أليكس كين | نشر في ٢٠ نوفمبر ٢٠١٨,

برنامج تجسس إسرائيلي يساعد أنظمة دكتاتورية في الشرق الأوسط على قمع المعارضين

ترجمة وتحرير نون بوست

في بداية أغسطس/آب الماضي، تلقى عمر عبد العزيز مكالمة تحذيرية من شخص، ينبهه فيها إلى أن هاتفه قد يكون مخترقا بواسطة برمجية تجسس.

هذا المعارض السعودي البارز، والذي يعيش حاليا في المنفى قرب مدينة مونتريال الكندية، تعرض في السابق للمضايقات من قبل عملاء الحكومة السعودية، وقد وصل بهم الأمر إلى اعتقال اثنين من أشقائه في بداية الصيف. ولكن اختراق هاتفه هو شيء جديد كليا، ولذلك يريد عمر فهم كيفية حصول هذا العملية.

وبعد أيام قليلة، جلس عمر مع الشخص الذي كان قد بعث له الرسالة التحذيرية حول تعرض هاتفه للاختراق، وهو يدعى بيل ماركزاك، الباحث المتخصص في مجال برمجيات التجسس.

لقد اكتشف ماركزاك أن شخصا ما في السعودية، وهو على الأرجح يعمل لحساب الحكومة، اخترق هاتف شخص آخر في كندا، بواسطة برمجية مراقبة مصنوعة في إسرائيل، ولذلك قرر أن يقوم بأبحاث للوصول للضحية المستهدف في هذه العملية. ولهذا الغرض، طرح ماركزاك على عمر سؤالا شخصيا وغريبا: "أين تذهب كل يوم بين الخامسة والثامنة مساء"؟

قال عمر عبد العزيز أنه بشكل عام يذهب للتمرين في صالة الرياضة التابعة لجامعته خلال هذه الساعات الثلاث. وقد جاءت هذه التحركات متطابقة مع بيانات الشخص المستهدف ببرمجية التجسس، فبياناته تشير إلى أنه يغلق خدمة الإنترنت في هاتفه بين الخامسة والثامنة في المساء.

وبعد البحث في هاتف عمر، وجد ماركزاك رسالة نصية تبدو غير ذات أهمية، إلا أنه يعتقد أنها المسؤولة عن اختراق جهاز هذا المعارض السعودي. وبعد شهرين، تمكن سيتيزن لاب، وهو مركز أبحاث في جامعة تورنتو يدافع عن الحقوق الرقمية، وينشط فيه ماركزاك كباحث، من من نشر تقرير إعلامي يكشف

فيه أن هاتف عمر تعرض للاختراق بواسطة برمجية خبيثة تسمى "بيغاسوس"، مصنوعة لدى الشركة الإسرائيلية "أن أس أو غروب".

وتعد "بيغاسوس" واحدة من أكثر برمجيات المراقبة تعقيدا في العالم، وهي قادرة على اختراق هواتف آيفون وأندرويد. وحالما تتمكن من التسلل إلى الجهاز، فإن هذه البرمجية تقوم بنسخ كل أرقام الهواتف والصور والرسائل النصية، ويمكنها أيضا التنصت على المكالمات.

إلا أن عمر، الذي يقضي أيامه بين التغريد على تويتر ونشر مقاطع الفيديو في يوتيوب منددا بسياسات الحكومة السعودية، أكد أنه ليس متفاجئا بعد انكشاف هذا الأمر. ففي مايو/آيار الماضي، سافر عملاء من السعودية إلى كيبيك لإقناعه بالعودة إلى السعودية، وأخبروه أن أمامه خياران: إما أن يعود إلى وطنه ويحصل على المال في مقابل التزام الصمت، أو يتم اعتقاله في أحد المطارات وترحيله إلى السجن، وذلك بحسب تسجيلات لهذه الحوارات اطلعت عليها صحيفة "واشنطن بوست" الأمريكية.

