

المجرم «الذكي»

عندما تقم تقنيات الذكاء الاصطناعي في الأيدي الخطأ

تؤدي تقنيات الذكاء الاصطناعي إلى تفاقم المشكلات والمخاطر الأمنية الحالية، وتساهم في خلق مساحة جديدة للمجرمين من أجل العبث في مساحة الفضاء الافتراضي، كالتالي:



باستخدام
برنامج مثل
ChatGPT

لا تحتاج إلى خبرة
تقنية عالية في
برامج التشفير

بطريقة
سريعة

من خلال أتمتة (Automation)
وتفعيل عملية كتابة نصوص
البرمجيات الخبيثة

عبر إنشاء
برمجيات
ضارة

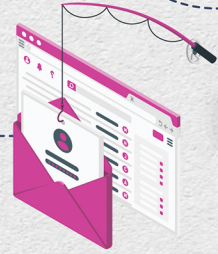
تنفيذ هجوم
إلكتروني

التصيد
الاحتمالي

كتابة محتوى الهندسة
الاجتماعية بطريقة
أكثر فعالية

صياغة المحتوى المستخدم
في الاتصالات والنصوص
ورسائل البريد المخادعة

جعل الاتصالات تبدو أكثر
احترافية لخلوها من الأخطاء
الإعلانية والنحوية



سرقة
البيانات

فك 51% من كلمات السر
الشائعة في غضون دقيقة
و71% منها في يوم واحد!

فرص عالية جداً
لاختراق كلمة المرور
في وقت قياسي

اختراق برامج
وأنظمة

تسليط الضوء للمهاجم على الكثير
من الثغرات الأمنية والعيوب في
البرامج بهدف استغلالها

تستفيد شركات الحماية والأمن السيبراني
من هذه الميزة للعثور على نقاط الضعف
ومعالجتها قبل استغلالها



تحليل البيانات
المسرودة

تقليل الوقت الذي
يستغرقه المهاجم
لاستغلالها

تبسيط عملية البحث عن
المعلومات المهمة في قواعد
البيانات الضخمة المسروقة

استخدام الروبوتات
لاستقاط البيانات الحساسة
التي تُباع في «الدارك ويب»



جرائم
أخرى

إنشاء
مواقع
اختيالية

نشر
البريد
العشوائي

فبركة صور
تحاكي
الواقع

إنشاء مقاطع
فيديو وصوت
مزيفة

