**52 secondes suffisent pour qu’un Serveur Cloud se fasse attaquer par des cybercriminels, selon le rapport global de Sophos «Exposed:**

**Cyberattacks on Cloud Honeypots»**

*L’étude Sophos portant sur 10 serveurs cloud honeypots, répartis dans le monde, révèle un réel besoin en visibilité et de sécurité pour protéger ce que les entreprises mettent sur des plateformes hybrides et tout-cloud*

**Les principales conclusions du rapport :**

* Il a fallu moins de 40 minutes en moyenne pour que des cybercriminels attaquent des serveurs cloud honeypots déployés sur 10 sites différents répartis dans le monde entier, le site de São Paolo au Brésil faisant l’objet de l’attaque la plus rapide, au bout de 52 secondes seulement.
* Les serveurs basés à Paris ont subi une première tentative de connexion malveillante au bout de 17 minutes et 20 secondes seulement, ce qui fait de Paris la ville d’Europe touchée le plus rapidement par ces attaques (et la 4ème ville au niveau mondial).
* Paris est la deuxième ville d’Europe la plus ciblée en terme de nombre d’attaques - les honeypots hébergés sur des serveurs à Paris ont subi 612 885 attaques en trente jours (juste derrière l’Irlande avec 616 232 attaques).
* Les serveurs cloud ont été, en moyenne, la cible de 13 tentatives d'attaque par minute et par honeypot.
* Plus de 5 millions de tentatives d'attaque ont été détectées sur tous les honeypots, et ce sur une période de 30 jours.

**Bruxelles - 9 avril 2019** - **Sophos dévoile aujourd'hui les résultats de son rapport « Exposed: Cyberattacks on Cloud Honeypots » (« *Révélations sur des cyberattaques visant des serveurs cloud honeypots* »). Celui-ci révèle que des cybercriminels ont réussi à attaquer un honeypot actif et situé à Sao Paulo, au Brésil, en 52 secondes. En moyenne, les 10 serveurs cloud de l’étude au niveau monde ont été victimes de 13 tentatives d’attaque par minute et par honeypot. Ces 10 centres de données parmi les plus populaires au niveau d'Amazon Web Services (AWS) dans le monde, ont été testés pendant 30 jours. On compte parmi eux des emplacements à Paris, à Francfort, à Londres, en Irlande, en Californie, en Ohio, à Mumbai, à São Paulo, Singapour ou encore à Sydney.**

Dans le cadre de cette étude, plus de 5 millions d'attaques ont été observées sur les honeypots, systèmes conçus pour imiter les potentielles cibles de cyber-attaquants, afin que les experts en cybersécurité puissent suivre et analyser les comportements cybercriminels. Les résultats montrent ainsi comment les cybercriminels recherchent automatiquement les [buckets open cloud](https://nakedsecurity.sophos.com/2018/09/19/here-we-mongo-again-millions-of-records-exposed-by-insecure-database/) vulnérables. Si les attaquants réussissent à entrer, les entreprises peuvent alors voir des données vulnérables exposées. Les cybercriminels utilisent également des serveurs cloud compromis comme relais pour accéder à d’autres serveurs ou réseaux.

*« Le rapport Sophos ‘*[*Exposed: Cyberattacks on Cloud Honeypots’*](http://www.sophos.com/CloudHoneypotsReport) *identifie les menaces auxquelles font face les entreprises qui migrent vers des plateformes hybrides et tout-cloud. La rapidité et l’ampleur des attaques contre les honeypots prouvent le niveau de menace persistant des cybercriminels et montrent qu’ils utilisent des botnets pour cibler les plateformes cloud d’une entreprise. Il peut s'agir parfois d'attaquants humain, mais quoi qu’il en soit, les entreprises ont besoin d'une stratégie de sécurité pour protéger ce qu'elles mettent sur le cloud »*, déclare Matthew Boddy, spécialiste cybersécurité chez Sophos. *« La question de la visibilité et de la sécurité au niveau des plateformes cloud est un défi majeur pour les entreprises. Et avec la migration croissante vers le cloud, cette tendance se confirme ».*

**Visibilité continue sur les faiblesses en matière de sécurité**

Une visibilité continue sur l'infrastructure du cloud public est vitale pour que les entreprises identifient ce qu’il faut protéger et puissent rester en conformité. Cependant, la multiplicité des équipes de développement en interne, ainsi qu’un environnement en constante évolution et une évolutivité automatique en font un problème sérieux pour la cybersécurité. Sophos s'attaque à ce problème majeur avec le lancement de [Sophos Cloud Optix](https://www.sophos.com/fr-fr/cloud-optix.aspx), qui utilise l'intelligence artificielle (AI) pour mieux mettre en évidence et réduire l'exposition des infrastructures cloud. Cette solution sans agent offre une visibilité, une conformité et une réponse intelligentes au niveau du cloud, et ce dans plusieurs environnements cloud.

Ross McKerchar, CISO bij Sophos, ajoute : *“ Au lieu de noyer les équipes de sécurité d’alertes non différentiées Sophos Cloud Optix minimise la fatigue vis-à-vis des alertes en identifiant ce qui est important et ce à quoi il faut réagir. En ajoutant la visibilité dans des cloud assets et des workloads la sécurité IT a une meilleure vue sur leurs priorités en matière de sécurité, indiquées par Sophos Cloud Optix.”*

**Les principales fonctionnalités de Sophos Cloud Optix incluent :**

* **Visibilité intelligente** : Découverte automatique des actifs d’une entreprise dans les environnements AWS, Microsoft Azure et Google Cloud Platform (GCP), via une console unique, permettant aux équipes sécurité de visualiser l’ensemble de leurs ressources dans le cloud et de réagir et remédier aux risques liés à la sécurité, le tout en quelques minutes.
* **Conformité continue du cloud** : Prise en compte de l'évolution constante des réglementations sur la conformité et des meilleures pratiques en détectant automatiquement les récentes modifications apportées aux environnements cloud.
* **Analyse et suivi basés sur l'IA** : Réduction des temps de réponse et de traitement des incidents de quelques jours ou semaines à quelques minutes seulement. La puissance de l’IA détecte les configurations de ressources à risque et les comportements réseau suspects grâce à des alertes intelligentes et à la correction automatique optionnelle des risques.

Sophos Cloud Optix exploite la technologie basée sur l'IA d'[Avid Secure](https://www.sophos.com/en-us/press-office/press-releases/2019/01/sophos-acquires-avid-secure-to-expand-protection-for-public-cloud-environments.aspx), acquise par Sophos en janvier 2019. Fondée en 2017 par une équipe de leaders réputés dans le domaine de la sécurité informatique, Avid Secure a révolutionné la sécurité des environnements cloud public en offrant des solutions de bout en bout efficaces pour la protection des principaux services cloud, tels que AWS, Azure et Google.

Les détails sur les prix et la disponibilité sont disponibles auprès des partenaires revendeurs Sophos.

Pour plus d’informations sur les résultats de l’étude menée par Sophos, veuillez lire le rapport complet [Exposed: Cyberattacks on Cloud Honeypots](http://www.sophos.com/CloudHoneypotsReport) et l’article dédié sur le blog Naked Security [Knock and Don't Run: The Tale of the Relentless Hackerbots](https://nakedsecurity.sophos.com/cloudhoneypots). Des informations supplémentaires sur Sophos Cloud Optix sont disponibles sur [Sophos.fr](https://www.sophos.com/fr-fr/cloud-optix.aspx).

**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](mailto:sandra@square-egg.be), GSM 0497 251816