كما بات عمر يشعر بالقلق حول سلامة أصدقائه وعائلته وباقي منتقدي السياسات السعودية، الذين قد يكونوا في خطر. وخلال الأسابيع الأخيرة، كان عمر يشعر بأن الاتصالات التي دارت بينه وبين الصحفي السعودي المغدور جمال خاشقجي، ربما تكون مراقبة من قبل الحكومة السعودية.

وهو يقول: "لم أرد أن يصاب أحد بالضرر بسبب هذا الأمر. واليوم الشعور بالذنب يقتلني، ربما كانوا يتنصتون على الحوارات التي دارت بيني أنا وجمال". ويعد عمر واحدا من قائمة متزايدة من المعارضين للدول المتنفذة في الشرق الأوسط، الذين يتم استهدافهم باستخدام برمجيات تجسس مصنوعة في إسرائيل.

إذ أن بعض الإسرائيليين المتمرسين في هذا المجال، بفضل خبرتهم الطويلة في فنون التجسس والتنصت التي كانوا يطبقونها على الفلسطينيين على مدى عقود، باتوا الآن مستعدين لبيع مهاراتهم لمن يدفع أكثر. وقد أصبحت التكنولوجيا الإسرائيلية في مجال المراقبة أداة مطلوبة أكثر من غيرها، بالنسبة للأنظمة الدكتاتورية التي تخوض حربا ضد معارضيها، من بينها المملكة العربية السعودية والبحرين والإمارات العربية المتحدة، على الرغم من أن هذه الدول لا تقيم علاقات دبلوماسية رسمية مع إسرائيل.

ويحذر النشطاء المدافعون عن الخصوصية من أن هذه التعاملات التجارية الجديدة بين الشركات الإسرائيلية الخاصة والوكالات الحكومية المتنفذة، بصدد إرساء مناخ يسمح للأنظمة القمعية بشراء برمجيات التجسس الفعالة، واستخدامها ضد أي شخص في أي مكان، وهو ما يهدد حرية التعبير والمعارضة في العالم.

ويقول إيدن أومانوفيتش، الذي يشرف على دراسة سياسات مراقبة الدول لمواطنيها، في المنظمة الدولية لحماية الخصوصية: "إن هذه التقنيات مطورة في واحدة من أكثر القوى السيبرانية تقدما في العالم، بالاعتماد على قوى تجسسية هي الأقوى، وكان أمامهم الشعب الفلسطيني لتطبيق هذه التقنيات عليه، والآن بات بإمكانهم إرسالها إلى بلدان تفتقد لعلوية القانون، وهي تستخدم بالأساس لاستهداف المدافعين عن حقوق الإنسان والمعارضين."

بدون أية ضوابط

بداية من أغسطس/آب 2016 وإلى غاية أغسطس/آب 2018 قام ماركزاك وزملاؤه الباحثين بمسح شبكة الإنترنت بحثا عن الخوادم المرتبطة بنوع محدد من تكنولوجيا التجسس المطورة في إسرائيل. وفي يوليو/تموز الماضي، اكتشفوا أن واحدا من هذه الخوادم يتواجد في المملكة السعودية، وقد استخدم لاختراق هاتف شخص في كندا، باستخدام برمجية تجسس صنعت في إسرائيل.

وبما أن هذا النوع من البرمجيات يباع فقط للحكومات، فقد رجح ماركزاك أن من نفذوا هذه العملية

يعملون لصالح الحكومة السعودية. وفي أغسطس/آب، نشرت منظمة العفو الدولية تقريرا حول استهداف أحد باحثيها، إلى جانب ناشط سعودي، باستخدام هذه البرمجية الخبيثة. ولكن هذه ليست المرة الأولى التي يكشف فيها الباحثون برمجيات تجسس إسرائيلية تستخدم من قبل أنظمة قمعية.

