في لبنان

النوع من الأجهزة والبرامج. تؤكد مصادر أمنية رفيعة (رضوان مرتضى) صحّة المراسلات، وتؤكّد أيضاً شراء أجهزة تنصت بملايين الدولارات، ولكنها تنفي نفياً قاطعاً أن تكون هذه الأجهزة توفر إمكانية المراقبة الشاملة للاتصالات، سواء عبر الهواتف الخلوية أو الشبكات الرقمية، مشيرةً إلى أنّ قدرة هذه الأجهزة تنحصر بتعقّب اتصالات محدودة. الأمر غير محصور بالجهات المحلية، فالخصوصية منتهكة من جهات خارجية، بتغطية من الحكومة أحياناً، كتسليم «داتا» الاتصالات كاملة إلى المحكمة الأمنية (بالإضافة إلى الأجهزة الأمنية المحلية)، أو عبر عمليات خاصة، كالتي كشفت عنها وثيقة، نشرها موقع censoo.com، تفيد بأنّ وكالة الأمن القومي الأميركية اخترقت منذ فترة طويلة سنترالات أوجيرو وتمكنت من التجسس على الداتا الصادرة من لبنان وتصفيتها ومعالجتها

يُحكى عنها دائماً، فضلاً عن طبيعة النظام المافيوية... يجعلنا كل ذلك نشعر بالخوف والقلق على حياتنا الخاصة، وبالتالي لا يمكن أن نستسلم لفوبيا الإرهاب والإجراءات الأمنية الاستباقية، ونحن مدركون لحجم الانتهاكات التي قد تحصل من خلال التجسس، خصوصاً أنّ امتلاك برامج وأجهزة التجسس جراء التطور التكنولوجي بات لا يقتصر فقط على الأجهزة الأمنية".

الشركات الخاصة تتجسس؟

ليست الأجهزة الأمنية فقط من يمتلك أجهزة وبرامج يمكنها التجسس على اللبنانيين، بل هناك شركات خاصة أيضاً. يكشف التقرير أنه "عُثر على تنصيبات (تركيبات) برامج لشبكة Blue Coat PacketShaper في مجموعتي عناوين لبروتوكولات الإنترنت، أو netblock، مرتبطتين بشركتين خاصتين مزوّدتين لخدمات الإنترنت هما IncoNet Data Management (المعروفة بـ IDM) وشركة Virtual ISP Lebanon، حسب تقرير لمؤسسة "مختبر المواطن" نشر عام 2013، وهذه الشركات المزوّدة لخدمات الإنترنت جزء من 24 شركة خاصة مزوّدة لخدمات الإنترنت التي تشتري إنترنت قانونياً من وزارة الاتصالات".

IDM، هي شركة مزودة لخدمة الإنترنت أنشئت عام 1995، وتقدم خدمة الوصول إلى الإنترنت إلى الأفراد والشركات. تقول الشركة على موقعها إنها تستحوذ على 60% من قطاع الشركات وأكثر من 50% من قطاع الأفراد في السوق اللبنانية، أما شركة Virtual-ISP المزودة أيضاً لخدمات الإنترنت، فقد تأسست عام 2004.

يشرح تقرير صادر عن مختبر Citizen Lab أنّ أجهزة Blue Coat PacketShaper توفر مجموعة واسعة من وظائف إدارة تصنيف حركة المرور، بما في ذلك تحديد ومراقبة حركة المرور التي أُنشئت بواسطة المئات من التطبيقات الشائعة وأنواع حركة المرور والسماح لمسؤول الشبكة بتصفيتها أو منعها. وبرغم أنَّ هذه الأجهزة يمكن أن تستخدم بغرض توفير أمن الشبكات وصيانتها، ولكن يمكن أيضاً استخدامها "لفرض قيود ذات دوافع سياسية تحدّ من قدرة الوصول إلى المعلومات، بالإضافة إلى مراقبة الاتصالات الخاصة وتسجيلها"، وفق تقرير المختبر. وبناءً عليه، تُطرح أسئلة كثيرة "حول بيع تكنولوجيا الاتصالات" "ثنائية الاستعمال" للسلطات في الدول، حيث لم يخضع استخدام هذه التكنولوجيا للنقاش العام أو سلطة القانون.

الأجهزة اللاقطة منتشرة

يكشف تقرير منظمة تبادل الإعلام الاجتماعي عن استخدام لبنان للاقطات "إمسي" IMSI Catcher، وهي "أجهزة تقوم بعمل شبيه بالأبراج الخلوية بغرض اعتراض اتصالات المحمول أو تتبّع حركة المستخدم، وهي تستخدم في لبنان بحسب وثائق نشرتها الحكومة السويسرية عام 2015. بالإضافة إلى ذلك، أكّدت الأجهزة الأمنية في لبنان أنها تستخدم هذا البرنامج منذ عام 2009، زاعمةً أن هناك حاجة لهذه الأجهزة اللاقطة لكشف عملاء إسرائيليين".

