S

OMPI
ORGANIZACIÓN MUNDIAL
DE LA PROPIEDAD
INTELECTUAL

WIPO/ACE/18/34
ORIGINAL: INGLÉS
FECHA: 19 DE MAYO DE 2024

Comité Asesor sobre Observancia

Decimoctava sesión
Ginebra, 2 a 4 de junio de 2026

EL NEXO ENTRE LOS PROGRAMAS MALICIOSOS Y LA PIRATERÍA: HERRAMIENTAS DE APLICACIÓN DE LA LEY Y OPORTUNIDADES PARA QUE LOS GOBIERNOS ADOPTEN MEDIDAS

Contribución elaborada por la Dra. Elena Blobel, directora de Litigios Mundiales de la Federación Internacional de la Industria Fonográfica, Londres (Reino Unido)[*]

RESUMEN

Esta contribución describe cómo los servicios de piratería en línea utilizan habitualmente la promesa de acceso gratuito a contenidos protegidos por derechos de autor para atraer a los consumidores hacia sitios web, aplicaciones y dispositivos que los exponen a riesgos significativos. Destaca el tipo de programas maliciosos utilizados en relación con la piratería en línea y la gama de herramientas de aplicación de la ley disponibles para impedir la distribución de programas maliciosos. La contribución aboga por que se preste mayor atención, a nivel de formulación de políticas, al nexo entre los programas maliciosos y la piratería y las múltiples formas de delincuencia asociadas. Concluye identificando áreas prioritarias para un estudio más detallado, con el fin de facilitar la toma de decisiones fundamentadas por parte de los responsables de políticas.

[*] Las opiniones expresadas en este documento son las del autor y no reflejan necesariamente las de la Secretaría ni las de los Estados miembros de la OMPI.

I. ¿POR QUÉ SE UTILIZA CONTENIDO PROTEGIDO POR DERECHOS DE AUTOR EN RELACIÓN CON LA DISTRIBUCIÓN DE PROGRAMAS MALICIOSOS?

1. La promesa de acceso a contenidos gratuitos protegidos por derechos de autor a través de servicios de piratería en línea es ampliamente utilizada por actores maliciosos para atraer a los consumidores a acceder a sitios web, aplicaciones y dispositivos que los exponen a diversos tipos de amenazas maliciosas. Esta contribución expone la situación actual en lo que respecta a los tipos de programas maliciosos implicados, la magnitud potencial del problema, los tipos de medidas de aplicación de la ley existentes, así como las oportunidades para que los gobiernos aborden esta cuestión, entre otras cosas, mediante la sensibilización de los consumidores.

A. TIPOS DE PROGRAMAS MALICIOSOS IMPLICADOS EN LA PIRATERÍA EN LÍNEA

2. Según la experiencia de la Federación Internacional de la Industria Fonográfica (IFPI), existen diversos tipos de programas maliciosos que pueden encontrarse en sitios y servicios de piratería musical. Algunos ejemplos de programas maliciosos relacionados con los servicios de piratería incluyen:

- *Ransomware* distribuido a través de ventanas emergentes engañosas u ocultas, botones de “clic para reproducir” o botones de descarga falsos en sitios de transmisión en directo pirata y de torrentes que cifran los archivos de la víctima. Posteriormente, se exige un pago para restablecer el acceso, normalmente en forma de criptomoneda.

- El *criptojacking*, en el que se ejecutan programas de minería de criptomonedas de forma encubierta en el navegador o el dispositivo de un usuario, al tiempo que consumen recursos de la computadora y degradan su rendimiento.

- El *spyware*, que realiza una supervisión encubierta de la actividad del usuario, registrando pulsaciones de teclas y credenciales y sustrayendo información confidencial o personal, como correos electrónicos, datos financieros y fotografías.

- Los troyanos, que consisten en programas maliciosos camuflados como programas legítimos que se descargan a través de actualizaciones falsas, reproductores multimedia o instaladores, y que crean puertas traseras o instalan otros programas maliciosos. La publicidad maliciosa consiste en anuncios agresivos, engañosos o intrusivos que conducen a la descarga de programas maliciosos, la recopilación de datos de los usuarios y el redireccionamiento de estos a páginas fraudulentas.

- El *scareware*, que imita las advertencias del sistema y, de este modo, engaña a las víctimas para que descarguen programas maliciosos. Estos son habituales tanto en los servicios de piratería para móviles como para ordenadores de sobremesa.

