Présentation de solution

# Protection contre la collusion entre applications mobiles

Les applications mobiles actuelles doivent disposer d'un moyen pratique pour échanger des informations entre elles. S'il est vrai que ces canaux de communication offrent leur lot d'avantages, il n'en reste pas moins qu'ils peuvent aussi masquer des comportements malveillants. Lorsque plusieurs applications sont analysées séparément, le comportement de chacune d'entre elles, pris individuellement, peut sembler totalement inoffensif. Toutefois, lorsque des applications mobiles agissant de connivence sont installées sur un même équipement, celles-ci peuvent échanger des informations et se livrer à des activités malveillantes.

Le *Rapport de McAfee Labs sur le paysage des menaces — Juin 2016* s'intéresse de près à la collusion entre applications mobiles, un nouveau mécanisme utilisé par les applications malveillantes pour compliquer la détection. Pour des raisons de sécurité, les systèmes d'exploitation mobiles isolent les applications dans des environnements restreints de type sandbox, limitent leurs fonctionnalités et contrôlent les autorisations dont elles bénéficient. Par contre, ils incluent également de nombreuses méthodes qui permettent aux applications de dépasser les frontières de ces environnements pour communiquer et échanger des informations entre elles.

Pour éviter d'être détectés, les attaquants tentent parfois d'exploiter plusieurs applications dotées de fonctionnalités et autorisations différentes pour atteindre leurs objectifs. Prenons l'exemple de l'application A capable d'accéder à des informations sensibles et de l'application B disposant d'un accès à Internet. Lorsque chacune de ces applications est installée seule sur un terminal, l'application A ne peut pas transmettre les informations vers l'extérieur et l'application B est dans l'impossibilité d'accéder aux informations sensibles. Ce n'est que lorsqu'elles sont installées côte à côte sur un terminal que l'application A peut envoyer les informations sensibles à l'application B qui, à son tour, peut les acheminer vers une destination externe.

intel Security

Cette collusion permet aux applications de contourner la détection lorsqu'elles se livrent aux comportements malveillants suivants :

- **Vol d'informations :** Une application autorisée à accéder à des informations sensibles collabore (volontairement ou non) avec une ou plusieurs autres applications pour envoyer des informations vers une destination externe.
- **Vol financier :** Une application envoie des informations à une autre application autorisée à exécuter des transactions financières ou des appels d'API financières.
- **Utilisation abusive de services :** Une application peut contrôler un service système et recevoir des informations ou des commandes d'une ou plusieurs autres applications.
- **Obtention de privilèges plus élevés :** Une application octroie à une autre application ses privilèges supérieurs pour recueillir des données sensibles ou se livrer à des activités malveillantes.

## Protection contre la collusion entre applications mobiles

Intel® Security a défini une série de bonnes pratiques pour vous protéger contre la collusion entre applications mobiles :

- **Utilisez des applications proposées par des boutiques d'applications et éditeurs de logiciels de confiance**, car les sources autorisées effectuent des analyses antimalware de routine.
- **Désactivez l'option d'installation d'applications de sources inconnues** pour éviter l'installation d'applications non approuvées.
- **Évitez les logiciels incorporant de la publicité**, vu que des annonces en trop grand nombre peuvent indiquer la présence de plusieurs bibliothèques publicitaires, ce qui augmente le risque de collusion.
- **Lisez les évaluations et les avis des clients avant de télécharger une application** pour vous assurer que d'autres utilisateurs de l'application n'ont pas rencontré de problèmes de sécurité.
- **Ne débridez pas l'équipement**, car cette manipulation permet aux applications de bénéficier d'un accès système et, le cas échéant, d'installer des logiciels malveillants.
- **Déployez une solution de gestion des équipements mobiles** pour contrôler les applications pouvant être installées par les utilisateurs.

## Comment Intel Security peut vous aider à vous protéger contre la collusion entre applications mobiles

### McAfee® Mobile Security for Android

Lorsque vous téléchargez de nouvelles applications, naviguez sur Internet ou exécutez des opérations bancaires en ligne, McAfee Mobile Security for Android protège votre terminal mobile contre les menaces. En se fondant sur les informations fournies par les chercheurs de McAfee Labs, cette solution identifie les applications malveillantes, notamment celles qui agissent de connivence, et en bloque le fonctionnement sur votre terminal mobile. McAfee Mobile Security for Android vous permet donc non seulement de protéger votre équipement, mais aussi d'utiliser vos applications en toute sérénité.

Fonctionnalités de McAfee Mobile Security for Android :

- Analyse automatique en temps réel des e-mails, SMS, pièces jointes et fichiers pour y détecter d'éventuels contenus malveillants
- Exécution d'analyses complètes planifiées à l'aide de Smart Scheduler
- Installation automatique des mises à jour pour assurer une protection optimale contre les menaces de tous types, y compris la collusion entre applications, grâce aux données les plus récentes sur la sécurité proposées par des chercheurs spécialisés dans les menaces
- Génération automatique de rapports et d'alertes lorsqu'une application porte atteinte à la confidentialité des données de l'utilisateur, avec la possibilité de désinstaller les applications à risque
- Blocage des sites web dangereux pouvant comporter des menaces

## Lectures supplémentaires

*Towards Automated Android App Collusion Detection* (Vers une solution automatisée de détection de la collusion entre applications Android), une étude menée conjointement par McAfee Labs et des chercheurs de plusieurs universités britanniques

*Colluding Apps: Tomorrow's Mobile Malware Threat* (La collusion entre applications : la nouvelle menace pour les terminaux mobiles), un article paru dans le magazine IEE Security & Privacy

*Analysis of the Communication Between Colluding Applications on Modern Smartphones* (Analyse de la communication interapplicative sur les smartphones modernes), Comptes rendus de la 28e édition de l'ACSAC (Annual Computer Security Applications Conference)

*A Survey on Application Collusion Attacks on Android Permission-Mechanism* (Étude sur les attaques perpétrées par des applications en collusion contre le mécanisme de gestion des autorisations Android), International Journal for Scientific Research & Development

*Towards a Systematic Study of the Covert Channel Attacks in Smartphones* (Vers une étude systématique des attaques exploitant des canaux clandestins sur les smartphones), International Conference on Security and Privacy in Communication Networks

*Automatic Detection of Inter-Application Permission Leaks in Android Applications* (Détection automatique des octrois abusifs d'autorisations entre applications Android), IBM Journal of Research and Development



**McAfee. Part of Intel Security.**
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com