IBM Security
Livre blanc

La mobilité : une nouvelle aire de jeu pour les voleurs

Comment se protéger contre les logiciels malveillants sur dispositifs mobiles ?

IBM

La mobilité progresse et les menaces aussi

Introduction

Avec la prolifération continue des appareils intelligents, l'explosion des applis mobiles et l'accès toujours plus étendu aux fichiers professionnels, la mobilité transforme les entreprises à un rythme sans précédent. Les employés sont invités par leur entreprise à améliorer leur productivité en tout lieu et à toute heure. Il se voient ainsi proposer des politiques de BYOD (Bring Your Own Device : apporter votre dispositif personnel) et la possibilité d'utiliser leurs applis personnelles pour leurs activités professionnelles.

Il se trouve cependant que les entreprises n'ont pas suivi le rythme de cette explosion de la mobilité et ont tardé à déployer une sécurité de niveau entreprise pour protéger leurs données sensibles. Les pirates et les malfaiteurs ont sauté sur l'occasion pour s'introduire sur les réseaux et s'approprier des informations professionnelles sensibles stockées sur des terminaux mobiles. Les responsables de l'informatique et de la sécurité ont besoin d'une solution de sécurité moderne et robuste pour détecter, analyser et éradiquer ces menaces de manière proactive.

D'après les estimations, 16 millions d'appareils mobiles sont déjà infectés par des logiciels malveillants.

L'explosion de la mobilité dans les entreprises

Les chiffres concernant la progression de la mobilité sont stupéfiants. Les prévisions annonçaient qu'en 2014 le nombre de téléphones portables (7,3 milliards) serait supérieur au nombre d'habitants sur la planète (7 milliards).[1]

Selon Arxan Technologies, 138 milliards d'applis mobiles ont été téléchargées en 2014. Ce nombre devrait presque être multiplié par deux d'ici 2017.[2]

Les consommateurs ont été les premiers catalyseurs de ce mouvement en adoptant des dispositifs et des applis mobiles pour leur usage personnel. Les entreprises ont donc certainement profité de l'accélération de ces tendances. La tendance du BYOD dans l'entreprise poursuit sa progression. Elle aide les entreprises à mobiliser l'ensemble de leurs équipes et à économiser sur les frais d'achat et de support. Gartner prévoit que la moitié des employeurs exigeront le BYOD d'ici 2017.[3]

Les applis mobiles créent de nouveaux workflows efficaces pour les employés. La transparence de l'accès aux données professionnelles, aux courriers électroniques et aux contenus progresse également, ce qui améliore encore la productivité. Les entreprises commencent à intégrer en priorité les appareils mobiles dans leurs différentes processus, ce qui génère à son tour une propagation de la mobilité dans l'entreprise.

Quand les applis mobiles attaquent

Cependant, les pirates et les malfaiteurs menacent de détourner les avantages considérables acquis par la transformation de l'entreprise. Les appareils mobiles sont de plus en plus infectés : 25 % en 2014 contre 20 % en 2013. On estime que 16 millions d'appareils mobiles sont déjà infectés par des logiciels malveillants.[4]

Des logiciels malveillants sont spécifiquement élaborés pour attaquer des appareils mobiles en exploitant certaines vulnérabilités des différents systèmes d'exploitation.

Toute faille de la protection des données peut s'avérer extrêmement onéreuse car toute atteinte à l'image d'une entreprise peut être aggravée par des pertes financières. Le Ponemon Institute a estimé qu'une seule violation de la sécurité coûtait 3,5 millions de dollars en 2014, soit 15 % de plus que l'année précédente.[5]

Figure 1 : Top des applis Android et iOS payantes ayant été piratées

Les dispositifs corrompus par des applis mobiles malveillantes constituent généralement la plus grande source de risques pour presque toutes les entreprises. Selon Arxan Technologies, lorsque les utilisateurs se connectent à des réseaux non sécurisés ou qu'ils installent des applis dangereuses provenant de sources peu fiables, les appareils mobiles deviennent vulnérables aux logiciels malveillants. 97 % des applis Android payantes et 87 % des applis iOS payantes ont été piratées et publiées dans des magasins d'applis tierces.[6]

Comme le démontre une autre étude du Ponemon Institute[7], même les applis provenant d'entreprises de confiance et disponibles dans des magasins d'applis classiques peuvent comporter des risques immenses. 82 % des personnes interrogées déclarent que l'introduction des applis mobiles au travail a très considérablement (50 %) ou considérablement (32 %) augmenté les risques de sécurité. Bien que la plupart des employés soient de « férus utilisateurs d'applis » (66 %), plus de la moitié d'entre eux (55 %) indiquent que leur entreprise n'a pas élaboré de politique pour définir des utilisations acceptables des applis mobiles au travail.

