GO**, utilizza i led presenti sui computer e periferiche (hard disk, power, etc...), controllabili via software/firmware, dove il malware codifica i dati tramite "lampeggi" che possono essere intercettati e decodificati da telecamere locali o remote, magari aiutandosi con un drone… tutto vero anche se difficilmente applicabile, come in questo video:

https://www.youtube.com/watch?v=4vIu8ld68fc

per maggiori info potete consultare: https://www.springerprofessional.de/led-it-go-leaking-a-lot-of-data-from-air-gapped-computers-via-th/12476142

Sempre basandosi sui led ma questa volta ad infrarossi, **aIR-Jumpe**r sfrutta le telecamere di sorveglianza per ricevere o trasmettere dati. Controllando le luci led ad infrarossi (luce invisibile all’occhio umano), normalmente utilizzate dalle telecamere per illuminare gli ambienti bui trasmettono con impulsi lampeggianti informazioni all’attaccante oppure le ricevono analizzando le immagini delle telecamere come lo dimostrano i seguenti video:

https://www.youtube.com/watch?v=auoYKSzdOj4

https://www.youtube.com/watch?v=om5fNqKjj2M

per maggiori approfondimenti: http://arxiv.org/abs/1709.05742

CONSIDERAZIONI FINALI

Le limitazioni di molte delle metodologie descritte restringono il campo di applicazione ad attacchi mirati alla raccolta di piccole quantità di dati (credenziali di accesso, codici, etc...) ma non per questo meno importanti, anzi.

So già che starete pensando al fatto che in ogni caso un sistema protetto da una misura di sicurezza “Air Gap” deve comunque essere prima infettato per poter permettere al malware di utilizzare una o più delle metodologie sopra illustrate, ma come preannunciato questo sarà oggetto del mio prossimo articolo.

Articolo a cura di: **Francesco Arruzzoli**