IBM Security scopre che oltre il 60 percento delle più diffuse app di dating è vulnerabile

In metà delle imprese analizzate i dipendenti accedono ad app di dating attraverso dispositivi mobili usati anche per lavoro; IBM consiglia a utenti e imprese come difendersi

Milano - 16 feb 2015: Un'analisi condotta da IBM Security ha rilevato che oltre il 60 percento delle principali app *mobile* per gli incontri è potenzialmente vulnerabile a svariati tipi di attacchi informatici, mettendo a rischio le informazioni personali dell'utente e i dati aziendali. Lo studio di IBM rivela che molte di queste applicazioni vulnerabili hanno accesso a funzionalità critiche dei dispositivi mobili, quali fotocamera, microfono, memoria, localizzazione GPS e informazioni di pagamento attraverso il mobile wallet, rendendole appetibili e facili prede degli hacker. IBM ha riscontrato inoltre che quasi il 50 percento delle organizzazioni analizzate ha almeno una di queste app di incontri installate su dispositivi mobile utilizzati per accedere alle informazioni aziendali.

Oggigiorno le app di dating sono frequentemente utilizzate da persone di tutte le età per incontrare potenziali partner. Infatti, uno studio di Pew Research ha rivelato che un americano su 10, ovvero 31 milioni di persone circa, ha usato un sito o un'app di incontri e il numero di persone che frequentano persone conosciute online è salito al 66 percento.

"Molti consumatori utilizzano e si affidano ai propri telefoni cellulari per svariate applicazioni. È proprio questa fiducia che dà agli hacker l'opportunità di sfruttare le vulnerabilità, come quelle che abbiamo riscontrato in queste app di incontri", spiega Caleb Barlow, Vice President, IBM Security. "I consumatori devono fare attenzione a non rivelare troppi dati personali su queste tipologie di siti. La nostra ricerca dimostra che alcuni utenti potrebbero essere coinvolti in uno scambio di dati e in un aumento della condivisione degli stessi, che si traducono in una riduzione della sicurezza personale e della privacy".

I ricercatori di IBM Security hanno scoperto che 26 delle 41 app di dating analizzate sulla piattaforma mobile Android avevano vulnerabilità di media o elevata gravità. L'analisi è stata eseguita sulla base delle app disponibili su Google Play nell'ottobre 2014.

Le vulnerabilità rilevate da IBM Security potrebbero essere sfruttate da un hacker per accedere a dati confidenziali . Anche se alcune app hanno adottato misure a tutela della privacy, IBM ha osservato che nonostante queste misure possono comunque verificarsi i seguenti scenari di attacco:

App di incontri utilizzate per scaricare malware: gli utenti abbassano la guardia quando si aspettano di suscitare interesse in un potenziale partner. Ed è proprio in questi momenti che gli hacker si muovono con i loro attacchi. Alcune delle app vulnerabili potrebbero essere compromesse per consentire agli hacker di inviare un messaggio per convincere gli utenti, per esempio, a cliccare su un link per ricevere un aggiornamento, per recuperare un messaggio etc. ma in realtà è solo un espediente per scaricare malware sul dispositivo dell'utente.

Informazioni GPS utilizzate per tracciare i movimenti: IBM ha rilevato che il 73% delle 41 più comuni app di incontri analizzate ha accesso ad informazioni di localizzazione GPS passate e presenti. Gli hacker possono acquisire tali informazioni per scoprire dove l'utente vive, lavora o trascorre la maggior parte del tempo.

Numeri di carta di credito sottratti dall'app: il 48% delle più comuni app di incontri analizzate ha accesso

ad informazioni di pagamento dell'utente, salvate sul dispositivo. Sfruttando una vulnerabilità dell'app di incontri, un hacker potrebbe riuscire ad accedere alle informazioni di pagamento salvate sul mobile wallet del dispositivo e sottrarre le informazioni per effettuare acquisti non autorizzati.

Controllo a distanza della fotocamera o del microfono di un telefono: accedere alla fotocamera o al microfono di un telefono, anche se l'utente non è collegato all'app. Ciò significa la possibilità di intercettare conversazioni private o d'affari riservate.

Hijacking del profilo dell'utente: un hacker può modificare contenuti e immagini sul profilo dell'utente di tali app, spacciarsi per l'utente e comunicare con altri o rivelare informazioni personali all'esterno per danneggiarne la reputazione. Ciò costituisce un rischio anche per altri utenti, perché l'account "compromesso" può essere sfruttato dall'hacker per convincerli a condividere informazioni personali e potenzialmente compromettenti.

Le vulnerabilità specifiche identificate sulle app di incontri comprendono:

- mancanza di validazione dell'input (consentendo attacchi tipo cross-site scripting)
- mancanza di encryption (consentendo attacchi tipo Man In The Middle)
- flag di debug abilitato (rivelando informazioni potenzialmente confidenziali)
- utilizzo di generatore di numeri casuali deboli (compromettendo la sicurezza dei dati cifrati)[A1]

Una volta sfruttate queste vulnerabilità, un hacker può utilizzare il dispositivo mobile per sferrare altri attacchi. Ad esempio, potrebbe intercettare i cookie provenienti dall'app attraverso una connessione Wi-Fi falsa (rougue access point) e poi sfruttare altre funzionalità del dispositivo, quali fotocamera, GPS e microfono, a cui l'app ha il permesso di accedere. Potrebbe creare inoltre una falsa schermata di login, tramite l'app di incontri, per acquisire le credenziali dell'utente. In questo modo, quando l'utente tenta di accedere a un sito web, le informazioni vengono condivise anche con l'hacker.