Seules 30 % des répondants ont déclaré que leur entreprise a déployé un magasin d'applis. Cependant, une large majorité (37 %) admet que, même s'ils disposent d'un magasin d'applis, les employés peuvent utiliser des applis non-contrôlées provenant de sources extérieures. En outre, 55 % des entreprises déclarent que les employés sont autorisés à télécharger et à utiliser des applis métier de leur magasin sur leur dispositif personnel.

Situation actuelle des logiciels malveillants sur dispositifs mobiles

Qu'est-ce qu'un logiciel malveillant sur dispositifs mobiles ?

Les logiciels malveillants sur dispositifs mobiles sont spécifiquement conçus pour attaquer des appareils mobiles en exploitant les vulnérabilités de leur système d'exploitation. Les trois types courants de logiciels malveillants sont les suivants :

- Les logiciels espions volent et espionnent certaines données sur les appareils, et les transmettent aux pirates pour qu'ils en tirent profit.
- Les chevaux de Troie affectent les fonctions des appareils ou des applis, réalisent automatiquement des transactions ou lancent des communications à l'insu de l'utilisateur.
- Le débridage ou rootage donne aux pirates des privilèges administrateur et un accès aux fichiers sur certains appareils.

Pour comprendre la menace et la raison pour laquelle elle se concentre sur les dispositifs mobiles, examinons les processus employés par les cyber-criminels. Les appareils mobiles sont l'une des voies les plus faciles à utiliser pour accéder à des données sensibles. Alors que les systèmes back-end des entreprises sont bien protégés par des pare-feu, des systèmes anti-intrusion et des logiciels antivirus, ce niveau de protection n'est généralement pas disponible sur des appareils professionnels ou privés. Les appareils personnels (BYOD) sont particulièrement vulnérables car ils sortent du périmètre de sécurité et échappent au contrôle de l'entreprise.

Si des pirates sont en mesure d'attaquer un dispositif, ils peuvent envoyer un logiciel malveillant pour piéger l'utilisateur, capturer des informations qui permettront son identification personnelle et des identifiants de connexion. Ils peuvent ensuite prendre le contrôle du compte de l'utilisateur et profiter des sessions avec authentification pour collecter des données personnelles et réaliser des transactions frauduleuses.

Android est une mine de vulnérabilités

Selon IDC, Android a dominé le marché des appareils mobiles en 2014 avec 81,2 % de part de marché et plus d'un milliard d'appareils vendus.[8] Android domine actuellement le marché grand public, mais son adoption dans les entreprises est pour le moins laborieuse.

La conception de base et la grande ouverture de la plateforme et de l'écosystème d'applis sont les raisons pour lesquelles Android est actuellement l'un des systèmes de l'industrie mobile les plus vulnérables aux infections par logiciels malveillants.

