متسللون يخترقون أنظمة شركة "أوبن إيه آي" ويكشفون محادثات داخلية

تمكّن متسللون من اختراق أنظمة شركة "أوبن إيه آي" التي طورت برنامج الدردشة الذي يعمل بالذكاء الاصطناعي "شات جي بي تي"، وفقاً لتقرير نشرته صحيفة "نيويورك تايمز".

وأوضح التقرير أن "المهاجمين السيبرانيين تمكنوا من الإطلاع على المحادثات الداخلية وربما سرقوا تفاصيل حول تصميم منتجات الذكاء الاصطناعي الخاصة بالشركة. لكن التقرير قال إن الشركة لم تبلغ سلطات إنفاذ القانون بشأن الاختراق".

وأفادت الصحيفة بأن "الحادث شهد قيام أحد المتسللين بسحب تفاصيل من المناقشات في منتدى داخلي بين موظفي "أوبن إيه آي" حول التقنيات التي تعمل عليها الشركة، لكنهم لم يصلوا إلى الأنظمة التي يتم فيها بناء وإيواء منتجات أوبن إيه آي"، حسبما ذكر التقرير.

ووجدت الشركة الأميركية نفسها في طليعة الطفرة الأخيرة في مجال الذكاء الاصطناعي، والتي أثارها إطلاق روبوت المحادثة "شات جي بي تي"، في أواخر عام 2022.

ومنذ ذلك الحين، بدأت العديد من كبرى شركات التكنولوجيا في العالم في الانتقال إلى هذا القطاع، حيث حدد الكثير من الخبراء أيضاً الذكاء الاصطناعي التوليدي باعتباره الابتكار الرئيسي لهذا الجيل.

ووفقاً للتقرير، أخبر المسؤولون التنفيذيون في أوبن إيه آي الموظفين ومجلس إدارة الشركة عن الاختراق في أبريل (نيسان) من العام الماضي، لكنهم لم يعلنوا عن التفاصيل لأنه لم تتم سرقة أي بيانات للعملاء أو الشركاء.

وقال التقرير إن: "الشركة لم تبلغ أيضاً وكالات إنفاذ القانون الأميركية بالحادث، لأنها اعتقدت أن المتسلل كان فرداً خاصاً ليست له علاقات معروفة بحكومة أجنبية".

وحذر الدكتور إيليا كولوتشينكو، خبير الأمن السيبراني والرئيس التنفيذي لشركة ImmuniWeb الأمنية، من أن "الهجمات على شركات الذكاء الاصطناعي من المرجح أن تستمر وتزداد، بالنظر إلى الأهمية المتزايدة للتكنولوجيا".

وقال: "رغم أن (أوبن إيه آي) لم تؤكد بعد تفاصيل الحادث، فإن هناك احتمالاً قوياً بأنه قد وقع بالفعل... وهو وليس الوحيد".

وتابع: "أصبح السباق العالمي للذكاء الاصطناعي مسألة تتعلق بالأمن القومي للعديد من البلدان؛ ولذلك، فإن مجموعات الجرائم الإلكترونية المدعومة من الدول تستهدف بشدة بائعي الذكاء الاصطناعي، من الشركات الناشئة الموهوبة إلى عمالقة التكنولوجيا مثل (غوغل) أو أوبن إيه آي".