Attacco ad una rete pubblica WiFi

Author : Milo Caranti

Date : 29 maggio 2018

Chissà quante volte ci è capitato di vedere affissi - presso esercizi commerciali, locali o parchi pubblici - cartelli che segnalano la presenza di reti WiFi gratuite o accessibili attraverso un semplice "like" su Facebook. Con buona probabilità, ognuno di noi ha utilizzato tali servizi almeno una volta, vuoi per necessità o semplicemente per quella che oggigiorno è una naturale attitudine a rimanere connessi a internet.

Come mai allora queste reti non godono di una buona reputazione? E in che modo vengono sfruttate da utenti malintenzionati? Nel prosieguo dell'articolo analizzeremo e creeremo un tipico potenziale scenario con lo scopo di intercettare le informazioni sensibili inserite dall'ignaro utente (la classica combinazione username/password, insomma).

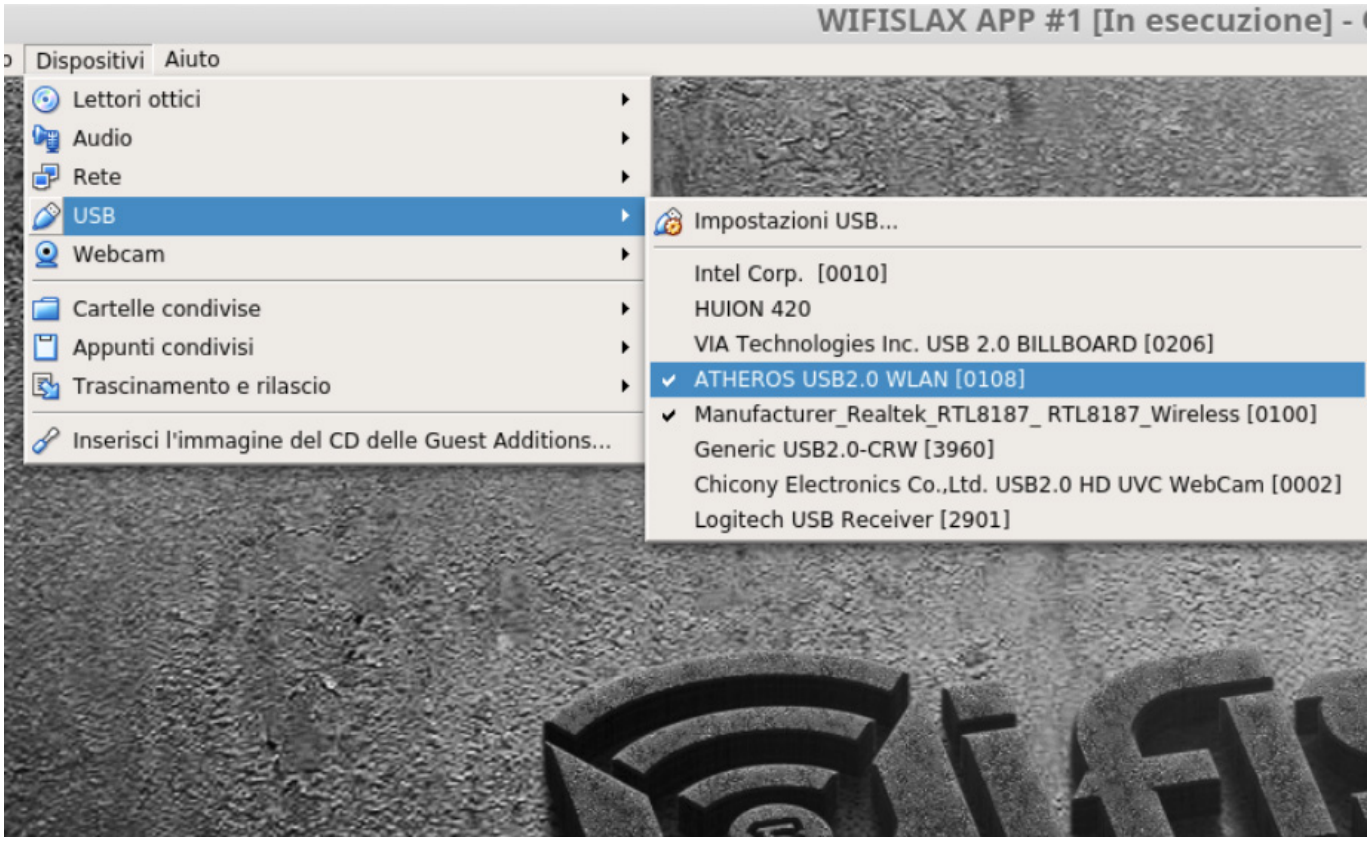
Dal momento che le possibilità di intercettare traffico e dati interessanti in chiaro - dunque non crittografati dal ben noto protocollo HTTPS - mediante sniffer di rete (come *wireshark*, *xplico*, *ferret*) sono piuttosto scarse per via delle policy sempre più stringenti in fatto di sicurezza adottate da browser e sistemi operativi, ci industrieremo in un ben più efficace tentativo di phishing: d'altra parte è risaputo, l'anello debole di un sistema informatico si trova sempre davanti allo schermo!