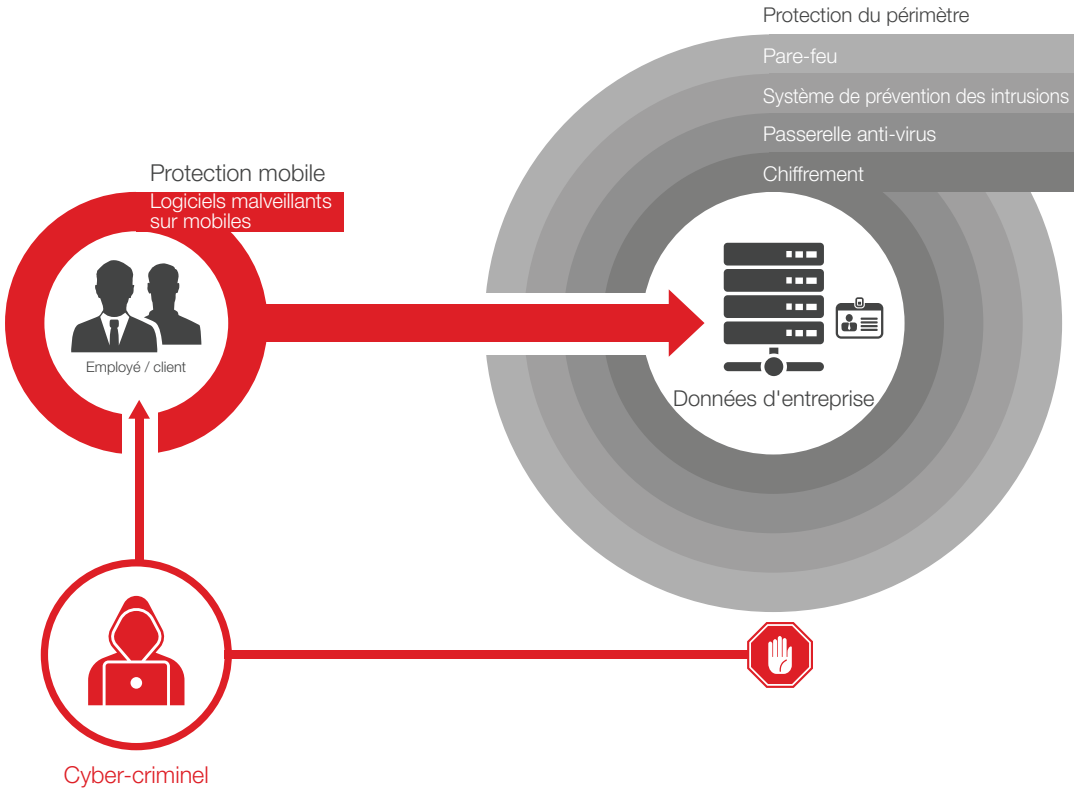

Figure 2 : Les malfaiteurs attaquent le maillon faible pour accéder aux données sensibles

La conception de base et la grande ouverture de la plateforme et de l'écosystème d'applis sont les raisons pour lesquelles Android est actuellement l'un des systèmes de l'industrie mobile les plus vulnérables aux infections par logiciels malveillants. Les caractéristiques qui font d'Android la cible la plus facile à exploiter pour les pirates et les malfaiteurs incluent :

- Les applis Android peuvent être téléchargées et installées à partir de n'importe quel magasin d'applis ou site Internet tiers.
- Google Play Store ne contrôle pas et n'approuve pas systématiquement chaque appli, contrairement à Apple avant qu'une appli iOS soit publiée sur iTunes.
- Il n'existe aucun contrôle des certificats numériques pour certifier des applis Android. Ces applis sont généralement auto-certifiées et il est impossible de remonter jusqu'à leur développeur. Voilà pourquoi il est facile d'attaquer une appli Android, d'y introduire un logiciel malveillant et de la re-certifier.

Les cybercriminels ne cessent d'inventer de nouvelles solutions créatives pour attaquer les vulnérabilités des plateformes des systèmes d'exploitation mobiles, qui sont différentes de celles des ordinateurs fixes.

Google a mis en œuvre des pratiques de sécurité pour éliminer les applis malveillantes dans le Google Play Store. Il balaie les applis chargées dans le magasin et exécute chacune d'entre elles pour détecter et supprimer les logiciels malveillants, les logiciels espions et les chevaux de Troie. Lorsque Google découvre de nouveaux logiciels malveillants, ses systèmes peuvent parcourir l'ensemble de Google Play afin de supprimer tous les fichiers suspects. Google désactive également les applis et comptes des développeurs qui ne respectent pas ses conditions générales et ses politiques sur les contenus.

Cependant, comme indiqué précédemment, 97 % des applis Android payantes les plus répandues ont déjà été piratées et apparaissent dans les magasins d'applis ou sur des sites Internet tiers. Par conséquent, si un de vos employés (ou même son enfant) télécharge et installe le dernier super jeu gratuit sur un appareil Android professionnel ou personnel à partir d'une source non officielle, vous pouvez vous attendre à ce que l'appareil soit infecté par un logiciel malveillant. Votre entreprise peut instituer des politiques et des formations pour éviter ces pratiques mais, sans protection automatisée, les appareils Android sont potentiellement vulnérables.

