حكومات عربية تستعين بشركات برمجية اسرائيلية للتجسس على مواطنيها

يبدو أن التعاون والتطبيع بين الكيان الاسرائيلي والحكومات العربية الخليجية منها بالذات، بدأ يأخذ مساراً تصاعدياً هذه الأيام، ليشمل العديد من الصعد، فبعد التقارير التي تحدثت عن تعاون سياسي وأمني وتجاري، بين دول مجلس التعاون مع الكيان الاسرائيلي، يقفز إلى الواجهة استعانة بعض الحكومات العربية بشركات برمجة اسرائيلية، بهدف التجسس على المواطن العربي، انتهاك خصوصيته، وملاحقته وقمع حريته.

فقد تناقلت وسائل الاعلام خلال الأيام القليلة الماضية قصة محاولة الاستخبارات الإماراتية اختراق هاتف أحد مواطنيها، الناشط الحقوقي "أحمد منصور"، مستخدمة تكنولوجيا "إسرائيلية" باهظة الثمن، مصدرها شركة Group NSO، التي تتخذ من مدينة هرتزيليا (داخل الأراضي المحتلة" مقراً لها، وتُعتبر من أكثر الشركات تصدّراً في مجالها، حيث وصفتها صحيفة "نيويورك تايمز" بأنها "من تجار السلاح الرقمي الأكبر والأكثر تملصاً في العالم".

ما كشف عن خيوط الارتباط بين الحكومة الإماراتية والشركة الاسرائيلية، هو التفاصيل التي حصلت مع

الناشط الإماراتي، حيث تلقى منصور رسائل نصية على هاتفه من نوع IPhone ، فيها روابط تقول الرسالة إنها تؤدي إلى معلومات تكشف "أسراراً جديدة" حول التعذيب في السجون الإماراتية. لكن منصور ارتاب بالأمر، ودفع بالرسائل إلى باحثين في مجال الأمن الإلكتروني في موقع شركة "Lab Citizen" وأكد الأخيرون أن الروابط في الرسائل النصية التي تلقاها منصور مصدرها "Group NSO"، وهي "شركة حرب إلكترونية مقرها الكيان الاسرائيلي، تبيع برنامج Pegasus الخاص بالحكومات"، ومهمته التجسس واعتراض الاتصالات.

وفقاً لتقريرَين صدرا الخميس الماضي، أحدهما عن شركة "Lookout" في سان فرانسيسكو الأميركية، متخصصة بأمن الهواتف الجوالة، والآخر عن "Lab Citizen" في جامعة تورونتو في كندا، فإن البرنامج الذي أُرسل الرابط الخاص به إلى هاتف منصور كان "قادراً على السيطرة التامة على الجهاز، بحيث يتجسس على الاتصالات، ويعترض الرسائل النصية، ويشغّل الكاميرا، ويحصد جميع المعلومات الشخصية المخزنة على الهاتف ومسار التحركات الجغرافية". وشبّه خبير في "Lookout" عملية عزل البرنامج بـ"تفكيك قنبلة"، معبراً عن ذهوله من الدرجة التي ذهب إليها معدو البرنامج لتجنب انكشافه، متحدثاً عن آلية فائقة الحساسية وُضعت في البرنامج بهدف "التدمير الذاتي". وبعد جهد استمر نحو أسبوعين، قدّر الخبراء في المؤسستين المذكورتين ثمن البرنامج "الفائق التطور" بمليون دولار أميركي.

وكشفت "يديعوت أحرونوت" بنسختها الورقية، الجمعة الماضي، عن أن شركة NSO حصلت قبل سنتين على تصريح من وزارة الأمن الإسرائيلية لبيع برنامج التجسس على الهواتف الخليوية إلى دولة خليجية. بينما أوضح تقرير نشرته صحيفة "هآرتس" نقلا عن صحيفة "نيويورك تايمز"، أن هذه الشركة الإسرائيلية لاءمت البرنامج كي يعمل في دول عديدة، وخلال السنوات الماضية استهدف برنامج التحسس الصحافي المكسيكي رفائيل كفرارا، الذي كشف فساد العائلة الحاكمة في بلاده، كما جرت ملاءمة البرنامج لأهداف في اليمن وتركيا وموزامبيق وكينيا والإمارات المتحدة.

ونقل عن الشركة الإسرائيلية "NSO" قولها إنه تطور منتجات تهدف إلى مساعدة الحكومات في مكافحة الجريمة والإرهاب، و أن الشركة معروفة لهيئات رسمية مخولة بموجب قوانين التصدير الأمني.

أما شركة أبل المنتجة لهواتف IPhone فقد سارعت إلى إصدار نسخة جديدة من نظام التشغيل ios من المفترض أن يمنع إمكانية تشغيل برنامج التجسس، وقد طلبت من مستخدميها تحديث نظام التشغيل لديهم بعد أن أبلغتهم برنامج التجسس قد تم زراعته في أعداد هائلة من الأجهزة.