Ancora una volta, precisiamo che effettuare le pratiche mostrate qui di seguito al di fuori di ambienti simulati o nei confronti di soggetti non consenzienti, può significare incorrere nelle prescrizioni di cui agli articoli *616*, *615-ter*, *615-quater*, *617-sexies*, *640-ter* del nostro Codice Penale.

Cominciamo configurando sulla nostra distribuzione Linux uno dei framework più famosi nell'ambito degli attacchi wireless, ovvero il progetto *wifiphisher*:

```
git clone https://github.com/wifiphisher/wifiphisher.git    cd wifiphi
sher    sudo python setup.py install
```

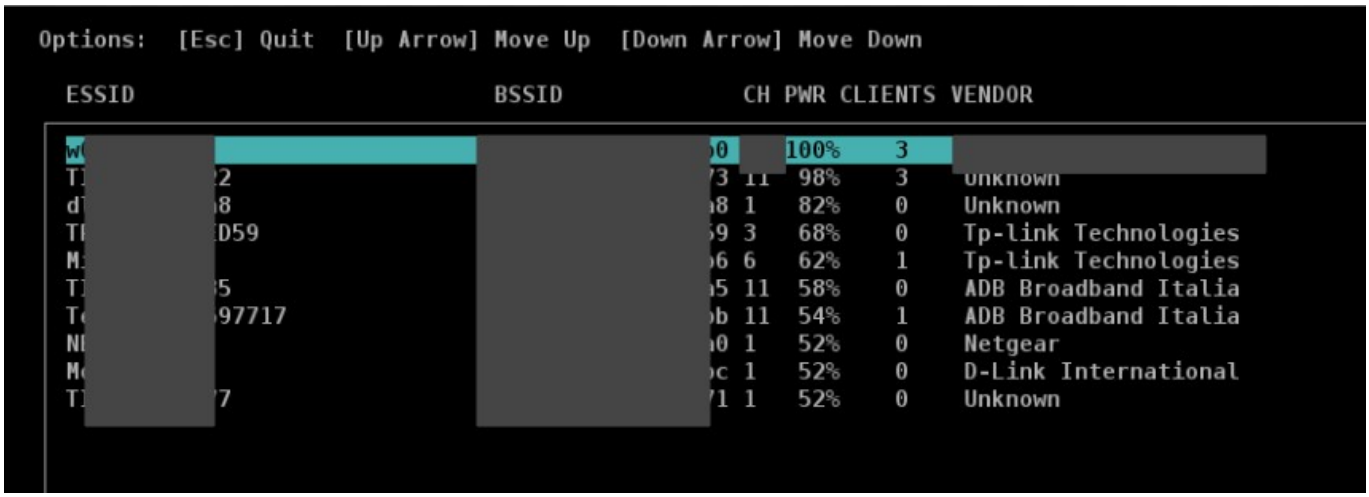
Troviamo lo strumento già preinstallato in *WifiSlax*, un ottimo sistema operativo di origini catalane dedicato per l'appunto al pentesting di applicazioni WiFi. Dobbiamo poi munire il nostro sistema (anche come macchina virtuale) di almeno una seconda scheda di rete WiFi che consenta l'iniezione di pacchetti e il *monitor mode*. Se stiamo utilizzando VirtualBox come piattaforma di virtualizzazione, ci basterà cliccare sull'apposito menù e spuntare il device:



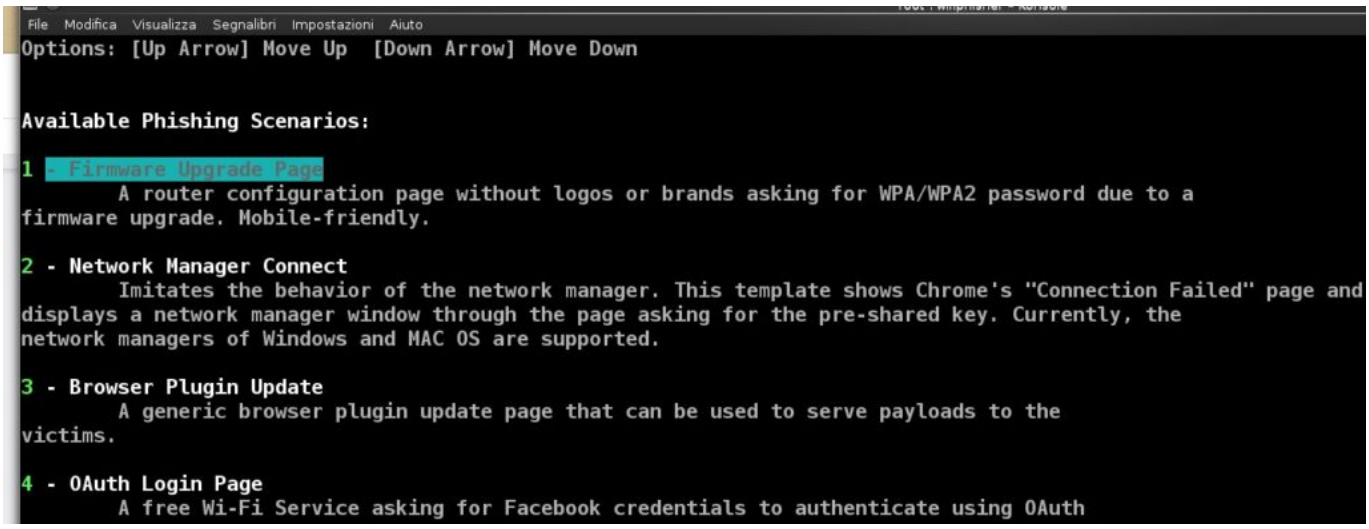
Lanciamo il programma nel suo utilizzo base con il comando:

```
sudo wifiphisher
```

