Une banque du classement Global 2000 sécurise 9 000 smartphones Android pour respecter des exigences de conformité internes

Le défi

Pour pouvoir appliquer sa politique de mobilité COPE (appareils appartenant à l'entreprise, mais utilisés également pour des besoins personnels), cette banque de premier rang avait besoin d'une solution de sécurité mobile compatible avec sa politique interne en matière de protection des données. Elle devait pouvoir être intégrée à VMware AirWatch et capable de fournir une visibilité sur les menaces mobiles pesant sur ses effectifs internationaux.

L'équipe informatique a décidé d'implémenter une politique de mobilité COPE pour réduire le temps d'assistance, ce modèle permettant de gérer un nombre limité de types d'appareil et de versions d'Android. La banque a également mis au point sa propre application d'entreprise, qui permet aux employés de proposer des services bancaires aux clients via des appareils mobiles. Sans aucune visibilité sur les menaces et les fuites de données sur mobile, l'équipe chargée de la mobilité informatique savait que les points de terminaison mobiles non protégés pouvaient être la cible d'attaques. C'était un risque de sécurité majeur.

Profil du client

Cette entreprise de services financiers implantée au Moyen-Orient possède un vaste réseau composé de 1 400 filiales dans le monde et figure au classement Global 2000 de Forbes.

Secteur d'activité : services financiers

Politique de mobilité : COPE

Solution EMM : VMware AirWatch

La solution

- Lookout Mobile Endpoint Security

Les résultats

- L'entreprise respecte les politiques internes en matière de protection des points de terminaison
- Elle bénéficie d'une visibilité sur les menaces à haut risque
- La productivité des employés a été améliorée et les demandes d'assistance n'ont pas augmenté

« La solution de Lookout recueille les données sur les menaces dans le monde entier et nous permet d'avoir une visibilité sur tous les risques qui pèsent sur nos données mobiles. »

Responsable, service de l'infrastructure informatique

Comme toute entreprise de services financiers, cette banque fait partie d'un secteur réglementé. Mais les règles de confidentialité et de conformité pour les appareils mobiles sont encore nouvelles et mal définies dans son pays d'origine. Toutefois, pour l'équipe chargée de la mobilité informatique, les appareils mobiles ne sont pas différents des ordinateurs portables. Ils constituent simplement un autre point de terminaison pour accéder aux ressources de l'entreprise. Pour respecter ses politiques internes en matière de sécurisation de l'ensemble des points de terminaison, cette banque avait besoin d'une solution de sécurité mobile pour compléter AirWatch, de ses propres stratégies de chiffrement et de sensibiliser ses employés à la sécurité.

La solution

L'équipe informatique a évalué un certain nombre de solutions pour résoudre les problèmes posés par la sécurité mobile, mais elle a constaté que la plupart des fournisseurs traditionnels de solutions de sécurisation des points de terminaison ne prenaient pas en charge Android ou utilisaient une méthode de détection des menaces basée sur les signatures, qui ne permet pas de faire face en temps réel aux menaces qui pèsent sur les plates-formes mobiles.

L'équipe informatique a choisi Lookout pour sa capacité à recueillir des données sur les menaces mobiles (Threat Intelligence) dans le monde entier. Lookout Mobile Endpoint Security était la solution qui permettrait au personnel mobile d'accéder librement aux applications de productivité, sans avoir à classer manuellement les applications dans des listes noires ou blanches. L'équipe a ensuite travaillé avec Lookout afin de déployer et d'activer Lookout Mobile Endpoint Security sur environ 9 000 smartphones Samsung Galaxy. Elle a pu facilement déployer l'application Lookout For Work via AirWatch sur les appareils des employés, sans aucune intervention de leur part.

Les résultats

La banque se félicite de la rapidité du déploiement de Lookout, et notamment de l'installation de l'application Lookout For Work sur 2 000 appareils par jour vers la fin du processus.

Pendant le déploiement, Lookout Mobile Endpoint Security a détecté un grand nombre d'applications à haut risque, des logiciels malveillants capables de rooter les appareils et des attaques de type man-in-the-middle dans le parc mobile de l'entreprise. De quoi conforter la banque dans sa décision de faire de la conformité avec ses politiques internes en matière de protection des points de terminaison sa priorité.

La conclusion

Depuis le déploiement, la banque est ravie de constater que le nombre de demandes d'assistance n'a pas augmenté, car les employés corrigent eux-mêmes les menaces mobiles dès qu'ils reçoivent une alerte de l'application Lookout For Work sur leur appareil.

Maintenant que l'équipe informatique de la banque a atteint ses objectifs en matière de conformité et de visibilité sur les menaces mobiles et les applications à risque dans le parc mobile, elle peut se concentrer sur les prochaines étapes, à savoir utiliser l'intégration de Lookout et AirWatch pour activer dans AirWatch des politiques de correction automatique des menaces détectées par Lookout et réduire encore un peu plus le temps de correction.

Nombre de menaces détectées	
Chevaux de Troie	
16 détections de chevaux de Troie 5 détections (Shedun)	Shedun est une famille de logiciels malveillants Android qui a été découverte par Lookout en 2015. Le logiciel malveillant se fait passer pour une application légitime, mais tente de rooter l'appareil pour permettre à un tiers d'installer des applications supplémentaires. Cela peut entraîner l'installation d'autres logiciels malveillants.
Appareils compromis	
37 détections d'activateurs de rootage	Le rootage permet aux attaquants potentiels d'obtenir des privilèges d'administration supérieurs et peut compromettre les fonctionnalités de sécurité natives d'Android, comme le cloisonnement par sandbox des applications.
Attaques basées sur le réseau	
91 attaques de type man-in-the-middle	Les attaquants utilisent différentes techniques pour intercepter le trafic réseau vers et depuis des appareils mobiles. Si l'attaquant se trouve à proximité physique d'un appareil cible, il peut utiliser un réseau Wi-Fi ou cellulaire malveillant pour accéder au trafic réseau. S'il est éloigné de l'appareil mobile, il peut utiliser un logiciel malveillant ou des techniques d'ingénierie sociale pour convaincre un utilisateur de configurer son appareil pour faire passer tout le trafic réseau via une connexion VPN ou un proxy malveillant.
Menaces applicatives	
172 détections de riskware 61 détections de adware 3 détections de chargeware	Les applications riskware comprennent le code, les bibliothèques ou les services réseau qui présentent un risque pour les appareils en raison de vulnérabilités connues ou de la faible fiabilité des fournisseurs de services utilisés par les applications. Les chargewares entraînent une facturation indue et les adwares affichent des publicités intrusives ou envoient des données personnelles potentiellement confidentielles aux réseaux publicitaires, hors des pratiques publicitaires courantes.