Alerte Média

     **Sophos dévoile son rapport annuel et met en lumière les cyberattaques majeures pour 2020**

*Le rapport 2020 de Sophos sur les menaces montre comment les cyberattaquants utilisent de plus en plus de ransomwares, augmentent leur furtivité au sein d’applications Android malveillantes, exploitent les erreurs de configuration dans le Cloud et parviennent à contourner l'apprentissage automatique*

Oosterhout, le 6 novembre 2019 -**[Sophos](https://www.sophos.com/en-us.aspx) vient de publier son**[**rapport 2020**](https://www.sophos.com/threatreport2020)**sur les menaces. Ce dernier fournit des informations cruciales sur les cybermenaces actuelles et en constante évolution. Le rapport, réalisé par les chercheurs des [SophosLabs](https://www.sophos.com/en-us/labs.aspx), passe en revue les changements opérés ces 12 derniers mois en matière de menace, et révèle les tendances susceptibles d'avoir une incidence sur la cybersécurité en 2020.**

*« Le paysage des menaces ne cesse d'évoluer. De plus, la vitesse et l’ampleur de cette évolution semblent s’accélérer et devenir imprévisibles. Les seules certitudes que nous ayons se basent sur les tendances observables. Ainsi, dans notre rapport 2020 sur les menaces, nous avons examiné l'impact potentiel des tendances actuelles au niveau mondial au cours de la prochaine année. Nous avons également mis en avant* *la manière avec laquelle les adversaires parviennent à être de plus en plus furtifs et* *à mieux exploiter les erreurs. Nous expliquons aussi comment ils arrivent à cacher leurs activités et à éviter les technologies de détection, et bien plus encore au niveau du Cloud, via des applications mobiles et des réseaux internes. Le rapport 2020 sur les menaces n'est pas tant une cartographie qu'une série d'indicateurs permettant aux défenseurs de mieux comprendre les menaces auxquelles ils pourraient faire face dans les mois à venir et comment s’y préparer », a déclaré John Shier, Senior Security Advisor chez Sophos.*

Le rapport 2020 des SophosLabs, qui est également synthétisé dans [l’article SophosLabs Uncut](http://www.sophos.com/threatreport2020), présente six domaines pour lesquels les chercheurs ont identifié des développements particuliers au cours de l’année écoulée. Ces derniers, qui devraient avoir un impact significatif sur le paysage des cybermenaces d'ici 2020 et au-delà, sont les suivants :

**Les cybercriminels utilisant des ransomwares renforcent toujours un peu plus leur présence par le biais d’attaques actives automatisées**. Elles exploitent les outils de gestion sécurisés des entreprises en les retournant contre ces dernières, échappant aux contrôles de sécurité et désactivant les sauvegardes afin d’obtenir un impact maximal, et ce en un minimum de temps.

**Les applications indésirables adoptent des comportements proches de ceux des malwares**. Au cours de cette année, des applications Androidtelles que [Fleeceware](https://news.sophos.com/en-us/2019/09/25/fleeceware-apps-overcharge-users-for-basic-app-functionality/) (abusant les utilisateurs au niveau de l’abonnement), et des adwares de plus en plus agressifs et furtifs ont vu le jour. Le rapport sur les menaces montre bien comment ces applications, ainsi que d'autres potentiellement indésirables (PUA), telles que les plugins de navigateur, deviennent de véritables relais pour la propagation et le lancement de malwares et d’attaques sans fichier.

**La plus grande vulnérabilité au niveau du cloud computing est une mauvaise configuration de la part des opérateurs**. Les systèmes Cloud devenant de plus en plus complexes et flexibles, les erreurs provenant des opérateurs représentent un risque croissant. Combiné à un manque général de visibilité, les environnements liés au Cloud Computing deviennent ainsi des cibles privilégiées pour les cyberattaquants.

**L'apprentissage automatique, conçu pour combattre les malwares, se trouve lui-même attaqué**. L’année 2019 a clairement mis en évidence le potentiel en matière d’attaque contre les systèmes de sécurité basés sur l'apprentissage automatique. L’étude a notamment montré comment les modèles de détection basés sur l'apprentissage automatique pouvaient être contournés et comment ce dernier pouvait être utilisé pour des activités offensives visant à générer du contenu malveillant, hautement convaincant, à des fins d’ingénierie sociale. En parallèle, les défenseurs utilisent l'apprentissage automatique au niveau du langage, afin de détecter les emails et les URL malveillants. Ce petit jeu du chat et de la souris, relativement évolué, devrait se développer très nettement à l'avenir.

Parmi les autres domaines abordés dans le rapport 2020 sur les menaces, citons le risque de ne pas détecter les activités de reconnaissance lancées par des cybercriminels et cachées dans le bruit global généré par l’analyse du web, la surface d'attaque persistante du RDP (Remote Desktop Protocol) et la progression des attaques actives automatisées (AAA).

Pour obtenir plus d'informations et de détails sur les tendances au sein de ce paysage des menaces et l'évolution des comportements cybercriminels, veuillez consulter l'intégralité du rapport 2020 sur les menaces des SophosLabs en vous rendant à l'adresse suivante : [Sophos.com/ThreatReport](https://www.sophos.com/threatreport2020).

Un rapport complémentaire, décrivant les techniques d’attaques utilisées par onze familles de ransomwares, parmi les plus importantes et persistantes, sera publié prochainement. Sophos Naked Security fera également prochainement référence au rapport 2020 sur les menaces dans son actualité cybersécurité.

**À propos de Sophos**

En tant que leader mondial en solution 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, GSM 0497251816.