Le cheval de Troie SVPENG représente un bon exemple de logiciel malveillant Android dans le secteur de la banque. Il a été découvert alors qu'il ciblait les institutions financières russes et européennes. SVPENG représente une avancée considérable dans le domaine des logiciels malveillants sur mobiles. Cette attaque cible directement les utilisateurs d'applis bancaires en trompant la victime et en lui demandant ses identifiants via une technique répandue sur ordinateurs de bureau appelée « attaque de couverture ».

Au cours de cette attaque, le logiciel malveillant se trouvant sur l'appareil infecté attend que l'utilisateur ouvre l'appli mobile de sa banque. Une fois que le logiciel malveillant comprend qu'une session d'appli bancaire commence, il affiche un écran par dessus l'appli (d'où le terme « couverture ») qui ressemble exactement à l'appli de la banque, sauf qu'il s'agit d'une fausse page. L'utilisateur est ainsi obligé d'interagir avec la page générée par le logiciel malveillant en pensant qu'il s'agit de la véritable page de sa banque. Il lui fournit donc ses identifiants bancaires.

Ce même type d'attaques de couverture peut menacer les données sensibles d'une entreprise. Un employé peut innocemment saisir ses identifiants professionnels et transmettre ainsi aux malfaiteurs les informations dont ils ont besoin pour s'authentifier dans les systèmes de l'entreprise et ravager ses données.

Dernièrement, l'équipe IBM X-Force® Application Security Research Team a découvert une vulnérabilité dans le SDK Dropbox d'Android qui permettait aux malfaiteurs de connecter des applis d'appareils mobiles à un compte Dropbox contrôlé par l'attaquant à l'insu de la victime.[9] Cette vulnérabilité, appelée DroppedIn, peut être exploitée de deux manières : soit à l'aide d'une appli malveillante installée sur l'appareil de l'utilisateur, soit à distance, par un site Internet, à l'aide de techniques d'infiltration.

Il s'agit d'une faille importante du mécanisme d'authentification de l'appli Android utilisant un SDK Dropbox de la version 1.5.4 à la version 1.6.1. Toutefois, suite au signalement du problème à Dropbox par l'équipe IBM Security, une correction a été apportée dans le SDK Dropbox for Android v1.6.2 en seulement 4 jours. La présentation du programme DroppedIn apparaît dans une publication de blog (note de pied de page 9) sur le site SecurityIntelligence.com.

Et c'est bien à cause de la facilité d'installation des applis malveillantes sur les appareils Android que les pirates ont pu exploiter le programme DroppedIn. Les cybercriminels ne cessent d'inventer de nouvelles solutions créatives pour attaquer les vulnérabilités des plateformes des systèmes d'exploitation mobiles, qui sont différentes de celles des ordinateurs fixes.

Bien qu'Android continue à être confronté à de nombreux défis pour s'implanter dans les entreprises, les dernières avancées en matière de sécurité de Google et des fabricants d'appareils, ainsi que le support apporté par les fournisseurs de solutions EMM (Enterprise Mobility Management) aident à asseoir sa présence dans le privé et dans l'administration publique. Lorsque le grand public, et donc vos employés, choisissent d'utiliser des appareils Android, votre entreprise doit fournir la sécurité et la protection nécessaires pour bloquer les logiciels malveillants.

iOS n'est pas invulnérable

Les appareils iOS dominent le marché de l'entreprise pour plusieurs raisons clés. Lorsque l'iPhone est apparu en 2007, les professionnels ont commencé à utiliser leurs iPhones personnels pour le travail plutôt que leurs vieux smartphones fournis par l'entreprise. L'architecture et le comportement « sandbox » des applis iOS intègrent une sécurité naturelle à la plateforme. Il est ainsi difficile pour les pirates d'infecter l'ensemble de l'appareil et des applis, sauf si les utilisateurs contournent volontairement leurs systèmes de sécurité.

Après s'être initialement concentré sur le grand public, Apple a rapidement compris le potentiel du marché de l'entreprise. Apple a commencé à incorporer des contrôles pour que les responsables informatiques puissent mieux sécuriser et gérer les appareils, les applis et les données en travaillant avec des fournisseurs de solutions MDM (Mobile Device Management).

Contrairement à l'architecture et à l'écosystème d'applis Android, l'environnement d'applis Apple est beaucoup plus fermé. Les applis iOS publiques peuvent uniquement être téléchargées et installées à partir d'iTunes App Store, sauf si le dispositif iOS a été débridé. Les applis chargées dans iTunes passent par un processus d'approbation rigoureux avant d'être officiellement publiées par Apple. En outre, des certificats numériques sont nécessaires pour autoriser les applis iOS et il est donc possible de remonter jusqu'au développeur de chaque appli.

