

Comité consultatif sur l'application des droits

Dix-huitième session
Genève, 2 – 4 juin 2026

LE LIEN ENTRE LES LOGICIELS MALVEILLANTS ET LE PIRATAGE – OUTILS D'APPLICATION DES DROITS ET POSSIBILITÉS D'ACTION POUR LES POUVOIRS PUBLICS

*Contribution établie par Mme Elena Blobel, directrice, Contentieux mondial, Fédération internationale de l'industrie phonographique, Londres (Royaume-Uni) **

RÉSUMÉ

La présente contribution décrit comment les services de piratage en ligne utilisent régulièrement la promesse d'un accès gratuit à des contenus protégés par le droit d'auteur pour attirer les consommateurs vers des sites Web, des applications et des appareils qui les exposent à des risques importants. Elle met en évidence les types de logiciels malveillants utilisés dans le cadre du piratage en ligne ainsi que l'éventail des outils d'application des droits disponibles pour entraver leur diffusion. Cette contribution préconise d'accorder davantage d'attention, au niveau de l'élaboration des politiques, au lien entre les logiciels malveillants et le piratage, ainsi qu'aux multiples formes de criminalité qui y sont associées. Il conclut en identifiant les domaines prioritaires pour une étude plus approfondie, en vue de faciliter la prise de décision éclairée par les décideurs politiques.

* Les opinions exprimées dans le présent document sont celles de l'auteur et pas nécessairement celles du Secrétariat ou des États membres de l'OMPI.

I. POURQUOI LES CONTENUS PROTÉGÉS PAR LE DROIT D'AUTEUR SONT-ILS UTILISÉS DANS LE CADRE DE LA DIFFUSION DE LOGICIELS MALVEILLANTS?

1. La promesse d'un accès gratuit à des contenus protégés par le droit d'auteur via des services de piratage en ligne est largement utilisée par des acteurs malveillants pour inciter les consommateurs à accéder à des sites, des applications et des appareils qui les exposent à divers types de vecteurs de menaces malveillantes. Cette contribution fait le point sur les types de logiciels malveillants concernés, l'ampleur potentielle du problème, les types de mesures d'application des droits existantes, ainsi que les possibilités pour les gouvernements de s'attaquer à ce problème, notamment en sensibilisant les consommateurs.

A. TYPES DE LOGICIELS MALVEILLANTS LIÉS AU PIRATAGE EN LIGNE

2. D'après l'expérience de la Fédération internationale de l'industrie phonographique (IFPI), il existe différents types de logiciels malveillants que l'on peut trouver sur les sites et services de piratage de musique. Voici quelques exemples de logiciels malveillants associés aux services de piratage :

- Des ransomwares diffusés via des fenêtres contextuelles trompeuses, des fenêtres contextuelles en arrière-plan, des boutons "cliquer pour lire" ou de faux boutons de téléchargement sur des sites de streaming pirates et de torrent, qui chiffrent les fichiers de la victime. Par la suite, un paiement est exigé pour rétablir l'accès, généralement sous forme de cryptomonnaie.
- Le cryptojacking, qui consiste à exécuter subrepticement des scripts de minage de cryptomonnaies dans le navigateur ou sur l'appareil d'un utilisateur, ce qui épuise les ressources informatiques et nuit aux performances.
- Les logiciels espions, qui surveillent discrètement l'activité des utilisateurs, enregistrent les frappes au clavier et les identifiants, et dérobent des informations confidentielles ou personnelles telles que des courriers électroniques, des données financières et des photos.
- Les chevaux de Troie, qui sont des logiciels malveillants déguisés en logiciels légitimes, sont téléchargés via de fausses mises à jour, des lecteurs multimédias ou des programmes d'installation, et permettent la création de portes dérobées ou l'installation d'autres outils malveillants. La publicité en ligne comportant du code malveillant (malvertising) désigne les publicités agressives, trompeuses ou intrusives qui conduisent au téléchargement de logiciels malveillants, à la collecte de données utilisateur et à la redirection des utilisateurs vers des pages frauduleuses.
- Les scarewares, qui imitent les avertissements du système et incitent ainsi les victimes à télécharger des programmes malveillants. On les retrouve couramment sur les services de piratage, tant sur mobile que sur ordinateur.
- Les outils de vol d'identifiants et les fausses pages de connexion et de paiement visent principalement à récupérer les noms d'utilisateur, les mots de passe et les codes d'authentification à deux facteurs. Ces identifiants volés peuvent être réutilisés sur des comptes bancaires ou des comptes de réseaux sociaux, ce qui facilite l'usurpation d'identité, les virements non autorisés et la prise de contrôle de comptes; ils peuvent également être revendus sur le marché noir. Des identifiants piratés peuvent être utilisés pour accéder à des comptes dans le but de commettre des fraudes en matière de streaming (c'est-à-dire pour générer de fausses écoutes de titres sur les plateformes de streaming musical qui ne reflètent pas la