Le misure per proteggere le app di incontri dagli hacker

Anche se IBM ha scoperto una serie di vulnerabilità in più del 60 percento delle app di incontri Android più diffuse, sia i consumatori che le imprese possono adottare misure per proteggersi dalle potenziali minacce.

Che cosa possono fare i consumatori?

· **Essere riservati:** non divulgare troppi dati personali su questi siti, ad esempio luogo di lavoro, compleanno o profili sui social media fino a quando non si è sicuri della persona con cui si interagisce tramite l'app.

· **Attenzione alle autorizzazioni:** scoprire se si vuole usare un'app controllando le autorizzazioni che essa richiede attraverso la visualizzazione delle impostazioni sul proprio dispositivo mobile. Negli aggiornamenti, le app spesso reimpostano automaticamente le autorizzazioni, stabilendo a quali funzionalità del telefono accedere, ad esempio la rubrica o i dati GPS.

· **Utilizzare password differenti:** utilizzare password univoche per ogni account online posseduto. Se si usa la stessa password per tutti gli account, si è esposti a diversi attacchi in caso di compromissione di un account.

· **Applicazione puntuale delle patch:** applicare sempre le patch e gli aggiornamenti più recenti alle proprie app e al proprio dispositivo non appena disponibili. Questo risolve i bug individuati nel dispositivo e nelle applicazioni e si traduce in una "user-experience" più sicura.

· **Connessioni fidate:** usare solo connessioni Wi-Fi fidate quando si accede a un'app di incontri. Gli hacker usano abitualmente punti di accesso Wi-Fi falsi, che collegano l'utente direttamente al suo dispositivo per eseguire questo tipo di attacchi.

Che cosa possono fare le imprese?
Anche le imprese devono essere pronte a difendersi dalle vulnerabilità delle app di incontri utilizzate all'interno della loro struttura, soprattutto per l'utilizzo del BYOD (Bring Your Own Device). IBM ha riscontrato che quasi il 50 percento delle organizzazioni analizzate per questa ricerca ha almeno una di queste comuni app di incontri installate su dispositivi mobili personali o di proprietà dell'azienda utilizzati per lavoro. Per proteggere le risorse aziendali riservate, le imprese devono:

· **Proteggere i dispositivi:** sfruttare le offerte di Enterprise Mobility Management (EMM) con funzionalità di gestione delle minacce *mobile* (MTM), per consentire ai dipendenti di utilizzare i propri dispositivi senza compromettere la sicurezza dell'organizzazione.

· **Definire le app scaricabili:** permettere ai dipendenti di scaricare solo le app da store autorizzati, come Google Play, iTunes e app store aziendali.

· **La formazione è essenziale:** insegnare ai dipendenti i pericoli legati al download di applicazioni di terzi e di ciò che significa concedere all'app autorizzazioni specifiche di accesso al dispositivo.

· **Comunicare immediatamente le potenziali minacce:** impostare security policy su smartphone e tablet, che intervengono immediatamente qualora si rilevino una compromissione del dispositivo o app pericolose. Ciò consente di proteggere le risorse aziendali mentre si risolve il problema.

Informazioni sulla ricerca
Gli analisti di IBM Security del team IBM Application Security Research hanno utilizzato il nuovo IBM AppScan Mobile Analyzer per analizzare 41 app di incontri disponibili sui dispositivi Android, allo scopo di individuare le vulnerabilità che possono esporre gli utenti a potenziali cyber-attacchi e minacce. Queste app sono state analizzate anche per stabilire le autorizzazioni concesse, scoprendo un gran numero di privilegi eccessivi. Per comprendere l'adozione di queste 41 app di incontri da parte degli utenti aziendali, i dati delle app sono stati analizzati da IBM MobileFirst Protect, ex MaaS360. Prima di rendere questa ricerca accessibile al pubblico, IBM Security ha reso noti i nomi di tutti i fornitori delle app interessate, identificate con questa ricerca. Per ulteriori informazioni su questa ricerca, visitate il sito: www.securityintelligence.com/datingapps

Per una prova gratuita di 30 giorni di IBM AppScan Mobile Analyzer, cliccare qui: http://ibm.co/1zNBl6u
Per una prova gratuita di 30 giorni di IBM MobileFirst Protect (ex MaaS360), cliccare qui: http://bit.ly/1DG5AtF

IBM Security
La piattaforma IBM per la sicurezza fornisce security intelligence per aiutare le imprese a proteggere in modo olistico collaboratori, dati, applicazioni e infrastruttura. IBM offre soluzioni per gestione delle identità e degli accessi, gestione delle informazioni e degli eventi di sicurezza, sicurezza di database, sviluppo applicativo, gestione del rischio, gestione degli endpoint, protezione dalle intrusioni della prossima generazione e molto altro ancora. IBM gestisce una delle maggiori organizzazioni al mondo di ricerca e sviluppo in ambito security, e un'altrettanto vasta organizzazione globale per il delivery dei servizi di sicurezza.
Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il blog di IBM Security Intelligence.