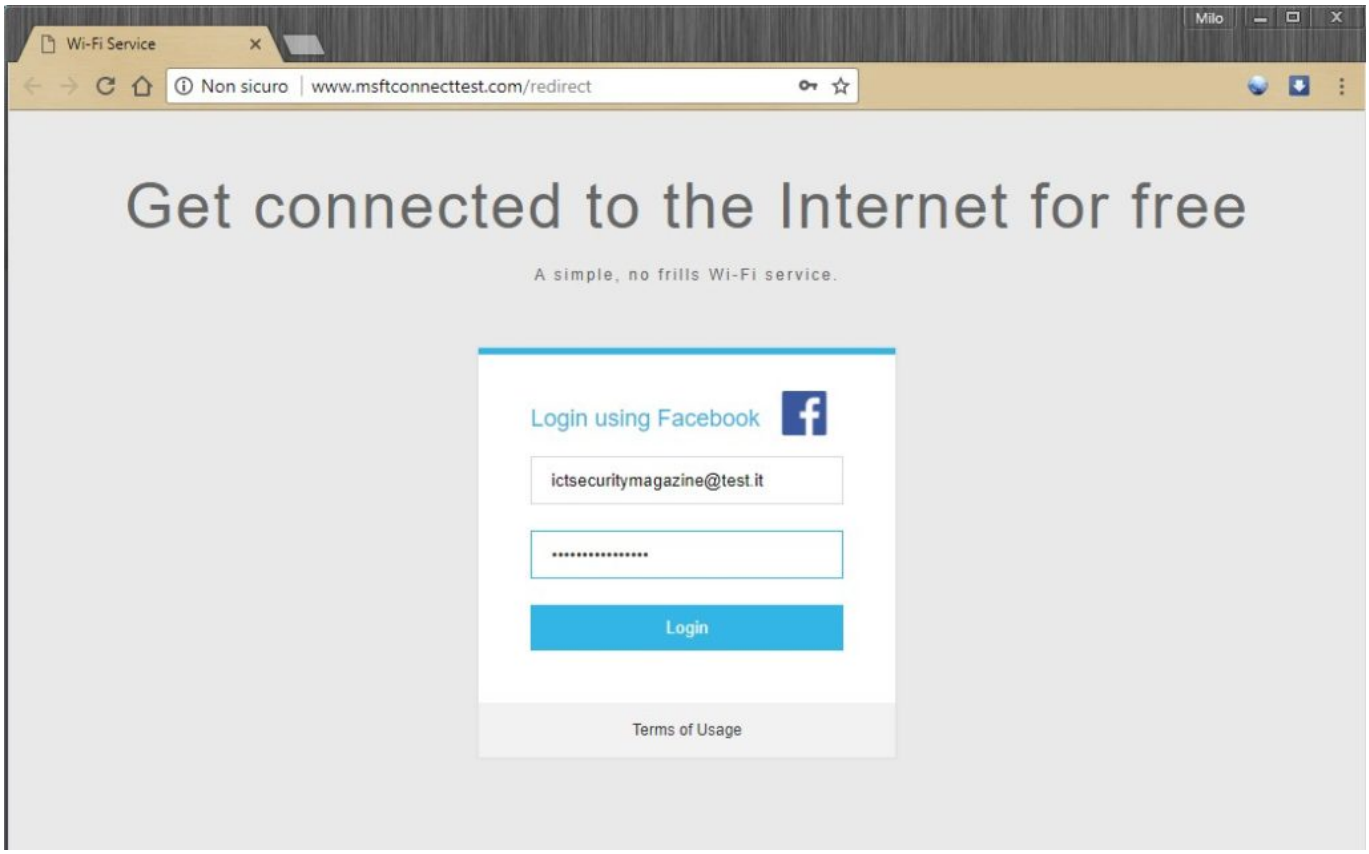
Una prima modalità prevede la possibilità di clonare un Access point - e creare il cosiddetto *Evil twin* - inviando pacchetti di modo da deautenticare tutti i client connessi in quel momento per poi forzarli a riconnettersi all'AP creato dal nostro script. Dopo aver modificato l'indirizzo MAC della scheda di rete attaccante per garantirci un minimo di anonimato, selezioniamo la rete target da clonare tra quelle proposte nel menù:



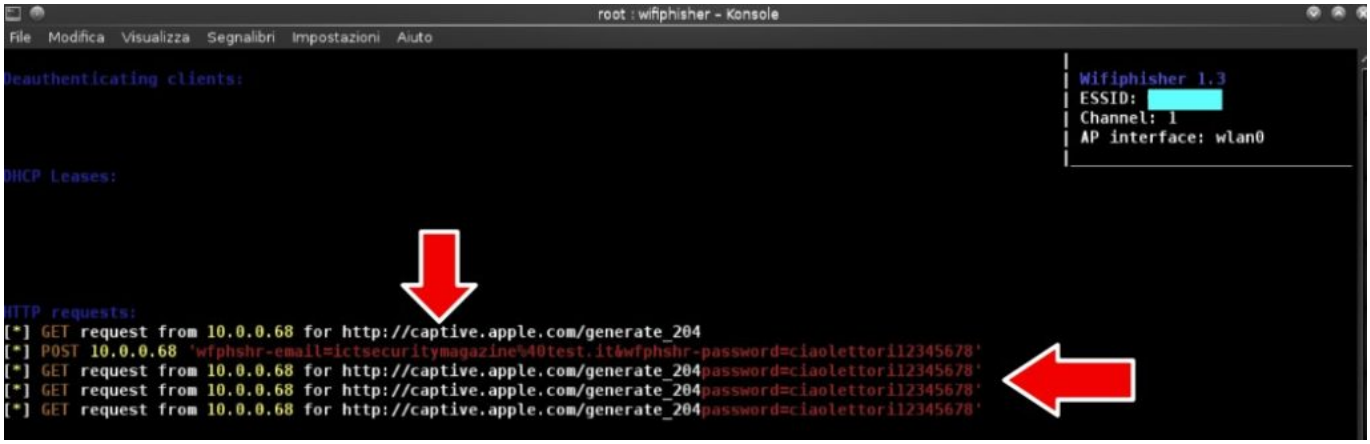
Vengono messi a disposizione quattro possibili scenari con cui adescare il client vittima; nella fattispecie, selezioniamo il numero *4 - OAuth login Page*:



Un aspetto interessante di questa modalità di attacco, è che il tutto avviene in maniera automatica e piuttosto sbrigativa: la vittima vedrà apparire una finestra del proprio browser - sia desktop che mobile - la quale richiede l'inserimento di credenziali per poter proseguire nella navigazione (in questo caso quelle di Facebook):



Ed ecco come il terminale del programma ci restituirà indirizzo mail e password della vittima:



Se volessimo essere ancor più diabolici e aumentare le probabilità di successo, potremmo modificare a nostro piacimento i tag HTML della pagina web, magari inserendo un titolo più accattivante e in lingua italiana oppure rendere ancora più credibile l'URL generato dal server web. Troviamo le cartelle delle pagine HTML del server al percorso:

wifiphisher/data/phishing-pages

Una seconda modalità molto efficace del framework, prevede invece la creazione ex novo di un

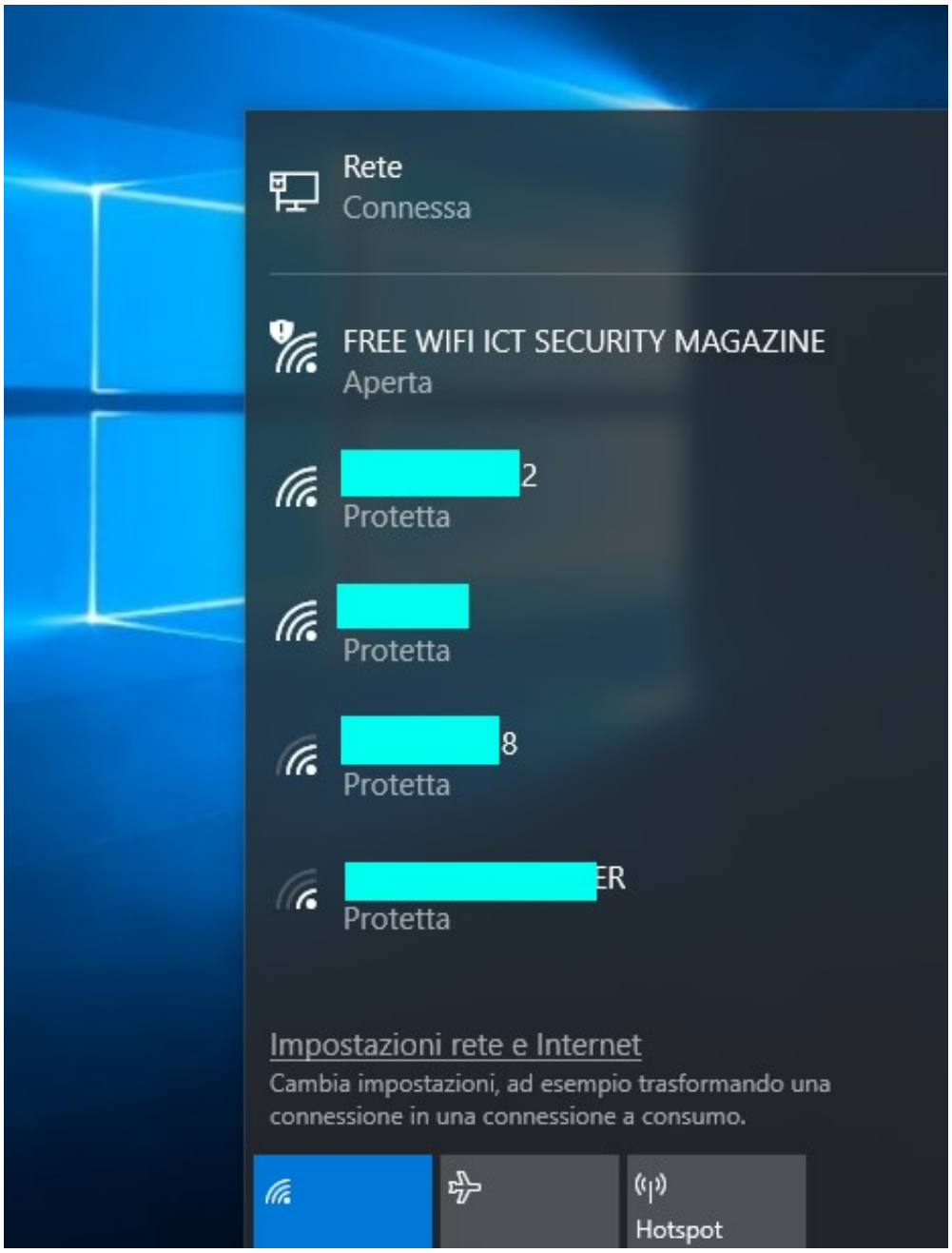
hotspot WiFi aperto da lasciare attivo in attesa di un malcapitato utente alla ricerca di una connessione internet. La community di wifiphisher, inoltre, si è adoperata per ampliare il numero di scenari di quest'ultima tipologia di attacco, mettendo a disposizione il seguente materiale:

