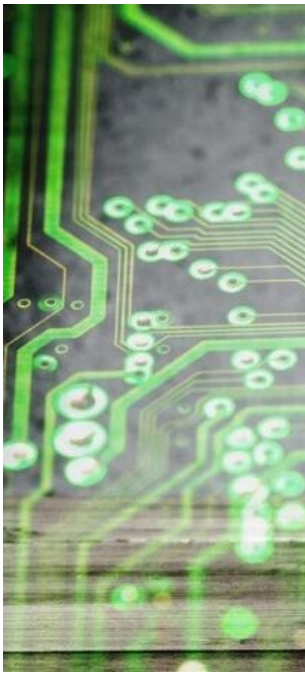
اختراق خلف القناع... كيف تسللت طهران إلى نخب إسرائيل الإلكترونية؟



كشف تقرير أمني جديد عن تورط مجموعة قرصنة إلكترونية مدعومة من الحكومة الإيرانية، على صلة بالحرس الثوري، في تنفيذ حملة تصيّد احتيالي متطورة استهدفت صحفيين إسرائيليين بارزين، إلى جانب باحثين وخبراء في مجال الأمن السيبراني وأكاديميين في علوم الحاسوب داخل إسرائيل.

وذكر تقرير من شركة "تشيك بوينت"، أمس الأربعاء، وتابعته "المطلع"، أنها:"في بعض هذه الحملات، تواصَل مهاجمون مع متخصصين إسرائيليين في التكنولوجيا والأمن السيبراني، متظاهرين بأنهم مساعدون وهميون لمديرين تنفيذيين أو باحثين في مجال التكنولوجيا، عبر رسائل بريد إلكتروني ورسائل واتساب".

وأضاف أن:"القراصنة وجّهوا الضحايا الذين تواصلوا معهم إلى صفحات تسجيل دخول جيميل أو دعوات غوغل ميت مزيفة".

وللمجموعة الإيرانية تاريخ طويل في تنظيم هجمات الهندسة الاجتماعية باستخدام أساليب مُضللة،

والتواصل مع الأهداف على منصات مُختلفة مثل "فيسبوك" و"لينكدإن' باستخدام شخصيات وهمية لخداع الضحايا وحملهم على نشر برامج ضارة على أنظمتهم.

وأفادت "تشيك بوينت" أنها:"رصدت موجة جديدة من هذه الهجمات بدأت في منتصف يونيو/حزيران 2025 عقب اندلاع حرب الاثني عشرة يومياً بين إسرائيل وإيران، واستهدفت إسرائيليين باستخدام أدوات وهمية تُشبه الاجتماعات، إما عبر رسائل البريد الإلكتروني أو رسائل "واتساب" المُصممة خصيصاً للأهداف. ويُعتقد أن الرسائل مُصممة باستخدام أدوات الذكاء الاصطناعي".

قراصنة إيران يستغلون الحرب

واستغلت إحدى رسائل "واتساب"، التي رصدتها الشركة، التوترات الجيوسياسية الحالية بين البلدين لإقناع الضحية بالانضمام إلى اجتماع، مدّعيةً حاجتها إلى مساعدتهم الفورية في نظام كشف التهديدات القائم على الذكاء الاصطناعي لمواجهة تصاعد الهجمات الإلكترونية التي تستهدف إسرائيل منذ 12 يونيو/حزيران.

وبمجرد أن يبني المهاجمون علاقة وطيدة خلال المحادثة، ينتقل الهجوم إلى المرحلة التالية، من خلال مشاركة روابط تُوجّه الضحايا إلى صفحات مزيفة، قادرة على جمع بيانات دخول حسابات "غوغل" الخاصة بالضحايا.

وأفادت "تشيك بوينت"، بأنه:"قبل إرسال رابط التصيد الاحتيالي، يطلب المهاجمون من الضحية عنوان بريده الإلكتروني. ثم يُملأ هذا العنوان مسبقاً في صفحة التصيد الاحتيالي لبيانات الدخول لزيادة المصداقية ومحاكاة مظهر عملية مصادقة غوغل شرعية".

وتُحاكي مجموعة أدوات التصيد الاحتيالي صفحات تسجيل الدخول المألوفة، مثل تلك التي تُقدمها "غوغل"، باستخدام تقنيات الويب الحديثة، كما تستخدم اتصالات فورية لإرسال البيانات المسروقة، ويسمح تصميمها بإخفاء شيفرتها عن أي تدقيق إضافي.