IMSI Catchers هي فئة من أجهزة المراقبة التي تستخدمها أجهزة الدولة الكندية، وهي تتيح لها اعتراض الاتصالات من الأجهزة النقالة وتستخدم أساساً لتحديد الأشخاص المجهولين المرتبطين بأجهزة محمولة وتعقبهم.

يضيف التقرير أنَّ "مزوّدي خدمات الإنترنت اللبنانيين تلقوا تعليمات صدرت عن المدعي العام في 7 حزيران 2103 بوجوب "القيام بكل ما يلزم لتفعيل وحفظ ملفات الدخول إلى الإنترنت التي تتمّ عبر الخوادم والموجّهات التابعة لها، ولتحضير نسخة احتياطية دورية من نظام حفظ البيانات لحمايتها من الفقدان، لمدة عام على الأقل". ونصّت التعليمات على وجوب أن تتضمن البيانات التي يتمّ جمعها وحفظها اسم المستخدم وعنوان بروتوكول الإنترنت IP address والمواقع التي تمّت زيارتها والبروتوكولات المستخدمة وموقع المستخدم".

يلفت التقرير أيضاً إلى بعض المخاوف الجديرة بالاهتمام والتي تتعلق بالانتقال إلى تكنولوجيا القياس البيومتري في جوازات السفر، وفي بيانات اللاجئين إضافة إلى نشر كاميرات مراقبة في بيروت تبث صورها عبر الإنترنت إلى غرفة الرصد الفوري. فجميع هذه البيانات معرضة للاختراق نظراً إلى عدم وجود ضمانات لحمايتها.

(الأخبار)

داتا الإنترنت بيد الأميركيين
أوجيرو مخترَقة

محمد وهبة

تظهر وثيقة، نشرها موقع censoo.com أنّ وكالة الأمن القومي الأميركية اخترقت منذ فترة طويلة سنترالات أوجيرو، وتمكنت من التجسس على الداتا الصادرة من لبنان وتصفيتها ومعالجتها. لا توضح هذه الوثيقة إذا كان مصدر هذه القدرة ناتجاً من برنامج معلوماتية أو أجهزة تكنولوجية متطورة أو مزيج من الاثنين تحت اختصار «هامركس»، إلا أنها تؤكّد أن التجسس عبر «أوجيرو» أتاح لها تصفية داتا بحجم 100 ميغابيت، خاصة بما تزعم أنه «الوحدة 1800» في حزب الله.

هذه الوثيقة مؤرّخة في 24 نيسان 2013 بعنوان برنامج «سيغينت ديفلوبمنت سوبورت II ـ قراءة برنامج الإدارة». الوثيقة مختومة بشعار وكالة الأمن القومي الأميركي في داخلها كلمة «SIGDEV»، أي إن هذه الوثيقة عرضت في مؤتمر SIGDEV الذي يحضره ممثلون عن وكالة الاستخبارات الأميركية حول العالم. ويتضمن المؤتمر محاضرات وورش عمل واجتماعات ضمن طاولة دائرية وسواها، حول قضايا استخباراتية وتطورات التكنولوجيا في هذا المجال، وهو يعقد منذ سنوات عديدة في إطار برنامج Support Development «SIGNIT» الذي يحمل أكثر من نسخة اختصاراً لعبارة «تطوير أنظمة الدفاع العسكرية لاستخبارات الإشارة».

بتاريخ نشر هذه الوثيقة، أي في نيسان 2013، كان عمر المؤتمر تسع سنوات، وقد ذيّلت الوثيقة بعبارة «سري جداً»، مع أنها عبارة عن ورقة معدّة لمحاضرة خاصة شاركت فيها شركة «بوز ألن هاملتون». الورقة مكتوبة بلغة تقنية معقّدة نسبياً، ما يشير إلى أن هذا الاجتماع كان يجمع خبراء ومحللين تقنيين في مجال الاتصالات والمعلوماتية والتكنولوجيا الحديثة وغيرهم.

تتضمن الوثيقة لمحة عامة عن الاستراتيجية وتقنية العمل الذي قُدّم لـ «الزبون». ويفهم منها أنها خلاصة عمل يمكن اعتماده بوصفه مثالاً طُبق في لبنان وأفغانستان، غير أنها تتحدث بالتفصيل عن لبنان وعن عمليات التجسس على «داتا الإنترنت» الصادرة عنه إلى الخارج عبر سنترالات «أوجيرو» وموزّعاتها.

