**Sophos publie son rapport sur les menaces 2021***Quelles sont les tendances en matière de cyberattaques susceptibles de façonner la sécurité IT en 2021 ?*

**Oosterhout, le 18 novembre 2020** – [**Sophos**](http://www.sophos.com/) **annonce la publication de son rapport sur les menaces 2021 (*[Sophos 2021 Threat Report](http://www.sophos.com/threatreport)*), qui met en lumière la manière dont les ransomwares et les comportements rapidement changeants des attaquants, quel que soit leur niveau, va façonner le paysage des menaces et de la sécurité IT en 2021. Ce rapport fournit une perspective en trois dimensions sur les menaces et les tendances en matière de sécurité, depuis leur conception jusqu’à leur impact dans le monde réel.**

Les trois tendances majeures analysées au sein du *Sophos 2021 Threat Report* sont le suivantes :

1. **Le fossé entre les opérateurs de ransomwares situés aux deux extrémités du spectre en matière de compétences et de ressources va se creuser.**

Les familles de criminels hautement compétentes et dotées de nombreuses ressources qui utilisent des ransomwares vont continuer à affiner et à modifier leurs tactiques, techniques et procédures (TTP) en matière de pêche au gros. Cela va leur permettre d’échapper plus facilement à la détection et d’atteindre le même niveau de sophistication que certains États-nations, en ciblant des entreprises de plus grande envergure et en émettant des demandes de rançons qui atteindront plusieurs millions d’euros. À l’autre extrémité du spectre, Sophos s’attend à une hausse du nombre d’attaquants de faible envergure et dotés de compétences élémentaires, cherchant à mettre la main sur des ransomwares as-a-service et équipés d’un menu contre des sommes modiques.

Une autre [tendance s’appuie sur le recours à « l’extorsion secondaire »](https://news.sophos.com/en-us/2020/08/04/the-realities-of-ransomware-extortion-goes-social-in-2020/) ; en plus du chiffrement des données, les attaquants dérobent des informations sensibles ou confidentielles et menacent de les rendre publiques si leurs exigences ne sont pas satisfaites.

« *Le modèle commercial des ransomwares est dynamique et complexe. Au cours de l’année 2020, Sophos a constaté une tendance claire chez les criminels à se différencier en fonction de leur degré de compétences et des cibles qu’ils choisissent. Toutefois, nous avons également vu des familles de ransomwares partager avec d’autres des outils de grande qualité et former des “cartels” collaboratifs dotés d’un fonctionnement propre*, » déclare Chester Wisniewski, principal chercheur chez Sophos. « *Certains, comme Maze, semblent plier bagage et se diriger vers une vie d’oisiveté ; toutefois, certains de leurs outils et techniques ont refait surface sous un nouveau nom, Egregor. Le paysage des cybermenaces a horreur du vide. Lorsqu’une menace disparaît, une autre vient rapidement prendre sa place. Sous bien des aspects, il est presque impossible de prédire la voie qu’empruntera un ransomware, mais les tendances en matière d’attaques observées dans le* [*rapport sur les menaces de Sophos*](http://www.sophos.com/threatreport) *cette année sont susceptibles de se poursuivre en 2021*. »

1. **Les menaces quotidiennes comme les malwares de base, notamment de type *loaders* et *botnets*, ou encore les opérations menées par des individus visant à gagner un accès initial à un réseau avant de le revendre (*Initial Access Brokers*), nécessiteront une attention particulière de la part des équipes de sécurité.**

Ces menaces peuvent ressembler à un brouillard diffus de logiciels malveillants peu développés, mais elles sont conçues pour garantir un point d’entrée au sein d’un système cible, afin de collecter des données essentielles ou de partager des informations vers un réseau *command-and-control* qui leur fournira par la suite des instructions supplémentaires. Si des opérateurs humains sont à l’origine de ces menaces, ils passent en revue chaque appareil infecté en fonction de sa géolocalisation et d’autres signes de valeur, puis ils vendent un accès aux cibles les plus lucratives au plus offrant, comme un opérateur de ransomwares de grande envergure. À titre d’exemple, en 2020, [Ryuk](https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/) a utilisé le *loader* Buer afin de disséminer son ransomware.