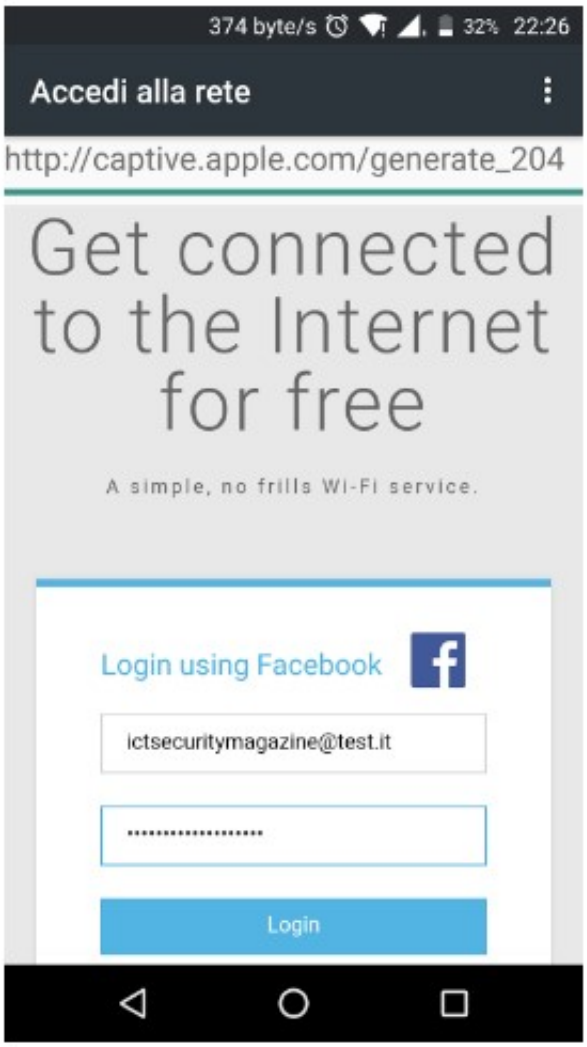
https://github.com/wifiphisher/extra-phishing-pages

