

QUELLE EST L'AMPLEUR DU PIRATAGE EN LIGNE AU CANADA

26 % des consommateurs de contenu canadien ont piraté de la musique, des films, des émissions télévisées, des jeux vidéo, des livres numériques et/ou des logiciels. Les films et émissions télévisées ont été les plus susceptibles de téléchargement, visionnement en continu ou consultation illégale, et 74 % des consommateurs s'en sont tenus à la consultation illégale.¹

36 %

des cinéphiles canadiens ont consulté des films piratés.

34 %

des consommateurs canadiens d'émissions de télé ont consulté des émissions piratées.

Analyse personnalisée de MPA à l'aide de données de SimilarWeb :

3,9 milliards de visites de Canadiens sur des sites pirates en 2021.

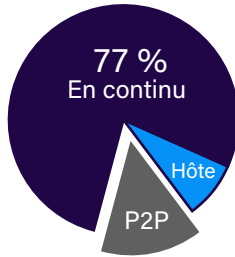


L'IIPA (Alliance internationale de la propriété intellectuelle) rapporte les sujets de préoccupation suivants :²

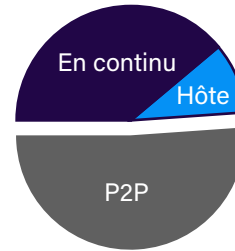
- **Services d'abonnements pirates** (télévision sur IP à péage et services de **vidéo sur demande**)
- **Sites de diffusion** en continu et autres sources de contenu (film ou télé) non autorisés
- **Dispositifs et applications de piratage** facilement disponibles en ligne et sur le marché du détail

QUELS GENRES DE SITES ET D'APPLICATIONS PIRATES LES CANADIENS UTILISENT-ILS

77 % des visites de Canadiens sur des sites de piratage en ligne s'effectuent sur des sites de diffusion en continu.



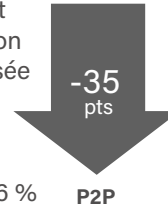
2021
Données de SimilarWeb



2015
Analyse personnalisée d'Alexa Data



Depuis 2015, la part des sites de diffusion en continu est passée de 39 % à 77 %, et celle des sites P2P (pair-à-pair) est passée de 51 % à 16 %



Sites de piratage en ligne les plus populaires au Canada en décembre 2021 :

En continu	Hôte	P2P
9anime.to	mixdrop.co	rarbg.to
fmovies.to	filesusr.com	yts.mx
soap2day.to	1fichier.com	1337x.to

Sandvine estime ainsi l'ampleur du recours aux formes de piratage émergentes :

12 % des ménages ont utilisé des services inconnus de piratage télévisuel en 2020, soit 9 % de plus qu'en 2019 et 8 % de plus qu'en 2018.³



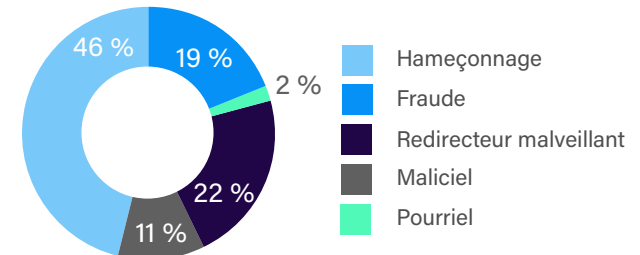
Beaucoup de consommateurs ignorent que les dispositifs illégaux de lecture en continu (ISD) peuvent menacer sérieusement la cybersécurité en devenant des vecteurs méconnus de piratage et de cyberintrusions.⁴

CE QUE LES CONSOMMATEURS RISQUENT SUR LES SITES PIRATES

Selon une enquête réalisée par RiskIQ pour MPA-Canada :⁵

1 sur 4 sites de vol de contenu visités par des Canadiens expose les consommateurs à un **contenu malveillant**.

46 % du contenu malveillant des sites de vol de contenu visités par des Canadiens est une forme de **hameçonnage** qui permet aux faux sites d'obtenir illégalement des noms d'utilisateurs et des mots de passe, souvent en redirigeant les utilisateurs vers des sites légaux par la suite.



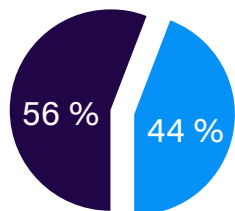
RiskIQ a aussi découvert que les Canadiens sont :

30 X plus susceptibles d'être exposés à un contenu malveillant sur un site de vol de contenu que sur un site Web ordinaire, et que



56 % des maliciels sont livrés au moyen de « téléchargeements furtifs » qui exposent les utilisateurs sans qu'ils cliquent sur quoi que ce soit ou fassent quelque chose pour confirmer le téléchargement. Si l'opération est initiée par les utilisateurs, ceux-ci sont attirés par de fausses instructions sur lesquelles ils cliquent pour autoriser le téléchargement.

maliciel par téléchargement furtif



maliciel par téléchargement initié par les utilisateurs

Selon une étude des chercheurs de Carnegie Mellon :⁶

2 X plus de temps sur les sites pirates = **20 %** plus d'infections de maliciel

En d'autres termes, plus les utilisateurs se rendent sur les sites pirates, plus leurs appareils risquent de s'infecter.