لقد حققت صناعة التجسس في إسرائيل تقدما غير مسبوق، إذ أن هذا الكيان الذي لا تزيد مساحته عن ولاية نيو جيرسي، يتواجد فيه أكبر عدد من شركات التجسس مقارنة بعدد سكانه. وبحسب تقرير صدر في 2016 من المنظمة الدولية لحماية الخصوصية، فإن منتجات الصناعة الإسرائيلية تستخدم في عشرات البلدان، من الولايات المتحدة إلى كولومبيا، ومن السودان إلى أذربيجان.

ولذلك يقول إيران ليرمان، العقيد المتقاعد الذي خدم في مناصب رفيعة في المخابرات العسكرية الإسرائيلية لأكثر من 20 عاما: "نحن نعتبر الأفضل في هذا المجال."

إلا أن هذا النجاح ليس وليد الصدفة، بل هو نتاج للتعاون الوثيق بين الجيش الإسرائيلي وشركات القطاع الخاص، والعقود الطويلة التي قضتها إسرائيل في بناء قدراتها التجسسية، من أجل مراقبة الفلسطينيين الذين تحتلهم، والدول المجاورة المعادية لها.

ومن أبرز الجهات التي ساهمت في التطور التقني الإسرائيلي، هنالك الوحدة 8200، وهي النسخة الإسرائيلية من وكالة الأمن القومي في الولايات المتحدة، وتعد أكبر وحدة مخابرات عسكرية في إسرائيل. ويتم تجنيد أفضل الطلبة للخدمة في الوحدة 8200، أين يتعلمون كيفية القرصنة والتجسس على الجميع، من العملاء الإيرانيين إلى المراهقين الفلسطينيين.

وعندما يغادرون الخدمة العسكرية، فإن أغلب من عملوا مع الوحدة 8200 يذهبون للعمل في قطاع التكنولوجيا الذي يشهد انتعاشة في إسرائيل. وبعض المنتمين سابقة للوحدة 8200، بعد انضمامهم لشركات القطاع الخاص، يعودون للعمل بالشراكة مع الجيش، إلا أنهم يتقاضون أجورا أعلى بكثير، لأن شركاتهم تكون قد حصلت على عقود مربحة جدا مع وزارة الدفاع.

وحول هذا الأمر، يقول أحد الجنود السابقين في الوحدة 8200، الذي تحدث لموقع "فايس نيوز" حول فترة خدمته العسكرية بشرط عدم الكشف عن هويته: "إن أمي كانت تقول لي إن هذه الوحدة هي أكبر شركة تقنية متطورة في إسرائيل".

ويشار إلى أن العديد من شركات تقنيات التجسس البارزة في إسرائيل تربطها علاقات مع الوحدة 8200. وعلى سبيل المثال، فإن "سيلبرايت"، الشركة التي اشتهرت باختراقها لأجهزة آيفون المحمية بكلمات سر، وهي مهارة تقوم بتسويقها لوكالات أمنية حكومية، تقوم بانتداب موظفيها من هذه الوحدة.

كما أن شركة "مير غروب"، التي تبيع منتجات التجسس والمراقبة لعديد البلدان حول العالم، يديرها نير ليمبرت، رئيس مجلس إدارة رابطة خريجي الوحدة 8200. وهنالك أيضا شركة "كومفيرس"، التي يقول عنها الجنرال الإسرائيلي المتقاعد هانان غيفين، المستشار لدى شركات التقنية، أنها تأثرت بشكل مباشر بالتكنولوجيات المتطورة في الوحدة 8200.

كما أنه من السهل العثور على الجنود السابقين في هذه الوحدة، ضمن شركة "أن أس أو غروب"، التي أسسها ضباط سابقون في الجيش الإسرائيلي. واليوم تعد "أن أس أو غروب" الشركة الأسوأ سمعة بين عمالقة تقنيات المراقبة والتجسس. والطرف المالك لغالبية الأسهم في هذه الشركة هو صندوق إدارة استثمارات خاصة، مرتبط بمؤسستي بلاكستون وغولدمان ساكس.

