COMMENTAIRE DE OCTOBRE

Fonds indiciel cybersécurité Evolve

CYBR investit principalement dans des titres de participation de sociétés situées au pays ou à l'étranger qui sont impliquées dans le secteur de la cybersécurité grâce au développement de matériel et de logiciels.

TSX **CYBR**

SYMBOLE FNB: CYBR (COUVERTE); CYBR.B (NON COUVERTE); CYBR.U (USD)
CODE FUNDSERV FONDS COMMUNS DE PLACEMENT: EVF150 (CATÉGORIE F); EVF151 (CATÉGORIE A)

Thèse d'investissement: Les dépenses de cybersécurité sont non discrétionnaires et en augmentation. Il s'est transformé en un service de première nécessité.

Les dépenses en cybersécurité sont motivées par cyberattaques sur :

- Individus
- Entreprises
- Gouvernements

La cybersécurité n'est pas discrétionnaire en raison de :

- Le coût croissant des violations de données
- Des exigences réglementaires accrues
- La sophistication croissante des cybercriminels
- Utilisation accrue du cloud

MISE À JOUR GÉNÉRALE DE L'INDUSTRIE

Octobre est le mois de la sensibilisation à la cybersécurité. Elle doit être utilisée comme un moment de réflexion sur les pratiques de cybersécurité des individus et des entreprises afin de garantir des habitudes sûres. Deloitte a publié son enquête Future of Cyber 2021 fin octobre qui a **révélé que 98 % des dirigeants américains ont déclaré que leur entreprise avait connu au moins un incident de cybersécurité** au cours de l'année écoulée. En outre, 14 % de ces dirigeants ont admis que leur entreprise n'avait actuellement aucun plan de défense contre les cybermenaces.[1]

Rien que cette année, le nombre et l'ampleur des attaques ont été sans précédent. Un rapport de Bloomberg a révélé que **les ransomwares en 2021 pourraient dépasser l'ensemble de la dernière décennie combinée.** Une activité suspecte de 590 millions de dollars liée à des rançongiciels a eu lieu au cours du premier semestre de 2021,

dépassant ainsi le montant total de 416 millions de dollars déclaré en 2020. Selon le Financial Crimes Enforcement Network du département du Trésor américain, si cette tendance se poursuit 2021 est " devrait avoir une valeur de transaction liée au ransomware plus élevée que celle déposée au cours des 10 années précédentes ». [3]

À quoi ressemble l'avenir de la cybersécurité? Ce mois-ci, Gartner a publié des prédictions pour le secteur de la cybersécurité au cours des prochaines années. D'ici 2024, Gartner prédit que **30 % des pays du monde** adopteront une sorte de législation sur les ransomwares et que **40 % des conseils d'administration de l'entreprise** auront des équipes dédiées supervisant les efforts de cybersécurité. Leurs recherches prédisent également une consolidation importante dans le secteur de la cybersécurité et de l'informatique en nuage. Plus précisément, ils prédisent que 30 % des personnes finiront par utiliser le même fournisseur d'ici 2024. of directors will have dedicated teams overseeing cybersecurity efforts Their research also predicts there will be significant consolidation in both the cybersecurity and cloud computing industry. Specifically, they predict that 30% of people will end up using the same provider by 2024.[4]

En reconnaissance du mois de la cybersécurité, examinons comment la cybersécurité a évolué au cours des deux dernières décennies. En remontant le temps jusqu'en 2010, les États et les collectivités locales commençaient seulement à prendre conscience de l'adoption des technologies mobiles

TSX CYBR Fonds indiciel cybersécurité Evolve

MISE À JOUR GÉNÉRALE DE L'INDUSTRIE

et de ce que cette adoption numérique pouvait signifier pour les cybercriminels. Avance rapide jusqu'en 2021, et la cybersécurité est devenue une préoccupation nationale et internationale. Vous trouverez ci-dessous une chronologie de certains incidents notables au cours de la dernière décennie.[2]

Une décennie de cyberincidents

2011	Le piratage de Sony a exposé les informations personnelles de 77 millions d'utilisateurs – l'une des plus grandes attaques au monde à l'époque.
2015	L'Office of Personnel Management des États-Unis a fait l'objet d'une violation et a exposé les informations de 22,1 millions de personnes dans une attaque d'espionnage attribuée à la Chine.
2016	Les mauvais acteurs russes ont tenté d'influencer les élections américaines en divulguant des courriels du Comité national démocratique et d'Hillary Clinton, ainsi qu'en piratant les bases de données d'inscription des électeurs.
2017	Le piratage d'Equifax a exposé les informations de 147 millions de personnes. Environ 45 % de la population américaine a été touchée.
2018	Atlanta a été la cible d'une attaque par rançongiciel qui a été considérée comme l'attaque la plus coûteuse contre une ville.
2019	SolarWinds a envoyé un correctif logiciel qui incluait un logiciel malveillant provenant de pirates russes. Les criminels ont eu accès aux systèmes de divers clients de SolarWinds, dont le gouvernement américain, Microsoft et certaines des plus grandes sociétés de cybersécurité.
2021	JBS a payé 11 millions de dollars de rançon à la suite d'une cyberattaque et Colonial Pipeline a fait l'objet d'un piratage qui a détruit le plus grand pipeline de carburant.[2]

