**Sophos présente Intercept X for Mobile**

* *Une nouvelle sécurité pour Chrome OS et une Défense contre les Menaces Mobiles (Mobile Threat Defense) pour les équipements Android et iOS*
* *Une solution qui protège les utilisateurs contre les nouvelles applications Fleeceware découvertes par les SophosLabs*

**OXFORD, Royaume-Uni** - 14 janvier 2020 - **Sophos (LSE: SOPH), leader mondial en solutions de cybersécurité Next-Gen, a présenté aujourd'hui Sophos Intercept X for Mobile avec de nouvelles fonctionnalités de sécurité pour les appareils Chrome OS et une défense améliorée contre les menaces mobiles pour les équipements Android et iOS.**

Sophos a également publié aujourd'hui une étude : [Fleeceware Apps Persist on the Play Store](http://news.sophos.com/en-us/2020/01/14/fleeceware-apps-persist-on-the-play-store/) (*Les applications Fleeceware toujours présentes sur le Play Store*), qui présente de nouvelles découvertes concernant ces applications Fleeceware qui surfacturent les consommateurs crédules pour des fonctionnalités largement disponibles dans d'autres, qui sont quant à elles, gratuites ou peu coûteuses. Découvertes par les SophosLabs sur Google Play en septembre 2019, ces applications Fleeceware restent un véritable problème avec plus de vingt applications récemment repérées, comptabilisant, à priori selon Google, près de 600 millions d'installations.

« Les applications Fleeceware ainsi que des développeurs d'applications peu scrupuleux flirtent en permanence avec les limites du système pour éviter d'enfreindre les règles strictes et intraitables de l'App Store. Ce comportement sournois est contraire à l'éthique, mais pas illégal », a déclaré Dan Schiappa, chief product officer chez Sophos. « Peut-être plus inquiétants encore sont les cybercriminels discrets qui ciblent de plus en plus les appareils mobiles afin de lancer des attaques à des fins financières, ou bien pour obtenir tout simplement un ‘accès facile’ aux réseaux d'entreprises connectés. Aucun appareil mobile n'est à l'abri, et les attaquants comptent sur des appareils non protégés et des failles non corrigées pour lancer leurs attaques. Intercept X for Mobile protège les utilisateurs conte les applications risquées et les contenus malveillants, et sécurise les données professionnelles sur les appareils mobiles ».

Tirant parti de la même technologie deep learning anti-malware utilisée dans Intercept X for Windows, macOS et server, Intercept X for Mobile protège les utilisateurs, leurs appareils et leurs données contre les menaces mobiles connues et celles jamais vues auparavant. Une interface entièrement repensée simplifie la gestion de la sécurité et facilite l'accessibilité pour les utilisateurs à mobilité réduite :

* **La sécurité des appareils** : Intercept X for Mobile surveille en permanence et avertit les utilisateurs ainsi que les administrateurs IT en cas de signes de compromis potentiels afin qu'ils puissent rapidement et automatiquement remédier aux problèmes et révoquer l'accès aux ressources de l'entreprise. Les vérifications de conformité détectent le jailbreaking, le rooting, les versions du système d'exploitation, et bien plus encore, informant les utilisateurs et les administrateurs IT en cas de violations et prenant automatiquement les mesures nécessaires.
* **La sécurité du réseau** : Intercept X for Mobile surveille les connexions réseau en temps réel afin de détecter toute activité suspecte, avertissant les utilisateurs et les administrateurs IT d'éventuelles attaques de type Man-in-the-Middle (MitM). Le filtrage web et la vérification des URL empêchent également l'accès aux sites malveillants connus, protégeant ainsi les utilisateurs contre du contenu inapproprié et la détection du phishing par SMS permet de repérer, quant à elle, les URL malveillantes.
* **La sécurité des applications** : Intercept X for Mobile détecte les applications malveillantes et suspectes installées sur les appareils, protégeant ainsi contre les malwares, les ransomwares et les applications potentiellement indésirables telles que les Fleeceware. L'intégration avec des solutions UEM (Unified Endpoint Management) comme Sophos Mobile et Microsoft Intune permet aux administrateurs de créer des politiques d'accès conditionnel, restreignant ainsi l'accès aux applications, aux données et aux ressources de l'entreprise lorsque des menaces sont détectées.
* **La sécurité de Chromebook** : La nouvelle extension de sécurité Chromebook protège les utilisateurs de Chrome OS contre les contenus web inappropriés et malveillants, fournissant une liste blanche et une liste de blocage des applications et permettant aux administrateurs IT de rendre compte de l'état et de la configuration de l'appareil.

Intercept X for Mobile est facilement géré au niveau de la plateforme Sophos Central basée dans le Cloud, en parallèle de l'ensemble de la gamme de solutions de cybersécurité Next-Gen de Sophos. L'approche Synchronized Security (Sécurité Synchronisée) unique de Sophos permet à ces solutions de fonctionner ensemble et en temps réel pour le partage d'informations et la réponse aux menaces.

Sophos Intercept X for Mobile est désormais disponible sous forme de licence autonome ou bien intégré au nouveau Sophos Mobile 9.5 UEM avec des fonctionnalités supplémentaires en matière de gestion des systèmes endpoint, fournissant ainsi une plateforme UEM complète et sécurisée avec une solution intégrée de Défense contre les Menaces Mobiles (Mobile Threat Defense). Pour une utilisation individuelle et non gérée, Intercept X for Mobile est disponible gratuitement sur l'App Store d'Apple et sur Google Play.

**À propos de Sophos**En tant que leader mondial en solutions de cybersécurité Next-Gen, Sophos protège plus de 400 000 entreprises, de toutes tailles et dans plus de 150 pays, contre les cybermenaces actuelles les plus avancées. Développées par les SophosLabs, une équipe présente dans le monde entier et spécialisée dans le renseignement sur les menaces et la science des données, les solutions Cloud-Native et basées sur l'IA de Sophos protègent les systèmes endpoint (les ordinateurs portables, les serveurs et les périphériques mobiles) ainsi que les réseaux contre les techniques de cyberattaque évolutives, notamment les ransomwares, les malwares, les exploits, l'exfiltration de données, les violations par adversaire-actif, le phishing, et bien plus encore. Sophos Central, une plateforme de management Cloud-Native, intègre l'ensemble des produits Next-Gen de Sophos, y compris la solution Intercept X endpoint et le pare-feu XG Next-Gen, via un système unique de «sécurité synchronisée» accessible via un ensemble d'API. Sophos a favorisé la transition vers une cybersécurité moderne en exploitant des fonctionnalités avancées au niveau du Cloud, de l'apprentissage automatique, des API, de l'automatisation, du service MTR (Managed Threat Response), entre autres, afin d’offrir une protection de niveau professionnel à toutes les entreprises. Sophos commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 47 000 partenaires et fournisseurs de services gérés (MSP : Managed Service Provider). Sophos met également ses technologies commerciales innovantes à la disposition des particuliers via Sophos Home. Le siège de l’entreprise est basé à Oxford, au Royaume-Uni, et Sophos est cotée à la Bourse de Londres sous le symbole «SOPH». Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contact presse :**Square Egg Communications, Sandra Van Hauwaert, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.