Communiqué de presse

**Sophos introduit la protection prédictive dans Intercept X**

**avec le Deep Learning avancé**

*Plus précis que l'apprentissage automatique traditionnel, le Deep Learning confère à Intercept X   
les taux de détection les plus élevés et les taux de faux-positifs les plus bas du marché de la sécurité Next-Gen Endpoint.*

**Bruxelles, le 30 janvier 2018 :** [Sophos](http://www.sophos.fr/) (LSE: SOPH), leader mondial de la sécurité des réseaux et des systèmes Endpoint, annonce aujourd'hui la disponibilité d’une nouvelle version de la solution [Intercept X](https://www.sophos.com/fr-fr/products/intercept-x.aspx), qui intègre la détection des malwares grâce à des techniques de Deep Learning à base de réseaux neuronaux. Combinée à de nouvelles fonctionnalités de protection active contre les attaques, à un verrouillage avancé des applications et à une défense améliorée contre les ransomwares, cette dernière version de protection Next-Gen Endpoint offre des niveaux de détection et de prévention inédits.

« La protection prédictive est sans nul doute l'avenir de la sécurité informatique. Sophos a réalisé une avancée significative en intégrant le Deep Learning à base de réseaux neuronaux dans Intercept X, la solution de protection contre les exploits et les ransomwares leader dans son secteur », déclare Dan Schiappa, Senior Vice-President et General Manager des produits chez Sophos. « Etre capable de se protéger contre la prochaine attaque, encore inconnue, au lieu d'attendre qu’elle survienne, va changer la manière dont les services informatiques protègent leurs utilisateurs et leurs données dans chaque organisation. Intercept X peut apporter la protection Next-Gen la plus avancée à n'importe quelle entreprise, quelle que soit la stratégie déjà adoptée ».

Les nouvelles fonctionnalités d'Intercept X incluent:

**La détection de malwares par Deep Learning**

* Le modèle de Deap Learning détecte les malwares connus et inconnus, ainsi que les applications potentiellement indésirables (PUAs), avant qu’ils ne s’exécutent, sans s’appuyer sur des signatures.
* Le modèle a une taille inférieure à 20 MB et nécessite très peu de mises à jour.

**Mécanismes de défense active contre les attaques**

* Protection contre les vols d’informations d'identification - Prévention contre les vols de mots de passe d'authentification et les informations de hash à partir de la mémoire, de la base de registre et des espaces de stockage persistants - tels que ceux mis en œuvre par Mimikatz.
* Protection contre les attaques par « Code Cave » - Détecte la présence de code déployé dans une autre application, souvent utilisé pour la persistance et le contournement des antivirus.
* Protection APC - Détecte les abus d’Asynchronous Procedure Calls (APC), souvent utilisés dans le cadre de la technique d'injection de code AtomBombing, et plus récemment comme méthode de propagation du ver WannaCry et de NotPetya via EternalBlue et DoublePulsar (certains pirates utilisent ces appels d’une manière abusive pour déclencher un autre processus afin d’exécuter leur code malveillant).

**Nouvelles Techniques de prévention contre les exploits**

* Prévention de la migration malveillante entre processus : détecte une injection DLL à distance utilisée par des pirates pour se déplacer latéralement entre les processus s'exécutant au sein d’un système.
* Prévention de l’élévation de privilège : empêche un processus à faible privilège de bénéficier d’un privilège plus élevé, une tactique souvent utilisée par les pirates actifs pour obtenir des droits d’accès supérieurs au système.

**Verrouillage d'application renforcé**

* Verrouillage du comportement du navigateur - Intercept X empêche l'utilisation malveillante de PowerShell à partir des navigateurs, en agissant en tant que verrou pour les comportements de base.
* Verrouillage des applications HTA - Les applications HTML chargées par le navigateur se voient appliquer le verrouillage comme si elles étaient des navigateurs.

Le Deep Learning est l’évolution la plus avancée en matière d'apprentissage automatique. Il fournit un modèle de détection extrêmement évolutif, capable d'intégrer l'ensemble des menaces observables dans son apprentissage. Grâce à sa capacité à analyser des centaines de millions d’échantillons, le Deep Learning peut faire des prédictions plus précises, plus rapides et générant beaucoup moins de faux-positifs que le Machine Learning traditionnel.

Cette nouvelle version de Sophos Intercept X comprend également des innovations dans le domaine de la prévention contre les exploits et les ransomwares, ainsi que des mesures de protection actives contre les attaques, telles que la protection contre le vol d’informations d'identification. Avec l’amélioration des protections anti-malwares, les attaques se sont de plus en plus concentrées sur le vol des informations d'identification, afin de pénétrer systèmes et réseaux en tant qu'utilisateur autorisé. Intercept X détecte et empêche spécifiquement ce type d’attaque. Déployé via Sophos Central, la plateforme de gestion basée dans le Cloud, Intercept X peut être installé en parallèle des logiciels de sécurité des systèmes endpoint existants, quel que soit le fournisseur, améliorant ainsi immédiatement la protection des systèmes Endpoint. Combiné à Sophos XG Firewall, Intercept X permet d’ajouter des capacités de [sécurité synchronisée](https://www.sophos.com/fr-fr/lp/synchronized-security.aspx) pour optimiser la protection.

Lancé en septembre 2016, Intercept X a démontré son efficacité au sein de dizaines de milliers d’organisations à travers le monde. Les informations sur les prix et les licences sont disponibles auprès des partenaires Sophos enregistrés dans le monde. Pour plus d'informations, veuillez visiter: [www.sophos.com](http://www.sophos.com)

Connectez-vous à Sophos où que vous soyez via :

[Twitter](http://twitter.com/sophos), [LinkedIn](http://soph.so/Cfv36), [Facebook](http://soph.so/CfvaA), [Spiceworks](http://soph.so/Cgbwa%20), [YouTube](http://www.youtube.com/user/sophoslabs), [Google+](https://plus.google.com/+sophos)

**Informations presse:**

Sandra Van Hauwaert, Square Egg, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816

**Au sujet de Sophos**Sophos est un leader dans la sécurité des réseaux et des systèmes Endpoint Next-Generation. En tant que pionnier en matière de sécurité synchronisée, Sophos développe son offre innovante qui comprend des solutions pour le chiffrement, les systèmes Endpoint, le web, les emails, les mobiles et les réseaux, capables de mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de solutions de sécurité informatique comme la meilleure option 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 30 000 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)