Sito internet: http://nbtimes.it
C. P.30054 Roma 47 – 00193 ROMA
Segreteria: 02/39198533
Fax: 02/39198534

The New Blog Times

Responsabile del sito:
dott. Marco Valerio Principato
(http://nibble.it)

Fatti, opinioni e critiche su scienze, tecnologie e comunicazione

- Software, Evidenza -

Meitu, rischi privacy su iOS e Android: ma davvero?

di Marco Valerio Principato

Stupisce che ci sia chi si «allarma» per la (notevole) raccolta di dati e informazioni da parte di quest'App: per caso pensava che altri fossero da meno? Illudersi va bene, ma essere «allocchi» è imperdonabile.

Immagini dell'App Meitu.

Roma – C'è un titolo che impazza sulle news da qualche giorno: Meitu, l'App per iOS e Android, conosciutissima dagli amanti dei *selfie*, sarebbe un'oscura macchina rastrella-dati al servizio di chissà quale potenza commerciale, che si appropria di una quantità abnorme di informazioni contenute nel proprio *device* mobile.

Le notizie in circolazione sono “alterne”: c'è chi ne illustra i prodigi, ma c'è anche chi ne sottolinea i rischi per la privacy. Tutto è partito da un *tweet* di Johathan Zdziarski, fotografo digitale per O'Reilly, che dice (vedi figura in colonna, trad. di chi scrive): «Sommario: Meitu è un'accozzaglia di molteplici pacchetti di tracciamenti analitici e di marketing/pubblicità, che include qualcosa di carino per farsi usare dalla gente».

La situazione

Per farla breve: chi ha inteso mettere in guardia i propri lettori ha sottolineato come questa App, nella sua versione Android, richieda accesso a una molteplicità di *feature* oggettivamente non necessarie per il proprio funzionamento.

Cosa se ne fa, un'App che – in fin dei conti – è un programma di fotoritocco (una specie di Photoshop, che ormai ne è quasi antonomasia), di informazioni come IMEI, nome dell'operatore cellulare, indirizzo MAC dell'interfaccia Wi-Fi, accesso alle chiamate voce e SMS, eccetera, eccetera... (vedi screenshot Android in colonna)?

I mercati di riferimento

Quello di Android, del resto, è un mercato dozzinale, popolato da persone – in media – scarsamente o per nulla alfabetizzate dal punto di vista informatico/telematico, dove il consumatore è assuefatto alla procedura, da superare a suon di “avanti, avanti” al cui interno sono elencati tutti i dati e gli archivi a cui un'App chiede accesso. Oggi Android occupa circa l'87 per cento del mercato mondiale (dati Comscore).

Non altrettanto è per iOS: un mercato eterogeneo dove senz'altro c'è l'analfabeta informatico/telematico arricchito, ma c'è anche la persona competente. E a questo mercato, Apple si è rivolta con un sistema molto più “fine” che, anche a rischio di risultare pedante, chiede il permesso all'utente prima di concedere accesso a qualsiasi dato o caratteristica “delicati”. I device mobili ba-

sati su iOS occupano circa il 14 per cento del mercato mondiale (dati Comscore).

Il software

I dati di cui Meitu si approprierebbe, tra l'altro, sono estremamente facili da ottenere da uno smartphone Android, ma non altrettanto da uno smartphone iOS (cioè iPhone/iPad), nel quale servono "trucchi" per averli senza chiedere il permesso al proprietario.

I bene informati raccontano che la versione iOS, per "aggirare l'ostacolo" della richiesta di accesso all'utente, si serva (tra l'altro) di un Software Development Kit (SDK) sviluppato per WeChat (il WhatsApp cinese), grazie al quale l'App riuscirebbe a far *cose turche*, ottenendo senza problemi le coordinate GPS e altri dati importanti, come ad esempio sapere se il proprio *device* è *jailbroken* o meno (chi lo possiede sa cosa vuol dire, agli androidi non interessa). E l'indicazione parrebbe tutt'altro che inattendibile, anche solo osservando su iTunes che la versione 6.1.1 di Meitu per iOS porta via ben 102 Megabyte di spazio, manco fosse Facebook.

La difesa

L'azienda, accusata, si è difesa dichiarando di non vendere ad alcuno questi dati e di farne impiego solo internamente, pur memorizzandoli in modo sicuro ("server con cifrature multiple, firewall e protezione da attacchi telematici", racconta un portavoce dell'azienda a *Cnet*) e ammettendo, comunque, di raccoglierli per "migliorare l'esperienza utente" e "studiare la reazione alle pubblicità mostrate", si legge nelle notizie.

Gli utenti/utonti

Singolare è che il portale news di Fastweb, notoriamente *mass-oriented*, si sia prodigato in un articolo dal quale si vorrebbe far intendere che siano proprio queste intromissioni nella privacy ad aver decretato uno scarso successo dell'App. Lasciamo immaginare a chi legge quanto sia credibile tale affermazione: zero.