consommation réelle des fans), privant ainsi les artistes légitimes et les autres titulaires de droits d'une partie de leurs revenus.

- Recrutement de botnets : cette technique consiste à utiliser des clients peer-to-peer, des outils réseau pirates ou des appareils de streaming illicites préchargés avec des extensions non autorisées pour infiltrer des réseaux locaux et des appareils, qui se retrouvent ainsi, à leur insu, intégrés à des botnets chargés de coordonner des attaques par déni de service distribué, des campagnes de spam ou la diffusion d'autres logiciels malveillants. Ces botnets peuvent également servir à commettre des fraudes, notamment des fraudes liées au streaming.
- Les pirates du système de noms de domaine (DNS) modifient les paramètres DNS ou la configuration du navigateur afin de rediriger le trafic vers des pages de destination malveillantes ou affiliées, en acheminant les requêtes Web de l'utilisateur via des services contrôlés par les pirates.

B. L'AMPLEUR DU PROBLÈME

3. À ce jour, des millions d'internautes à travers le monde se rendent sur des sites de piratage en ligne pour accéder à des contenus protégés par le droit d'auteur sans autorisation. De nombreuses études ont évalué l'ampleur potentielle du problème et les risques liés aux logiciels malveillants auxquels sont exposés les internautes dans le cadre du piratage en ligne. Dans l'ensemble, ces rapports, qui portent principalement sur le secteur audiovisuel, ont mis en évidence l'existence de menaces d'une ampleur stupéfiante à l'échelle mondiale. Par exemple :

- En Asie du Sud-Est, les consommateurs sont confrontés, en moyenne, à un nombre de cybermenaces détectées sur les sites de piratage plus de 22 fois supérieur à celui des sites classiques¹.
- En Inde, les sites de piratage présentent un risque de 59% d'infection par des logiciels malveillants, un chiffre supérieur à celui des sites de divertissement pour adultes ou de jeux d'argent, les jeunes utilisateurs (18-24 ans) étant particulièrement vulnérables².
- La publicité en ligne comportant du code malveillant représentait 12% du total des publicités diffusées sur les sites de piratage, générant au moins 121 millions de dollars É.-U. de recettes par an. Près de 80% des sites pirates inspectés proposaient des publicités infectées par des logiciels malveillants. Une visite sur un site de piratage donne lieu, en moyenne, à une tentative d'injection de logiciels malveillants à l'utilisateur une fois sur six³.
- En Pologne, les consommateurs sont, en moyenne, 38,5 fois plus exposés aux cybermenaces sur les sites de partage entre particuliers que sur les sites grand public⁴.

¹ <https://www.alliance4creativity.com/wp-content/uploads/2025/07/Watters-PiracyInSEA-071025-v2.pdf>.

² https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4766797.

³ <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Unholy-Triangle-Report.pdf>.

⁴ https://www.mpa-emea.org/wp-content/uploads/2024/09/Watters-Consumer-Risk-from_Piracy-in-Poland.pdf.

- Une étude a révélé que les consommateurs européens pouvaient être victimes d'une attaque dans les 71 secondes suivant leur arrivée sur des sites de piratage, et qu'il y avait en moyenne 57% de chances que les applications de piratage audiovisuel soient préinstallées avec des logiciels malveillants intégrés⁵.

