IBM MaaS360 Mobile Threat Management

Arrêtez les logiciels malveillants sur les appareils mobiles iOS et Android

Principaux avantages

- Soutenez en toute sécurité le BYOD et les terminaux appartenant à l'entreprise
- Gérez de manière proactive les menaces mobiles quasiment en temps réel
- Réduisez les risques de fuite de données sensibles d'informations d'entreprise et personnelles
- Prenez des mesures automatisées pour remédier à des risques de sécurité mobiles

Logiciels malveillants sur mobiles : la prochaine grande menace pour la sécurité

Les entreprises sont transformées à un rythme sans précédent par la mobilité. La mode du BYOD (Bring Your Own Devise) continue de s'étendre dans le monde de l'entreprise. Les applications mobiles créent des flux de travail nouveaux et efficaces pour les employés. Un accès transparent aux données professionnelles, aux e-mails et à du contenu se développe en parallèle, augmentant les gains de productivité de ces tendances.

En raison de la popularité et de la vitesse à laquelle les appareils mobiles sont devenus l'un des piliers de l'entreprise, les pirates informatiques et les voleurs ciblent les appareils mobiles avec des logiciels malveillants, créant ainsi la prochaine grande menace pour la sécurité. Les données d'entreprise sont particulièrement vulnérables aux applications non autorisées et aux sites Internet malveillants.

- 138 milliards d'applications ont été téléchargées en 2014.[1]
- Les logiciels malveillants sur mobiles sont en pleine croissance. Les codes malveillants infectent plus de 11,6 millions d'appareils mobiles à tout moment.[2]
- Les attaques récentes WireLurker et Masque menacent les appareils iOS.[3,4]
- Le préjudice causé à la marque d'une entreprise est aggravé par la perte financière, le coût d'une seule violation étant estimé à plus de 11 millions de dollars.[5]

Les responsables de l'informatique et de la sécurité ont besoin d'une solution de sécurité moderne et robuste pour détecter, analyser et remédier aux logiciels malveillants sur mobiles de manière proactive.

Arrêtez les menaces mobiles dans votre entreprise

IBM® MaaS360® Mobile Threat Management offre un système de pointe pour protéger les appareils iOS et Android des logiciels malveillants. Vous pouvez détecter les risques et gérer les menaces avant qu'ils ne compromettent vos données d'entreprise.

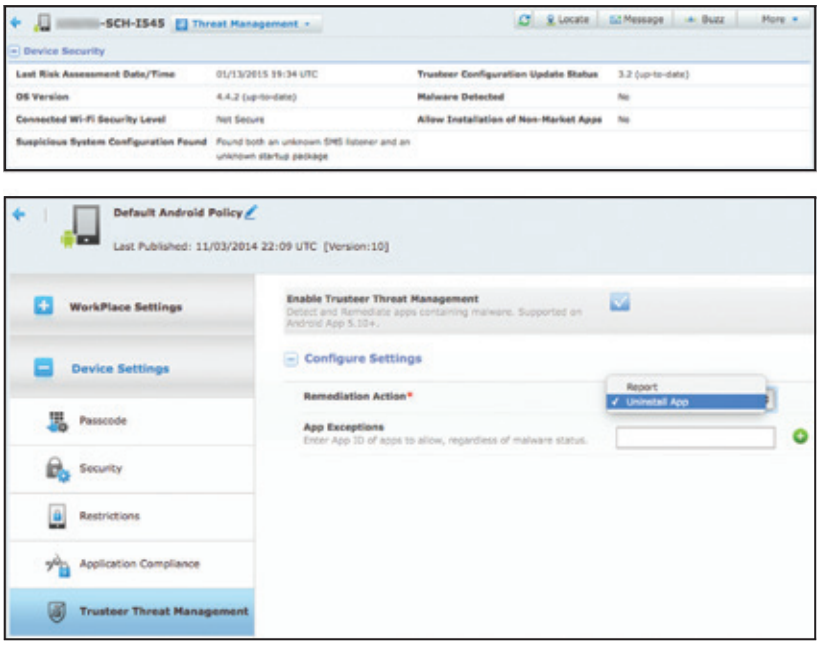

Figure 1 : Exemples de données rapportées sur un appareil protégé et paramétrage des règles dans MaaS360 Mobile Threat Management

Grâce à l'intégration avec IBM Trusteer®, utilisé par des centaines de millions d'utilisateurs pour protéger les entreprises contre la fraude et les violations de données, MaaS360 offre une nouvelle couche de sécurité à la gestion de la mobilité d'entreprise (Entreprise Mobility Management).

Ne laissez pas de logiciels malveillants faire dérailler la transformation mobile de votre entreprise. Équilibrez les initiatives de productivité de votre entreprise avec la sécurité prodiguée par MaaS360.

