****

**Sophos nous explique comment les familles de ransomware les plus répandues et les plus persistantes attaquent leurs victimes.**

*Ce playbook, à l’usage des défenseurs, passe en revue les outils et techniques d'attaque utilisés par 11 grandes familles de ransomware, notamment WannaCry, SamSam, RobbinHood, Ryuk, MegaCortex et bien plus encore.*

*Les attaques actives automatisées ont été celles les plus couramment utilisées par les principales familles de ransomware décrites dans ce rapport.*

**OXFORD, Royaume-Uni - 19 novembre 2019** - Sophos a publié ‘*How Ransomware Attacks*’, un playbook à l’usage des défenseurs qui explique comment les diverses variantes de ransomware attaquent et impactent leurs victimes. Ce playbook complète le rapport 2020 sur les menaces publiées récemment et contient une analyse détaillée portant sur les 11 familles de ransomware les plus répandues et les plus persistantes, y compris Ryuk, BitPaymer et MegaCortex.

Les recherches menées par les SophosLabs mettent en évidence la manière avec laquelle les ransomwares tentent d’échapper aux contrôles de sécurité en contournant les processus légitimes et approuvés, puis exploitent les systèmes internes pour chiffrer un nombre maximal de fichiers et désactiver les processus de sauvegarde et de récupération, et ce avant qu'une équipe de cybersécurité ne puisse reprendre le contrôle.

Les outils et techniques présentés dans ce playbook incluent :

**Les principaux modes de distribution de ces grandes familles de ransomware**. Les ransomwares se propagent généralement en utilisant l’une des trois techniques suivantes : tel un cryptoworm, se répliquant rapidement sur d’autres ordinateurs pour avoir un impact maximal (par exemple, WannaCry); sous la forme d’un *Ransomware-as-a-Service* (RaaS), vendu sur le Dark Web comme un kit de distribution (par exemple, Sodinokibi); ou par le biais d'une attaque automatisée par adversaire actif, au cours de laquelle des attaquants déploient manuellement le ransomware après avoir lancé une analyse automatisée des réseaux à la recherche de systèmes avec une protection faible. Ce style d’attaque active et automatisée s’est avéré être l’approche la plus répandue parmi les principales familles répertoriées dans ce rapport.

**Les ransomwares délivrant une signature par code cryptographique** en utilisant un certificat numérique légitime, acheté ou volé, dans le but de convaincre certains logiciels de sécurité que le code est digne de confiance et n’a pas besoin d’être analysé.

**L’élévation de privilège** s’appuyant sur des exploits facilement disponibles, tels que EternalBlue, afin d’augmenter les privilèges d'accès. Une telle technique permet à l'attaquant d'installer des programmes tels que des outils d'accès à distance (RAT), d'afficher, de modifier ou de supprimer des données, de créer de nouveaux comptes avec des droits utilisateur complets et de désactiver le logiciel de sécurité.

**Les déplacements latéraux** et la traque mis en œuvre au niveau du réseau dans le but de trouver des serveurs de fichiers et de sauvegarde, tout en restant indétectable, et ce afin de pouvoir libérer toute la puissance d’une attaque de ransomware. En moins d'une heure, les attaquants peuvent créer un script pour copier et exécuter le ransomware au niveau des systèmes endpoint et des serveurs en réseau. Afin d'accélérer l'attaque, le ransomware peut hiérarchiser les données sur des lecteurs distants/partagés, en ciblant d'abord les documents de taille réduite et en exécutant plusieurs processus de chiffrement simultanément.

**Les attaques à distance**. Les serveurs de fichiers eux-mêmes ne sont pas souvent infectés par les ransomwares. Au lieu de cela, la menace est exécutée généralement sur un ou plusieurs systèmes endpoint compromis, en exploitant un compte utilisateur privilégié pour attaquer des documents à distance, parfois via le RDP (Remote Desktop Protocol) ou bien en ciblant des solutions de type RMM (*Remote Monitoring and Management*) généralement utilisées par les MSP (*Managed Service Providers*) afin de gérer l’infrastructure informatique des clients et/ou les systèmes des utilisateurs finaux.

**Le chiffrement de fichier et le renommage**. Il existe différentes méthodes de chiffrement de fichier, comme notamment l’écrasement pur et simple du document, mais la plupart sont accompagnées de la suppression de la sauvegarde ou de la copie originale pour entraver le processus de récupération.

Ce playbook explique comment ces outils et techniques, entre autres, sont mis en œuvre par 11 familles de ransomware : WannaCry, GandCrab, SamSam, Dharma, BitPaymer, Ryuk, LockerGoga, MegaCortex, RobbinHood, Matrix et Sodinokibi.

« Les créateurs de ransomwares ont très bien compris le fonctionnement des logiciels de sécurité et adaptent ainsi leurs attaques en conséquence. Ils ont développé leur stratégie afin d’éviter toute détection pendant que le malware chiffre un maximum de documents, et ce le plus rapidement possible, rendant ainsi difficile, voire impossible, la récupération des données. Dans certains cas, l’attaque se déroule la nuit lorsque l’équipe informatique est en train de dormir bien tranquillement. Ainsi, lorsque la victime découvre qu’une cyberattaque a eu lieu, il est déjà trop tard. Il est donc essentiel de mettre en place des contrôles de sécurité, une surveillance et une réponse robustes couvrant tous les systèmes endpoint, réseaux et systèmes, et d'installer des mises à jour logicielles à chaque fois qu'elles sont publiées », a déclaré Mark Loman, *director of engineering for threat mitigation technology* chez Sophos et auteur de ce rapport.

**Comment se protéger contre les ransomwares :**

* Vérifiez que vous disposez d'un inventaire complet de tous les périphériques connectés à votre réseau et que tous les logiciels de sécurité que vous utilisez sur ces derniers sont bien à jour.
* Installez toujours les dernières mises à jour de sécurité, dès que possible, sur tous les périphériques de votre réseau.
* Vérifiez que vos ordinateurs ont bien reçu les mises à jour nécéssaires les protégeant contre l'exploit EternalBlue utilisé dans WannaCry grâce aux instructions suivantes : [How to Verify if a Machine is Vulnerable to EternalBlue - MS17-010](https://sophos.com/kb/132107).
* Faites des sauvegardes régulières de vos données les plus importantes et les plus récentes sur un périphérique de stockage hors ligne, car il s'agit du meilleur moyen pour ne pas avoir à payer une rançon lorsqu’un ransomware vous attaquera.
* Les administrateurs doivent activer l'authentification multi-facteurs sur tous les systèmes de management qui la prennent en charge, afin d'empêcher que les attaquants ne désactivent les produits de sécurité lors d'une attaque.
* La cybersécurité ne propose pas de solution miracle, néanmoins un modèle de sécurité multicouches est sans aucun doute la meilleure stratégie que toutes les entreprises devraient mettre en œuvre.
* Par exemple, Sophos Intercept X utilise une approche complète de défense en profondeur pour protéger les systèmes endpoint, combinant plusieurs techniques Next-Gen de pointe permettant de détecter les malwares, de se protéger contre les exploits et de disposer d’une fonctionnalité EDR intégrée (Endpoint Detection and Response).

Le playbook ‘*How Ransomware Attacks*’ dans son intégralité, ainsi que l’article SophosLabs Uncut intitulé « *Comment les ransomwares les plus dévastateurs échappent aux solutions de cybersécurité* » sont maintenant disponibles.

**À propos de Sophos**

En tant que leader mondial en solution 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.