مملكة آل سعود أبرزهم.. إبرام عقود تجسس إسرائيلية مع دول خليجية

التغيير

كشفت صحيفة إسرائيلية النقاب عن عقود تجسس أبرمتها شركة NSO التكنولوجية الواقعة بـ"هرتسليا" القريبة من تل أبيب، مع عدد من الدول الخليجية أبرزها مملكة آل سعود، خلال السنوات الأخيرة، تقدر بمئات ملايين الدولارات.

وذكرت صحيفة "هآرتس" العبرية، أن عقود إسرائيل مرتبطة مع مملكة آل سعود والبحرين وسلطنة عُمان والإمارات، وأن تل أبيب تشجع بشكل رسمي شركة NSO التي يتركز عملها على الاستخبارات الإلكترونية، من أجل بيعها برنامج "بيغاسوس" للدول الخليجية، لكي تتمكن من التجسس على المعارضين لأنظمتها وخصومها السياسيين.

ولفتت الصحيفة إلى أن برنامج "بيغاسوس 3" الذي طورته الشركة، يستطيع اختراق الهواتف النقالة، ونسخ محتوياتها واستخدامها عن بعد، من أجل التصوير والتسجيل، منوهة إلى أن طواقم بالشركة تعمل

على رصد الثغرات، بعد التعديلات المتسارعة التي تجريها شركات الهواتف الخلوية.

وزعمت الصحيفة أن "الشركة تعمل فقط مع جهات رسمية في الدول وعبر عقود رسمية، وتل أبيب التي كانت متحمسة لقدرات الشركة، توسطت بينها وبين دول عربية في المنطقة، وشارك ممثلون رسميون إسرائيليون في لقاءات بين رؤساء أجهزة الاستخبارات في دول عربية وبين رؤساء الشركة، علما بأن عددا من هذه اللقاءات تم في إسرائيل".

وأكدت أن NSO عملها على تشغيل طاقم يعمل بشكل خاص مع دول الخليج من خلال عقود رسمية، ولجميع موظفيها توجد جوازات سفر أجنبية، وهذا هو القسم الأكثر ربحا في الشركة؛ وهو يكسب مئات ملايين الدولارات في السنة.

وذكرت أن لكل دولة في الخليج يوجد لها لقب يتكون من الحرف الأول من اسمها واسم سيارة؛ مملكة آل سعود مثلا، تسمى في وثائق الشركة "سوبارو" والبحرين "بي.أم.في" والأردن "جاغوار"، منوهة إلى أن "التوجيهات في الشركة، بعدم استخدام أسماء الدول، بل فقط اللقب".

وذكرت أن ممثلي الشركة، اعتادوا خلال اللقاءات مع دول الخليج، على استعراض قدراتهم في اختراق الهواتف، في حين بلغت قيمة إحدى صفقات عقود المبيعات ربع مليار دولار، مؤكدة أن NSO تستثمر "جهودا كبيرة في الخليج بسبب الجيوب العميقة لإمارات النفط، فالمنتج الذي يباع في أوروبا بعشرة ملايين دولار، يمكن بيعه في الخليج بعشرة أضعاف".

وبينت أن "الرزمة الأساسية للشركة، تمكن فقط من اختراق هواتف في الدولة المشترية، والتي يوجد لها رقم محلي يشمل 25 "تصريحا" لما سمي بلغة الشركة "عملاء"، يسيطرون على الهواتف.

كما أن مشغل المعلومات في الدولة التي اشترت برنامج التجسس، مزود برقم هاتف في داخل البرنامج، وبذلك يمكنه اختراق الجهاز خلال بضع ساعات، وبعد ذلك يمكن للمشغل أن ينسخ كل محتويات الجهاز.

ونبهت صحيفة "هآرتس" إلى أن الشركة الإسرائيلية "استأجرت إسرائيليين عملوا سابقا في الأجهزة الأمنية، لتوفير تحليل لمعلومات استخبارية إلى جانب خدمة اختراق الهواتف، وذلك إزاء الصعوبات في دول الخليج التي تتمثل بالحصول على معلومات نوعية من إجمالي الرسائل والملفات.

وأشارت إلى أن الشركة المصنعة لبرنامج التجسس، "يمكنها السيطرة على البرنامج عن بعد بشكل كامل، كما يمكنها الدخول ورؤية أي معلومات تم جمعها في أي وقت".

ونوهت إلى أن شهادات عاملين في الشركة، تؤكد أن "الرقابة معدومة، ولا توجد للشركة قدرة على المتابعة بصورة معمقة للأهداف الاستخبارية لجهات مختلفة، بسبب قيود قانونية ولغوية وقيود مصلحية".

