A

WIPO
المنظمة العالمية للملكية الفكرية

WIPO/ACE/18/34
الأصل: الإنجليزية
التاريخ: 19 مايو 2026

# اللجنة الاستشارية المعنية بالإنفاذ

الدورة الثامنة عشرة
جنيف، من 2 إلى 4 يونيو 2026

العلاقة بين البرمجيات الخبيثة والقرصنة – أدوات الإنفاذ وفرص اتخاذ الإجراءات الحكومية

مساهمة أعدتها الدكتورة إيلينا بلوبيل، مديرة شؤون التقاضي العالمي، الاتحاد الدولي لصناعة التسجيلات الصوتية، لندن، المملكة المتحدة*

## ملخص

توضح هذه المساهمة كيف تستخدم خدمات القرصنة عبر الإنترنت بشكل روتيني الوعد بالوصول مجاناً إلى المحتوى المحمي بحق المؤلف لجذب المستهلكين إلى مواقع الويب والتطبيقات والأجهزة التي تعرضهم لمخاطر كبيرة. وتسلط الضوء على نوع البرامج الضارة المستخدمة في القرصنة عبر الإنترنت ومجموعة أدوات الإنفاذ المتاحة لعرقلة توزيع البرامج الضارة. وتدعو هذه المساهمة إلى إيلاء مزيد من الاهتمام على مستوى وضع السياسات للصلة بين البرامج الضارة والقرصنة والأشكال المتعددة من الجرائم المرتبطة بها. وتختتم بتحديد المجالات ذات الأولوية لمزيد من الدراسة، بهدف تسهيل اتخاذ قرارات مستنيرة من قبل واضعي السياسات.

* الآراء الواردة في هذا المستند هي آراء المؤلف ولا تعبر بالضرورة عن آراء الأمانة العامة أو الدول الأعضاء في الويبو.

## أولاً. لماذا يُستخدم المحتوى المحمي بحق المؤلف في توزيع البرامج الضارة؟

1. تستخدم الجهات الفاعلة السيئة على نطاق واسع الوعد بالوصول إلى محتوى مجاني محمي بحق المؤلف من خلال خدمات القرصنة عبر الإنترنت لإغراء المستهلكين بالوصول إلى المواقع والتطبيقات والأجهزة التي تعرضهم لأنواع مختلفة من ناقلات التهديدات الخبيثة. وتحدد هذه المساهمة الوضع الحالي فيما يتعلق بأنواع البرامج الضارة المعنية، والحجم المحتمل للمشكلة، وأنواع إجراءات الإنفاذ الحالية، فضلاً عن الفرص المتاحة للحكومات لمعالجة هذه المشكلة، بما في ذلك من خلال توعية المستهلكين.

### ألف. أنواع البرامج الضارة المرتبطة بالقرصنة عبر الإنترنت

2. وفقًا لتجربة الاتحاد الدولي لصناعة التسجيلات الصوتية (IFPI)، هناك أنواع مختلفة من البرامج الضارة التي يمكن العثور عليها في مواقع وخدمات قرصنة الموسيقى. ومن أمثلة البرامج الضارة المرتبطة بخدمات القرصنة ما يلي:

- برامج الفدية التي يتم توزيعها عبر النوافذ المنبثقة الخادعة، أو النوافذ المنبثقة الخلفية، أو أزرار "انقر للتشغيل"، أو أزرار التنزيل المزيفة على مواقع البث والتورنت المقرصنة التي تقوم بتشفير ملفات الضحية. وبعد ذلك، يُطلب الدفع لاستعادة الوصول، وعادةً ما يكون ذلك في شكل عملة مشفرة.

- التعدين الخفي، حيث يتم تشغيل برامج التعدين الخفي سراً في متصفح المستخدم أو جهازه، مما يستهلك موارد الكمبيوتر ويؤدي إلى تدهور الأداء.

- برامج التجسس، التي تراقب نشاط المستخدم سراً، وتسجل ضغطات المفاتيح وبيانات الاعتماد، وتسرب المعلومات السرية أو الشخصية مثل رسائل البريد الإلكتروني والمعلومات المالية والصور.

- أحصنة طروادة، وهي برامج ضارة تتنكر في شكل برامج شرعية يتم تنزيلها من خلال تحديثات مزيفة أو مشغلات وسائط أو برامج تثبيت، وتقوم بإنشاء أبواب خلفية أو تثبيت أدوات ضارة أخرى. والإعلانات الخبيثة، وهي إعلانات عدوانية أو خادعة أو متطفلة، تؤدي إلى تنزيل برامج ضارة، وجمع بيانات المستخدم، وإعادة توجيه المستخدمين إلى صفحات احتيالية.