C'est pourquoi au fil des années, les iPhones et iPads sont devenus très présents dans les entreprises, l'administration publique et les établissements d'enseignement. Cependant, la rigueur de ces mesures de sécurité n'a pas empêché les cyber-criminels d'essayer de pirater des appareils iOS. Ainsi, des pirates ont fait preuve de créativité et ont réussi à infecter des iPhones et des iPads, notamment avec de nouveaux logiciels malveillants appelés WireLurker et Masque Attack.

WireLurker est une nouvelle catégorie de logiciels malveillants qui cible aussi bien les ordinateurs Mac OS que les mobiles iOS.[10] WireLurker est unique dans le sens où il peut infecter un dispositif iOS non débridé qui se connecte à un ordinateur Mac OS via un câble USB.

Voici comment WireLurker procède généralement pour attaquer les appareils :

- L'utilisateur télécharge et installe une appli OS X infectée par un logiciel malveillant sur son ordinateur Mac OS. En règle générale, cette appli provient d'un magasin d'applis tiers et non officiel.
- L'utilisateur exécute ensuite l'appli infectée et lui attribue des autorisations racines qui impliquent de connaître le mot de passe administrateur de l'ordinateur Mac OS.
- Lorsqu'elle s'exécute, l'appli OS X infectée télécharge plusieurs applis iOS et attend qu'un dispositif iOS faisant confiance à l'ordinateur se connecte via un câble USB.
- Lorsque l'appareil iOS se connecte en toute confiance à l'ordinateur Mac OS infecté, le logiciel malveillant charge les applis iOS malveillantes sur l'iPhone ou l'iPad.
- Les applis iOS sont des applis certifiées, ce qui signifie que les cyber-criminels ont soit détourné le compte d'une autre entreprise ou ont soit réussi à faire approuver leurs applis par Apple. Ces applis s'accompagnent également de profils de provisionnement, donc les dispositifs iOS leur font confiance.

Lorsque les applis iOS malveillantes sont chargées sur les appareils iOS non débridés d'utilisateurs peu méfiants, elles peuvent voler des informations et les communiquer régulièrement aux serveurs des attaquants.

Peut-être encore plus pernicieux que WireLurker, Masque Attack est l'un des derniers logiciels malveillants découverts[11] . Il peut lui aussi infecter des appareils iOS non débridés, mais sans nécessiter de connexion à un appareil Mac OS infecté. Dans cette forme d'attaque, une appli iOS installée avec une procédure d'entreprise/ad-hoc peut remplacer une appli approuvée par iTunes App Store, tant que ces deux applis utilisent le même identifiant séquentiel.

Voici comment Masque Attack procède pour remplacer des applis authentiques de l'utilisateur et voler des informations :

- L'utilisateur clique sur un lien posté sur un quelconque site Internet. Il télécharge et installe alors sans le savoir une appli malveillante signée avec un certificat d'entreprise et qui pourrait s'appeler « Nouvel Angry Bird », par exemple.
- L'appli malveillante remplace l'appli officielle, par exemple une appli bancaire ou de messagerie, qui possède le même identifiant séquentiel.
- Les malfaiteurs peuvent reproduire à l'identique l'interface de connexion de l'appli d'origine afin de voler les identifiants de l'utilisateur.
- L'appli peut également s'appuyer sur les caches de données locaux pour plagier la fonctionnalité remplacée, par exemple les derniers courriers électroniques d'une appli de messagerie.

Lorsque les cyber-criminels sont en possession des identifiants et des informations en cache, les données confidentielles et les informations financières des utilisateurs sont exposées aux attaques et aux fuites.

Quand la protection contre les logiciels malveillants rencontre la gestion de la mobilité d'entreprise

IBM® MaaS360® Mobile Threat Management

IBM apporte une couche de sécurité supplémentaire à l'EMM avec l'intégration d'IBM Security Trusteer® pour assurer la protection contre les logiciels malveillants sur mobiles et les appareils infectés, tels que tablettes ou des smartphones débridés ou rootés.