- Las herramientas de robo de credenciales y las páginas falsas de inicio de sesión y pago se centran en la recopilación de nombres de usuario, contraseñas y códigos de doble autenticación. Estas credenciales robadas pueden reutilizarse en cuentas bancarias o de redes sociales, lo que permite el robo de identidad, las transferencias de fondos no autorizadas y la usurpación de cuentas, y también pueden revenderse en el mercado ilícito. Las credenciales comprometidas pueden utilizarse para acceder a cuentas con el fin de llevar a cabo fraudes de transmisión en directo (es decir, para generar reproducciones falsas de canciones en plataformas de transmisión en directo musicales que no representan un consumo real por parte de los fans), desviando así los ingresos de los artistas legítimos y otros titulares de derechos.

- La incorporación a las redes de bots implica el uso de programas punto a punto, herramientas de red pirateadas o dispositivos de transmisión en directo ilegales que vienen precargados con complementos sin licencia para infiltrarse en redes y dispositivos locales. A continuación, estos dispositivos se incorporan sin que los usuarios lo sepan a redes de bots que coordinan ataques de denegación de servicio distribuidos, campañas de correo no deseado o la distribución de programas maliciosos adicionales. Estas redes de bots también pueden utilizarse para cometer fraudes, incluido el fraude en la transmisión en directo.

- Los secuestradores del Sistema de Nombres de Dominio (DNS) alteran los ajustes del DNS o la configuración del navegador para redirigir el tráfico hacia páginas de destino maliciosas o afiliadas, desviando las solicitudes web del usuario a través de servicios controlados por los atacantes.

B. LA MAGNITUD DEL PROBLEMA

3. Hasta la fecha, millones de usuarios de Internet acceden a sitios piratas en línea a escala mundial para acceder a contenidos protegidos por derechos de autor sin licencia. Existe un importante corpus de investigación que ha evaluado la magnitud potencial del problema y los riesgos de programas maliciosos a los que se enfrentan los usuarios de Internet en relación con la piratería en línea. En general, los informes, centrados principalmente en el sector audiovisual, han puesto de relieve que las amenazas existen a gran escala en todo el mundo. Por ejemplo:

- Los consumidores del sudeste asiático se enfrentan, de media, a un aumento de más de 22 veces en la detección de ciberamenazas en los sitios de piratería en comparación con los sitios de control convencionales.[1]

- En la India, los sitios de piratería conllevan un riesgo del 59 % de infección por programas maliciosos, superior al de los sitios de entretenimiento para adultos o de apuestas, siendo los usuarios más jóvenes (18-24 años) especialmente vulnerables.[2]

- La denominada “publicidad maliciosa” representaba el 12 % del total de anuncios en los sitios de piratería, generando unos ingresos mínimos de 121 millones de USD al año. Casi el 80 % de los sitios de piratería investigados mostraban anuncios plagados de programas maliciosos. Una visita a un sitio de piratería conlleva, de media, un intento de infectar al usuario con programas maliciosos una de cada seis veces.[3]

- Los consumidores de Polonia tienen, de media, 38,5 veces más probabilidades de encontrarse con ciberamenazas en sitios de intercambio entre pares que en los sitios convencionales.[4]

- Un estudio reveló que los consumidores europeos podían sufrir un ataque en tan solo 71 segundos tras acceder a sitios de piratería y que, de media, existía un 57 % de probabilidades de que las aplicaciones de piratería audiovisual vinieran preinstaladas con programas maliciosos integrados.[5]

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

4. Se dispone de menos datos en otros sectores, pero los principios son ampliamente aplicables a cualquier sitio web, aplicación o dispositivo fraudulento que ofrezca contenido sin licencia para atraer a los usuarios, y las pruebas del sector musical también respaldan esta afirmación.

5. Una investigación llevada a cabo por la IFPI en América Latina reveló que el 33 % de una muestra de 174 sitios web de descarga de MP3 que operan en la región estaban relacionados con la distribución de programas maliciosos. Entre esos sitios web de música ilegales, el 17 % distribuía programas maliciosos directamente, mientras que otro 26 % distribuía indirectamente archivos de programas maliciosos sospechosos a través de páginas secundarias bajo diferentes nombres de dominio. La misma investigación también reveló que el 10 % de esos sitios web de música ilegales que distribuían programas maliciosos contaban con aplicaciones móviles infractoras de derechos de propiedad intelectual, lo que aumentaba los riesgos de acceso indebido y robo de datos personales, así como de otros tipos de delitos cibernéticos. En términos más generales, los usuarios de Internet en Brasil sufrieron un aumento del 408 % en el fraude en línea desde 2018, con 2,1 millones de casos denunciados en 2024.[6]

C. ¿DE QUÉ HERRAMIENTAS DE APLICACIÓN DE LA LEY SE DISPONE PARA ABORDAR ESTE PROBLEMA?

6. Existen varias iniciativas para hacer frente a la distribución de programas maliciosos, entre las que se incluyen las siguientes:

- La Operación Endgame de Europol, una iniciativa a gran escala centrada en desarticular las redes de bots y las infraestructuras delictivas asociadas.[7]

- El Laboratorio Nacional de Análisis Forense de Delitos Cibernéticos, dependiente del Centro de Coordinación de Delitos Cibernéticos de la India, que presta servicios especializados de análisis forense y análisis de programas maliciosos a las autoridades policiales.[8]

- La Autoridad Central de Protección del Consumidor de la India, que ha emitido una recomendación en la que se establece que las plataformas digitales deben identificar y eliminar los “patrones oscuros” de sus interfaces, incluidos los programas maliciosos.[9]

7. En otros países deberían estar disponibles herramientas similares para hacer frente a los programas maliciosos en el contexto de la piratería, como se observa en las iniciativas coordinadas por el Ministerio de Justicia y Seguridad Pública y el Laboratorio de Operaciones Cibernéticas de Brasil:

- La Operación 404, que se centró en más de 3000 sitios web y aplicaciones móviles infractores en siete rondas durante los últimos seis años, algunos de los cuales distribuían programas maliciosos directamente y robaban datos personales.[10]

- La Operación Redirect, que se centró específicamente en sitios de piratería asociados a la distribución de programas maliciosos (incluidos sitios de enlaces musicales ilegales, sitios de captura de transmisiones en directo y sistemas de

[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-litercy/information-security/indian-cyber-crime-coordination-centre?lgn=en.
[9] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2134765. Esto se ajusta a las Directrices de 2023 para la prevención y regulación de los patrones oscuros de la Autoridad Central de Protección al Consumidor.
[10] https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-internacional-contra-pirataria-tira-do-ar-675-sites-e-14-aplicativos-de-streaming.

búsqueda de torrentes).[11] La operación coordinada incautó dominios, bloqueó sitios y cerró sitios web ilegales mediante la aplicación combinada de medidas disruptivas.[12]

8. Además de las medidas penales, también pueden adoptarse medidas civiles. Por ejemplo, Google anunció recientemente la presentación de una demanda contra los operadores de la red de bots Badbox 2.0, que, según afirma, ha infectado más de 10 millones de dispositivos que ejecutan el sistema de código abierto Android.[13]

9. Las plataformas en línea y los intermediarios también deben desempeñar un papel en la interrupción de estas actividades. En las plataformas de comercio electrónico se venden dispositivos precargados con contenido infractor y programas maliciosos; en las tiendas de aplicaciones oficiales y sin licencia se encuentran aplicaciones móviles que contienen programas maliciosos; mediante búsquedas se pueden descubrir sitios web fraudulentos que distribuyen programas maliciosos; y los intermediarios de dominios y alojamiento proporcionan la infraestructura que permite el funcionamiento de estos sitios. Aun cuando esta actividad esté prohibida en virtud de sus respectivas condiciones, los actores maliciosos pueden seguir operando. Por ello, se requieren medidas proactivas, junto con un mecanismo de denuncia escalable y una eliminación rápida y eficaz. También existen organizaciones independientes que ofrecen canales de denuncia.[14]

D. ¿POR QUÉ DEBERÍA SER ESTO IMPORTANTE PARA LOS GOBIERNOS?

10. Es importante que se ponga en conocimiento de las autoridades y gobiernos de todo el mundo la relación existente entre la piratería en línea y los programas maliciosos, así como las tendencias cambiantes en este ámbito. La utilización de sitios de piratería para distribuir programas maliciosos es un ejemplo de delincuencia múltiple que puede resultar extremadamente perjudicial para los consumidores de todo el mundo. Junto con el daño causado por la piratería, esto constituye un riesgo no solo para los titulares de derechos, sino también para la sociedad en general.

11. Las tendencias recientes también demuestran que los ecosistemas de piratería se entrecruzan cada vez más con formas más amplias de ciberdelincuencia y delincuencia múltiple. En particular, los ecosistemas de aplicaciones no oficiales, las tiendas de aplicaciones no autorizadas, los sitios de descarga de APK y otros canales de instalación paralela se utilizan con frecuencia para distribuir aplicaciones asociadas con programas maliciosos, spyware, robo de credenciales, fraude y otras actividades maliciosas.

12. Los consumidores que buscan acceso no autorizado a contenidos musicales, audiovisuales o de transmisión en directo pueden instalar, sin saberlo, aplicaciones fuera de entornos de distribución fiables, exponiendo sus dispositivos y datos personales a importantes riesgos de ciberseguridad.