Détection et assainissement des logiciels malveillants sur mobiles

- Détectez et analysez les applications iOS et Android avec une base de données des signatures virales et des comportements malveillants continuellement mise à jour
- Ajoutez des exceptions d'applications pour personnaliser l'utilisation des applications autorisées
- Établissez des commandes de règles granulaires pour prendre les mesures appropriées
- Utilisez un moteur de règles de conformité quasiment en temps réel pour automatiser la remédiation
- Alertez l'utilisateur et les parties responsables quand un logiciel malveillant est détecté
- Affichez les appareils compromis dans My Alert Center (mon centre d'alertes) et des évènements de détection dans les tableaux de My Activity Feed (Alimentation de mon activité)
- Désinstallez automatiquement les applications infectées (pour les appareils Android sélectionnés tels que Samsung SAFE™)
- Bloquez l'accès, nettoyez les appareils sélectivement ou intégralement
- Restreignez l'utilisation des solutions de conteneurs MaaS360
- Collectez et affichez les caractéristiques des menaces d'appareils incluant :
  - logiciel malveillant détecté ;
  - configurations de système suspectes trouvées, comme un lecteur de SMS ou un logiciel de lancement d'application inconnu ;
  - connexion à un point Wi-Fi non sécurisé ;
  - installation d'applications non marchandes autorisées ;
  - version du système d'exploitation.
- Révisez l'historique d'audit des évènements de détection de logiciels malveillants

Détection supplémentaire du débridage iOS et Android

- Détectez les appareils mobiles compromis ou vulnérables
- Protégez contre les appareils iOS et Android débridés qui peuvent offrir aux pirates informatiques des privilèges supplémentaires sur les systèmes d'exploitation
- Découvrez les techniques de dissimulation actives qui essaient de masquer la détection d'appareils débridés et d'appareils ancrés
- Utilisez la logique de détection mise à jour par liaison sans-fil sans avoir besoin d'application de mise à jour pour être plus réactif face aux pirates informatiques en mouvement rapide
- Paramétrez les règles de sécurité et de conformité pour automatiser le remédiation
- Bloquez l'accès, effacez les appareils sélectivement ou intégralement

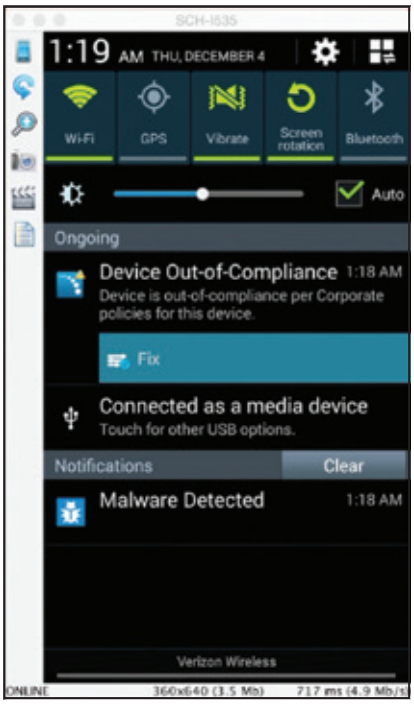

Figure 2 : Exemple d'une notification de logiciel malveillant sur un appareil

IBM Security Trusteer Mobile Risk Engine

- Fournit des couches de protection et des renseignements cybercriminels pour une prévention adaptative face aux logiciels malveillants
- Détecte rapidement et s'adapte aux comportements d'attaque les plus récents pour que les logiciels malveillants n'aient presque aucune chance de commettre une fraude
- Réalise une évaluation des risques mobiles quasiment en temps réel basée sur les facteurs de risque des appareils et des applications
- Se met à jour continuellement pour fournir les derniers contrôles sur les logiciels malveillants, les débridages iOs et Android

Pour en savoir plus sur les solutions de prévention des fraudes d'IBM Security, contactez votre ingénieur ou partenaire commercial IBM. Vous pouvez également consulter le site Web suivant : **ibm.com**/security/fr-fr.

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

Produit aux États-Unis
Août 2016

Recyclable

1 Rapport annuel d'Arxan : "*State of Mobile App Security Reveals an Increase in App Hacks for Top 100 Mobile Apps*", novembre 2014, Arxan Technologies, Inc., https://www.arxan.com/2014/11/17/arxans-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/

2 Kindsight Security Labs Malware Report – Q4 2013, Alcatel-Lucent, http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf

3 Xiao, Claud, WireLurker: A New Era in OS X and iOS Malware, Blog post on Palo Alto Networks, 5 novembre 2014, http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

4 Zue, Hui, Wei, Tao and Zhang, Yulong; Masque Attack: All Your iOS Apps Belong to Us, 10 novembre 2014, https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

5 2013 Cost of Cyber Crime Study: United States, Sponsored by HP Enterprise Security, Ponemon Institute, octobre 2014, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

WGD03057-FRFR-02