Cette intégration et cette synergie créent une protection puissante contre les pirates et les malfaiteurs qui essaient d'obtenir des informations professionnelles et personnelles à des fins délictueuses.

Grâce à une base de données continuellement mise à jour, vous pouvez détecter et analyser des applis iOS et Android infectées par des logiciels malveillants certifiés.

Utilisé par des centaines de millions de personnes pour protéger les entreprises contre la fraude et les fuites de données, Trusteer confère une intelligence et une clairvoyance orientées sécurité au MaaS360.

Détection et élimination des logiciels malveillants sur mobiles :

- Détectez et analysez des applis iOS et Android infectées par des logiciels malveillants certifiés, grâce à une base de données continuellement mise à jour.
- Ajoutez des exceptions d'applis pour personnaliser l'utilisation des applis acceptables.
- Etablissez des contrôles régis par des politiques granulaires pour prendre les mesures appropriées.
- Utilisez un moteur de règles de conformité quasiment en temps réel pour automatiser l'assainissement.
- Alertez l'utilisateur et les parties responsables quand un logiciel malveillant est détecté.
- Affichez les dispositifs infectés dans My Alert Center et les évènements de détection dans les tableaux de My Activity Feed.
- Désinstallez automatiquement les applis infectées (pour les appareils Android sélectionnés tels que Samsung SAFE)
- Bloquez l'accès aux appareils, ou effacez-les de manière sélective ou intégrale
- Collectez et affichez les caractéristiques des menaces sur les appareils, notamment :
  - Logiciels malveillants détectés
  - Configurations de système suspectes détectées, par exemple un auditeur de SMS ou un paquet de démarrage inconnu
  - Connexion à un point Wi-Fi non sécurisé
  - Installation autorisée d'applis non marchandes
  - Version du système d'exploitation
- Etudiez l'historique d'audit des événements de détection de logiciels malveillants.

Figure 3 : MaaS360 intègre Trusteer pour détecter, analyser et éradiquer les logiciels malveillants sur les appareils corrompus

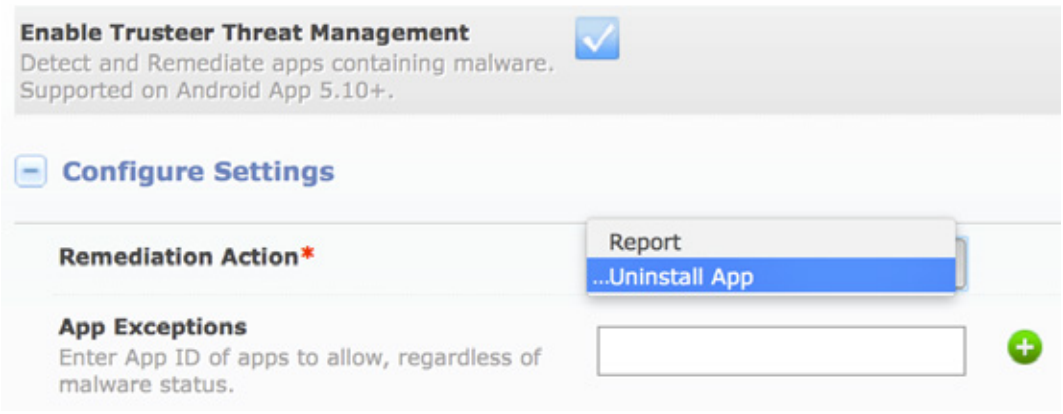

Figure 4 : Certains paramètres de configuration du MaaS360

Détection supplémentaire du débridage et du rootage :

- Détectez les appareils mobiles corrompus ou vulnérables
- Protégez-vous contre les appareils iOS débridés et les appareils Android rootés qui peuvent offrir aux pirates informatiques des privilèges supplémentaires sur les systèmes d'exploitation, ce qui favorise les attaques
- Découvrez les techniques de dissimulation actives qui essaient de masquer la détection d'appareils débridés et d'appareils rootés
- Appliquez une logique de détection mise à jour par liaison sans fil et sans actualisation des applis offrant une réactivité inégalée face à la réactivité des pirates
- Paramétrez les règles de sécurité et de conformité pour automatiser l'assainissement
- Bloquez l'accès aux appareils, effacez-les de manière sélective ou intégrale, ou excluez-les de vos contrôles

Les appareils et les données des utilisateurs peuvent également être protégés par une couche de sécurité qui n'est directement accessible aux utilisateurs.