4. On a moins de données concernant les autres secteurs, mais ces principes s'appliquent globalement à tous les sites Web, applications et appareils malveillants qui proposent du contenu sans licence pour attirer les utilisateurs, ce qui se vérifie également de manière empirique dans le secteur de la musique.

5. Une étude menée par l'IFPI en Amérique latine a révélé que 33% des sites sur un échantillon de 174 sites de téléchargement de fichiers MP3 opérant dans la région étaient liés à la diffusion de logiciels malveillants. Parmi ces sites de musique illégaux, 17% diffusaient directement des logiciels malveillants, tandis que 26% diffusaient indirectement des fichiers suspects via des pages secondaires hébergées sous différents noms de domaine. La même étude a également révélé que 10% des sites de musique illégaux diffusant des logiciels malveillants proposaient des applications mobiles contrefaisantes, ce qui accroît les risques d'accès abusif et de vol de données personnelles, ainsi que d'autres types de cybercriminalité. De manière plus générale, les internautes brésiliens ont vu les cas de fraude en ligne augmenter de 408% depuis 2018, avec 2,1 millions de cas signalés en 2024⁶.

C. QUELS SONT LES OUTILS D'APPLICATION DES DROITS DISPONIBLES POUR TRAITER CE PROBLÈME?

6. Plusieurs mesures ont été prises pour lutter contre la diffusion de logiciels malveillants :

- L'opération "Endgame" d'Europol, une initiative de grande envergure visant à démanteler les botnets et les infrastructures criminelles qui y sont associées⁷.
- Le Laboratoire national de criminalistique numérique, rattaché au Centre indien de coordination contre la cybercriminalité, qui fournit aux autorités chargées de l'application des droits des services spécialisés d'analyse et de criminalistique numérique en matière de logiciels malveillants⁸.
- L'Autorité centrale indienne de la protection des consommateurs a publié des recommandations selon lesquelles les plateformes numériques devraient identifier et éliminer les "dark patterns" de leurs interfaces, y compris les logiciels malveillants⁹.

7. Des outils similaires devraient être facilement accessibles dans d'autres pays pour lutter contre les logiciels malveillants dans le cadre du piratage, à l'instar des mesures coordonnées par le Ministère de la justice et de la sécurité publique et le Laboratoire des opérations cybernétiques au Brésil :

- L'opération 404, qui a ciblé plus de 3 000 sites et applications mobiles contrefaisants au cours de sept vagues menées ces six dernières années, dont

⁵ <https://www.aapa.eu/study-on-malware-and-audiovisual-piracy-highlights-significant-risks-to-european-consumers>.

⁶ <https://forumseguranca.org.br/publicacoes/anuario-brasileiro-de-seguranca-publica/>.

⁷ <https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-endgame>.

⁸ <https://education.vikaspedia.in/viewcontent/education/digital-literacy/information-security/indian-cyber-crime-coordination-centre?lgn=en>.

⁹ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2134765>. Cette mesure s'inscrit dans le cadre des lignes directrices de 2023 de l'Autorité centrale de la protection des consommateurs relatives à la prévention et à la réglementation des "dark patterns".

certaines se livraient à la diffusion directe de logiciels malveillants et au vol de données personnelles¹⁰.

- L'opération Redirect, qui visait spécifiquement les sites de piratage liés à la diffusion de logiciels malveillants (notamment les sites de partage illégal de musique, les sites de capture de flux audio et les moteurs de recherche de torrents)¹¹. Cette opération coordonnée a permis de saisir des noms de domaine, de bloquer des sites et de fermer des sites Web illégaux grâce à la mise en œuvre combinée de mesures dissuasives¹².

8. Outre les mesures pénales, des mesures civiles peuvent également être envisagées. Par exemple, Google a récemment annoncé avoir engagé une action en justice contre les exploitants du botnet Badbox 2.0, qui, selon l'entreprise, aurait infecté plus de 10 millions d'appareils fonctionnant sous le système d'exploitation open-source Android¹³.