وتفرض شركة "أن أس أو غروب" على زبائنها من الحكومات مبالغ تصل إلى 650 ألف دولار، في مقابل تمكينها من اختراق 10 هواتف أبل أو أندرويد، إلى جانب دفع 500 ألف دولار كرسوم تركيب أجهزة المراقبة، وذلك بحسب وثائق تابعة للشركة اطلعت عليها صحيفة نيويورك تايمز.

وقد أكدت هذه الشركة في عدة مناسبات أن منتجاتها تباع بشكل حصري للحكومات، وأنها تستخدم لتعقب المجرمين والإرهابيين. كما تدعي "أن أس أو غروب" إنشاء لجنة أخلاقية مهمتها ضمان استخدام منتجاتها لأغراض قانونية. وقد ذكرت هذه الشركة في مراسلة لمنظمة العفو الدولية: "إن "أن أس أو غروب" تطور التقنيات السيبرانية لتمكين الوكالات الحكومية من كشف وإفشال المخططات الإجرامية والإرهابية. ومنتجاتنا مصممة للاستخدام بشكل حصري في التحقيقات والتوقي من الجرائم والإرهاب، وكل استخدام لها بشكل مخالف لهذه الأهداف يعد انتهاكا لسياستنا والعقود القانونية والقيم التي تتبناها الشركة."

إلا أن مركز الأبحاث "سيتيزن لاب"، ومنظمة العفو الدولية، قاما بكشف برمجية "بيغاسوس"، التي استخدمها زبائن "أن أس أو غروب" لاستهداف المعارضين والصحفيين في أنحاء العالم، من خلال تحويل هواتفهم إلى أجهزة متنقلة للتجسس عليهم.

وفي سنة 2016، اكتشف "سيتيزن لاب" أن برمجية "بيغاسوس" اخترقت هاتف أحمد منصور، الناشط الديمقراطي في الإمارات العربية المتحدة. ويقضي هذا الرجل حاليا حكما بالسجن لمدة 10 سنوات، لأنه نشر على مواقع التواصل الاجتماعي انتقادات للسلطات الإماراتية.

لم تكن هذه هي المرة الوحيدة التي باعت فيها "أن أس أو غروب" برمجياتها إلى الإمارات، الدولة التي لا تتسامح مع أي رأي معارض. إذ أن إحدى الشركات الفرعية المنضوية تحتهاوهي "سيركلز تكنولوجيز"، ساعدت عنصرا أمنيا إماراتيا على اختراق هاتف عبد العزيز الخميس، الصحفي الذي يكتب بشكل دائم حول السياسة في الخليج العربي، وذلك بحسب مراسلات نشرت في دعوى قضائية مرفوعة ضد "أن أس أو غروب" اطلع عليها موقع "فايس نيوز"، وكانت "نيويورك تايمز" هي أول من كشف عن هذه المراسلات.

وقد توصل مركز "سيتيزن لاب" أيضا إلى أن اثنين من الموظفين الذين يبدو أنهم استخدموا برمجية "أن أس أو غروب" متواجدون في الإمارات، ويبدو أن هنالك واحدا آخر في البحرين وآخر في السعودية.

وإلى جانب عمر عبد العزيز، فإن الوكالة السعودية التي تستخدم برمجية "بيغاسوس" لاحقت أيضا محررا في منظمة العفو الدولية، وهو يحيى عسيري، الذي كان يدافع عن السعوديات المعتقلات بسبب نشاطهن في الدفاع عن المرأة، ونشطاء حقوق الإنسان في السعودية، وفقا لما أورده "سيتيزن لاب".

