تحذير أمني: قراصنة يستغلون "Spotify" لنشر الفيروسات عبر روابط خادعة

حذر خبراء الأمن السيبراني من تطور أساليب قراصنة الإنترنت الذين أصبحوا يستغلون منصات ذات سمعة طيبة مثل "Spotify" لتوزيع البرامج الضارة والفيروسات، وفقًا لتقرير نشرته موقع "إنفوباي" الإخباري، يستخدم المجرمون قوائم التشغيل ووصف "البودكاست" على المنصة لإخفاء الروابط الضارة، مستهدفين جذب المستخدمين عبر وعود بتنزيلات مجانية لمحتوى متميز.

وباستغلال تحسين محركات البحث (SEO)، يتمكن القراصنة من خداع الضحايا عبر عرض روابط تبدو شرعية في نتائج البحث على غوغل، مما يدفع المستخدمين إلى تنزيل برامج مقرصنة أو ملفات مصابة تحتوي على برامج إعلانية أو برامج ضارة أكثر خطورة.

وقد لجأ مجرمو الانترنت إلى هذه الطريقة بعد تشديد سياسات محركات البحث ضد المحتوى غير القانوني، حيث كانوا يعتمدون سابقًا على مواقع وهمية ورسائل بريد الكتروني احتيالية وروابط في أوصاف مقاطع الفيديو على يوتيوب.

وتعتمد الاستراتيجية الجديدة على إنشاء قوائم تشغيل أو حلقات بودكاست بعناوين جذابة مرتبطة بمحتوى شائع مثل ألعاب الفيديو أو البرامج أو الكتب الصوتية، يتم بعد ذلك إدراج روابط في أوصاف هذه القوائم توهم المستخدمين بفرصة الحصول على تنزيلات مجانية لبرامج متميزة أو كتب الكترونية أو عملات افتراضية لألعاب مثل "فورت نايت".

وعندما يبحث المستخدم عن نسخة "مقرصنة" لبرنامج ما، قد تظهر له نتائج بحث تؤدي إلى صفحات على "Spotify"، مما يخلق شعوراً زائفاً بالأمان، وبالنقر على الروابط الموجودة في الوصف، يتم توجيه الضحية إلى مواقع وهمية حيث يتم حثه على تنزيل ملفات مصابة.

وكشف باحثون في شركة الأمن السيبراني "ESET" عن حالات عديدة لهذه الاستراتيجية، حيث تؤدي الروابط على "Spotify" إلى تنزيل ملفات "MSI" تم تحليلها وتبين احتواؤها على برامج ضارة، وتشمل هذه البرامج أدوات لإغراق الأجهزة بالإعلانات المنبثقة، وإعادة التوجيه إلى مواقع مشبوهة، وحتى تنزيل برامج أكثر خطورة مثل أحصنة طروادة المصرفية أو برامج تسجيل ضغطات المفاتيح التي تسرق المعلومات الشخصية وبيانات الاعتماد.

ويأتي هذا التطور في أساليب القرصنة كتذكير بأهمية الحذر عند النقر على الروابط، خاصة تلك التي تعد بتنزيلات مجانية لمحتوى متميز، حتى لو كانت منصات موثوقة مثل "Spotify".