المجرم «الذكي»

عندما تقع تقنيات الذكاء الاصطناعي في الأيدي الخطأ

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

تنفيذ هجوم إلكتروني

- عبر إنشاء برمجيات ضارّة
- من خلال أتمتة (Automation) وتفعيل عملية كتابة نصوص البرمجيات الخبيثة
- بطريقة سريعة
- لا تحتاج إلى خبرة تقنية عالية في برامج التشفير
- باستخدام برنامج مثل ChatGPT

التصيّد الاحتيالي

- جعل الاتصالات تبدو أكثر احترافية لخلوّها من الأخطاء الإملائية والنحوية
- صياغة المحتوى المستخدم في الاتصالات والنصوص ورسائل البريد المخادعة
- كتابة محتوى الهندسة الاجتماعية بطريقة أكثر فعاليّة

سرقة البيانات

- فرص عالية جداً لاختراق كلمة المرور في وقت قياسيّ
- فكّ 51% من كلمات السرّ الشائعة في غضون دقيقة و71% منها في يوم واحد!

اختراق برامج وأنظمة

- تستفيد شركات الحماية والأمن السيبراني من هذه الميزة للعثور على نقاط الضعف ومعالجتها قبل استغلالها
- تسليط الضوء للمهاجم على الكثير من الثغرات الأمنية والعيوب في البرامج بهدف استغلالها

تحليل البيانات المسروقة

- استخدام الروبوتات لالتقاط البيانات الحسّاسة التي تُباع في «الدارك ويب»
- تبسيط عملية البحث عن المعلومات المهمّة في قواعد البيانات الضخمة المسروقة
- تقليل الوقت الذي يستغرقه المهاجم لاستغلالها

جرائم أخرى

- إنشاء مقاطع فيديو وصوت مزيّفة
- فبركة صور تحاكي الواقع
- نشر البريد العشوائي
- إنشاء مواقع احتيال

إعداد
ياسر الموسوي، جنان الخطيب