**Communiqué de presse**

**Sophos dote son service Server Protection de la technologie anti-rançongiciel CryptoGuard**

Bruxelles, le 21 avril 2017 – **Sophos intègre CryptoGuard, la dernière génération de technologies anti-rançongiciel, à son service Server Protection. Celui-ci dispose ainsi de capacités de détection sans signature permettant de mieux combattre les rançongiciels, à l’instar de l’Intercept X de Sophos pour les points d’accès. En septembre dernier, Sophos lançait en effet le service Intercept X, muni de CryptoGuard, une solution qui met directement le holà au cryptage des données par les logiciels de rançon.**

En étoffant la protection de serveur avec CryptoGuard, Sophos comble une faille cruciale qui permet aux rançongiciels de s’introduire dans le réseau d’une entreprise à distance ou via d’autres points faibles. Quand une entreprise adopte une politique AVEC (« Apportez votre équipement personnel de communication » ou *BYOD* en anglais, pour *Bring your own device*) et autorise ses travailleurs à accéder à distance à son réseau ou est victime d’une cybermenace interne, ses serveurs deviennent extrêmement vulnérables face aux rançongiciels. De plus, les partages réseau sur les serveurs constituent des cibles de choix : ils reprennent de nombreuses informations financières et d’identification personnelle ainsi que d’autres données importantes qui méritent une protection digne de ce nom.

« Les cybercriminels voient les serveurs comme un véritable jackpot, car ceux-ci peuvent contenir des informations commerciales confidentielles, des dossiers médicaux mentionnant le numéro d’identification sociale et fiscale du patient ou encore des documents à caractère privé. Les conséquences peuvent s’avérer désastreuses pour les organisations qui perdent ce genre de données sensibles à cause des rançongiciels », explique Dan Schiappa, Senior Vice President et General Manager de Sophos’ Enduser and Network Security Groups. « La plupart des organisations réalisent des sauvegardes, mais l’exploitation de celles-ci n’est pas toujours évidente. Les entreprises, les écoles ou les hôpitaux ne veulent pas de ‘tout ce remue-ménage’ ou des activités chronophages nécessaires à la restauration des données à partir d’une sauvegarde. La technologie anti-rançongiciel tient donc un rôle de premier plan dans la protection et l’accessibilité permanente des informations envoyées sur les serveurs. Sophos a optimisé son offre Server Protection en y ajoutant CryptoGuard, une couche supplémentaire de protection à la pointe de la technologie, afin de contrer ces menaces numériques si dommageables. »

Sophos a également enrichi la sécurité synchronisée en ajoutant Security Heartbeat à son service Central Server Protection Advanced. Grâce à cette optimisation, les administrateurs IT peuvent désormais profiter du XG Firewall Sophos afin d’isoler automatiquement les serveurs et points d’accès infectés et agir plus rapidement à la source du problème. L’offre Central Server Protection Sophos reprend par ailleurs la fonctionnalité Malicious Traffic Detection, qui surveille le trafic vers les serveurs de commande et de contrôle, ainsi qu’une liste blanche des applications et un verrouillage du serveur en un clic. Cette option met les serveurs en sécurité et empêche l’exécution d’applications non autorisées.

Le service Server Protection Sophos doté de CryptoGuard comprend désormais Central Server Protection Advanced sur la plate-forme Sophos Central, basée dans le nuage, ainsi que Sophos Server Protection Enterprise, qui est géré depuis une console sur site traditionnelle.

**Suivez Sophos**

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

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

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

[Google+](https://plus.google.com/+sophos)

[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](mailto:Sandra@square-egg.be)