**Sophos lance la version « Xstream » du XG Firewall**

*Une étude menée par les SophosLabs indique que 44% des voleurs d'informations les plus répandus utilisent le chiffrement pour cacher les données dérobées*

**OXFORD, Royaume-Uni** - 18 février 2020 - Sophos (LSE: SOPH), leader mondial en solutions de cybersécurité Next-Gen, a présenté aujourd'hui une nouvelle architecture « Xstream » pour Sophos XG Firewall offrant des capacités très élevées de déchiffrement du trafic TLS (Transport Layer Security) qui éliminent les importants risques de sécurité associés au trafic réseau chiffré, qui sont souvent négligés par les équipes de sécurité en raison de leur complexité et de leur impact au niveau des performances. Sophos XG Firewall propose désormais également une analyse des menaces améliorée, basée sur l'IA et fournie par les SophosLabs, ainsi que de meilleures performances au niveau des applications.

Sophos a également publié aujourd'hui son article [SophosLabs Uncut](https://news.sophos.com/en-us/category/sophoslabs/sophoslabs-uncut/): « *Nearly a Quarter of Malware now Communicates Using TLS* » (‘Près d'un quart des malwares communiquent désormais à l'aide du protocole TLS’), qui explique comment 23% des familles de malware utilisent des communications chiffrées pour dialoguer avec leurs serveurs de contrôle à distance (C2) ou pour s’installer. Par exemple, l'article présente en détail trois chevaux de Troie (*Trojans*) courants et toujours bien présents aujourd’hui : Trickbot, IcedID et Dridex, qui utilisent le protocole TLS lors du déroulement de leurs attaques. Les cybercriminels utilisent également le protocole TLS pour cacher leurs exploits, leurs charges virales ainsi que le contenu dérobé afin d’éviter toute détection. En fait, 44% des voleurs d'informations les plus répandus utilisent le chiffrement pour dissimuler des données piratées, telles que des mots de passe de compte bancaire et d'autres identifiants sensibles, et ce sans que les entreprises ciblées ne s’en rendent compte.

« Comme le montre l’étude menée par les SophosLabs, les cybercriminels utilisent en priorité le chiffrement pour contourner les solutions de sécurité. Malheureusement, la plupart des pare-feux ne disposent pas de capacités cryptographiques TLS évolutives et ne sont pas donc en mesure d'inspecter le trafic chiffré sans que les applications ne bloquent le réseau ou ne dégradent ses performances », a déclaré Dan Schiappa, chief product officer chez Sophos. « Avec la nouvelle architecture Xstream intégrée dans le Sophos XG Firewall, Sophos offre une visibilité cruciale du trafic chiffré tout en éliminant les problèmes frustrants de latence et de compatibilité, et ce avec une prise en charge complète de la dernière norme TLS 1.3. Les tests en interne ont permis de mettre en lumière des performances multipliées par deux au niveau du nouveau moteur XG d’inspection TLS par rapport aux versions XG précédentes. Il s’agit véritablement d’une avancée majeure dans ce secteur.

La latence dissuade trop souvent les administrateurs IT d'utiliser le déchiffrement, comme le montre d’ailleurs une enquête indépendante menée par Sophos auprès de 3 100 responsables IT dans 12 pays. Le livre blanc détaillant cette enquête : «[The Achilles Heel of Next-Gen Firewalls](https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-achilles-heel-next-gen-firewalls-wp.pdf)», souligne que si 82% des personnes interrogées ont admis qu'une inspection TLS était nécessaire, seulement 3,5% des entreprises déchiffrent effectivement leur trafic afin de l'inspecter correctement.

**Les nouvelles fonctionnalités majeures du Sophos XG Firewall comprennent :**

* **Une inspection TLS 1.3 pour détecter les malwares cachés** : le nouveau moteur TLS permet de multiplier par deux les performances des opérations cryptographiques par rapport aux versions du Sophos XG Firewall précédentes.
* **Des performances d’applications critiques optimisées** : la nouvelle politique de contrôles FastPath permet d’accélérer les performances SD-WAN des applications et du trafic, y compris la voix sur IP, SaaS et bien autres, jusqu'à atteindre la vitesse maximale d’un réseau câblé traditionnel.
* **Une analyse adaptative du trafic** : le moteur Deep Packet Inspection (DPI) récemment amélioré évalue de manière dynamique les risques au niveau des flux de trafic et établit les correspondances appropriées en matière d'analyse des menaces, améliorant ainsi le débit de plus de 33% dans la plupart des environnements réseau.
* **Une analyse des menaces utilisant les renseignements des SophosLabs** : elle permet aux administrateurs réseau disposant de cette analyse des menaces indispensable, fournie par les SophosLabs et optimisée grâce à l’utilisation de l'IA, de comprendre et d’ajuster leurs défenses afin de se protéger contre un paysage de menaces en constante évolution.
* **Gestion et génération de rapports globaux dans la console SaaS, Sophos Central** : les capacités centralisées de gestion et de génération de rapports dans Sophos Central offrent aux clients une gestion des groupes de pare-feux et une génération de rapports Cloud flexibles au niveau d’un parc entier, et ce sans coût supplémentaire.
* **Une intégration avec le service Sophos Managed Threat Response (MTR)** : les clients de Sophos XG Firewall qui ont également souscrit au service Sophos MTR Advanced disposeront, grâce à cette intégration, de renseignements exploitables plus détaillés pour prévenir, détecter et répondre aux menaces*.*

**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.