ويقول مازن مصري، وهو عضو في الفريق القانوني الذي رفع الدعوى القضائية ضد "أن أس أو غروب" في إسرائيل وقبرص: "إن هذه الشركة أصبحت الوجهة المفضلة لكل الأنظمة التي تنتهك حقوق الإنسان. وكلما كانت هذه الأنظمة مستعدة لدفع الثمن، بإمكانها الحصول على البرمجيات والتجسس على أي شخص يمتلك هاتف ذكي".

ولكن "أن أس أو غروب" ليست الشركة الوحيدة التي تروج منتجاتها لدى دول الخليج. إذ أن البحرين أيضا يبدو أنها استخدمت برمجية من إنتاج شركة "سيلبرايت" لاختراق الهواتف الجوالة. وقد كشف موقع "إنترسبت" الأمريكي أن هذه البرمجية استخدمت لاختراق هاتف الناشط البحريني محمد السنكيس، الذي تعرض للتعذيب والسجن، بتهمة معارضة نظام الحكم، وقد استندت السلطات جزئيا إلى الأدلة التي تم الحصول عليها من هاتفه بعد اختراقه.

وحول هذا الأمر يقول ماركزاك الباحث في مركز "سيتيزن لاب": "عندما تبيع هذه هذه الشركات تقنياتها لدول مثل البحرين والسعودية، التي تعتبر نشر انتقادات على تويتر جريمة خطيرة، فإن منتجات هذه الشركات، مهما كان اسمها، "أن أس أو غروب" أو "سيلبرايت"، ستستخدم لانتهاك حقوق الإنسان."

شركة أخرى إسرائيلية اسمها "فيرينت سيستمز"، باعت تقنيات مراقبة وتجسس للبحرين، هذه الدولة

الخليجية الصغيرة ذات الأغلبية الشيعية، والتي يحكمها قادة من السنة بسياسة القبضة الحديدية. وقد ذكرت صحيفة هآرتس الإسرائيلية أن "فيرينت سيستمز" باعت للبحرين أنظمة تستخدم عادة في مراكز المراقبة، إلى جانب نظام آخر لجمع المعلومات من شبكات التواصل الاجتماعي.

وقد سافر بعض الإسرائيليين إلى هذه المملكة لتدريب ضباط أمن بحريين حول كيفية استخدام أنظمة المراقبة. ونشير إلى أن وزارة الدفاع الإسرائيلية، وهي الجهة التي تمنح التراخيص لتصدير أدوات المراقبة، رفضت الإجابة عن طلبنا بالتعليق على هذه المسألة. كما أن السفارات الأمريكية في البحرين والسعودية والإمارات رفضت أيضا التعليق. وشركات "أن أس أو غروب" و"فيرينت سيستمز" و"سيلبرايت" لم تجب عن تساؤلاتنا.

ويبدو أن الطبيعة المعقدة لهذه التقنيات، والسرية التي تحيط بعمليات البيع التي تتم بين شركات إسرائيلية خاصة وحكومات أجنبية، تجعل من شبه المستحيل على الباحثين في هذا المجال تحديد الدول التي تستخدم برمجيات التجسس ضد معارضيها، إلا أن تأثيرها على أرض الواقع يبدو واضحا.

إذ أن نشطاء حقوق الإنسان يحذرون من أن هذه الشركات المطورة لمعدات المراقبة والتجسس، خلقت عالما يمكّن زعماء الأنظمة الدكتاتورية من مد أياديهم إلى ما أبعد من حدودهم، من أجل تعقب وتهديد معارضيهم.

وتقول دانا إنغلتون، مستشارة الأبحاث والسياسات في منظمة العفو الدولية: "إن هذا المجال لا يخضع لأي رقابة أو ضوابط، والطبيعة الضبابية لهذه الصناعة تحرم الضحايا والمستهدفين من الاستنجاد بالقانون وإحلال العدالة. وتبعات هذا الأمر خطيرة فعلا، فهو يؤدي لإسكات المجتمع المدني ويهدد حقنا جميعا في الخصوصية."

المصدر: فايس نيوز

رابط المقال: https://www.noonpost.com/25580/