PRÉJUDICE ÉCONOMIQUE DU PIRATAGE

Selon un rapport de l'APEC :

Les consommateurs ont de plus en plus recours à des sources illégales de divertissement. L'utilisation des dispositifs illégaux de lecture en continu (ISD) nuit sérieusement à l'industrie créative et aux titulaires de droits. Ces dispositifs vont à l'encontre de l'innovation et des droits de propriété intellectuelle, profitent des investissements financiers d'autrui et affaiblissent la viabilité commerciale des services légaux de diffusion en continu.⁷

285,7 milliards \$ C'est la valeur commerciale estimative des contenus cinématographiques numériques piratés, et 280,5 millions \$ est la valeur commerciale estimative des contenus cinématographiques numériques dans le monde en 2017, selon une étude économique de NERA Economic Consulting. La perte d'activité économique légale en raison du piratage a un effet négatif sur la croissance économique.⁸

Sources :

¹Gouvernement du Canada, Étude sur la consommation en ligne de contenu protégé par le droit d'auteur : Attitudes à l'égard de la violation du droit d'auteur au Canada et prévalence de cette pratique, mai 2018.

²IIPA, 2022 Special 301 Report on Copyright Protection and Enforcement, janvier 2022.

³Sandvine, The State of Affairs: A Spotlight on Video and Television Piracy Worldwide, février 2020, accompagné d'un blogue de Veroljub Mihajlovic, Sandvine, 2/25/20.

⁴Intellectual Property Experts Group, Domestic Treatment of Illicit Streaming Devices by APEC Economies, mars 2021.

⁵RiskIQ, 2018 Study of the Presence of Malicious Content at Content Theft Sites Visited by Canadian Consumers, avril 2019.

⁶Rahul Telang, Does Online Piracy Make Computers Insecure? Evidence from Panel Data, mars 2018.

⁷Intellectual Property Experts Group, Domestic Treatment of Illicit Streaming Devices by APEC Economies, mars 2021.

⁸NERA Economic Consulting and Global Innovation Policy Center (GIPC), "Impacts of Digital Video Piracy on the U.S. Economy," juin 2019.

Publié en février 2023

Méthodologie

Visites de sites : Cette analyse personnalisée utilise les données de SimilarWeb pour des rapports concernant un groupe de sites communément utilisés dans diverses catégories de piratage en ligne. Elle mesure l'accès aux sites, mais n'indique pas le type de contenu consulté (e.g., film, télévision, jeux, logiciel, etc.). Les données de SimilarWeb utilisées dans ce rapport représentent les visites de sites Web par des utilisateurs d'ordinateurs de bureau et d'appareils mobiles entre janvier 2021 et décembre 2021. SimilarWeb est une entreprise d'information commerciale qui utilise à la fois des données recueillies au moyen d'un panel, d'un robot Web, d'un fournisseur d'accès internet ou autre pour ses analyses de données. Voir :

<https://www.similarweb.com/ourdata> et

<https://support.similarweb.com/hc/en-us/articles/360001631538-SimilarWeb-Data-Methodology> pour en savoir plus :

Aux fins de la présente analyse, les sites utilisés pour le piratage en ligne sont :

- Des sites accumulant plus de 10 000 demandes de suppression de contenu selon de rapport Transparence des informations de Google (<http://www.google.com/transparencyreport/>) au mois de décembre 2021.
 - o Y compris des sites à contenu télévisuel et/ou cinématographique.
 - o Sauf les sites réservés aux adultes, à la musique, aux jeux, au contenu soumis par les utilisateurs et aux livres électroniques.
- Sites bloqués dans divers pays ou fermés contenant des émissions et/ou des films.
- Sites de <http://www.operationcreative.uk>, <https://piracybank.org/> et autres sources internes et externes.

25 933 sites ont été recensés, selon les données de SimilarWeb. MPA les a divisés en catégories d'analyse personnalisée dont la diffusion en continu (20 933), le P2P (3 911) et les services de partage de fichiers de tiers/hébergeur (1 090). Les hébergeurs incluent les services de partage de fichiers de tiers et sites semblables.

Analyse du contenu malveillant : MPA-Canada a invité RiskIQ à analyser la prévalence et la nature du contenu malveillant des sites de violation du droit d'auteur (sites de vol de contenu) visités par les consommateurs canadiens. RiskIQ a analysé les taux d'exposition au contenu malveillant d'un échantillon de sites de vol de contenu contre un groupe témoin représentatif de la population générale des sites Web. RiskIQ définit le contenu malveillant comme un logiciel conçu dans l'intention potentiellement malveillante d'accéder sans autorisation à des données privées, de les prélever ou de causer intentionnellement (maliciel) des torts par voie d'hameçonnage, de pourriel, de fraude et de redirecteurs malveillants. Dans son évaluation de l'exposition au contenu malveillant, RiskIQ a détecté à la fois des « appariements exacts » (cas de contenu malicieux déjà présent dans une base de données connue) et des « appariements présumés » hautement probables (suite à la comparaison de diverses caractéristiques qui les apparentent au maliciel). Les principales conclusions de l'étude ne tiennent compte que les appariements exacts.

www.mpa-canada.org/research_docs/riskiq-study-2018/