- برامج التخويف، التي تحاكي تحذيرات النظام وبالتالي تخدع الضحايا لتنزيل برامج ضارة. وهذه شائعة في خدمات القرصنة على كل من الأجهزة المحمولة وأجهزة سطح المكتب.

- تركز أدوات سرقة بيانات الاعتماد وصفحات تسجيل الدخول والدفع المزيفة على جمع أسماء المستخدمين وكلمات المرور ورموز المصادقة الثنائية. ويمكن إعادة استخدام بيانات الاعتماد المسروقة هذه في الحسابات المصرفية أو حسابات وسائل التواصل الاجتماعي، مما يتيح سرقة الهوية وتحويل الأموال دون إذن والاستيلاء على الحسابات، كما يمكن إعادة بيعها في السوق السوداء. ويمكن استخدام بيانات الاعتماد المخترقة للوصول إلى الحسابات بغرض ارتكاب احتيال البث (أي إنشاء تدفقات مزيفة للأغاني على منصات بث الموسيقى لا تمثل استهلاكًا حقيقيًا من قبل المعجبين)، مما يؤدي إلى تحويل الإيرادات عن الفنانين الشرعيين وأصحاب الحقوق الآخرين.

- تجنيد شبكات الروبوتات (Botnet) حيث يتم استخدام عملاء الند للند (peer-to-peer) أو أدوات الشبكة المخترقة أو أجهزة البث غير المشروعة المزودة مسبقًا بإضافات غير مرخصة للتسلل إلى الشبكات والأجهزة المحلية، مما يؤدي إلى تجنيدها دون علمها في شبكات الروبوتات التي تنسق هجمات الحرمان من الخدمة الموزعة أو حملات البريد العشوائي أو توزيع برامج ضارة إضافية. يمكن أيضًا استخدام شبكات الروبوتات هذه لارتكاب الاحتيال، بما في ذلك الاحتيال في البث.

- يقوم مخترقو نظام أسماء الحقول (DNS) بتغيير إعدادات DNS أو تكوين المتصفح لإعادة توجيه حركة المرور إلى صفحات هبوط ضارة أو تابعة، وإعادة توجيه طلبات الويب الخاصة بالمستخدم عبر خدمات يسيطر عليها المهاجمون.

### باء. حجم المشكلة

3. حتى الآن، يزور ملايين مستخدمي الإنترنت مواقع القرصنة عبر الإنترنت على مستوى العالم للوصول إلى محتوى محمي بحق المؤلف غير مرخص. وهناك مجموعة كبيرة من الأبحاث التي قيمت الحجم المحتمل للمشكلة ومخاطر البرامج الضارة التي يواجهها مستخدمو الإنترنت فيما يتعلق بالقرصنة عبر الإنترنت. وبشكل عام، أبرزت التقارير، التي ركزت في الغالب على القطاع السمعي البصري، أن التهديدات موجودة على نطاق مذهل في جميع أنحاء العالم. فعلى سبيل المثال:

- يواجه المستهلكون في جنوب شرق آسيا في المتوسط زيادة تزيد عن 22 ضعفًا في اكتشاف التهديدات السيبرانية على مواقع القرصنة مقارنة بالمواقع الرئيسية الخاضعة للرقابة.[1]

- في الهند، تنطوي مواقع القرصنة على خطر الإصابة بالبرامج الضارة بنسبة 59 في المائة، وهو أعلى من مواقع الترفيه للبالغين أو مواقع المقامرة، مع تعرض المستخدمين الأصغر سنًا (18-24) للخطر بشكل خاص.[2]

- شكلت ما يُسمى بالإعلانات الخبيثة 12 في المائة من إجمالي الإعلانات على مواقع القرصنة، مما يدر إيرادات لا تقل عن 121 مليون دولار أمريكي سنويًا. وقدم ما يقرب من 80 في المائة من مواقع القرصنة التي تم التحقيق فيها إعلانات مليئة بالبرامج الضارة. وتؤدي زيارة موقع قرصنة إلى محاولة تزويد المستخدم ببرامج ضارة بمعدل مرة واحدة من كل ست مرات في المتوسط.[3]

- المستهلكون في بولندا، في المتوسط، أكثر عرضة بمقدار 38.5 مرة لمواجهة تهديدات إلكترونية على مواقع الند للند مقارنة بالمواقع السائدة.[4]