تقول الوثيقة إنّ فريق العمل تمكن من الاتصال بالبوابات الرئيسية للإنترنت في لبنان ومن تصفية المعطيات التي جمعت من هذه العملية. وقد أدت عملية جمع «الداتا» وتصفيتها إلى حصول وكالة الأمن القومي الأميركية على 100 ميغابايت خاصة بما تسمّيه «الوحدة 1800 التابعة لحزب الله»، والصادرة من لبنان إلى الخارج. وقد جرت هذه العملية من خلال الاتصال بموزع رأس بيروت للإنترنت، وهو أحد الموزّعين الاثنين الأساسيين في لبنان والمتصل بالكابل البحري الذي ينقل الداتا من لبنان إلى الخارج وبالعكس.

> الخرق لا يمكن ان يحصل عن بعد ويتطلّب وجود عميل في «أوجيرو»

تشير الوثيقة إلى أنّ آلية الاتصال جرت بـ«خفية»، أي إنه كان تسللاً خفياً، بواسطة عملية «ريكس كوايندو» التي نفذت من خلال «هامركس» (ليس واضحاً ما إذا كانت هذه التسمية تتعلق ببرنامج معلوماتية أو بجهاز تنصت متطور أو بمزيج من الاثنين). وليس ذلك فحسب، بل أتاحت هذه العملية الاتصال بمركز التحكم الأساسي في أوجيرو الموجود في رأس النبع، فيما أتيح لفريق العمل أن ينشئ موزّعاً خاصاً رديفاً يتيح جمع المعلومات أو داتا الإنترنت ومعالجتها وتصفيتها. وبنتيجة ذلك، جرى الدخول إلى حسابات المشتركين وعناوينهم الأساسية على الشبكة.

بحسب الوثيقة، فإن كل حركة الداتا والمعلومات المتعلقة بما تسمّيه «الوحدة 1800» جمعت من خلال هذه العملية، وإن ربط المعلومات المحصلة بالوحدة جرى بعد 24 ساعة من إجراء الاتصال، أي بعد 24 ساعة من بدء التجسس. وقد أشار محلل تقني لدى الوكالة، إلى أنه، بنتيجة هذا البرنامج، باتت هناك قدرة أكيدة لدى فريق العمل، على التدقيق في أي عنوان (IP Address). وتقول الوثيقة إنه في السابق لم تكن هناك القدرة على تنفيذ مثل هذا الاتصال خلافاً للتطور الحاصل بنتيجة «هامركس». وتضيف أن هذه العملية نفذت سابقاً في أفغانستان حيث جرى الاتصال بالشبكة التي يستعملها كبار القادة العسكريين والسياسيين والمدنيين أيضاً.

لم تُعرف مدّة التجسس الذي قامت به الوكالة عبر عمليتها المذكورة، ولم تعرف مدّة الاتصال بموزّعات «أوجيرو»، ولا عن توقيت الاتصال والتجسس، إلا أن التقنيين في لبنان يؤكدون أن عملية كهذه أتاحت للوكالة الحصول على كل الداتا المنقولة عبر الموزّع وغرفة التحكم، وعلى الأرجح أنها أتاحت لهم الدخول إلى كل الداتا المتصلة بعمل شبكة الإنترنت في لبنان. وليس ذلك فقط، بل يمكن التساؤل عن تقصير «أوجيرو» في حماية الشبكة اللبنانية من خرق كهذا، وخصوصاً أنه لم يجرِ الاستثمار في الشبكة الحالية منذ فترات طويلة، فيما يزداد الحديث بين التقنيين عن استعمال الشبكة من أجل منافع خاصة وأنها، على فرض حسن النيّة، أهملت لهذا الهدف.

إزاء هذا الخرق الهائل، يبرز سؤال أساسي عن كيفية حصول الاتصال بالموزّع وغرفة التحكم، إذ إن هذا الأمر، تقنياً، لا يمكن أن يحصل عن بُعد، وفق رأي الخبراء التقنيين، بل يجب أن يكون هناك عميل ميداني سهّل لهم هذا الأمر، وبالتحديد عميل في «أوجيرو».

وبالنسبة إلى حجم الضرر الواقع على لبنان بنتيجة هذا الخرق الاستخباراتي الأميركي، فإن الداتا المشار إليها في هذه العملية لا يمكن حصرها، وهي تتعلق بالرسائل البريدية الإلكترونية وبحسابات اللبنانيين على مواقع التواصل الاجتماعي من فايسبوك وواتس آب وانستغرام وسواها... كل الرسائل والتسجيلات والصور وغيرها من أنواع الداتا المستهلكة باتت مكشوفة لوكالة الأمن القومي الأميركي، لا بل إن التحويلات المصرفية والحسابات المرتبطة بها هي أيضاً انكشفت... لا يمكن تعداد وحصر حجم الداتا بهذه التطبيقات والتحويلات، فهناك الكثير الكثير مما انتشلته الوكالة بهذه العملية من حسابات اللبنانيين على مواقع الإنترنت والتطبيقات المستعملة.