Communiqué de presse

**Une étude des SophosLabs révèle le développement rapide des cybermenaces sur mesure**

* *Des cybermenaces régionalisées, avec des langues, des styles et des méthodes de paiement locaux*
* *Des ransomwares savamment dissimulés au sein de spams à cliquer et conçus sur-mesure.*
* *Des techniques locales de blanchiment d’argent et de cyber-braquage de banques déployées globalement*
* *Des cybercriminels qui sélectionnent leurs victimes en fonction de leur position géographique.*

Bruxelles, 11 Mai 2016 **- Sophos (LES : SOPH), leader mondial de la sécurité des réseaux et des systèmes, révèle aujourd’hui une étude menée par les SophosLabs qui indique une tendance à l’augmentation, chez les cybercriminels, du ciblage et de la sélection spécifique de certains pays lors de la conception de leurs ransomwares et autres cyberattaques malveillantes. Cette étude intègre des informations émanant de plus d’un million de systèmes de par le monde qui ont été analysées par les équipes des SophosLabs.**

Selon Sophos, afin d’atteindre davantage de victimes avec leurs attaques, les cybercriminels conçoivent aujourd’hui des spams sur-mesure pour déployer leurs menaces en utilisant un langage, des styles et des méthodes de paiement locaux, pour une meilleure compatibilité culturelle. Les ransomwares sont malicieusement déguisés en authentiques notifications par email, en imitant des logos locaux, pour plus de crédibilité, plus de probabilité d’être cliquées et une meilleure rentabilité pour les cybercriminels. Afin d’avoir la meilleure efficacité possible, ces scams par email imitent par exemple l’agence postale locale, les services des impôts ou de police, les entreprises fournissant l’eau, le gaz, l’électricité, en utilisant des fausses confirmations d’envoi et de remboursement, de fausses amendes pour excès de vitesse, ou encore de fausses factures d’électricité. Les SophosLabs ont vu une augmentation notable des spams dans lesquels les textes sont mieux orthographiés et ponctués, avec une meilleure structure grammaticale.

«Vous devez faire davantage attention pour différencier les faux emails des vrais», déclare Chester Wisniewski, senior security advisor chez Sophos. «Etre au courant des tactiques et techniques utilisées dans votre région ou pays devient un aspect fondamental de la cybersécurité».

Les experts ont aussi repéré une tendance nette à l’apparition de différents types de ransomwares qui ciblent des lieux spécifiques. Les différentes versions de *CryptoWall* frappent en priorité les Etats-Unis, le Royaume-Uni, le Canada, l’Australie, l’Allemagne et la France. *TorrentLocker* attaque principalement le Royaume-Uni, l’Italie, l’Australie et l’Espagne et *TeslatCrypt*, quant à lui, sévit au Royaume-Uni, aux Etats-Unis, au Canada, à Singapour et en Thaïlande.

Les analyses montrent également le TER[[1]](#footnote-1)[1] (Threat Exposure Rates) par pays, sur les 3 premiers mois de 2016. Bien que les économies des pays occidentaux soient une cible principale, leurs TER sont plutôt faibles. Les pays classés avec un TER faible sont la France avec 5.2%, le Canada avec 4.6%, l’Australie avec 4.1%, les Etats-Unis avec 3%, et le Royaume-Uni avec 2.8%. L’Algérie avec 30.7%, la Bolivie avec 20.3%, le Pakistan avec 19.9%, la Chine avec 18.5% et l’Inde avec 16.9%, sont les pays avec les plus forts pourcentages de systèmes exposés à des attaques par malwares. Les pourcentages pour le Benelux : le Luxemburg (4,2%), la Belgique (4%) et les Pays-Bas (3,9%).

«Même le blanchiment d’argent est ciblé géographiquement afin d’être plus lucratif. L’utilisation des cartes de crédit peut s’avérer risquée pour les cybercriminels. Ils ont ainsi commencé à utiliser des méthodes de paiement anonymes sur Internet, afin d’extorquer de l’argent à leurs cybervictimes via les ransomwares», a déclaré Wisniewski. «Nous avons pu observer des cybercriminels utiliser les équivalents locaux de cartes de paiement en ligne ou en magasin, telles que la carte prépayée Green Dot MoneyPak chez Walgreens aux Etats-Unis, ou encore Ukash, à présent paysafecard, utilisée dans plusieurs magasins au Royaume-Uni. »

L’idée de sélectionner des pays en particulier est aussi ressortie de l’étude comme une tendance forte.