وأفادت بأنه من أجل منع تسرب معلومات، هناك خمس دول "ينتحر العميل" عندما يصل إليها وهي: إسرائيل، إيران، روسيا، الصين والولايات المتحدة. أي إنه في حال قام شخص من مملكة آل سعود تم اختراق هاتفه بالهبوط في موسكو، فإن الهاتف يشخص بأنه وصل إلى روسيا ويمسح العميل من الجهاز، والهدف؛ هو عدم التورط مع دول لا تتسامح بالتجسس على أراضيها مثل الصين والولايات المتحدة أو الكشف عن أسرار لدول معادية.

وفي تحقيق سابق نشرته "هآرتس" في 2018، كشف أن "الشركة أجرت مفاوضات لبيع برنامج تجسس لآل سعود، وبعد قتل الصحفي السعودي جمال خاشقجي، قيل إن مخابرات آل سعود استخدمت تكنولوجيا "NSO" لملاحقة معارضي النظام، وحينها احتج الكثير من موظفي الشركة على الاستخدام غير الأخلاقي لهذه التكنولوجيا".

وسبق أن نشر موقع "سيتيزين لاب" مركز أبحاث تابع لجامعة تورونتو، في كندا، تحقيقاً يكشف فيه عن تعرض هاتف رئيس مكتب صحيفة "نيويورك تايمز" في بيروت، بن هابارد، لهجوم سيبراني عبر برنامج تجسس يدعى "بيغاسوس" تنتجه مجموعة "إن إس أو" الإسرائيلية، وهي شركة متخصصة بتكنولوجيا المراقبة.

ويشير التحقيق إلى أن الرابط الذي أرسل إلى هاتف هابارد، مصدره موقع يستخدمه أحد مشغلي "بيغاسوس" يدعوه فريق التحقيق في "سيتيزين لاب" بـ"مملكة" (KINGDOM)، والذي يعتقد الفريق أنه مرتبط بنظام آل سعود.

ويظهر التحقيق أنه تم منذ عام 2016، توثيق استخدام "بيغاسوس" للتجسس على عدد من الصحافيين والمدافعين في مجال حقوق الإنسان، والناشطين في المجتمع المدني.

وأكدت تقارير سابقة صادرة عن "سيتيزان لاب" ومنظمة العفو الدولية، في عام 2018 أن المشغل "مملكة" كان يستهدف معارضين وناقدين للمملكة.

وسبق أن أكد تقرير نشرته منظمة العفو الدولية في 31 تموز/ يوليو عام 2018، أن أحد موظفي المنظمة قد تعرض لهجوم من قبل بيغاسوس، إلى جانب ناشط سعودي يعيش خارج المملكة، اتضح لاحقاً أنه يحيى العسيري المقيم في بريطانيا.

وفي تشرين الأول/ أكتوبر من العام ذاته، نشر "سيتيزين لاب" تقريراً يكشف تعرض المعارض السعودي المقيم في كندا، عمر عبد العزيز إلى هجوم عبر "بيغاسوس".

وكان عبدالعزيز، خلال هذه الفترة، على تواصل وثيق مع الصحافي السعودي جمال خاشقجي، الذي قتل في عام 2018 داخل سفارة بلاده في تركيا.

وبعد ذلك بأيام، نشر موقع "فوربز" تقريراً يكشف تعرض المعارض السعودي غانم الدوسري، بدوره، لاستهداف عبر "بيغاسوس".

وفي حال قام هؤلاء بالضغط على الرابط الذين تلقوه، كان مشغل "مملكة" ليتمكن من مراقبة جميع اتصالاتهم ونشاطاتهم الهاتفية. وقام عبدالعزيز برفع دعوة ضد شركة "إن إس أو" في إسرائيل، فيما اختار الدوسري مملكة آل سعود هدفاً لدعوته التي رفعها من المملكة المتحدة.

أما بن هابارد، فكان، قبل أن يتم تعيينه رئيساً لمكتب "نيويورك تايمز" في بيروت، يركز في تغطياته على مملكة آل سعود، لا سيما نشاطات محمد بن سلمان.

ويعود شراء المملكة لأسلحة التجسس الإلكتروني لعقد أو عقدين من الزمان، حيث كانت المملكة تركز على نشاطات الرقابة.

وقال خبراء إن نظام آل سعود متورط بشراء برامج التجسس التي يحتاجها لترسانتها من جهات خارجية، وهي نفس الطريقة التي يعتقد المحللون أن المملكة لجأت إليها لاختراق هاتف الملياردير الأمريكي جيف بيزوس.

وأجمعوا على أن ترسانة المملكة من السلاح السايبري تتكون من أدوات مشتراة من متعهدين خارجيين وتجمع ما بين أساليب التضليل الإعلامي على منصات التواصل الاجتماعي.