**Sophos booste
‘Intercept X for Server’ avec la fonctionnalité EDR**

Bruxelles – 3 juin 2019 - **Sophos annonce le lancement** [**d’Intercept X for Server avec la fonctionnalité EDR**](https://www.sophos.com/en-us/products/server-security.aspx) **(Endpoint Detection and Response). Cette nouvelle fonctionnalité permettra aux responsables informatiques d’enquêter sur les cyberattaques lancées contre les serveurs, une cible très prisée en raison de la grande valeur des données qui y sont généralement stockées. Les cybercriminels font évoluer en permanence leurs méthodes et associent désormais l’automatisation avec les compétences humaines en matière de piratage, et ceci afin de mener à bien des attaques contre des serveurs. Ce nouveau type d’attaque hybride associe l’utilisation de bots, pour identifier les victimes potentielles, et des attaquants actifs pour décider qui et comment attaquer.**

Le rapport [Worms Deliver Cryptomining Malware](https://news.sophos.com/en-us/2019/05/30/worms-deliver-cryptomining-malware-to-web-servers/) to Web Servers publié par SophosLabs Uncut, souligne à quel point il est facile pour les cybercriminels d'exploiter les bots pour identifier des cibles vulnérables. Le rapport décrit une attaque automatisée capable de transmettre une large gamme de codes malveillants à des serveurs qui, en tant que catégorie, ont tendance à être en retard sur les cycles de mise à jour normaux.

**Anatomie d'une cyberattaque hybride**

Une fois les cibles potentielles identifiées par les bots, les cybercriminels utilisent leur savoir-faire pour sélectionner les victimes en fonction de la portée des données sensibles, de la propriété intellectuelle de l’entreprise, de sa capacité à payer une forte rançon ou de l'accès qui est offert à d'autres serveurs et réseaux. Les étapes finales sont cérébrales et manuelles : pénétrer dans le système, éviter la détection et se déplacer latéralement pour mener à bien la mission. L’objectif peut être de se faufiler discrètement pour dérober des renseignements sans se faire prendre, désactiver les sauvegardes et chiffrer les serveurs pour exiger de fortes rançons, ou encore utiliser les serveurs comme bases pour attaquer d’autres entreprises.

*« Les cyberattaques hybrides, qui faisaient auparavant exclusivement partie du playbook des attaquants ciblant les Etats-Nations, sont dorénavant couramment utilisées par les cybercriminels car elles sont rentables. La différence réside dans le fait que les attaquants ciblant les États-Nations ont tendance à rester dans le réseau de longues périodes alors que les cybercriminels ordinaires recherchent des moyens de gagner de l'argent rapidement »,* a déclaré Dan Schiappa, chef de produit chez Sophos. *« La plupart des malwares sont désormais automatisés. Il est donc facile pour les attaquants de trouver des entreprises dont la sécurité présente des faiblesses, d'évaluer leur potentiel de paiement et d'utiliser des techniques de piratage manuel pour maximiser le plus possible les dégâts qui seront causés ».*

Sophos explique comment les [cyberattaques hybrides fonctionnent dans cette vidéo : Intercept X for Server avec Endpoint Detection and Response (EDR).](https://vimeo.com/335485067)

**Sophos Intercept X for server avec EDR**

Grâce à Sophos Intercept X for Server avec EDR, les responsables informatiques des entreprises de toutes tailles ont désormais une visibilité globale. Cette possibilité leur permet de détecter de manière proactive les attaques furtives, de mieux comprendre l’impact d’un incident de sécurité et de signaler rapidement ce qui s’est passé ou bien ce qui n’a pas eu lieu.

*« Lorsque des attaquants s’introduisent dans un réseau, ils se dirigent directement vers le serveur. Malheureusement, la nature critique de ces derniers empêche de nombreuses entreprises d’apporter des changements, retardant souvent considérablement le déploiement des correctifs. Les cybercriminels profitent de cette opportunité. Si une entreprise est victime d'une attaque, elle doit connaître exactement le contexte des périphériques et des serveurs qui ont été touchés pour pouvoir améliorer leur sécurité et répondre aux questions relatives à la réglementation. Le fait d’avoir accès à ces informations avec exactitude, et ce dès le départ, peut aider les entreprises à résoudre les problèmes beaucoup plus rapidement et empêcher qu’ils ne se reproduisent »,* a déclaré Schiappa. *« Si les régulateurs s'appuient sur l’analyse forensique digitale comme preuve de la perte de données, les entreprises peuvent alors s'appuyer sur cette même expertise pour démontrer que leurs données n'ont pas été volées. Sophos Intercept X for Server avec EDR fournit cette visibilité nécessaire et apporte les informations requises en matière de sécurité ».*

Sophos Intercept X for serveur avec EDR élargit l’offre EDR de Sophos, lancée pour la première fois pour [Intercept X for endpoint en octobre 2018](https://www.sophos.com/en-us/press-office/press-releases/2018/10/sophos-adds-endpoint-detection-and-response-to-intercept-x-advanced.aspx). La fonctionnalité EDR utilise la technologie Deep Learning qui permet une recherche plus poussée des malwares. Le réseau neuronal Deep Learning de Sophos est formé sur des centaines de millions d'échantillons pour rechercher les attributs suspects de code malveillant afin de détecter des menaces jamais vues auparavant. Il fournit une analyse large et pointue des attaques potentielles en comparant l'ADN des fichiers suspects avec les échantillons de malwares déjà répertoriés par les [SophosLabs](https://www.sophos.com/en-us/labs.aspx).

Grâce à la fonctionnalité EDR de Sophos, les responsables informatiques ont également un accès à la demande aux données précises et structurées fournies par les [SophosLabs](https://www.sophos.com/en-us/labs.aspx), des études/analyses détaillées sur des événements suspects, et des recommandations pour mettre en place un plan d’action. Pour conserver une visibilité totale sur les menaces existantes, les SophosLabs suivent, déconstruisent et analysent chaque jour 400 000 attaques de malwares uniques et inédites.

Pour plus d’informations, veuillez consulter les articles [Worms Deliver Cryptomining Malware to Web Servers](https://news.sophos.com/en-us/2019/05/30/worms-deliver-cryptomining-malware-to-web-servers/) et [Naked Security](https://nakedsecurity.sophos.com/2019/05/30/the-cryptominer-that-kept-coming-back/). Des informations supplémentaires sur [Sophos EDR pour Intercept X for Server](https://www.sophos.com/en-us/products/server-security.aspx) sont disponibles sur [Sophos.com](https://www.sophos.com/en-us/products/server-security.aspx).

**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).

**Contacts Presse :**Sandra Van Hauwaert, Square Egg, sandra@square-egg.be, GSM 0497 251816