TSX CYBR

COMMENTAIRE MENSUEL

Fonds indiciel cybersécurité Evolve

CYBR investit principalement dans des titres de capitaux propres de sociétés nationales ou internationales qui conçoivent du matériel et des logiciels dans le secteur de la cybersécurité.

Au 31 janvier 2020

SYMBOLE FNB : CYBR (Couvert); CYBR.B (Non couvert); CYBR.U (USD)
CODE FUNDSERV FONDS COMMUNS DE PLACEMENT : EVF150 (Catégorie F); EVF151 (Catégorie A)

APERÇU MACROÉCONOMIQUE :

En janvier, Microsoft a confirmé avoir été victime d'une importante atteinte à la protection des données entre le 5 décembre et le 31 décembre 2019 visant des données anonymisées de sa base de données du service à la clientèle. Jusqu'à 250 millions de dossiers – notamment des adresses courriel, des adresses IP et des renseignements sur des activités de soutien – ont été exposés en ligne, mais il reste à voir si des individus malveillants ont obtenu ces données. Des chercheurs en sécurité à Comparitech ont découvert la vulnérabilité la veille du Nouvel An et ont avisé Microsoft. Microsoft a attribué l'erreur aux changements apportés aux groupes de sécurité réseau des bases de données, qui ont entraîné une mauvaise configuration des règles de sécurité et rendu les serveurs vulnérables.[i]

Dixons Carphone a reçu une amende de 500 000 £ de l'Information Commissioner's Office (ICO) du Royaume-Uni pour une cyberattaque qui a touché des millions de clients. L'enquête de l'ICO a révélé que les cybercriminels avaient compromis les systèmes de paiement du commerçant au moyen de logiciels malveillants qui ont permis de dérober des renseignements sur des cartes de crédit et de débit de 14 millions de clients entre juillet 2017 et avril 2018. Le montant de 500 000 £ représente l'amende maximale qui pouvait être imposée en vertu de la loi sur la protection des données (Data Protection Act, 1998), car l'atteinte à la protection des données a eu lieu avant que le Règlement général sur la protection des données (RGPD) de l'Union européenne entre en vigueur. Seul côté positif pour Dixons Carphone : si l'atteinte à la protection avait eu lieu en vertu des règles du RGPD, la société se serait vue imposer une amende pouvant aller jusqu'à 4 % de son chiffre d'affaires annuel mondial, ce qui représente des dizaines de millions de livres.[ii]

Les conséquences causées par une atteinte massive à la sécurité des renseignements sur les cartes survenues l'année dernière ont continué en 2020. En effet, la chaîne de dépanneurs américaine Wawa a été piratée et les renseignements sur les cartes de paiement de plus de 30 millions d'Américains et de plus de 1 million d'étrangers se sont retrouvés en vente sur le Web. Wawa – qui exploite 860 dépanneurs et 600 stations-service – avait divulgué l'atteinte à la sécurité, qui a touché des clients qui ont payé par carte de crédit ou de débit dans ses magasins entre le 4 mars et le 12 décembre 2019. Étant donné que les renseignements de paiement de 30 millions de clients ont été compromis, l'atteinte à la sécurité de Wawa est maintenant l'une des plus importantes de l'histoire, comme celles qui ont visé Home Depot et Target dans les années précédentes.[iii]

Evolve ETFs
Brookfield Place, 161 Rue Bay, Bureau 2700, Toronto ON M5J 2S1
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com

La société de cybersécurité Trend Micro Inc. (détenue dans le portefeuille du FNB CYBR) a publié les résultats d'une étude qui s'est déroulée sur plusieurs mois et qui a permis de montrer à quel point les individus malveillants sont intelligents et ingénieux pour compromettre une usine de fabrication. Trend Micro a créé un faux fabricant de produits de haute technologie présentant plusieurs vulnérabilités courantes liées à la cybersécurité et a pu utiliser ce piège pour étudier les cibles et les méthodes des pirates malveillants.[iv]

L'entreprise bidon a été la cible de multiples logiciels malveillants et cyberattaques, y compris au moyen de logiciels de rançon et de minage de cryptomonnaies, en plus d'attaques plus directes. Dans certains cas, les pirates ont eu accès à des postes de travail, ce qui aurait pu leur permettre de perturber physiquement les opérations sur le plancher de l'usine. Les pirates ont également émis de nombreuses commandes d'arrêt du système, ce qui aurait pu avoir de graves répercussions dans une véritable usine intelligente.

Cette étude sert de signal d'alarme, surtout pour les propriétaires de plus petites usines et installations industrielles qui se croyaient peut-être trop petits pour attirer l'attention des pirates. L'étude a démontré que les pirates agissaient souvent seuls et ne faisaient pas partie de groupes cybercriminels soutenus par un État, heureux de cibler de plus petites sociétés. Leurs méthodes – que ce soit l'extorsion à l'aide d'un logiciel ou le minage clandestin – peuvent avoir de graves conséquences sur le bénéfice des entreprises, voire mettre en péril la continuité de ses activités.[v]

ATTRIBUTION DU RENDEMENT :

Pour janvier 2020, Crowdstrike Holdings Inc. est l'action du FNB qui a inscrit le meilleur rendement, suivie par Limelight Networks Inc. et Zscaler Inc. Le FNB présentait les plus fortes pondérations dans Fortinet Inc., suivie par Palo Alto Networks Inc. et Booz Allen Hamilton Holdings.

SOURCES :

[i] https://www.itgovernance.co.uk/blog/microsoft-suffers-data-breach-affecting-up-to-250-million-people
[ii] https://www.itgovernance.co.uk/blog/dixons-carphone-hit-with-500000-fine-for-massive-data-breach
[iii] https://www.zdnet.com/article/wawa-card-breach-may-rank-as-one-of-the-biggest-of-all-times
[iv] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot
[v] https://www.zdnet.com/article/ransomware-snooping-and-attempted-shutdowns-the-state-of-this-honeypot-shows-what-hackers-do-to-systems-left-unprotected-online

---

AVIS DE NON RESPONSABILITÉ :

Un placement dans un fonds négocié en bourse (FNB) et fonds communs de placement (fonds communs) peut donner lieu à des commissions, à des frais de gestion et à d'autres frais. Veuillez lire le prospectus avant d'investir. Les FNB et fonds communs ne sont pas garantis, leur valeur fluctue fréquemment et leur rendement passé pourrait ne pas se reproduire. Un placement dans un FNB ou un fonds communs comporte des risques. Veuillez lire le prospectus, qui comporte une description complète des risques associés au FNB et fonds communs. Les investisseurs pourraient devoir payer les commissions de courtage usuelles pour l'achat ou la vente de parts de FNB et fonds communs.

Evolve ETFs
Brookfield Place, 161 Rue Bay, Bureau 2700, Toronto ON M5J 2S1
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com