- وجدت دراسة أن المستهلكين الأوروبيين قد يتعرضون للهجوم في غضون 71 ثانية من دخولهم إلى مواقع القرصنة، وأنه في المتوسط تبلغ احتمالية أن تكون تطبيقات القرصنة السمعية البصرية مثبتة مسبقًا مع برامج ضارة مدمجة فيها 57 في المائة.[5]

4. والبيانات في القطاعات الأخرى أقل توفرًا، لكن المبادئ قابلة للتطبيق بشكل عام على أي مواقع ويب وتطبيقات وأجهزة غير شرعية تقدم محتوى غير مرخص لجذب المستخدمين، وهذا يتأكد أيضًا بشكل غير رسمي في قطاع الموسيقى.

5. وكشفت دراسة أجراها الاتحاد (IFPI) في أمريكا اللاتينية أن 33 في المائة من عينة شملت 174 موقعًا لتنزيل ملفات MP3 تعمل في المنطقة كانت مرتبطة بتوزيع البرامج الضارة. ومن بين تلك المواقع الموسيقية غير القانونية، كان 17 في المائة يوزع البرامج الضارة بشكل مباشر، في حين كان 26 في المائة آخرون يوزعون ملفات برامج ضارة مشبوهة بشكل غير مباشر عبر صفحات فرعية تحت أسماء حقول مختلفة. وأظهر البحث نفسه أيضًا أن 10 في المائة من مواقع الموسيقى غير القانونية التي توزع برامج ضارة لديها تطبيقات جوال تنتهك حقوق الملكية الفكرية، مما يزيد من مخاطر الوصول غير المشروع وسرقة البيانات الشخصية، فضلاً عن أنواع أخرى من الجرائم الإلكترونية. وبشكل عام، عانى مستخدمو الإنترنت في البرازيل من زيادة بنسبة 408 في المائة في حالات الاحتيال عبر الإنترنت منذ عام 2018، حيث تم الإبلاغ عن 2.1 مليون حالة في عام 2024.[6]

## جيم. ما هي أدوات الإنفاذ المتاحة لمعالجة هذه المشكلة؟

6. توجد عدة مبادرات لمعالجة مشكلة توزيع البرامج الضارة، بما في ذلك ما يلي:

- عملية "إندغيم" (Endgame) التابعة لليوروبول، وهي مبادرة واسعة النطاق تركز على تعطيل شبكات الروبوتات والبنى التحتية الإجرامية المرتبطة بها.[7]

- المختبر الوطني لتحليل الجرائم الإلكترونية التابع لمركز تنسيق الجرائم الإلكترونية الهندي، الذي يقدم خدمات متخصصة في تحليل البرامج الضارة لصالح سلطات إنفاذ القانون.[8]

- الهيئة المركزية لحماية المستهلك في الهند، التي أصدرت توصية تنص على أن المنصات الرقمية يجب أن تحدد وتزيل الأنماط الخفية من واجهاتها، بما في ذلك البرامج الضارة الخبيثة.[9]

---

[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.
[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. وهذا يتماشى مع المبادئ التوجيهية لعام 2023 الخاصة بالوقاية من الأنماط الخادعة وتنظيمها الصادرة عن الهيئة المركزية لحماية المستهلك.

7. ويجب أن تكون أدوات مماثلة متاحة بسهولة في البلدان الأخرى لمعالجة البرمجيات الخبيثة في سياق القرصنة، كما يتضح من المبادرات التي تنسقها وزارة العدل والأمن العام ومختبر العمليات الإلكترونية في البرازيل:

- عملية 404، التي استهدفت أكثر من 3000 موقع وتطبيق جوال مخالف في سبع جولات خلال السنوات الست الماضية، بعضها يتضمن توزيعًا مباشرًا للبرامج الضارة وسرقة البيانات الشخصية.[10]

- عملية Redirect، التي استهدفت على وجه التحديد مواقع القرصنة المرتبطة بتوزيع البرامج الضارة (بما في ذلك مواقع الموسيقى التي توفر روابط غير قانونية، ومواقع نسخ البث المباشر، ومحركات بحث التورنت).[11] أدت العملية المنسقة إلى مصادرة النطاقات وحجب المواقع وإغلاق المواقع غير القانونية من خلال التطبيق المشترك لتدابير تعطيلية.[12]

8. وبالإضافة إلى سبل الانتصاف الجنائية، قد تتوفر أيضًا سبل انتصاف مدنية. على سبيل المثال، أعلنت Google مؤخرًا عن رفع دعوى قضائية ضد مشغلي شبكة الروبوتات Badbox 2.0، التي تدعي أنها أصابت أكثر من 10 ملايين جهاز يعمل بنظام Android مفتوح المصدر.[13]