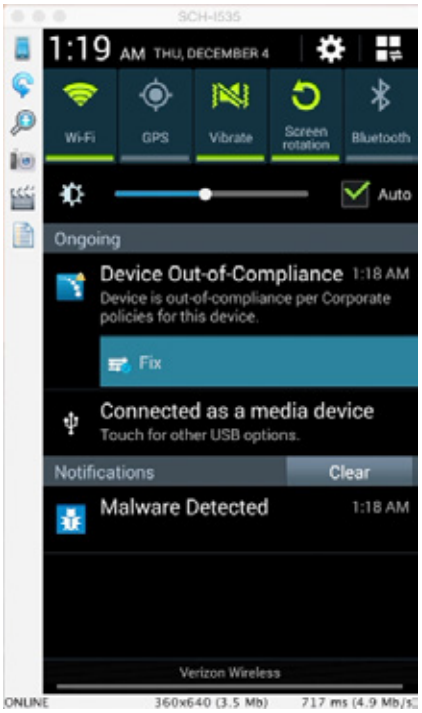

Figure 5 : Capture d'écran montrant un logiciel malveillant détecté et un appareil non conforme

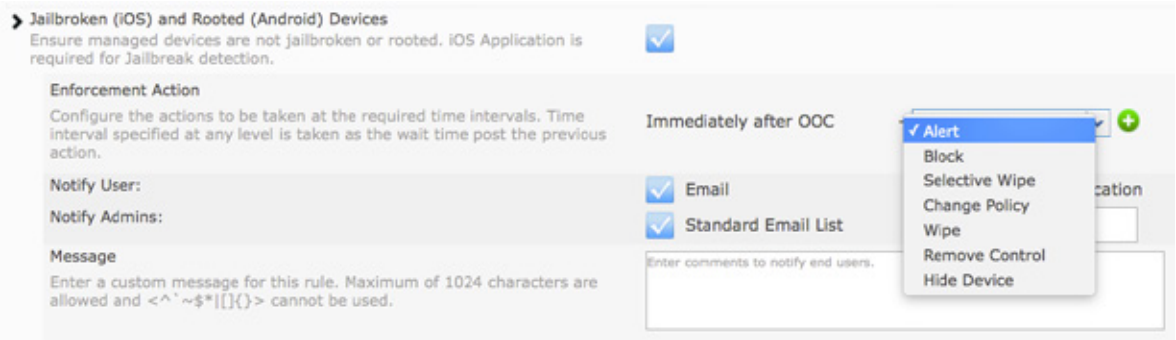

Figure 6 : Configurer des actions de mise en conformité pour les appareils débridés ou rootés

Trusteer Mobile Risk Engine active des couches de protection et une intelligence anti-cybercriminalité qui assurent une prévention flexible contre les logiciels malveillants afin de permettre une détection et une adaptation plus rapides aux derniers types d'attaque. Les logiciels malveillants n'ont donc quasiment aucune possibilité d'atteindre les objectifs. Mis à jour de façon continue pour être capable de rechercher les derniers types de logiciels malveillants, de débridage ou de routages, le moteur réalise des évaluations du risque mobile quasiment en temps réel sur les appareils et les applis.

Principaux avantages

Les avantages de la solution MaaS360 Mobile Threat Management dépassent la simple protection des appareils et des données de l'entreprise. Les appareils et les données des utilisateurs peuvent également être protégés par cette couche de sécurité qui n'est pas directement accessible par les utilisateurs.

Les entreprises peuvent aller encore plus loin pour former leurs utilisateurs et protéger leurs données.

- Prendre en charge et assurer la sécurité des appareils appartenant à l'entreprise et des dispositifs appartenant aux employés (BYOD)
- Protéger les données personnelles sous forme d'avantage salarial apporté par le BYOD
- Gérer de manière proactive les menaces mobiles quasiment en temps réel
- Réduire les risques de fuite de données d'entreprise et personnelles sensibles
- Rationaliser l'adoption d'Android pour l'entreprise, notamment avec le BYOD
- Appliquer des mesures automatisées pour remédier aux risques de sécurité mobiles dès qu'ils surviennent

Sensibilisation et protection des utilisateurs

Outre cette solution MaaS360 Mobile Threat Management, les entreprises peuvent aller encore plus loin pour former leurs utilisateurs et protéger leurs données.