9. Les plateformes en ligne et les intermédiaires doivent également contribuer à mettre un terme à ces activités. Des appareils préchargés avec du contenu illicite et des logiciels malveillants sont vendus sur des plateformes de commerce électronique; des applications mobiles contenant des logiciels malveillants sont disponibles sur les boutiques d'applications officielles et celles sans licence; des sites Web frauduleux distribuant des logiciels malveillants peuvent être trouvés via les moteurs de recherche; et des intermédiaires spécialisés dans les noms de domaine et l'hébergement fournissent l'infrastructure qui permet à ces sites de fonctionner. Même si cette activité est interdite par leurs conditions générales respectives, les acteurs malveillants parviennent à poursuivre leurs activités. Il est donc nécessaire de prendre des mesures préventives, associées à des mécanismes de signalement adaptables permettant une suppression rapide et efficace. Il existe également des organisations indépendantes qui proposent des canaux de signalement¹⁴.

D. POURQUOI CETTE QUESTION EST-ELLE IMPORTANTE POUR LES GOUVERNEMENTS?

10. Il importe que la question du lien entre le piratage en ligne et les logiciels malveillants, ainsi que l'évolution des tendances dans ce domaine, soient portées à l'attention des autorités et des gouvernements du monde entier. Le recours à des sites de piratage pour diffuser des logiciels malveillants est un exemple de criminalité multiple qui peut causer un préjudice considérable aux consommateurs du monde entier. Conjugué aux préjudices causés par le piratage, cela représente un risque non seulement pour les titulaires de droits, mais aussi pour la société dans son ensemble.

11. Les tendances récentes montrent également que les écosystèmes du piratage sont de plus en plus étroitement liés à des formes plus générales de cybercriminalité et de polycriminalité. En particulier, les écosystèmes d'applications non officiels, les boutiques d'applications non autorisées, les sites de téléchargement d'APK et d'autres canaux de téléchargement parallèles sont fréquemment utilisés pour diffuser des applications associées à des logiciels malveillants, des logiciels espions, le vol d'identifiants, la fraude et d'autres activités malveillantes.

¹⁰ <https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-internacional-contra-pirataria-tira-do-ar-675-sites-e-14-aplicativos-de-streaming>.

¹¹ <https://www.ifpi.org/brazilian-authorities-launch-operation-redirect-targeting-illegal-music-sites-responsible-for-malware-distribution/>.

¹² <https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-redirect-bloqueia-oito-sites-piratas-de-musica-1>.

¹³ <https://www.securityweek.com/google-sues-operators-of-10-million-device-badbox-2-0-botnet/>.

¹⁴ Par exemple, Netbeacon met à disposition un canal permettant de signaler les abus liés au DNS : <https://netbeacon.org/>.

12. Les consommateurs qui cherchent à accéder sans autorisation à de la musique, à des contenus audiovisuels ou à des diffusions en direct risquent, sans s'en rendre compte, d'installer des applications provenant d'environnements de distribution non fiables, exposant ainsi leurs appareils et leurs données personnelles à des risques importants en matière de cybersécurité.

13. Ces activités montrent que les services de piratage peuvent servir non seulement de vecteurs d'atteinte au droit d'auteur, mais aussi de passerelles vers des activités criminelles plus larges, telles que l'hameçonnage, la fraude financière, le recrutement de botnets, la fraude publicitaire et la collecte massive d'identifiants.

14. Dans certains cas, des acteurs malveillants exploitent la demande pour des contenus populaires ou pour des contenus qui ont été retirés des boutiques d'applications grand public afin d'inciter les consommateurs à télécharger des applications infectées ou à cliquer sur des liens trompeurs et de fausses mises à jour logicielles.

15. La prolifération des applications mobiles installées hors des canaux officiels et des canaux de distribution d'applications non agréés accentue encore ces risques, en particulier lorsque des acteurs malveillants peuvent rapidement reconditionner et redistribuer des applications contrefaisantes ou malveillantes en contournant les processus de vérification et de sécurité établis. Cela souligne la nécessité d'une collaboration coordonnée entre les gouvernements, les autorités chargées de la cybersécurité, les forces de l'ordre, les intermédiaires en ligne et les opérateurs d'écosystèmes d'applications afin de lutter contre les préjudices sociétaux plus larges liés à la diffusion de logiciels malveillants associés au piratage.