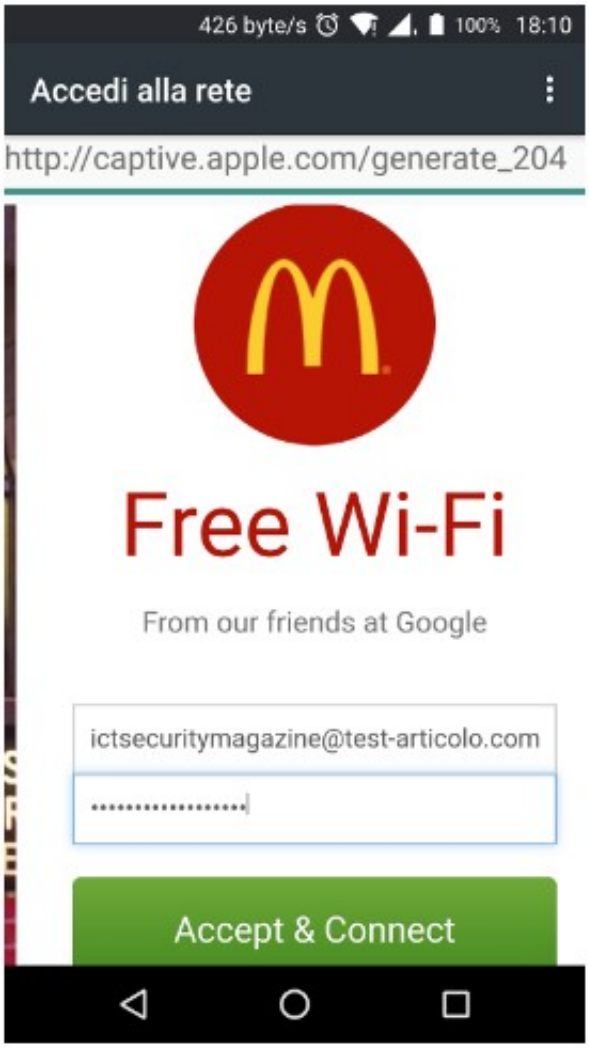
Copiamo le cartelle scaricate al percorso indicato poc'anzi e rilanciamo lo script iniziale di installazione per avere anche questi add-on operativi. Eseguiamo dunque il programma con la seguente sintassi, specificando il nome della rete da usare come trappola e quello della pagina web dello scenario desiderato (parametro -p):

```
sudo wifiphisher --noextensio
ns --essid "FREE WIFI ICT SECURITY MAGAZINE" -p oauth-login -kB
```

La vittima rileverà dal proprio device una nuova rete: come è possibile vedere dagli screenshot successivi, la finta maschera di login appare in primo piano anche con dispositivi Android:


Rete
Connessa
FREE WIFI ICT SECURITY MAGAZINE
Aperta
2
Protetta
Protetta
8
Protetta
ER
Protetta
Impostazioni rete e Internet
Cambia impostazioni, ad esempio trasformando una connessione in una connessione a consumo.
Hotspot





Dopo aver visto ciò che può mettere in atto un potenziale attaccante, ci chiediamo quello che possiamo fare da internauti consapevoli per non incappare in brutte sorprese. Il mondo del software in questo caso ci dà solo parzialmente una mano: è possibile che qualche antivirus metta genericamente in allerta della pericolosità di una nuova rete rilevata ma di certo non fermerà l'utente in fase di inserimento delle credenziali. Nemmeno una VPN ci mette al riparo dalla malevola intercettazione: l'incapsulamento del traffico internet avverrà solo successivamente alla connessione all'Access point, e dunque quando avremmo già inserito i nostri preziosi dati.

E’ invece sicuramente utile tenere aggiornati i propri browser e prestare attenzione alla compilazione automatica che spesso propongono innanzi a nuovi form: URL e pop-up vari devono essere sempre esaminati con la dovuta perizia, premendo invio solo quando siamo certi di inviare i nostri dati al legittimo destinatario. Infine, per i siti più sensibili è consigliabile implementare il meccanismo di doppia autenticazione tramite SMS o token monouso a sei cifre generato da applicazioni per smartphone.

A cura di: **Milo Caranti**