Panoramica sulla soluzione

# Tutela contro le app mobili colluse

Le app mobili di oggi possono parlarsi facilmente. Purtroppo, questi canali comunicativi possono nascondere anche dei comportamenti insidiosi. Quando si analizzano separatamente due o più app, il comportamento di una di esse può sembrare completamente innocuo. Ma quando nello stesso dispositivo vengono installate delle app mobili che colludono, queste possono scambiarsi informazioni ed eseguire azioni ostili.

Nel *Report McAfee Labs sulle Minacce: giugno 2016* rivolgiamo uno sguardo approfondito alla collusione, che è un nuovo metodo utilizzato dalle app mobili ostili per ostacolare il rilevamento. Per motivi di sicurezza i sistemi operativi mobili isolano le proprie app nelle sandbox, ne limitano le capacità e controllano chiaramente le autorizzazioni che possiedono. Però i sistemi operativi mobili includono anche molti modi con i quali queste app possono comunicare e scambiarsi reciprocamente delle informazioni attraverso i confini delle sandbox.

Nel tentativo di eludere il rilevamento, gli autori degli attacchi possono sfruttare più app con diverse capacità e autorizzazioni al fine di raggiungere i propri obiettivi. Per esempio, l'app A è autorizzata ad accedere ai dati sensibili, mentre l'app B ha accesso a Internet. Quando le app sono installate singolarmente, l'app A non può inviare informazioni all'esterno del dispositivo, mentre l'app B non può accedere ai dati sensibili. Solo quando installate nello stesso dispositivo, l'app A può inviare i dati sensibili all'app B, che a sua volta li trasmette a una destinazione esterna.

La collusione permette alle app mobili di evitare il rilevamento mentre svolgono delle attività ostili come:

- **Furto di informazioni:** un'app con accesso a informazioni sensibili o confidenziali collabora (volente o nolente) con una o più altre app per inviare informazioni oltre i confini del dispositivo.
- **Furto finanziario:** un'app invia informazioni a un'altra che è in grado di eseguire transazioni finanziarie o di richiamare delle API finanziarie.
- **Abuso di servizio:** un'app può controllare un servizio di sistema e ricevere informazioni o comandi da una o più altre app.
- **Aumento dei privilegi:** un'app fornisce privilegi più alti ad altre app per raccogliere dati o eseguire azioni ostili.

intel Security

## Tutela contro le app mobili colluse

Per proteggersi contro le app mobili colluse Intel® Security raccomanda alcune buone pratiche:

- **Usare app provenienti da app store ed editori affidabili** perché le fonti autorizzate eseguono periodicamente scansioni antimalware sulle app in catalogo.
- **Disattivare la capacità di installare le app da "origini sconosciute"** per impedire l'installazione delle app che non sono state autorizzate.
- **Evitare l'utilizzo di software con pubblicità incorporate** perché un eccesso di annunci può indicare la presenza di numerose librerie, che aumentano la possibilità di collusioni.
- **Cercare le classificazioni e recensioni di un'app prima di installarla** per vedere se altri utenti hanno avuto dei problemi di sicurezza con essa.
- **Non sottoporre il dispositivo a "jailbreak" o a "rooting"** per non consentire alle app di ottenere l'accesso al livello di sistema, con l'eventuale installazione di software ostile.
- **Distribuire una soluzione di gestione mobile** come meccanismo per controllare le app che gli utenti possono installare.

## In che modo Intel Security protegge contro le app mobili colluse

**McAfee® Mobile Security for Android**

Quando scarichi delle nuove app, navighi in Internet o addirittura accedi al tuo conto corrente online, McAfee Mobile Security for Android protegge dalle minacce il tuo dispositivo mobile. McAfee Mobile Security for Android utilizza le informazioni fornite dai ricercatori di McAfee Labs per identificare le app ostili, comprese le app mobili colluse, e impedirne l'esecuzione nel dispositivo mobile. Con McAfee Mobile Security for Android il tuo dispositivo mobile è protetto e puoi usare qualsiasi app o loro combinazione in tutta sicurezza.

Caratteristiche di McAfee Mobile Security for Android:

- Scansione in tempo reale che esamina automaticamente email, messaggi di testo, allegati e file per l'eventuale presenza di contenuti ostili.
- Esegue scansioni pianificate complete tramite Smart Scheduler.
- Attiva gli aggiornamenti automatici per fare in modo che le informazioni di intelligence più recenti raccolte dai ricercatori ti proteggano da tutti i tipi di minaccia, comprese le app mobili colluse.
- Segnala e avvisa automaticamente nel caso in cui un'app violi la privacy e consente di disinstallare le app non sicure.
- Blocca i siti web rischiosi che potrebbero contenere delle minacce ostili.

## Ulteriori letture

*Towards Automated Android App Collusion Detection* (Verso il rilevamento automatizzato della collusione fra le app di Android), una ricerca svolta congiuntamente da McAfee Labs e dai ricercatori di diverse università britanniche.

*Colluding Apps: Tomorrow's Mobile Malware Threat* (Le app colluse: il malware mobile di domani), un articolo tratto dalla rivista IEEE Security & Privacy.

*Analysis of the Communication Between Colluding Applications on Modern Smartphones* (L'analisi delle comunicazioni fra le applicazioni colluse nei moderni smartphone), i lavori della XXVIII Conferenza Annua sulle Applicazioni di Sicurezza Informatica.

*A Survey on Application Collusion Attacks on Android Permission-Mechanism* (Sondaggio sugli attacchi derivanti dalla collusione delle applicazioni nel meccanismo delle autorizzazioni di Android), International Journal for Scientific Research & Development.

*Towards a Systematic Study of the Covert Channel Attacks in Smartphones* (Verso uno studio sistematico degli attacchi del canale occulto negli smartphone), International Conference on Security and Privacy in Communication Networks.

*Automatic Detection of Inter-Application Permission Leaks in Android Applications* (Il rilevamento automatico delle fughe di autorizzazioni fra le applicazioni di Android), IBM Journal of Research and Development.



**McAfee. Part of Intel Security.**
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com