OUCH! | Gennaio 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Usare le app in modo sicuro

Introduzione

I tablet e gli smartphone sono tra le tecnologie più utilizzate nella vita professionale e personale di tutti noi. Ciò che li rende così versatili è la grande quantità di app disponibili che consentono agli utenti di essere più produttivi, di comunicare e condividere in modo istantaneo, di imparare nuove cose e divertirsi. A queste possibilità si accompagnano però anche dei rischi. In questa newsletter esamineremo come usare e mantenere le app in modo sicuro.

L'autore di questo numero

Chris Crowley è un consulente indipendente, istruttore SANS certificato e autore di corsi. Potete seguirlo su Twitter **@CCrowMontance** e su Google plus: **+ChrisCrowley**.

Ottenere le app

Il primo passo consiste nello scaricare app unicamente da fonti sicure e di cui avete fiducia. Ricordate che chiunque può creare un'app per cui è consigliabile fare attenzione alla fonte da cui provengono. I criminali informatici hanno affinato le loro abilità per creare e distribuire app infette in grado di apparire del tutto normali: qualora vengano installate, permetterebbero ai criminali di prendere il controllo del vostro dispositivo mobile e leggere le vostre mail, ascoltare le vostre conversazioni e raccogliere i vostri contatti. Scaricando app unicamente da fonti sicure ridurrete la probabilità di installare software infetto.

È il tipo di dispositivo che determina le opzioni a disposizione. I dispositivi Apple, come l'iPad e l'iPhone, consentono di scaricare app solo da ambienti gestiti, come l'app store di Apple. Il vantaggio di questo sta nel fatto che l'azienda di Cupertino sottopone tutte le nuove app a controlli di sicurezza, verificando anche l'affidabilità degli autori. Sebbene quindi Apple non possa individuare la totalità delle app mobili pericolose, gestisce un ambiente in grado di ridurre drasticamente il rischio di installare app infette. Nel caso in cui si sospetti che un'app contenga codice maligno, essa verrebbe rapidamente rimossa dall'app store. Anche i dispositivi Windows Phone utilizzano un approccio simile.

Con i dispositivi Android è diverso, perché Google consente una maggior flessibilità, permettendo di scaricare app da qualsiasi sito Internet. Questa maggior flessibilità richiede però altrettanta responsabilità. Dovete porre molta attenzione alle app che scaricate poiché non tutte vengono analizzate. Anche Google gestisce Google Play, un app store simile

Usare le app in modo sicuro

a quello di Apple, che sottopone le app a un controllo di base. Proprio per questo motivo vi raccomandiamo di scaricare le app solo da Google Play, evitando di farlo da altri siti web, poiché ognuno potrebbe essere in grado di creare e distribuire app maligne e ingannarvi per infettare il vostro tablet o smartphone. Come protezione ulteriore, considerate anche l'installazione di un anti-virus.

Per ridurre ulteriormente il rischio, evitate le app che sono state appena pubblicate, scaricate da poche persone e che hanno ricevuto pochissimi commenti positivi; le app disponibili da più tempo o con più commenti positivi hanno un maggior grado di fiducia. Installate solo app di cui avete bisogno e che utilizzerete. Ogni app installata non solo può introdurre nuove vulnerabilità, ma anche problematiche di privacy. Quando terminate di utilizzare un'app rimuovetela dal vostro dispositivo (potrete sempre reinstallarla più tardi nel caso ne aveste bisogno).

Per maggior sicurezza, installate app solo da fonti affidabili, assicuratevi di aggiornarle regolarmente e verificatene i permessi.

Infine, qualche parola sul jailbreak e il rooting: si tratta di attività per forzare il dispositivo in modo da poter installare app normalmente non autorizzate o modificare funzionalità di sistema già esistenti. Vi raccomandiamo di non eseguire questa operazione poiché non solo permette di scavalcare o eliminare molti controlli di sicurezza presenti nel dispositivo, ma infrange anche la garanzia e il contratto di supporto.

I permessi

Una volta che avrete installato un app da una fonte affidabile, il passo successivo consiste nel verificare che sia stata configurata in modo sicuro e che la vostra privacy sia protetta. Installare app spesso richiede la concessione di permessi. Prima di autorizzare ogni accesso pensate se l'app che state installando ha realmente bisogno di quei permessi. Alcune app, ad esempio, utilizzano servizi di geolocalizzazione: se permettete a un'app di sapere sempre dove vi trovate potreste permettere anche al suo creatore di tracciare i vostri movimenti. Si tratta di informazioni che hanno un valore e che possono essere rivendute ad altri. Se un app richiede permessi che voi non volete dare, cercatene un'altra che rispetti i vostri requisiti. Ricordate: avete molte opzioni a disposizione. I dispositivi Apple permettono la modifica di alcuni permessi nella Configurazione o al momento in cui le app vengono eseguite. I dispositivi Windows e Android sono diversi in quanto adottano un approcio "tutto o niente": se non concedete tutti i permessi richiesti non potrete installare l'app.

Usare le app in modo sicuro

Gli aggiornamenti

Le app, così come i sistemi operativi di computer e dispositivi mobili, devono essere costantemente aggiornate. I criminali informatici sono alla costante ricerca di vulnerabilità da sfruttare con attacchi sviluppati appositamente. Chi ha creato l'app rilascia anche gli aggiornamenti per eliminare queste vulnerabilità. Vi suggeriamo di controllare spesso la disponibilità degli aggiornamenti. Alcune piattaforme possono essere configurate per aggiornare le app automaticamente: questa è la configurazione da preferire. Nel caso non fosse possibile, dovreste controllare manualmente la disponibilità di aggiornamenti almeno ogni due settimane. Ricordate infine di verificare sempre i permessi durante la fase di aggiornamento.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
http://www.securingthehuman.org

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Social Engineering:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_it.pdf
Lo smaltimento dei dispositivi mobili:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201406_it.pdf
Rendere sicuro il Tablet:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis