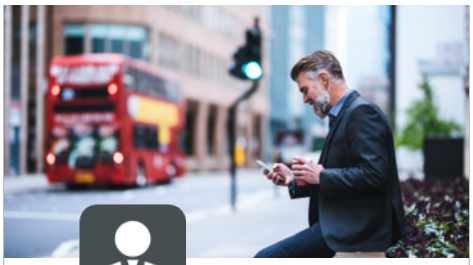
Comment Lookout protège les dirigeants

Lookout assure une protection mobile pour les dirigeants et les responsables d'entreprise

Des préoccupations de sécurité à grande échelle

Les dirigeants sont constamment en déplacement, ce qui signifie que les données les plus sensibles d'une organisation sont consultées à partir de smartphones et de tablettes, notamment les performances financières, la tarification des produits, ou encore les plans de développement de l'entreprise. Plus important encore, ces données sont fréquemment consultées en dehors des quatre murs de l'entreprise et hors de la portée des outils de sécurité traditionnels. Ce qui signifie que les outils de sécurité traditionnels contre le phishing et les logiciels malveillants ne protègent pas les dirigeants pendant une grande partie de leur journée de travail.



Défis

1. Constamment en déplacement, les dirigeants se connectent à des réseaux cellulaires étrangers et à des réseaux Wi-Fi à risque.
2. Les dirigeants sont des cibles privilégiées pour les attaques de whaling aux motivations financières.
3. Des données extrêmement sensibles sont consultées à partir d'appareils mobiles hors de la portée des outils de sécurité traditionnels.

Étude de cas concrète concernant les dirigeants

En déplacement, la pratique courante consiste à se connecter aux points d'accès Wi-Fi, en particulier à l'étranger. Cependant, la sécurité de ces réseaux est souvent insuffisante et les dirigeants sont donc plus susceptibles d'être la cible d'attaques de type man-in-the-middle. L'acteur malveillant peut alors faire passer tout le trafic via un routeur non autorisé, ou déposer discrètement des logiciels malveillants sur l'appareil. Dans les deux cas, cela crée une passerelle facile vers un appareil qui dispose d'un accès à des données d'entreprise sur le Cloud.

Les dirigeants sont des cibles privilégiées pour les attaques de phishing hautement ciblées qui exploitent l'ingénierie sociale, c'est-à-dire les « attaques de whaling ». Alors que ces attaques peuvent nuire à une entreprise aussi bien au niveau de la marque que sur le plan financier, plus de 50 % des organisations pointent du doigt les attaques de whaling et la fraude du PDG pour évoquer leur principale menace associée aux e-mails. Les motivations des attaques de whaling sont presque toujours financières, qu'il s'agisse d'essayer de voler des fonds ou d'accéder à des données de recherche de grande valeur, qu'un acteur malveillant pourrait détourner et revendre à un concurrent.

Les fonctionnalités stratégiques de Lookout

Lookout Phishing and Content Protection inspecte toutes les demandes d'URL, notamment les e-mails personnels et professionnels, les SMS, les applications de messagerie et les applications comportant des URL pour télécharger des plug-ins malveillants. Lookout bloque de façon dynamique les demandes d'URL pour accéder à des sites Web identifiés comme étant des sites malveillants ou de phishing. De plus, Lookout détecte les attaques basées sur le réseau qui tentent de voler des données personnelles ou des données sensibles d'entreprise via des réseaux cellulaires ou Wi-Fi. L'utilisateur final est alors informé que le réseau qu'il utilise présente un danger, puis reçoit des consignes lui expliquant comment se déconnecter. En parallèle, les administrateurs mettent en place des politiques visant à bloquer l'accès aux ressources d'entreprise au cas où la connexion serait non sécurisée.

Pourquoi choisir Lookout ?

La solution Lookout Mobile Endpoint Security avec accès conditionnel continu assure la sécurité et la conformité de tous les appareils grâce à un ensemble de données considérable, alimenté par plus de 170 millions d'appareils et l'analyse de plus de 70 millions d'applications mobiles. Lookout Security Cloud facilite le déploiement de Lookout et la mise en place de politiques de sécurité dans l'ensemble de l'organisation, tant pour les appareils gérés que pour les appareils non gérés. Les utilisateurs reçoivent en temps réel des alertes et des étapes à suivre pour corriger les problèmes concernant les applications malveillantes, les connexions au réseau et les anomalies du système. Ils bénéficient également d'une vérification dynamique de l'état de santé de l'appareil afin d'assurer un accès conditionnel continu aux applications et aux données sensibles d'entreprise.

[1] Phishing Response Trends UK: Stop the Chaos. Cofense 2019