*« Les malwares de base peuvent être perçus comme une tempête de sable faite de petites particules qui viennent gripper les rouages d’un système en charge des alertes de sécurité. D’après les analyses de Sophos, il est clair que les défenseurs doivent prendre ces attaques au sérieux, en raison de leurs débouchés possibles. Une infection peut mener à tous les autres types d’infection. Beaucoup d’équipes de sécurité ont l’impression qu’un incident a été empêché une fois qu’un malware a été bloqué ou supprimé et que la machine infectée a été nettoyée,* » déclare Wisniewski. *« Il est possible qu’elles n’aient pas perçu que l’attaque visait plus d’une seule machine et que des malwares qui peuvent sembler élémentaires, comme Emotet ou le loader Buer, sont susceptibles de mener à des attaques par Ryuk, Netwalker ou d’autres malwares avancés. Parfois, les départements IT ne le remarquent pas jusqu’à ce que le ransomware soit* [*déployé*](https://news.sophos.com/en-us/2020/08/04/the-realities-of-ransomware-five-signs-youre-about-to-be-attacked/)*et cela peut arriver au milieu de la nuit ou au cours du week-end. Le fait de sous-estimer des infections considérées comme “mineures” peut coûter très cher.*»

1. **Les attaquants de tous niveaux vont de plus en plus souvent détourner des outils légitimes, des services publics bien connus et des réseaux habituels pour éviter la détection, déjouer les mesures de sécurité et empêcher l’analyse et l’attribution des attaques**.

L’utilisation abusive d’outils légitimes permet aux criminels d’éviter d’être détectés lorsqu’ils opèrent sur un réseau jusqu’à ce qu’ils soient prêts à lancer la phase principale d’une attaque, comme la dissémination d’un ransomware. Pour les attaquants sponsorisés par des États-nations, un avantage supplémentaire consiste à rendre difficile l’attribution d’une attaque. En 2020, Sophos a publié un [rapport](https://news.sophos.com/en-us/2020/02/25/how-i-learned-to-stop-worrying-and-love-grey-hat-tools/) sur le grand nombre d’outils standards qui sont à présent détournés par les cybercriminels.

« *L’utilisation détournée des outils et techniques d’utilisation quotidienne pour déguiser une attaque active est un sujet longuement abordé au sein d’une* [*étude*](https://news.sophos.com/en-us/2020/08/04/the-realities-of-ransomware-the-evasion-arms-race/) *menée par Sophos sur le paysage des menaces en 2020. Cette méthode remet en question les approches sécuritaires traditionnelles, car l’apparition d’outils connus ne déclenche pas automatiquement une alerte. C’est là que le domaine de la chasse aux menaces et de l’intervention managée, qui connaît actuellement une croissance rapide, montre pleinement son utilité,* » déclare Wisniewski. *« Les experts savent concentrer leurs recherches sur certaines anomalies et autres traces subtiles, comme un outil légitime utilisé au mauvais moment ou au mauvais endroit. Pour les chasseurs de menaces et les managers IT formés à l’utilisation de fonctionnalités de l’EDR), ces indications sont autant de signaux d’alerte qui permettent aux équipes de sécurité de détecter un intrus potentiel ou une attaque en cours*. »

**Les autres tendances analysées au sein du Sophos 2021 Threat Report incluent :**

* Les attaques sur les serveurs : les criminels ciblent des plateformes de serveurs qui utilisent à la fois Windows et Linux et s’en servent pour attaquer des entreprises de l’intérieur
* L’impact de la pandémie de COVID-19 sur la sécurité IT, comme les défis sécuritaires liés au télétravail et à l’utilisation d’une multitude de réseaux personnels dotés d’une grande variété de couches de sécurité
* Les défis en matière de sécurité auxquels les environnements cloud font face : le cloud a répondu avec succès à la demande des entreprises qui avaient besoin d’environnements informatiques plus sûrs, mais il fait face à des défis différents de ceux d’un réseau d’entreprise traditionnel
* Les services habituels, comme les protocoles de bureau à distance (RDP) et les concentrateurs VPN demeurent une cible préférentielle pour les attaques sur le périmètre d’un réseau. Les attaquants utilisent les RDP pour se déplacer latéralement au sein des réseaux infiltrés.
* Les applications logicielles traditionnellement désignées comme « potentiellement indésirables », car elles émettaient un grand nombre de publicités, mais employaient des tactiques qui sont de moins en moins faciles à distinguer de celles des logiciels ouvertement malveillants
* La réapparition surprenante d’un ancien bug, VelvetSweatshop – une fonctionnalité de mot de passe par défaut pour d’anciennes versions de Microsoft Excel – utilisé pour cacher des macros et d’autres types de contenus malveillants dans des documents et échapper ainsi à la détection avancée des menaces
* La nécessité de mettre en place des approches inspirées de l’épidémiologie pour quantifier les cybermenaces qui n’ont pas été constatées, détectées ou repérées afin de mieux combler les lacunes en matière de détection, d’évaluation des risques et de définition des priorités

Le rapport complet est disponible sur [www.sophos.com/threatreport](http://www.sophos.com/threatreport).

**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, le phishing, et bien plus encore. Sophos Central, la 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 commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 53 000 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. Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts presse :**

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