****

**Enquête mondiale de Sophos:**

**“Les entreprises ne sont plus jamais les mêmes après avoir été touchées par des ransomwares”**

* *La confiance des responsables informatiques et leur approche pour lutter contre les cyberattaques sont très différentes entre ceux qui ont été touchés par les ransomwares et ceux qui ne l'ont pas été, selon cette enquête*
* *Les nouvelles techniques de Ryuk Ransomware montrent la rapidité avec laquelle les attaquants changent de vitesse*

**Oosterhout, le 14 octobre 2020** – Sophos a annoncé aujourd'hui les résultats de son enquête mondiale, Cybersecurity: [The Human Challenge](https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx), qui révèle que les entreprises ne sont plus jamais les mêmes après avoir été touchées par un ransomware. En particulier, la confiance des responsables informatiques et leur approche dans la lutte contre les cyberattaques diffèrent considérablement selon que leur entreprise ait été ou non attaquée par des ransomwares.

Par exemple, les responsables informatiques des entreprises touchées par les ransomwares sont près de trois fois plus susceptibles de se sentir «significativement en retard» en ce qui concerne la compréhension des cybermenaces, par rapport à leurs pairs des organisations non concernées (17% contre 6%).

Plus d'un tiers (35%) des victimes de ransomwares ont déclaré que le recrutement et la rétention de professionnels de la sécurité informatique qualifiés était leur plus grand défi en matière de cybersécurité, contre seulement 19% de ceux qui n'avaient pas été touchés.

En ce qui concerne la sécurité, l'enquête a révélé que les victimes de ransomware consacrent proportionnellement moins de temps à la prévention des menaces (42,6%) et plus de temps à répondre (27%) par rapport à celles qui n'ont pas été touchées (49% et 22% respectivement) , détournant les ressources vers la gestion des incidents plutôt que pour les arrêter en premier lieu.

Le fait que les attaquants de ransomware continuent à faire évoluer leurs tactiques, techniques et procédures (TTP) contribue à faire pression sur les équipes de sécurité informatique, comme en témoigne l'article de [SophosLabs Uncut](https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/). L'article déconstruit une attaque récente impliquant le ransomware Ryuk. Les intervenants Sophos ont découvert que les attaquants de Ryuk utilisaient des versions mises à jour d'outils légitimes largement disponibles pour compromettre un réseau ciblé et déployer un ransomware. Exceptionnellement, l'attaque a progressé à grande vitesse - moins de trois heures et demie après l'ouverture d'une pièce jointe d'hameçonnage malveillant par un employé, les attaquants effectuaient déjà activement une reconnaissance du réseau. Dans les 24 heures, les attaquants ont eu accès à un contrôleur de domaine et se préparaient à lancer Ryuk.

«Notre enquête sur la récente attaque du ransomware Ryuk met en évidence ce à quoi les victimes sont confrontées. Les équipes de sécurité informatique doivent être en alerte 24 heures sur 24, 7 jours sur 7 et avoir une parfaite maîtrise des dernières informations sur les menaces sur les outils et les comportements des attaquants. Les résultats de l'enquête illustrent clairement l'impact de ces demandes quasi impossibles. Entre autres choses, il a été constaté que les personnes touchées par les ransomwares avaient gravement entamé la confiance sur leurs connaissances des cybermenaces. Cependant, leurs expériences avec les ransomwares semblent également leur avoir donné une meilleure appréciation de l'importance des professionnels qualifiés en cybersécurité, ainsi qu'un sentiment d'urgence concernant la mise en place de la chasse aux menaces dirigée par l'homme pour mieux comprendre et identifier les dernières tendances des attaquants », a déclaré Chester Wisniewski, Principal researcher chez Sophos. «Quelles qu'en soient les raisons, il est clair qu'en matière de sécurité, une entreprise n'est plus jamais la même après avoir été touchée par un ransomware.»

**À propos de l'enquête**

**L'enquête Cybersecurity:** **The Human Challenge** a été menée par Vanson Bourne, spécialiste indépendant en études de marché, en janvier et février 2020. 5000 décideurs informatiques dans 26 pays ont été interrogés, aux États-Unis, au Canada, au Brésil, en Colombie, au Mexique, en France , Allemagne, Royaume-Uni, Italie, Pays-Bas, Belgique, Espagne, Suède, Pologne, République tchèque, Turquie, Inde, Nigéria, Afrique du Sud, Australie, Chine, Japon, Singapour, Malaisie, Philippines et Emirats Arabes Unis. Tous les répondants provenaient d'entreprises comptant entre 100 et 5 000 employés.

**À propos de Sophos**En tant que leader mondial en solutions 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).

**Contact presse :**  
Square Egg Communications, Sandra Van Hauwaert, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.