الإنتربول

طرائق القرصنة الرقمية

مشروع I-SOP

الجرائم المرتكبة عبر الإنترنت التي تستهدف المستهلكين والحكومات والقطاعات الإبداعية.

أيلول/سبتمبر 2023

تتعلق القرصنة الرقمية أو المرتكبة عبر الإنترنت بانتهاكات حقوق الملكية الفكرية وتتمثل في الوصول إلى محتوى رقمي مثل البرمجيات والموسيقى والمسلسلات التلفزيونية والأفلام وألعاب الفيديو والقصص الكاريكاتورية المصورة على الإنترنت (الويب كوميكس) والكتب و/أو تنزيلها و/أو توزيعها بشكل غير قانوني.

ولهذه الجريمة عواقب اقتصادية خطيرة، إذ إنها تستتبع خسائر مالية على القطاعات الإبداعية وخسائر في الإيرادات الضريبية على السلطات الحكومية. وهي تعرّض أيضا المستهلكين لمخاطر أمنية مثل البرمجيات الضارة أو الفيروسات أو سرقة الهوية أو الوقوع على محتوى غير لائق.

7 طرائق بارزة للقرصنة الرقمية:

التطبيقات المزورة

أضحت التطبيقات المزورة طريقة القرصنة الرقمية التي أفادت أجهزة الشرطة والجهات الفاعلة في القطاع الخاص بأنها الأوسع انتشارا من بين طرائق القرصنة الرقمية الناشئة. وهي تتيح للمستخدمين بث أو تنزيل محتوى محميّ بحقوق الطبع والنشر وذلك بدون الحصول على الترخيص أو الإذن اللازم. ويمكن الوصول إلى هذه التطبيقات على نطاق واسع لأنها مصممة للعمل على أنظمة تشغيل الأجهزة المحمولة أو منصات التلفزيون الذكية الأكثر شيوعا.

سرقة محتوى قبل نشره

أدت جائحة كوفيد-19 إلى حدوث زيادة حادة في أشكال الترفيه الرقمي المنزلي. واستغل القراصنة الرقميون هذا التحول لسرقة محتوى ونشره على منتديات شتى أو بيعه على مواقعهم الإلكترونية ومنصات إلكترونية ووسائل تواصل اجتماعي مختلفة. وإتاحة المحتوى قبل إصداره رسميا يسبب أضرارا مالية كبيرة للمبدعين والمنتجين والمستثمرين.

مقدمو خدمة الاستضافة الخارجية

الاستضافة الخارجية تعني أن الخادم يقع في بلد يختلف عن البلد الذي تجري فيه أنشطة المؤسسة. والطبيعة المجهولة للاستضافة وضعف القوانين المتعلقة بالملكية الفكرية في بلد التسجيل تسهّل أنشطة القرصنة.

الحصول على نسخة من محتوى بث تدفقي (STREAM RIPPING)

المقصود من استنساخ محتوى من البث التدفقي هو استخراج أو التقاط محتوى صوتي أو فيديو من منصة بث تدفقي وتحويله إلى ملف قابل للتنزيل. ويتيح ذلك للمستخدمين الاستماع إلى المحتوى أو مشاهدته بشكل غير قانوني بدون إنترنت أو تشاركه عبر أجهزة متعددة بدون الحصول على الإذن اللازم. ولهذه الظاهرة ضرر خاص على قطاع الموسيقى وأصحاب الحقوق.

مقدمو خدمات تخزين الملفات وتشاركها (CYBERLOCKERS)

Cyberlockers هم مقدمو خدمات استضافة بيانات عبر الإنترنت توفر إطارا لتخزينها عن بعد. وخدمات cyberlockers ، على خلاف خدمات تشارك الملفات بشكل مشروع، لا تمتلك الأطر الداخلية لمنع استضافة المحتوى غير المشروع. و cyberlockers يحصّلون إيراداتهم من الإعلانات، ولاسيما من الصور والنوافذ الدعائية. ويمكن لهم أيضا جني أرباح إضافية بعرض سرعات أعلى للتنزيل.

العملات المشفرة

غالبا ما تموّل التدفقات المالية غير المشروعة الأنشطة الإجرامية الخطيرة عبر الوطنية. وبسبب حجمها يصعب على أجهزة إنفاذ القانون ملاحقة الجناة واستعادة الأصول التي تدرها الجريمة. وأصبحت المشكلة أكثر تعقُّدًا مع ظهور العملات المشفرة. ويزداد استغلال المجرمين الذين ينشئون مواقع القراصنة لهذه العملات الافتراضية بغية إخفاء حركة الأموال غير القانونية في إطار عمليات غسيل الأموال.

التكنولوجيا الناشئة

إن ميتافيرس (Metaverse)، باستنادها إلى مجموعة واسعة من التكنولوجيا بما يشمل الواقع الافتراضي (VR)، ترمي إلى تمكين الناس في العالم أجمع من الوصول إلى بيئات افتراضية ثلاثية الأبعاد متشارَكة.

وتشكل الرموز غير القابلة للاستبدال (NFTs) أصولا رقمية فريدة تمثل ملكية مقالة ما أو جزء من محتوى بعينه أو دليلا على صحتهما. وتستضيفها منصات لا مركزية مثل blockchain ويزداد استخدامها في الجرائم السيبرية.

وتطرح NFTs وMetaverse سلسلة من المشاكل، أبرزها انتهاك الملكية الفكرية. وعلى وجه التحديد، يمكن للمستخدمين تحميل محتوى بصري أو محتوى إعلامي غير مأذون فيه على هذه المنصات بدون إجراء أي تحقق بواسطة برمجيات تصفية المحتوى أو التعرف على الصور.

الإنتربول

مشروع I-SOP

(وقف القرصنة على الإنترنت)

أُطلق مشروع I-SOP في عام 2021 ردّا على التهديد المتزايد الذي تشكله القرصنة الرقمية. وهذا المشروع الذي يمتد خمس سنوات يساهم في التوعية بالجرائم التي تمس الملكية الفكرية، وتحسين تبادل المعلومات، والمساعدة في معالجة القضايا عبر الوطنية، وبناء قدرات أجهزة إنفاذ القانون.

بالتعاون مع:

Ministry of Culture,
Sports and Tourism
Republic of Korea