9. كما يجب على المنصات والوسطاء عبر الإنترنت أن يلعبوا دوراً في وقف هذه الأنشطة. فهناك أجهزة مزودة مسبقاً بمحتوى مخالف للقانون وبرامج ضارة تُباع على منصات التجارة الإلكترونية؛ وتتوفر تطبيقات الهاتف المحمول التي تحتوي على برامج ضارة في متاجر التطبيقات الرسمية وغير المرخصة؛ ويمكن العثور على المواقع الإلكترونية المارقة التي توزع البرامج الضارة من خلال محركات البحث؛ كما يوفر وسطاء النطاقات والاستضافة البنية التحتية التي تمكّن هذه المواقع من العمل. وحتى لو كانت هذه الأنشطة محظورة بموجب الشروط والأحكام الخاصة بهم، فإن الجهات الخبيثة قادرة على مواصلة عملها. لذلك، يلزم اتخاذ خطوات استباقية، إلى جانب آليات إبلاغ قابلة للتطوير وإزالة سريعة وفعالة. كما توجد منظمات مستقلة توفر قنوات للإبلاغ.[14]

## دال. لماذا ينبغي أن تهتم الحكومات بهذه المشكلة؟

10. من المهم لفت انتباه السلطات والحكومات على مستوى العالم إلى مسألة الصلة بين القرصنة عبر الإنترنت والبرامج الضارة، فضلاً عن الاتجاهات المتطورة في هذا المجال. يعد استخدام مواقع القرصنة لتوزيع البرامج الضارة مثالاً على الجرائم المتعددة التي يمكن أن تكون ضارة للغاية للمستهلكين في جميع أنحاء العالم. إلى جانب الضرر الناجم عن القرصنة، يشكل هذا خطرًا ليس فقط على أصحاب الحقوق ولكن أيضًا على المجتمع ككل.

11. وتُظهر الاتجاهات الحديثة أيضًا أن أنظمة القرصنة تتقاطع بشكل متزايد مع أشكال أوسع من الجرائم الإلكترونية والجرائم المتعددة. وعلى وجه الخصوص، غالبًا ما تُستخدم أنظمة التطبيقات غير الرسمية ومتاجر التطبيقات غير المرخصة ومواقع تنزيل ملفات APK وقنوات التحميل الجانبي الأخرى لتوزيع التطبيقات المرتبطة بالبرامج الضارة وبرامج التجسس وسرقة بيانات الاعتماد والاحتيال والأنشطة الخبيثة الأخرى.

12. وقد يقوم المستهلكون الذين يسعون إلى الوصول غير المصرح به إلى المحتوى الموسيقي أو السمعي البصري أو البث المباشر بتثبيت تطبيقات خارج بيئات التوزيع الموثوقة دون علمهم، مما يعرض أجهزتهم وبياناتهم الشخصية لمخاطر أمنية إلكترونية كبيرة.

13. وتوضح هذه الأنشطة كيف يمكن لخدمات القرصنة أن تعمل ليس فقط كآليات لانتهاك حق المؤلف، ولكن أيضًا كبوابات لسلوك إجرامي أوسع نطاقًا، بما في ذلك التصيد الاحتيالي، والاحتيال المالي، وتجنيد شبكات الروبوتات، والاحتيال الإعلاني، وجمع بيانات الاعتماد على نطاق واسع.

14. وفي بعض الحالات، يستغل الفاعلون الخبيثون الطلب على المحتوى الشائع أو المحتوى الذي تمت إزالته من متاجر التطبيقات الرئيسية لإغراء المستهلكين بتنزيل تطبيقات خبيثة أو التفاعل مع روابط خادعة وتحديثات برمجية مزيفة.

15. ويؤدي الانتشار المتزايد لتطبيقات الهواتف المحمولة التي يتم تحميلها من مصادر خارجية وقنوات توزيع التطبيقات غير المرخصة إلى زيادة هذه المخاطر، لا سيما عندما يتمكن الجهات الفاعلة السيئة من إعادة تجميع وإعادة توزيع التطبيقات المخالفة أو الخبيثة بسرعة خارج نطاق عمليات المراجعة والأمن المعمول بها. وهذا يعزز الحاجة إلى تعاون منسق بين الحكومات وسلطات الأمن

---

[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] على سبيل المثال، يوفر Netbeacon قناة للإبلاغ عن إساءة استخدام نظام أسماء الحقول https://netbeacon.org (DNS).

