**Communiqué de presse**

**« Android est constamment la cible de cybercriminels »**

Bruxelles, 10 avril 2017 – **Une étude récente réalisée par SophosLabs a démontré que des malwares PUA (pour *Potentially Unwanted Applications* ou applications potentiellement indésirables) pour Windows, Mac et Android visaient spécifiquement les appareils Android.**

Les résultats de l'étude indiquent également que les cybercriminels utilisent les PUA (programmes contenant par exemple des adwares et qui installent des barres d'outils indésirables) pour contourner les systèmes de sécurité et accéder ainsi aux appareils Android et Mac. Windows est toujours le système d'exploitation dans la ligne de mire des criminels, mais l'acharnement à l'égard d'Android est manifeste.

« *Plus le système est ouvert, plus il est sensible aux malwares »*, explique Lars Putteneers, Security Advisor chez Sophos. *« Les auteurs de malwares considèrent les PUA comme le moyen par excellence pour contourner les systèmes de sécurité et atteindre le même objectif qu'avec les autres malwares : extorquer de l'argent. »*

**Les chiffres ne mentent jamais**

Les chiffres analysés par SophosLabs en 2016 indiquent ce qui suit :

* *Parmi toutes les attaques visant Windows, 6 % étaient des PUA tandis que 95 % étaient des « straight up malwares » ;*
* *Parmi toutes les attaques visant Android, 74 % étaient de purs malwares et 25 % des PUA ;*
* *Enfin pour Mac : les malwares représentaient 6 % des attaques contre 94 % pour les PUA.*

**Les malwares Android sous la loupe**

Dans le *malware forecast* de Sophos publié au début de l'année, les chercheurs ont découvert des malwares spécialement conçus pour les appareils Android. Plus de 8 500 000 applications Android suspectes ont ainsi été analysées en 2016. Plus de la moitié étaient soit des malwares, soit des PUA (dont aussi des adwares). Parmi les dix familles de malwares les plus importantes visant Android, Andr/PornClk est la plus grande (20 %).

**Comment se protéger ?**

Même si la protection d'Android reste une question délicate, plusieurs mesures s'offrent à vous pour vous protéger correctement :

* Utilisez Google Play
* Envisagez l'installation d'une solution antivirus
* Évitez les applications ayant une mauvaise réputation
* Effectuez les mises à jour avant qu'il ne soit trop tard et exécutez-les le plus souvent possible

Pour Mac, il est conseillé d'utiliser une solution antivirus en temps réel ou la solution de sécurité d'Apple.

Les mêmes conseils s'appliquent pour les malwares et PUA visant Windows. La mise à jour est essentielle, mais soyez également prudents avec les annexes (et leur ouverture) et les liens qui sont transférés via Outlook.

**Restez connectés avec Sophos**

[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/%2Bsophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Sophos Blog](http://blogs.sophos.com/)

[Naked Security News](http://nakedsecurity.sophos.com/)

**A propos de Sophos**Plus de 100 millions d’utilisateurs dans 150 pays font confiance à [Sophos](http://www.sophos.fr/) en tant que meilleure protection contre les menaces complexes et les pertes de données. Sophos propose des solutions de protection simples à administrer, déployer et utiliser pour le [Web](http://www.sophos.com/fr-fr/products/web.aspx), les [courriers électroniques](http://www.sophos.com/fr-fr/products/email.aspx), les [mobiles](http://www.sophos.com/fr-fr/products/mobile.aspx), les [données avec le chiffrement](http://www.sophos.com/fr-fr/products/encryption.aspx), les [systèmes](http://www.sophos.com/fr-fr/products/endpoint.aspx) et les [réseaux](http://www.sophos.com/fr-fr/products/network.aspx), qui s’appuient sur les SophosLabs, réseau mondial de centres d’analyse des menaces.

Le siège de Sophos est situé Oxford, au Royaume-Uni, et la société est cotée à la bourse de Londres (London Stock Exchange) sous le symbole “SOPH”. Des informations supplémentaires sont disponibles sur le site [www.sophos.com](http://www.sophos.com).

**Contacts Presse :**Square Egg, Sandra Van Hauwaert, GSM 0032 497251816, Sandra@square-egg.be