وهذه ليست المرة الأولى التي يتم فيها الكشف عن استعانة الحكومة الإماراتية أو حكومات عربية بالشركات الاسرائيلية للتجسس على مواطنيها، فقد كشف تقرير نشره موقع "ميدل إيست آي" في 2 يوليو/تموز الماضي، أن السلطات في الإمارات عمدت بالتعاون مع شركات أجنبية تبيع برامج تجسس في ايطاليا واسرائيل والمانيا وامريكا، لزرع برامج تجسسية في حواسيب 1100 معارض سياسي وصحفي، وأكد التقارير بأنه بالإضافة إلى محاولة السلطات الإماراتية التجسس على اتصالات المعارضين والنشطاء، فإنها قامت أيضا ببناء نظام ضخم من المراقبة المدنية، الذي ركبته شركة إسرائيلية، ويراقب حياة كل شخص يعيش في أبو ظبي".

وفي أغسطس 2015 كشف تقرير اسرائيلي نُشر في الملحق الاقتصادي لصحيفة "يديعوت أحرنوت" الاسرائيلية عن بيع شركات برمجة إسرائيلية، لبرامج تجسس خبيثة لمجموعة من مخابرات العالم، منها مخابرات دول عربية من بينها دول خليجية والمغرب.

وأضافت الصحيفة أن الشركات الاسرائيلية التي يعمل بها ضباط سابقون في الأمن الاسرائيلي، تقوم بتصدير منتجاتها إلى الدول العربية، بالتعاون مع الشركة الإيطالية "هاكينغ تيم"، التي تربطها علاقات مع العديد من الدول القمعية حول العالم.

فضائح "هاكينغ تيم" وصلاتها بحكومات عربية

تأسست شركة "هاكينغ تيم" عام 2003، بمدينة ميلانو في إيطاليا، وتعمل في مجال تكنولوجيا المراقبة والاختراق من خلال تصميم وتطوير برامج ذكية توفرها لدوائر الاستخبارات حول العالم وقطاعات الأمن بالدول، وتشير التقارير إلى ارتباطها بشكل وثيق مع أجهزة الأمن الاسرائيلية.

في 5 يوليو/تموز 2015، تعرضت شركة "هاكينغ تيم" (Team Hacking) الإيطالية العاملة في مجال تكنولوجيا التجسس ومراقبة المواطنين واختراق خصوصيتهم على الانترنت لعملية اختراق واسعة النطاق، نتج عنها تسريب عدد ضخم من مستندات تخص التعاقد مع قرابة 30 دولة، تتضمن مراسلات إلكترونية وعقود صفقات وفواتير وميزانيات مالية، وأكواد مشغلة، وبيانات عن منتجات الشركة.

وكشف الاختراق أن ثماني دول عربية على الاقل اشترت برامج تجسس على مواطنيها من هذه الشركة وخاصة برنامج RCS أو التجسس عن بعد، وهي : مصر والسعودية والإمارات وعمان والسودان والبحرين والمغرب وتونس، وأن الجهات التي قامت بالشراء تنوعت بين أجهزة الاستخبارات ووزارات الداخلية والدفاع، وأن

بعض الدول قامت بتوسيط شركات لرجال اعمال لشراء برامج التجسس كي لا تظهر في الصورة بشكل مباشر.

ويعد برنامج RCS من أقوى البرامج في سوق الاختراقات نظرًا لمدى خطورته، واشترته كل الدول العربية تقريبا، حيث تقوم فكرته الأساسية على تجميع وتعديل واستخراج البيانات من أي جهاز يتم استهدافه ببرمجية خبيثة يتم زرعها من خلال الجهاز القائم بالاختراق.

وتتضمن إمكانات النظام تجاوز التشفير وإعدادات الأمن في البرامج، وتسجيل مكالمات سكايب، وحفظ سجلات البريد الإلكتروني وبرامج المحادثات، وجمع بيانات استخدام متصفح الويب، وأخذ لقطات مصورة باستخدام الكاميرا المدمجة في الحواسيب، وتسجيل مقاطع صوتية باستخدام الميكروفونات المدمجة في الحواسيب.

و في 16 يوليو/تموز 2014 نشرت صحيفة الإيكونوميست تقريرا بعنوان (نحن نراقبك) فضح التجسس السعودي علي هواتف المواطنين، بعدما رصدت مجموعة "Lab Citizen"، استخدام المخابرات السعودية لبرنامج RCS، حينئذ قالت "Lab Citizen" إن البرنامج كان متنكرًا في شكل نسخة من تطبيق للأخبار على الهاتف المحمول يسمى (القطيف اليوم)، وإنه كان بمجرد تحميل النسخة المزيفة من ذلك التطبيق، فإنه يتم تثبيت برامج التجسس.