Alerte Média

**Sophos suit l'évolution de WannaCry,**

**du prédateur initial au récent vaccin à haut risque**

* *Les détections de WannaCry se comptent toujours par millions : rien qu’en août 2019, 4,3 millions de tentatives d'infection ont été stoppées*
* *Des milliers de variantes éphémères continuent à faire leur apparition : 12 480 variantes uniques observées par Sophos fin 2018, 6 963 en août 2019 (dont 80% étaient nouvelles).*
* *Une analyse d’environ 2 000 échantillons WannaCry, datant de 2018, montre qu’ils ont été adaptés pour contourner le fameux « kill switch », mais qu’ils ne peuvent plus chiffrer les données.*

Oosterhout, Pays-Bas - 18 septembre 2019 - **Sophos vient de publier** [**WannaCry Aftershock**](http://sophos.com/WannaCryReport)**, un article sur le malware WannaCry, devenu tristement célèbre suite à l'attaque mondiale qui a débuté le 12 Mai 2017. La recherche effectuée par les SophosLabs montre que la menace WannaCry demeure endémique, avec des millions de tentatives d'infection arrêtées tous les mois et que, même si le malware d'origine n'a pas été mis à jour, plusieurs milliers de variantes éphémères courent toujours.**

La persistance de la menace WannaCry est en grande partie due à la capacité de ces nouvelles variantes à contourner le « kill switch ». Toutefois, lorsque les chercheurs de Sophos ont analysé et exécuté un certain nombre de ces variantes, ils ont constaté que leur capacité à chiffrer les données avait été neutralisée : la conséquence à priori d’une corruption de code.

En raison de la manière avec laquelle WannaCry infecte ses nouvelles victimes (à savoir vérifier si un ordinateur est déjà infecté et, le cas échéant, passer à une autre cible), l'infection par une version inerte de ce malware empêche efficacement le périphérique d'être infecté par la souche active. En bref, les nouvelles variantes du malware agissent comme un vaccin accidentel, offrant aux ordinateurs encore non corrigés et vulnérables une sorte d’immunité contre les attaques ultérieures du même malware.

Cependant, le simple fait que ces ordinateurs puissent être infectés en premier lieu suggère que le correctif contre l’exploit principal, utilisé dans les attaques WannaCry, n'a pas été installé : un correctif publié il y a plus de deux ans.

Le malware WannaCry d'origine n'a été détecté que 40 fois. Depuis, les chercheurs des SophosLabs ont identifié 12 480 variantes du code d'origine. Une inspection plus minutieuse de plus de 2 700 échantillons (soit 98% des détections) a révélé qu'ils avaient tous évolué pour contourner le « kill switch ». Il s’agit d’une URL spécifique qui, une fois le malware connecté, met automatiquement fin au processus d'infection. Il s’avère que tous avaient un composant ransomware corrompu et étaient incapable de chiffrer les données.

En août 2019, la télémétrie Sophos a détecté 4,3 millions d'instances WannaCry. Le nombre de variantes différentes observées était de 6 963. Parmi elles, 5 555, soit 80%, étaient des nouveaux fichiers.

Les chercheurs de Sophos ont également pu tracer la première apparition de la variante corrompue. Celle-ci, qui est la plus répandue aujourd’hui, est apparue deux jours seulement après l’attaque initiale : le 14 mai 2017, date à laquelle elle a été uploadée au niveau de VirusTotal. Elle n’a toutefois pas encore été observée sur le terrain.

*« En 2017, l'épidémie WannaCry a changé le paysage des menaces pour toujours. Notre recherche met en évidence le nombre d’ordinateurs non corrigés sur le marché. Or, si vous n’avez pas installé les mises à jour publiées il y a plus de deux ans, à côté de combien d’autres correctifs êtes-vous passé ? Dans ce cas, certaines victimes ont eu de la chance car des variantes du malware les ont immunisées contre les nouvelles versions. Mais aucune entreprise ne devrait se contenter d’une telle stratégie. En effet, la pratique en matière de cybersécurité à adopter sans aucun doute consiste à installer des correctifs à chaque publication et à mettre en place une solution de sécurité robuste couvrant tous les systèmes endpoint, les réseaux et les systèmes »*, a déclaré Peter Mackenzie, spécialiste sécurité chez Sophos et auteur principal de la recherche.

**Comment se protéger contre le malware WannaCry et les ransomwares en général**

* Vérifiez que vous avez un inventaire complet de tous les périphériques connectés à votre réseau et qu'ils sont tous à jour au niveau du logiciel de sécurité.
* Installez toujours les derniers correctifs dès leur publication, et ce sur tous les périphériques de votre réseau.
* Vérifiez si vos ordinateurs sont corrigés contre l'exploit EternalBlue utilisé dans WannaCry en suivant les instructions suivantes : [How to Verify if a Machine is Vulnerable to EternalBlue - MS17-010](https://sophos.com/kb/132107).
* Le meilleur moyen d’éviter d’avoir à payer une rançon si vous venez d’être pris pour cible par un ransomware est de conserver des sauvegardes régulières de vos données les plus importantes et les plus récentes sur un périphérique de stockage hors ligne.
* En matière de cybersécurité, il n’existe pas de solution miracle, cependant, un modèle de cybersécurité multicouches s’avère être la meilleure pratique que toutes les entreprises devraient mettre en œuvre.
* Par exemple, Sophos Intercept X utilise une approche complète de défense en profondeur au niveau de la protection des systèmes endpoint. Celle-ci combine ainsi plusieurs techniques de pointe de dernière génération pour la détection des malwares, la protection contre les exploits en intégrant une fonctionnalité EDR (Endpoint Detection and Response).

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

**À propos de Sophos**Sophos est un leader dans la sécurité Next-Generation des systèmes Endpoint et des réseaux. En tant que pionnier en matière de sécurité synchronisée, Sophos développe son offre innovante qui comprend des solutions pour les systèmes Endpoint, les réseaux, le chiffrement, le web, les emails et les mobiles, afin de mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de produits de sécurité informatique comme la meilleure solution pour se protéger contre les menaces complexes et la perte de données. Les produits Sophos sont disponibles exclusivement via un réseau mondial de plus de 39 000 partenaires enregistrés. Le siège social de Sophos se situe à Oxford (Royaume-Uni), et Sophos a été introduit à la bourse de Londres sous le nom SOPH. Plus d’informations sont disponibles sur [www.sophos.com](http://www.sophos.com).