****

**Les SophosLabs publient un rapport sur Cloud Snooper, une attaque ciblée sophistiquée qui permet aux logiciels malveillants de communiquer à travers les pare-feux**

**Bruxelles, BE. – Fev.26, 2020** - [Sophos](https://www.sophos.com/fr-fr.aspx) (LES : SOPH), leader mondial en solutions de cybersécurité Next-Gen, publie aujourd'hui un rapport des SophosLabs sur Cloud Snooper, une attaque sophistiquée qui utilise une combinaison unique de techniques pour permettre aux logiciels malveillants présents sur les serveurs de communiquer librement avec ses serveurs de commande et de contrôle à travers des pare-feux. Le rapport présente les tactiques, techniques et procédures (TTP) utilisées dans l'attaque. Les SophosLabs estiment que l'attaque était l'œuvre d'un État-nation motivé par l'espionnage.

Comme l'explique le rapport, les TTP utilisées ensemble comprennent : un rootkit contournant les pare-feux, une technique rare pour accéder à des serveurs déguisés en trafic normal, et une porte dérobée qui partage le code malveillant entre les systèmes d'exploitation Windows et Linux, une approche connue mais peu commune. Bien que chaque élément individuel ait déjà été observé lors d'attaques menées par des adversaires hautement qualifiés, ils n'ont jamais été vus auparavant en combinaison. Sophos s'attend à ce que ce paquet de TTP descende jusqu'aux échelons inférieurs de la hiérarchie cybercriminelle et soit utilisé comme modèle pour les nouvelles attaques de pare-feu.

"*C'est la première fois que nous voyons une formule d'attaque qui combine une technique de contournement avec une charge utile multi-plateforme ciblant à la fois les systèmes Windows et Linux. Les équipes de sécurité informatique et les administrateurs de réseau doivent faire preuve de diligence pour appliquer des correctifs à tous les services externes afin d'empêcher les attaquants de se soustraire aux politiques de sécurité du cloud et des pare-feu*", a déclaré Sergei Shevchenko, responsable de la recherche sur les menaces aux SophosLabs. "*Les équipes de sécurité informatique doivent également se protéger contre les attaques multi-plateformes. Jusqu'à présent, les ressources basées sur Windows ont été la cible typique, mais les attaquants s'intéressent de plus en plus aux systèmes Linux car les services dans le cloud sont devenus des terrains de chasse populaires. C'est une question de temps avant que d'autres cybercriminels n'adoptent ces techniques*".

**Conseils aux défenseurs :**

- Dresser un inventaire complet de tous les appareils connectés au réseau et mettre à jour tous les logiciels de sécurité utilisés sur ces appareils

- Veiller à ce que tous les services connectés à Internet soient entièrement patchés. Les services hébergés dans le Cloud offrent souvent une sécurité au travers de pare-feux, mais cela ne doit pas se substituer aux mesures de sécurité propres à une organisation

- Vérifiez et revérifiez toutes les configurations Cloud. [Le rapport Sophos 2020](https://news.sophos.com/fr-fr/2019/11/20/rapport-2020-sophos-sur-les-menaces-ia-devenue-enjeu-majeur/) sur les menaces révèle que les mauvaises configurations appliquées par les utilisateurs et le manque de visibilité sont les principales causes d'attaques dans le Cloud

- Activer l'authentification multifacteur sur tous les tableaux de bord ou panneaux de contrôle de sécurité utilisés en interne pour empêcher les attaquants de désactiver les produits de sécurité lors d'une attaque

- N'oubliez pas qu'il n'y a pas de solution miracle pour la sécurité, et qu'un modèle de sécurité de nouvelle génération à plusieurs niveaux - comprenant des composants conçus spécifiquement pour protéger les données et les réseaux dans le Cloud, comme [Sophos Cloud Optix](https://www.sophos.com/fr-fr/products/cloud-optix.aspx) avec [Sophos Intercept X for Server](https://www.sophos.com/fr-fr/products/server-security.aspx) – fait partie des bonnes pratiques.

Pour plus d'informations, veuillez vous référer à cet article de[SophosLabs Uncut](https://news.sophos.com/en-us/2020/02/25/cloud-snooper-attack-bypasses-firewall-security-measures/)**.**

**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, GSM 0497251816.