13. Dichas actividades ilustran cómo los servicios de piratería pueden actuar no solo como mecanismos de infracción de los derechos de autor, sino también como puertas de entrada a conductas delictivas más amplias, como la suplantación de identidad, el fraude financiero, la captación de redes de bots, el fraude publicitario y la recopilación de credenciales a gran escala.

[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] Por ejemplo, Netbeacon ofrece un canal para la notificación de abusos del DNS: https://netbeacon.org/.

14. En algunos casos, los actores maliciosos aprovechan la demanda de contenidos populares o de contenidos que han sido retirados de las tiendas de aplicaciones convencionales para atraer a los consumidores a descargar aplicaciones infectadas o a interactuar con enlaces engañosos y actualizaciones falsas.

15. La creciente prevalencia de aplicaciones móviles instaladas de forma paralela y de canales de distribución de aplicaciones sin licencia aumenta aún más estos riesgos, especialmente cuando los actores maliciosos pueden reempaquetar y redistribuir rápidamente programas maliciosos o infractores al margen de los procesos establecidos de revisión y seguridad. Esto refuerza la necesidad de una colaboración coordinada entre gobiernos, autoridades de ciberseguridad, fuerzas del orden, intermediarios en línea y operadores del ecosistema de aplicaciones para abordar los daños sociales más amplios asociados a la distribución de programas maliciosos vinculados a la piratería.

16. Se prevé que los riesgos que plantean los programas maliciosos en los sitios web y aplicaciones de piratería sigan aumentando, facilitados por la inteligencia artificial (IA). Un informe reciente reconoció que la IA podría potenciar y facilitar ciertos tipos de delitos, incluida la distribución de programas maliciosos, gracias a su capacidad para combinar contenidos de aspecto más realista con una distribución automatizada a gran escala.[15] La ciberdelincuencia y el fraude tienen un efecto perjudicial en las víctimas, lo cual fue objeto de un estudio reciente publicado por el Ministerio del Interior del Reino Unido.[16]

II. CONCLUSIÓN

17. El nexo entre los programas maliciosos y la piratería en línea debería estudiarse más a fondo, incluso por parte de la Organización Mundial de la Propiedad Intelectual, con el fin de recopilar datos e información pertinentes que faciliten la toma de decisiones fundamentadas por parte de los responsables de políticas, con vistas a desarrollar las herramientas necesarias para abordar cualquier problema emergente.

18. Hay una serie de ámbitos que podrían estudiarse más a fondo, por ejemplo:

- La amenaza derivada de la piratería en las aplicaciones móviles, incluidas las populares aplicaciones para compartir contenidos como Discord y Telegram, especialmente teniendo en cuenta el crecimiento del consumo de contenidos a través del móvil y la mayor disponibilidad de dichas aplicaciones móviles en tiendas de aplicaciones no autorizadas o en sitios de descarga de paquetes Android (es decir, la instalación paralela).

- Los posibles nuevos tipos de amenaza que plantean las tecnologías emergentes, por ejemplo, el uso de la IA para generar contenido falso previo al lanzamiento u otro contenido ultrafalso que pueda utilizarse como cebo para la distribución de programas maliciosos.

- El papel de los programas maliciosos en la delincuencia múltiple, incluida la distribución de programas maliciosos a través de dispositivos que ofrecen acceso a contenidos sin licencia, que luego pueden utilizarse para recopilar credenciales o crear redes de bots con otros fines maliciosos, como el fraude en la transmisión en directo.

19. Ya existen una serie de herramientas de aplicación de la ley y medidas que se están adoptando y que pueden servir como punto de partida para el establecimiento de buenas

[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.

prácticas a escala mundial, y que deberían fomentar el diálogo y la colaboración con los intermediarios, alentándolos a adoptar más medidas voluntarias.

20. Además, la sensibilización y la educación continuas de los consumidores en relación con el daño causado por la piratería en línea deberían ir acompañadas, cuando proceda, de advertencias adecuadas sobre el riesgo de programas maliciosos.[17]

[Fin de la contribución]

[17] Por ejemplo, un estudio de 2023 de la Oficina de Propiedad Intelectual de la Unión Europea reveló que el 82 % de los ciudadanos europeos está de acuerdo en que la obtención ilegal de contenidos en línea conlleva el riesgo de exposición a prácticas perjudiciales, como estafas o contenidos inapropiados para menores. No obstante, era considerablemente menos habitual que las personas evitaran las fuentes ilegales debido a malas experiencias propias o ajenas (13 % y 19 %, respectivamente). Sin embargo, estas razones resultaban más convincentes para motivar a los usuarios habituales de servicios ilegales a dejar de utilizar contenidos pirateados en línea (el 31 % y el 29 %, respectivamente). Véase: 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.