**Le rapport 2019 de Sophos sur les menaces dévoile la montée en puissance des cyberattaques manuelles et ciblées, lancées par des cybercriminels qui traquent leurs victimes dans le but de gagner des millions**

Bruxelles, le 14 novembre 2018 - **Sophos publie aujourd'hui son rapport sur les menaces pour l’année 2019. Ce dernier fournit des informations sur les tendances émergentes et en évolution en matière de cybersécurité. Le rapport, réalisé par des chercheurs des SophosLabs, explore les changements survenus au sein du paysage des menaces au cours des 12 derniers mois, en faisant apparaître les tendances et leur impact attendu sur la cybersécurité pour 2019.**

*«Le paysage des menaces évolue: les cybercriminels les moins qualifiés sont contraints de se retirer, alors que ceux plus compétents durcissent leur jeu pour survivre. Nous allons donc nous retrouver avec moins d'adversaires, mais ils seront plus intelligents et plus forts. Ces nouveaux cybercriminels sont un croisement entre le cybercriminel d’autrefois, ésotérique et ciblé, et le fournisseur de malwares « prêts à l’emploi », avec l’utilisation accrue de techniques de piratage manuel, non pas à des fins d'espionnage ou de sabotage, mais pour maximiser leurs gains financiers malveillants », déclare Joe Levy, CTO de Sophos, dans le rapport sur les menaces Sophos 2019.*

Le rapport 2019 de Sophos sur les menaces Sophos met l'accent sur les principaux comportements et attaques des cybercriminels :

* **Les cybercriminels se tournent vers des attaques de ransomware ciblées et préméditées,
leur permettant ainsi de récolter des rançons pouvant atteindre des millions de dollars**.
En effet, l’année 2018 a été le théâtre d’attaques de ransomwares ciblées et manuelles qui, outre leur forte progression, ont rapporté des millions de dollars aux cybercriminels. Ces attaques sont différentes des attaques de type "*Spray and Pray*" (diffuser et prier) qui sont automatiquement distribuées via des millions d’emails. Les ransomwares ciblés causent plus de dégâts que s’ils avaient été acheminés par des bots, car les cybercriminels, a priori humains, peuvent débusquer et surveiller leurs victimes, adopter des stratégies d’attaques latérales, résoudre divers problèmes afin de surmonter d’éventuels obstacles rencontrés sur leur route, et enfin supprimer les sauvegardes, de sorte que payer la rançon soit l’ultime et unique solution pour leur victime. Ce « style interactif d’attaque », où les adversaires manœuvrent manuellement, pas à pas, au sein d’un réseau, gagne nettement en popularité. Les experts Sophos pensent que le succès financier de SamSam, BitPaymer et Dharma inspirera d’autres attaques du même style et estiment qu’ils en observeront davantage en 2019.
* **Les cybercriminels utilisent nos propres outils contre nous**.
Le rapport de cette année révèle un changement dans le déploiement des menaces, car de plus en plus de cybercriminels utilisent maintenant des techniques de Menaces Persistantes Avancées (APT) afin de mettre en œuvre des outils informatiques facilement disponibles comme moyen de progression au sein d’un système. Le but final étant d’atteindre leur objectif, que celui-ci soit le vol de données sensibles sur un serveur ou de lancer un ransomware :
	+ *Transformer les outils d’administration en outils de cyberattaque*

Ironiquement, ou à la manière ‘*Catch-22’*, les cybercriminels utilisent des outils d’administration Windows basiques ou intégrés, notamment les fichiers Powershell et les exécutables Windows Scripting, pour déployer des attaques de malware ciblant les utilisateurs.

* + *Les cybercriminels jouent au Domino Digital*

En créant une séquence qui enchaîne différents types de script et exécute au final une attaque, les pirates peuvent déclencher une réaction en chaîne avant même que les responsables informatiques ne détectent une menace opérationnelle sur leur réseau. Dès lors, il sera difficile d'empêcher le déploiement de la charge virale.

* + *Les cybercriminels ont adopté de nouveaux exploits Office pour duper leurs victimes*

Les exploits Office ont longtemps été un vecteur d'attaque privilégié, mais récemment, les cybercriminels ont abandonné les anciens exploits liés aux documents Office au profit de nouveaux.

* + *EternalBlue est devenu un outil incontournable pour lancer des attaques de cryptojacking*

Des mises à jour sont apparues pour corriger cette menace Windows il y a plus d'un an maintenant. Pourtant, l'exploit EternalBlue reste le grand favori des cybercriminels. Le couplage d'EternalBlue avec un logiciel de cryptominage a transformé ce hobby, plutôt malveillant, en une activité cybercriminelle à plein temps et très lucrative. La distribution latérale au niveau des réseaux professionnels a permis au cryptojacker d'infecter rapidement plusieurs machines, augmentant ainsi les paiements versés au hacker et générant des coûts additionnels élevés pour l'utilisateur.

* **Les menaces persistantes provenant de malwares ciblant les mobiles et objets connectés (IoT)**.
L’impact des malwares s’étend au-delà de l’infrastructure de l’entreprise, alors que nous constatons que la menace provenant des malwares mobiles se développe rapidement. Avec l'augmentation des applications Android illégales, 2018 a vu un développement accru de malwares poussés vers les téléphones, les tablettes et autres appareils IoT. Alors que les foyers et les entreprises utilisent de plus en plus d'objets connectés à Internet, les cybercriminels ont imaginé de nouveaux moyens de détourner ces derniers pour les utiliser comme nœuds lors d'attaques de botnet de grande ampleur. En 2018, VPNFilter a démontré le pouvoir destructeur des malwares instrumentalisés dans le but d'affecter les systèmes intégrés et les périphériques en réseau ne disposant pas d'une interface utilisateur claire et bien configurée. En parallèle, Mirai Aidra, Wifatch et Gafgyt ont mis au point toute une gamme d'attaques automatisées qui ont piraté des périphériques réseau utilisés comme nœuds au sein de botnets, afin de lancer des attaques par déni de service distribuées, de miner de la cryptomonnaie et d'infiltrer des réseaux.

Pour plus d'informations sur les tendances au niveau du paysage des menaces et l'évolution des comportements des cybercriminels, veuillez consulter l'intégralité du rapport 2019 des SophosLabs sur les menaces en vous rendant sur : [www.sophos.fr/threatreport](http://www.sophos.fr/threatreport).

**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 39 000 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).

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