16. Il est à prévoir que les risques liés aux logiciels malveillants présents sur les sites et les applications de piratage continueront de s'accroître, favorisés par l'intelligence artificielle (IA). Un rapport récent a souligné que l'IA pouvait favoriser et faciliter certains types de délits, notamment la diffusion de logiciels malveillants, grâce à sa capacité à associer des contenus d'apparence plus réaliste à une diffusion automatisée à grande échelle¹⁵. La cybercriminalité et la fraude ont des conséquences néfastes pour les victimes, comme l'a montré une étude récente publiée par le Ministère de l'Intérieur britannique¹⁶.

II. CONCLUSION

17. Le lien entre les logiciels malveillants et le piratage en ligne devrait faire l'objet d'études plus approfondies, notamment de la part de l'Organisation Mondiale de la Propriété Intellectuelle, afin de recueillir des données et des informations pertinentes permettant aux décideurs politiques de prendre des décisions éclairées, dans le but de mettre au point les outils nécessaires pour faire face aux nouveaux enjeux qui pourraient se présenter.

18. Plusieurs domaines mériteraient d'être approfondis, par exemple :

- La menace liée au piratage des applications mobiles, notamment des applications de partage de contenu très populaires telles que Discord et Telegram, compte tenu en particulier de l'augmentation de la consommation de contenu sur mobile et de la disponibilité croissante de ces applications dans des boutiques d'applications non officielles ou sur des sites de téléchargement de fichiers APK (c'est-à-dire par transfert de fichiers entre deux appareils (side-loading)).

¹⁵ https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas_research_report_-_ai_and_serious_online_crime_0.pdf.

¹⁶ <https://www.gov.uk/government/publications/understanding-the-cyber-crime-and-fraud-victim-journey/understanding-the-cyber-crime-and-fraud-victim-journey>.

- Les nouveaux vecteurs de menace potentiels liés aux technologies émergentes, par exemple l'utilisation de l'IA pour générer de faux contenus de prélançement ou d'autres contenus "deepfake" pouvant servir d'appât pour la diffusion de logiciels malveillants.
- Le rôle des logiciels malveillants dans la criminalité multiforme, notamment leur diffusion via des appareils permettant d'accéder à des contenus illicites, qui peuvent ensuite servir à récupérer des identifiants ou à mettre en place des botnets à des fins malveillantes, telles que la fraude au streaming.

19. Il existe déjà un certain nombre d'outils et de mesures d'application des droits qui peuvent servir de point de départ à l'élaboration de pratiques recommandées à l'échelle mondiale et qui devraient favoriser le dialogue et la collaboration avec les intermédiaires, en les encourageant à prendre davantage de mesures volontaires.

20. En outre, les actions de sensibilisation et d'éducation des consommateurs concernant les préjudices causés par le piratage en ligne devraient, le cas échéant, s'accompagner d'avertissements appropriés sur les risques liés aux logiciels malveillants¹⁷.

[Fin de la contribution]

¹⁷ Par exemple, une étude réalisée en 2023 par l'Office de l'Union européenne pour la propriété intellectuelle a révélé que 82% des citoyens européens estiment que l'obtention illégale de contenus en ligne comporte un risque d'exposition à des pratiques préjudiciables, telles que les escroqueries ou les contenus inappropriés pour les mineurs. Il était toutefois nettement moins fréquent que les gens évitent les sources illégales en raison de mauvaises expériences vécues par eux-mêmes ou par d'autres (respectivement 13% et 19%). Ces raisons se sont toutefois révélées plus convaincantes pour inciter les utilisateurs délibérés de services illégaux à cesser de recourir à des contenus piratés en ligne (respectivement 31% et 29%). Voir : https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_IP_Perception_Study/2023_IP_Perception_Study_FullR_en.pdf.