«Les cybercriminels programment leurs attaques afin d’éviter certains pays ou certains types de clavier avec un langage particulier», a déclaré Wisniewski. «Ce phénomène apparaît pour plusieurs raisons. Il peut s’agir de la volonté des cybercriminels que ces attaques ne se produisent pas à proximité du point d’envoi, afin d’éviter toute détection. Il peut s’agir aussi d’un sentiment de fierté nationale, ou encore d’une stratégie conspirationniste afin de créer le doute à propos d’un pays en particulier, en l’épargnant lors du lancement de l’attaque».

Les banques sont un bon exemple de l’utilisation par les cybercriminels de malwares ciblant un endroit en particulier pour augmenter leurs gains. L’étude de Sophos révèle, en effet, comment de manière historique les Trojans et malwares utilisés pour infiltrer les banques ou les institutions financières convergent vers des régions spécifiques :

* Brazilian Banker Trojans et ses variantes ciblent le Brésil.
* Dridex est présent davantage aux Etats-Unis et en Allemagne.
* Trustezeb se rencontre plus dans les pays germanophones.
* Yebot est populaire à Hong Kong et au Japon.
* Zbot est plus répandu aux Etats-Unis, au Royaume-Uni, au Canada, en Allemagne, en Italie, en Espagne et au Japon.

«Il existe une véritable industrie artisanale visant à créer des Trojans sur-mesure, prenant pour cible uniquement les banques brésiliennes”, déclare Wisniewski.

Maintenant que les cybercriminels créent des menaces qui semblent vraiment authentiques et qui sont ciblées, il est de plus en plus difficile de reconnaitre les spams malveillants. Les utilisateurs de PC domestiques sont souvent les cibles de telles attaques et doivent protéger leurs systèmes vis-à-vis de ces menaces sophistiquées. Un logiciel de sécurité gratuit, utilisant des technologies de protection professionnelles, est disponible pour les particuliers depuis la page [Sophos Home](https://www.sophos.com/en-us/lp/sophos-home.aspx) pour détecter les menaces et protéger à la fois les Mac et PC.

Cette étude et les analyses réalisées ont été menées par les SophosLabs, un réseau d’experts en cybersécurité à travers le monde qui détectent et pistent tous types de failles internet, 24h/24, 7j/7 et 365 jours par an, aux quatre coins de la planète, en incluant les virus, les malwares et les Trojans évolués, les spams, les menaces internet, les piratages et autres attaques en tous genres. Les SophosLabs reçoivent et analysent des millions d’emails, d’URLs, de fichiers et données quotidiennement, et utilisent leur large expertise au sein du groupe pour développer de nouvelles définitions, capables de détecter des classes entières de menaces, y compris les nouvelles variantes. Grâce à des bureaux installés de manière stratégique en Australie, en Hongrie, au Royaume-Uni et au Canada, les experts des SophosLabs suivent également et déterminent les tendances concernant les menaces, et gardent à jour et en temps réel, les tableaux de bord des malwares, spams et autres menaces internet. Pour plus d’informations et de graphiques, merci de visiter Sophos News Blog.

Consultez les dernières nouvelles en matière de sécurité informatique, visitez notre blog récompensé, et découvrez nous davantage sur le site [Sophos News](https://blogs.sophos.com/).

**Connectez-vous avec Sophos**

[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/+sophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Naked Security News](http://nakedsecurity.sophos.com/)

[Sophos Blog](http://blogs.sophos.com/)

**A propos de Sophos**

Plus de 100 millions d’utilisateurs dans 150 pays font confiance à [Sophos](http://www.sophos.fr/) en tant que meilleure protection contre les menaces complexes et les pertes de données. Sophos propose des solutions de protection simples à administrer, déployer et utiliser pour le [Web](http://www.sophos.com/fr-fr/products/web.aspx), les [courriers électroniques](http://www.sophos.com/fr-fr/products/email.aspx), les [mobiles](http://www.sophos.com/fr-fr/products/mobile.aspx), les [données avec le chiffrement](http://www.sophos.com/fr-fr/products/encryption.aspx), les [systèmes](http://www.sophos.com/fr-fr/products/endpoint.aspx) et les [réseaux](http://www.sophos.com/fr-fr/products/network.aspx), qui s’appuient sur les SophosLabs, réseau mondial de centres d’analyse des menaces.

Le siège de Sophos est situé Oxford, au Royaume-Uni, et la société est cotée à la bourse de Londres (London Stock Exchange) sous le symbole “SOPH”. Des informations supplémentaires sont disponibles sur le site [www.sophos.fr](http://www.sophos.fr/).

**Contacts Presse :**

Square Egg, Sandra Van Hauwaert, GSM 0032 497251816, [Sandra@square-egg.be](mailto:Sandra@square-egg.be)

1. [1] Les données TER représentent les infections et les attaques par malwares par 1000 endpoints Sophos, dans chaque pays, du 1er janvier 2016 au 8 Avril 2016. [↑](#footnote-ref-1)