Les entreprises devraient organiser les activités suivantes sur la sécurité mobile :

- Former les employés aux questions de sécurité des applis : Sensibiliser les employés aux dangers que représente le téléchargement d'applis tierces et le risque induit par de faibles niveaux d'autorisation des appareils.
- Protection des appareils BYOD : Mettre en place des fonctions de gestion de la mobilité d'entreprise pour permettre aux employés d'utiliser leurs propres appareils tout en préservant la sécurité de l'entreprise.
- Permettre aux employés de télécharger uniquement des applis dans des magasins autorisés : Limiter le téléchargement d'applis aux seuls magasins d'applis, par exemple : Google Play, Apple App Store et le magasin d'applis de votre entreprise, le cas échéant.
- Agir rapidement lorsqu'un appareil est infecté : Définir des politiques automatisées sur les smartphones et les tablettes pour que des mesures soient instantanément appliquées dès la découverte d'un appareil infecté ou d'applis malveillantes. Cette approche protège les données de votre entreprise et corrige le problème.

Pourquoi utiliser MaaS360 ?

Avec MaaS360, IBM a intégré une protection avancée contre les logiciels malveillants à un système leader de la gestion de la mobilité et de la sécurité. MaaS360 est facile et rapide à configurer et à utiliser pour protéger les données sensibles présentes sur des appareils mobiles d'entreprise ou personnels.

A propos d'IBM MaaS360

IBM MaaS360 est une plateforme de gestion de la mobilité d'entreprise qui soutient la productivité et assure la protection des données en fonction des habitudes de travail individuelles. Des milliers d'entreprises font confiance au MaaS360 comme fondation de leurs initiatives mobiles. MaaS360 offre une gestion intégrale, avec de puissants contrôles de sécurité pour tous les utilisateurs, les appareils, les applis et les contenus afin de supporter tous les déploiements mobiles. Pour plus d'informations sur l'IBM MaaS360 et pour commencer un essai gratuit de 30 jours, rendez-vous sur www.ibm.com/maas360

A propos d'IBM Security

La plateforme de sécurité IBM fournit les données de sécurité nécessaires pour aider les entreprises à gérer leurs utilisateurs, leurs données, leurs applis et leur infrastructure de manière globale. IBM propose des solutions de gestion des identités et des accès, de gestion des données et des événements relatifs à la sécurité, la sécurité des bases de données, le développement d'applis, la gestion des risques, la gestion des terminaux, la protection de dernière génération contre les intrusions, etc. IBM possède l'un des plus grands services du monde en matière de recherche, de développement et de mise en œuvre de services de sécurité. Pour en savoir plus, visitez le site : www.ibm.com/security

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Produit aux Etats-Unis
Mars 2016

Pensez à recycler

WGW03150-FRFR-01

1 Notre planète comptera plus d'abonnements de téléphonie mobile que d'habitants d'ici 2014, janvier 2013 International Telecommunications Union, http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

2 Bilan sur la sécurité des applis mobiles, novembre 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

3 Bring Your Own Device: Réalité et perspectives, mai 2013, Gartner, http://www.gartner.com/newsroom/id/2466615

4 Rapport sur les logiciels malveillants de Motive Security Labs, deuxième semestre 2014, Motive Security Labs, http://www.gartner.com/newsroom/id/2466615

5 Etude sur le coût des failles de sécurité 2014 : analyse mondiale, mai 2014, Ponemon Institute, http://www-03.ibm.com/security/data-breach/

6 Bilan sur la sécurité des applis mobiles, novembre 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

7 Bilan sur l'insécurité des applis mobiles, février 2015, Ponemon Institute, https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov33432&S_TACT=102PW2CW

8 Worldwide Mobile Phone Tracker trimestriel, février 2015, IDC, http://www.idc.com/getdoc.jsp?containerId=prUS25450615

9 DroppedIn : Vulnérabilité exploitable à distance dans SDK Dropbox pour Android, mars 2015, IBM Security, http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.Vb-1_SisG8W

10 Wirelurker : La nouvelle ère des logiciels malveillants sur OS X et iOS ; blog, PaloAlto Networks, 05/11/2014 http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

11 Xue, H., Wie, T., Yulong, Z.; Masque: Toutes vos appli iOS nous appartiennent, 10/11/2014, https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html