Communiqué de presse

**Email Security encore plus efficace grâce à l’intégration**

**du Deep Learning dans Sophos Email Advanced**

* *Sophos Email renforce la sécurité grâce à l'intelligence artificielle.*
* *Protection des emails sur Microsoft Office365, Google G-Suite, Exchange 2003+.*
* *Nouvelle authentification anti-phishing avec SPF, DKIM et DMARC.*
* *Protection gérée depuis le cloud via Sophos Central.*

Bruxelles - 13 juin 2018 - [**Sophos**](http://www.sophos.fr/) **(LSE: SOPH), leader mondial de la sécurité des réseaux et des systèmes Endpoint, annonce la disponibilité de Sophos Email Advanced, la première solution de protection des emails à offrir une sécurité prédictive intégrant la protection des menaces actives (Active Threat Protection), une authentification anti-phishing des emails et une gestion des flux sortants conformément aux politiques de sécurité.**

Les experts des SophosLabs observent que 75 % des malwares auxquels une entreprise est exposée sont spécifiques à celle-ci, indiquant ainsi que la majorité des cyberattaques sont de type « Zero-Day ». La seule manière de lutter efficacement contre ces malwares est d’utiliser le Deep Learning basé sur des réseaux neuronaux, technologie intégrée dans la technologie de sandboxing de Sophos Email, afin d’identifier rapidement les fichiers malveillants envoyés par email et jamais vus auparavant.

Les emails continuent d'être un vecteur d'attaque privilégié, utilisé par les cybercriminels pour lancer des campagnes de type « Spear-Phishing » localisée, ou de type « Spray & Pray ». Sophos traite les données de plus de dix millions de boîtes de messagerie protégées quotidiennement par Sophos Email. Environ 80 % des emails recensés comme spam portent une charge virale malveillante. Comme nous l'avons vu au cours des dernières années, les emails sont également largement utilisés pour diffuser les ransomwares.

Une [étude récente](https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx) menée par Sophos a montré que plus de 50 % des entreprises dans le monde ont subi une cyberattaque par ransomwares au cours des 12 derniers mois. Sophos Email Advanced intègre la technologie CryptoGuard dans sa technologie de sandboxing, afin de stopper les ransomwares avant qu'ils n'arrivent dans les boîtes de réception de vos employés. Une autre protection importante contre les attaques par ransomware et phishing est la protection Time-of-Click, qui analyse l'URL au moment du clic, évitant ainsi les attaques furtives et retardées. La gestion des flux sortants conformément aux politiques de sécurité multiples permet d’empêcher qu’une entreprise déjà infectée ne transmette involontairement des malwares ou n'envoie du spam à des clients ou partenaires. Cette fonctionnalité réduit ainsi l'impact d'une potentielle attaque sur la communauté et protège également la réputation de l’entreprise.

*« Avec l’augmentation des plateformes basées sur le cloud, telles que Office365 et Google G-Suite, les entreprises ont besoin d'une solution de sécurité avancée qui détecte les menaces Zero-Day et les malwares sophistiqués. Les Ransomware-As-A-Service (RaaS) et les kits de malwares prêts à l’emploi ont permis aux cybercriminels de personnaliser et de lancer des cyberattaques par email plus complexes et ciblées »*, déclare Bill Lucchini, Senior Vice President and General Manager, Messaging Security Group de Sophos.*« Le monde de l’informatique a besoin d'une sécurité plus intelligente et prédictive pour détecter et stopper les menaces actuelles. La gestion de Sophos Email Advanced via Sophos Central, basée dans le cloud, permet d’assurer le plus haut niveau de protection pour sécuriser n'importe quelle plateforme de messagerie, permettant ainsi à chaque utilisateur de faire à nouveau confiance à sa boîte de réception. »*

Sophos Email, géré via la plateforme d’administration Sophos Central, constitue le pilier essentiel d'un système de protection des données intégré. A partir de cette même console, les professionnels de l'informatique peuvent par exemple aussi gérer la protection de leurs systèmes Endpoint avec Intercept X, et mettre en place des formations de sensibilisation pour les utilisateurs sur les bonnes pratiques à adopter lors de la consultation de leurs emails avec Sophos Phish Threat. Ainsi les entreprises disposent d’une meilleure défense pour détecter et bloquer les menaces, tour en aidant les employés à ne plus être les maillons faibles de leur stratégie de cybersécurité. Les données sur les menaces en provenance de Sophos Email Advanced peuvent également venir enrichir les informations collectées dans le cadre de la sécurité synchronisée, contribuant ainsi à l'efficacité globale de la communauté au travers des SophosLabs.

Les nouvelles fonctionnalités de Sophos Email incluent :

**Protection contre les menaces actives (Active Threat Protection)**

* Le sandbox cloud Sandstorm de Sophos et la protection avancée des URL.
* L'intelligence artificielle intégrée dans le sandbox Sophos Email capable de détecter et de bloquer les malwares inconnus.
* Time-of-Click, la protection avancée des URL qui vérifie la réputation du site ou les liens des emails, avant réception et au moment où l’utilisateur clique sur le lien, afin de bloquer des attaques furtives et retardées.

**Authentication anti-phishing des emails**

* Combinaison des techniques d’authentication SPF, DKIM et DMARC et analyse des en-têtes d’emails.
* Sender Policy Framework (SPF) pour déclarer et vérifier qui peut envoyer des emails depuis un domaine donné.
* Système d'authentication des emails via le Domain Keys Identified Mail (DKIM), basé sur des clés cryptographiques asymétriques.
* Domain Message Authentication Reporting & Conformance (DMARC) pour déterminer la marche à suivre lorsque les messages sont recalés lors des vérifications SPF ou DKIM.

**Analyse des flux sortants et support multi-règles**

* Recherche de la présence de spams et de virus au niveau des scans des emails sortants pour empêcher la propagation involontaire de menaces et protéger la réputation.
* Des règles de sécurité personnalisées peuvent être créées pour des individus, des groupes ou bien l'ensemble du domaine, et ce en quelques minutes.

**Options de déploiement et de localisation du traitement des données**

* Disponible via la plateforme de management Sophos central, basée dans le cloud.
* Sophos Secure Email Gateways peut être déployée en tant qu'appliance sur site ou au sein de la dernière version du pare-feu Sophos XG.
* Des centres de traitement de messages en Irlande, en Allemagne et aux États-Unis.
* Des sites Sophos Sandstorm en Irlande, au Japon et aux États-Unis.

**Informations presse:**

Sandra Van Hauwaert, Square Egg, sandra@square-egg.be, GSM 0497 251816

**Au sujet de Sophos**

Sophos est un leader dans la sécurité Next-Generation des systèmes Endpoint et des réseaux. En tant que pionnier en matière de sécurité synchronisée, Sophos développe son offre innovante qui comprend des solutions pour les systèmes Endpoint, les réseaux, le chiffrement, le web, les emails et les mobiles, afin de mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de produits de sécurité informatique comme la meilleure solution pour se protéger contre les menaces complexes et la perte de données. Les produits Sophos sont disponibles exclusivement via un réseau mondial de plus de 34 000 partenaires enregistrés. Le siège social de Sophos se situe à Oxford (Royaume-Uni), et Sophos a été introduit à la bourse de Londres sous le nom SOPH. Plus d’informations sont disponibles sur [www.sophos.com](http://www.sophos.com)

.