Cyberattaques récentes dans l'actualité

Fortinet: Mot de passe divulgué par un pirate informatique pour 500 000 comptes VPN Fortinet.[5]

Twitch: Twitch a été ciblé par un pirate informatique qui a prétendu avoir divulgué le code source et les informations de paiement des utilisateurs . La société a confirmé le piratage dans un communiqué.[6]

Sinclair Broadcast: REvil, l'organisation de cybercriminalité russe était liée à une récente cyberattaque contre le Sinclair Broadcast Group.[7]

MISES À JOUR SPÉCIFIQUES À L'ENTREPRISE

Verizon

Verizon a annoncé son intention de s'associer à **Fortinet** pour offrir aux entreprises une solution « in-a-box » pour sécuriser et connecter les effectifs hybrides et distants. « Des solutions telles que Software Defined Secure Branch de Verizon avec Fortinet ajoutent des couches de sécurité qui aident à protéger les employés, les entreprises et, en fin de compte, les clients contre les cyberattaques. - Directeur des revenus de Verizon

Google

Google investit 50 millions de dollars dans une startup de cybersécurité, **Cybereason**.[9] Cet investissement démontre la tentative de Google de combler les lacunes de sa stratégie de cybersécurité. Google Cloud a organisé une conférence virtuelle ce mois-ci où ils ont également annoncé d'autres initiatives de cybersécurité, notamment la formation de l'équipe Google Cybersecurity Action, de nouvelles solutions de confiance zéro pour Google Workspace et l'extension des partenariats Work Safer avec **CrowdStrike et Palo Alto Networks**.[10]

Evolve ETFs
Scotia Plaza, 40 King Street West, Suite 3404, Toronto ON M5H3Y2
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com

TSX CYBR Fonds indiciel cybersécurité Evolve

RENDEMENT (%)

RETOURS TOTAL *	1 MOIS	YTD	1 AN	2 ANS	3 ANS	4 ANS	SI**
CYBR (COUVERTE)	8,77	13,54	44,76	41,24	31,42	26,91	26,89
CYBR.B (NON COUVERT)	6,39	10,29	35,40	39,14	30,58	26,97	28,59
CYBR.U (USD)	8,88	13,45	45,67	43,12	-	-	33,78

Source : Bloomberg, au 29 octobre 2021.
** Performance depuis la création de CYBR et CYRB.B le 18 septembre 2017.
Performance depuis la création de CYBR.U le 13 mai 2019.

Sources:

1. https://venturebeat.com/2021/10/26/deloitte-14-of-us-orgs-remain-defenseless-as-cybersecurity-threats-loom/

2. https://www.govtech.com/security/through-the-years-a-broad-look-at-two-decades-in-cybersecurity

3. https://news.bloomberglaw.com/tech-and-telecom-law/treasury-department-offers-crypto-guidance-amid-ransomware-surge

4. https://www.zdnet.com/article/gartner-predicts-privacy-law-changes-consolidation-of-cybersecurity-services-and-ransomware-laws-for-next-4-years/

5. https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

6. https://www.theverge.com/2021/10/6/22712250/twitch-hack-leak-data-streamer-revenue-steam-competitor

7. https://www.bloomberg.com/news/articles/2021-10-20/sinclair-broadcast-hack-linked-to-notorious-russian-cybergang

8. https://www.verizon.com/about/news/verizon-business-fortinet-secure-sd-wan

9. https://venturebeat.com/2021/10/19/google-cloud-invests-50-million-in-cybersecurity-startup-cybereason/

10. https://venturebeat.com/2021/10/24/googles-future-in-enterprises-hinges-on-strategic-cybersecurity/

Evolve ETFs
Scotia Plaza, 40 King Street West, Suite 3404, Toronto ON M5H3Y2
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com

TSX HERO FNB indiciel jeux électroniques Evolve

Evolve ETFs
Scotia Plaza, 40 King Street West, Suite 3404, Toronto ON M5H3Y2
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com