****

**Nouvelle étude de Sophos:**

**“Vol d'informations vieilles de 7 ans reste une menace puissante”**

*Les dernières fonctionnalités de l'agent Tesla*

**Oosterhout, 3 février 2021** – Une nouvelle étude de Sophos montre comment un vol d'informations vieilles de 7 ans continue de se propager par le biais de spams malveillants et reste une menace puissante. Dans un nouveau rapport, publié aujourd'hui, les chercheurs de Sophos expliquent les dernières fonctionnalités de l'agent Tesla.

L'agent Tesla vole des informations des navigateurs Web, des clients de messagerie, des clients de réseau privé virtuel et d'autres logiciels qui stockent les noms d'utilisateur et les mots de passe. Il peut capturer des frappes pendant que les utilisateurs tapent, par exemple en saisissant leur mot de passe, et enregistrer des captures d'écran, afin de voir ce qui est sur leur écran.

La version la plus récente de ce voleur d'informations peut utiliser le service de messagerie Telegram pour communiquer avec ses opérateurs, ainsi qu'un logiciel appelé Tor (qui est très populaire sur le dark web) pour masquer des activités telles que la suppression de données volées. Il essaie également de modifier le code du logiciel pour bloquer la protection de sécurité.

« Le malware de l'agent Tesla est actif depuis plus de sept ans, mais il reste l'une des menaces les plus courantes pour les utilisateurs de Windows », a déclaré Sean Gallagher, chercheur senior en sécurité chez Sophos. « La méthode de livraison la plus répandue pour l'agent Tesla ce sont les pièces jointes malveillantes de spam. Les comptes de messagerie utilisés pour diffuser l'agent Tesla sont souvent des comptes légitimes qui ont été compromis. Les entreprises et les particuliers doivent, comme toujours, traiter avec prudence les pièces jointes aux e-mails d'expéditeurs inconnus et vérifier toutes les pièces jointes avant de les ouvrir. »

**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, le phishing, et bien plus encore. Sophos Central, la 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 commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 53 000 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. Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts presse :**Sandra Van Hauwaert, Square Egg Communications, sandra@square-egg.be, GSM 0497251816