****

**NEWSFLASH**

**SophosLabs :**

**« Volume des arnaques par email utilisant «COVID-19» et «coronavirus» a explosé »**

**Londres, le 26 mars 2020** - Les SophosLabs analysent, dans un nouveau article de blog Uncut intitulé [« Facing down the myriad threats tied to CO VID-19](https://news.sophos.com/en-us/2020/03/24/covidmalware/) », comment l'utilisation des termes «COVID-19» et «coronavirus» au niveau des noms de domaine, des spams, des attaques de phishing et des malwares a littéralement explosé. Plus précisément, l'article montre que le volume des arnaques par email utilisant «COVID-19» et «coronavirus» a presque triplé au cours de la semaine dernière. Les attaquants usurpent également de plus en plus l'identité de l'OMS (Organisation Mondiale de la Santé) et des Nations Unies (ONU).

« Les cybercriminels ne perdent pas de temps pour réorienter leurs campagnes d'attaques malveillantes éprouvées vers des proies à priori plus profitables, en s’appuyant largement sur les craintes croissantes concernant ce virus. Il est facile de voir, par exemple, que les attaquants derrière une nouvelle arnaque à la Chloroquine (ci-joint) sont les mêmes que ceux qui se cachaient derrière une récente arnaque au Viagra à base de plantes », selon Chester Wisniewski, chercheur principal chez Sophos.

« Avec des volumes de spams au niveau mondial estimés à plusieurs centaines de milliards, les 2 à 3% qui utilisent la thématique du COVID-19 sont non négligeables. Tout comme les tests A/B des publicités et des pages Web, les cybercriminels tentent leur chance avec prudence lorsqu’un sujet d’actualité nouveau ou sensationnel fait soudainement son apparition. Si la nouvelle thématique s'avère être un appât potentiellement plus efficace que celui utilisé dans l’escroquerie précédente, ils commencent à basculer progressivement vers ces nouvelles opportunités qui leur sont offertes ».

« En fait, l'une des campagnes de spams que nous avons suivies cette semaine, a permis de valider les hypothèses présentées ci-dessus. En effet, les cybercriminels en question avaient utilisé de faux emails d'expédition et de livraison pour convaincre des victimes insouciantes d'ouvrir des pièces jointes et d'infecter leurs ordinateurs avec le cheval de Troie Kryptik. Actuellement, le corps principal de l'email prétend provenir de l’adresse ‘erecruit@who.int’ offrant des "conseils de santé" dans la pièce jointe, mais lorsque nous analysons attentivement le corps du texte brut, nous voyons qu'il correspond à une ancienne campagne de spams qui provenait de ce même cybercriminel et qui utilisait comme appât le fait qu’il s’agissait soi-disant de factures et de livraisons ».

« Les augmentations que nous constatons sont probablement dues à deux facteurs importants. Tout d’abord, avec le temps, de plus en plus de groupes cybercriminels rentrent dans la danse pour profiter de tout l’intérêt porté au COVID-19 afin d’extorquer de l'argent à leurs potentielles victimes. Ensuite, cette démarche prend du temps. Quel que soit le groupe cybercriminel concerné, ce dernier doit fabriquer minutieusement les spams pour convaincre et pousser le destinataire à passer à l’action. Dans la communauté des chercheurs, nous appelons cette phase l'appel à l'action (call-to-action). L'appel à l'action pourrait être d'ouvrir la pièce jointe, de visiter le site Web ou, dans le cas de l'escroquerie au Bitcoin de l'OMS (ci-joint), de donner des cryptomonnaies à des portefeuilles Bitcoin contrôlés par des cybercriminels. L'élaboration de tels messages prend du temps, en particulier pour ceux qui ne sont pas des natifs anglophones ».

« La moindre parole, à priori anodine, prononcée par un politicien ou une célébrité peut donner de la crédibilité à une arnaque ou bien présenter une nouvelle opportunité commerciale. Il y a quelques jours, le président Donald Trump a mentionné l'efficacité possible d'un médicament appelé Chloroquine contre le coronavirus, conduisant ainsi immédiatement des blogueurs sur WordPress à passer de la vente de Viagra à base de plantes à la vente de Chloroquine, lequel médicament peut être assez dangereux lorsqu'il n'est pas associé à une prescription médicale et sous le contrôle d’un docteur. Ainsi seulement deux jours après la création par l'OMS d'une association caritative appelée ‘Solidarity Response Fund’, des cybercriminels sollicitaient déjà des dons en Bitcoin se faisant passer pour l’association en question, vous garantissant même que votre don serait entièrement déductible de vos impôts aux États-Unis ou en Europe ».

**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](mailto:sandra@square-egg.be), GSM 0497251816.