Conclusioni

Gli utenti, oggi – è del tutto evidente, anche per quelli apparentemente tra i più "evoluti" – sono totalmente ignari di cosa dissemini in giro per i Big Data uno smartphone Android: se solo ne avessero la benché minima idea, prenderebbero il proprio smartphone e lo farebbero volare dalla finestra.

La quota di coloro che possono impiegarne uno con (relativamente) pochi rischi è davvero esigua. Per la medesima ragione, tutti gli androidiani stiano pure tranquilli: Meitu non fa niente di più di ciò che fanno la stragrande maggioranza delle altre App installate – e usate con estrema leggerezza – nei loro smartphone, inclusi Facebook, Twitter, Instagram, YouTube, Google, eccetera eccetera.

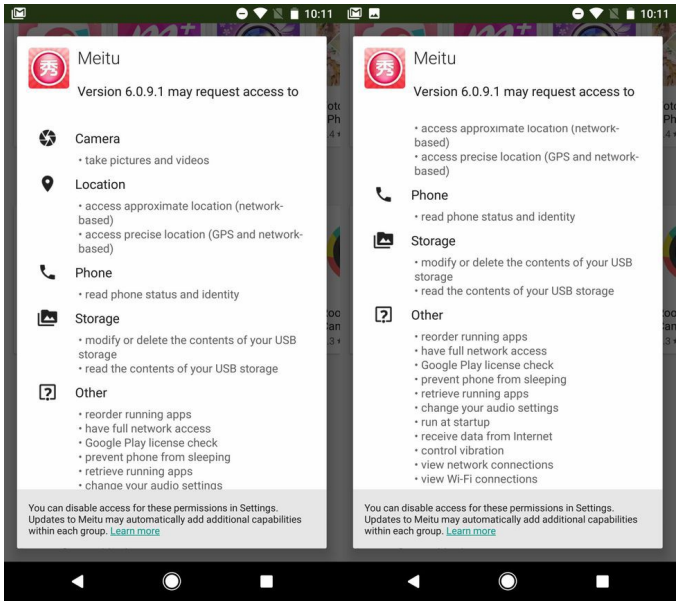
Meno tranquillizzante è la questione iOS: qui sarebbe il caso – a parere di chi scrive – che Apple intervenisse e limitasse la raccolta di simili dati, anche se tramite sistemi destinati normalmente agli sviluppatori (l'SDK di cui sopra). Uno smartphone come l'iPhone, per il solo fatto di costare circa mille euro nella sua versione più "dotata", non può non dar diritto al suo padrone di avere il dovuto controllo sulle informazioni e sulla dispersione delle medesime al di fuori del normale.

Meitu, rischi privacy su iOS e Android: ma davvero? (p. 3 di 3)

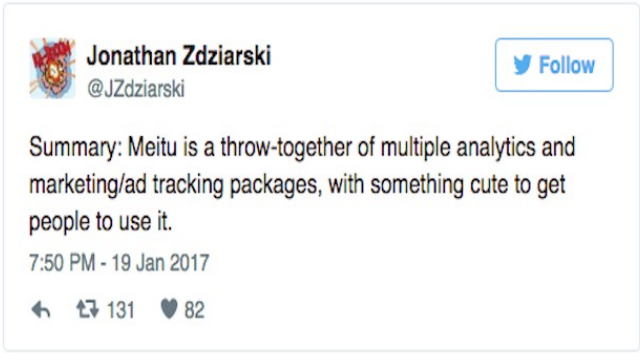
In alternativa, per chi ci tiene – e cosa che chi scrive sta tornando a prendere in considerazione, visto l'*andazzo* generale, che non è solo quello di Meitu – si tornerà a impiegare due apparecchi: uno in cui vi saranno l'intera propria rubrica, l'agenda, le note, gli appuntamenti e l'email, da affiancare alle funzioni di telefonia e SMS, senza alcuna pretesa di App, navigazione e multimedialità avanzata (e ancor oggi, su questo, si presta benissimo la vecchia serie BlackBerry basata su OS 7); l'altro, munito di una SIM economica, anche senza traffico voce, non destinato a contenere dati, con in rubrica solo i propri corrispondenti WhatsApp, nulla nell'agenda e nelle note, un'email "di servizio" (per esempio una su Gmail) e tutta la social-multimedialità che si vuole. I corrispondenti memorizzeranno due numeri: uno per parlarci a voce e inviare SMS, e uno per la... promiscuità.

Della quale, sia ben chiaro, occorrerà ricordarsi bene, specie quando si lasciasse accesso libero a microfono, telecamera, memoria, foto, filmati, GPS e quant'altro.

Marco Valerio Principato



La nutrita lista di permessi chiesti da Meitu su Android.



Il tweet che ha scatenato le «indagini».

Argomenti trattati:
mobile, privacy, android, ios

Questo articolo è online dal 22/01/2017 all'indirizzo:
http://nbtimes.it/?p=21628