**Alerte medias**

**Le suivi financier des Sextortion mène au financement de l'activité cybercriminelle, selon le rapport des SophosLabs**

*Le rapport des SophosLabs est le premier à retracer le trajet des bitcoins des sextorsion*

OXFORD, Royaume-Uni - 22 avril 2020 – **Sophos a publié aujourd'hui un article des SophosLabs**[**, Follow the Money in a Massive "Sextortion" Spam Scheme**](https://news.sophos.com/en-us/2020/04/22/following-the-sextortion-money/)**, qui montre comment les fonds extraits des victimes ont conduit à financer l'activité cybercriminelle. Les chercheurs ont retracé l'origine de millions de spams de sextorsions lancés entre septembre 2019 et février 2020, puis ont analysé ce qui est arrivé à l'argent déposé par les victimes dans les portefeuilles Bitcoin des attaquants. Le bitcoin extorqué des escroqueries a totalisé environ 500 000 $. Les SophosLabs pensent que ce rapport est le premier à retracer un transfert de bitcoins à partir de sextorsion.**

La sextorsion est une forme d'attaque de spam largement utilisée qui accuse le destinataire de visiter un site Web pornographique et menace de partager des preuves vidéo avec ses amis et sa famille à moins que le destinataire ne paie. Dans les exemples analysés, les destinataires ont été invités à payer jusqu'à 800 $ en bitcoins dans des adresses de portefeuille désignées.

Les chercheurs des SophosLabs ont travaillé avec CipherTrace pour suivre le flux d'argent provenant de ces portefeuilles. Ils ont constaté que les fonds extorqués ont été utilisés pour soutenir des activités illicites ultérieures, telles que des transactions avec des marchés Web sombres et l'achat de données de cartes de crédit volées. D'autres fonds ont été rapidement transférés via une série d'adresses de portefeuille à consolider, à passer par des «mélangeurs» pour tenter de blanchir les transactions ou à être convertis en espèces.

“Les bas-fonds cybercriminels sont des réseaux complexes et les recherches des SophosLabs montrent comment les attaquants ont utilisé l'argent collecté dans une opération pour investir dans une autre", a déclaré Tamás Kocsír, chercheur en sécurité aux SophosLabs qui a dirigé la recherche. «La sextorsion escroque les proies, ce qui en fait un moyen efficace de gagner rapidement de l'argent. Au cours des cinq mois de notre enquête, nous avons vu vague après vague des attaques, se déroulant souvent le week-end et représentant parfois jusqu'à un cinquième de tous les spams suivis dans les SophosLabs. Et tandis que la plupart des destinataires n'ont pas ouvert l'e-mail ou n'ont pas payé, suffisamment d'entre eux l'ont fait pour rapporter aux attaquants environ 50,9 bitcoins, soit près de 500 000 $.”

Les escroqueries ont exploité des botnets mondiaux sur des ordinateurs compromis pour envoyer des millions de courriers indésirables à des destinataires du monde entier. Le Vietnam, le Brésil, l'Argentine, la République de Corée, l'Inde, l'Italie, le Mexique, la Pologne, la Colombie et le Pérou sont les 10 premiers pays où ces ordinateurs compromis ont été utilisés pour envoyer les spams, dont 81% en anglais, 10% étaient en italien, 4% en allemand, 3,5% en français et 1,2% en chinois.

“Les campagnes de spam sont relativement bon marché et faciles à mettre en œuvre, mais l'hypothèse selon laquelle cela ne serait lancé que par des attaquants peu qualifiés et opportunistes pourrait être inexacte», a déclaré Kocsír. «Notre recherche a révélé que certains des courriels frauduleux comportaient des techniques d'obscurcissement innovantes conçues pour contourner les filtres anti-spam. Des exemples de cela incluent la rupture des mots avec des chaînes aléatoires invisibles, l'insertion de blocs de texte blanc ou l'ajout de mots dans l'alphabet cyrillique pour confondre le balayage de la machine. Ce ne sont pas des techniques pour débutants et elles rappellent que les attaques de spam de toute nature doivent être prises au sérieux. Une approche robuste de la cybersécurité est essentielle. Si vous craignez de devenir la cible d'une arnaque de sextorsion, désactivez ou couvrez la caméra de votre ordinateur.”

**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.