السيبراني وسلطات إنفاذ القانون والوسطاء عبر الإنترنت ومشغلي منظومة التطبيقات لمعالجة الأضرار المجتمعية الأوسع نطاقاً المرتبطة بتوزيع البرمجيات الخبيثة المرتبطة بالقرصنة.

16. ومن المتوقع أن تستمر المخاطر التي تشكلها البرامج الضارة على مواقع وتطبيقات القرصنة في الازدياد، مدعومة بالذكاء الاصطناعي. وأقر تقرير صدر مؤخرًا بأن الذكاء الاصطناعي يمكن أن يزيد من بعض أنواع الجرائم ويسهلها، بما في ذلك توزيع البرامج الضارة، من خلال قدرته على الجمع بين محتوى يبدو أكثر واقعية والتسليم الآلي على نطاق واسع.[15] تؤثر الجرائم الإلكترونية والاحتيال سلبًا على الضحايا، وهو ما كان موضوع دراسة حديثة نشرتها وزارة الداخلية في المملكة المتحدة.[16]

## ثانياً. الخلاصة

17. ينبغي دراسة العلاقة بين البرامج الضارة والقرصنة عبر الإنترنت بشكل أعمق، بما في ذلك من قبل المنظمة العالمية للملكية الفكرية، لجمع البيانات والمعلومات ذات الصلة لتسهيل اتخاذ قرارات مستنيرة من قبل واضعي السياسات، بهدف تطوير الأدوات اللازمة لمعالجة أي قضايا ناشئة.

18. هناك عدد من المجالات التي يمكن دراستها بشكل أعمق، على سبيل المثال:

- التهديد الناجم عن القرصنة في تطبيقات الهواتف المحمولة، بما في ذلك تطبيقات مشاركة المحتوى الشائعة مثل Discord وTelegram، لا سيما في ضوء تزايد استهلاك المحتوى عبر الهواتف المحمولة، وتوافر هذه التطبيقات على نطاق أوسع من متاجر التطبيقات غير المرخصة أو مواقع تنزيل حزم Android (أي التنزيل الجانبي).

- مصادر التهديد الجديدة المحتملة التي تشكلها التقنيات الناشئة، على سبيل المثال، استخدام الذكاء الاصطناعي لإنشاء محتوى مزيف قبل الإصدار أو محتوى مزيف آخر يمكن استخدامه كطعم لتوزيع البرمجيات الخبيثة.

- دور البرامج الضارة في الجرائم المتعددة، بما في ذلك توزيع البرامج الضارة عبر الأجهزة التي تتيح الوصول إلى محتوى غير مرخص، والتي يمكن استخدامها بعد ذلك لجمع بيانات الاعتماد أو إنشاء شبكات بوتنت لأغراض خبيثة أخرى مثل الاحتيال في البث المباشر.

19. وهناك بالفعل عدد من أدوات الإنفاذ والإجراءات المتخذة التي يمكن أن تكون نقطة انطلاق لوضع أفضل الممارسات العالمية، والتي ينبغي أن تعزز المناقشات والتفاعل مع الوسطاء، وتشجعهم على اتخاذ المزيد من الإجراءات الطوعية.

20. وعلاوة على ذلك، ينبغي أن يقترن التوعية المستمرة وتثقيف المستهلكين فيما يتعلق بالضرر الناجم عن القرصنة عبر الإنترنت، حيثما أمكن، بتحذيرات مناسبة تتعلق بمخاطر البرامج الضارة.[17]

[نهاية المساهمة]

---

[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.

[17] على سبيل المثال، وجدت دراسة أجراها مكتب الاتحاد الأوروبي للملكية الفكرية في عام 2023 أن 82 في المائة من المواطنين الأوروبيين يتفقون على أن الحصول غير القانوني على المحتوى عبر الإنترنت ينطوي على خطر التعرض لممارسات ضارة مثل عمليات الاحتيال أو المحتوى غير المناسب للقاصرين. ومع ذلك، كان تجنب المصادر غير القانونية بسبب تجارب سيئة مروا بها هم أو غيرهم أقل شيوعًا بكثير (13 في المائة و19 في المائة، على التوالي). ومع ذلك، كانت هذه الأسباب أكثر إقناعًا في تحفيز المستخدمين المتعمدين للخدمات غير القانونية على التوقف عن استخدام المحتوى المقرصن عبر الإنترنت (31 في المائة و29 في المائة على التوالي). انظر(ي): 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.