أتلانتك: هل هناك طرف ثالث بعملية تجسس المخابرات اللبنانية؟

السبت 20 يناير 2018 02:01 م

نشرت مجلة "ذا أتلانتك" مقالا للكاتب كافي ويدل، يعلق فيه على العملية السرية التي كشف عنها باحثون في "لوك أوت/ راقب" لأمن الهواتف و"مؤسسة الجبهة الإلكترونية" القانونية

ويقول الكاتب إن "جهاز الأمن العام اللبناني أدار عملية تجسس واسعة لمدة خمس سنوات، وشملت أكثر من عشرين دولة، وأطلق عليها (دارك كاركال/ السنور الأسود)، ونشرت مؤسسة البحث الأمريكية (راقب) و(مؤسسة الجبهة الإلكترونية) نتائج البحث يوم الخميس، وربط الباحثون المخابرات بست حملات مراقبة، استهدفت مسؤولي الحكومة والأكاديميين والصحافيين ورجال الأعمال في الشرق الأوسط وأوروبا والولايات المتحدة".

ويعلق ويدل في مقاله، قائلا: "هناك الكثير من الأحداث، وما هو غير عادي أنها ليست المرة الأولى التي يرى فيها الباحثون أساليب (السنور الأسود) تستخدم في عمليات تجسس، وبدأت (راقب) بالبحث مع (مؤسسة الجبهة الإلكترونية) بعدما قامت الأخيرة بالكشف عن عملية تجسس في كازاخستان عام 2015، التي استهدفت معارضين وصحافيين، وكشف الباحثون عن أن البنية الرقمية التي استخدمت لشن هذه الهجمات هي ذاتها التي عثر عليها لاحقا واستخدمت في حملات المراقبة في بيروت".

ويشير الكاتب إلى أن "حقيقة مشاركة السنور الأسود وعملية كازاخستان في المزايا التقنية تشير إلى قصة أكبر، وقد تعني أن هناك طرفا مجهولا يقوم بتقديم البنى التحتية والبرمجيات الخبيثة (مالوير) لعدد من الدول (العملاء) للقيام بعمليات قرصنة وتستخدم الوسائل ذاتها".

وتنقل المجلة عن الباحث الأمني في مؤسسة الجبهة الإلكترونية " كوبر كوينتين، قوله إنه "من المحتمل أن (دارك كاركال) لا تدير هذه البنية"، ويضيف كوينتين، وهو أحد مؤلفي التقرير: "نعتقد أن هذه البنية تدار من طرف ثالث قام ببيع خدماته إلى كازاخستان، وربما لدول أخرى".

ويعلق ويدل قائلا: "فكر بها بصفتها رقابة حكومية باعتبارها خدمة مدفوعة، وأشار تقرير هذا الأسبوع إلى أن هناك طرفا ثالثا، حيث قال كوينتين إن الباحثين يعملون للكشف عنه، وأضاف: (لدينا بعض الأفكار)".

ويرى الكاتب أن "عملية المراقبة هي بمثابة تحول عن الطريقة التي تعمل فيها الدول القطرية للرقابة، فالحكومات، خاصة تلك التي لا توجد فيها مواهب محلية للقرصنة عادة ما تشتري الأدوات من الشركات، فقط انظر للقائمة الطويلة للحكومات التي اشترت (سوفت وير) التجسس، الذي بنته الشركة الإيطالية (هاكينغ تيم، التي تعرضت نفسها للقرصنة عام 2015".

ويستدرك ويدل بأن "ما حدث هنا هو التقدم عدة خطوات للأمام، فبدلا من شراء أدوات القرصنة واستخدامها في القرصنة، فإن (السنور الأسود) دفع لآخر ليستخدم أدواته، حيث يقول كوينتين: (يقومون بالاشتراك في هذا، وبعد ذلك يقوم طرف آخر ببناء كل شيء لهم وكل ما عليهم فعله الدخول وتحميل التقارير حول الأشخاص الذين يقومون بمراقبتهم)، وبهذا المعنى فإنه (سوفت وير) للتجسس الرقمي يقوم بمتابعة توجهات المستهلكين، مثل منتجات (غوغل جي سويت)، التي تعرض على محرك (غوغل)، ويقوم المستهلكون بالدفع للحصول عليها، ولهذا يصفها التقرير بأنها خدمة تجسس تقوم على التخزين في (آي كلاود) أو الغيمة، لكن لا يعرف أين تقع هذه الغيمة".

ويقول الكاتب إن "النموذج التجاري قد يكون إبداعيا، إلا أن أساليب القرصنة، كما كشف التقرير، بدائية بشكل نسبي، فالسنور الأسود لا يحب استخدام شيفرة مثيرة أو أدوات غالية الثمن، وينبع نجاحه من عملية هندسة اجتماعية قديمة، فهم (أو الجماعة التي دفعوا لها لتقوم بعملية القرصنة) استخدموا أساليب مثل إنشاء حسابات (فيسبوك) مزيفة بصور لنساء عربيات ضاحكات؛ وذلك لدفع الهدف ليقوم

بتنزيل النسخ المزيفة لإرسال الرسائل مثل (واتساب)، وتقوم هذه التطبيقات بإرسال نصوص الثرثرة كلها إلى الجواسيس، بالإضافة إلى معلومات، عدة مثل الموقع على (جي بي أس)، وقائمة التواصل والرسائل الهاتفية القصيرة (أس أن أس)، وقد تقوم (مالوير) أو البرمجيات الخبيثة بالتقاط صور من الهواتف المصابة باستخدام الكاميرا الأمامية والخلفية للهاتف، وتسجيل أشرطة صوتية من سماعة الجهاز".

ويصف ويدل حجم العمليات التجسسية النابعة من جهاز الأمن العام اللبناني مثير للدهشة، بحسب ما قال محمد نجم، منسق "سيمكس"، وهي منظمة رقمية لبنانية، وكذلك قائمة الدول التي تم استهدافها، والكثير منها حلفاء للبنان

وتلفت المجلة إلى أن نجم تساءل عما إذا تمت المصادقة على العملية عبر الإجراءات القانونية الطبيعية، ما يعني وجود رقابة قضائية والسماح بالعملية لوقت قصير، وقال نجم: "إنهم يقومون بعمل أي شيء دون أي إجراءات قانونية، وهذا أمر خطير جدا".

وينوه الكانب إلى أن جهاز الأمن العام لم يرد على طلبات التعليق على التقرير، وقبل نشره قال رئيس الجهاز الجنرال عباس إبراهيم، لوكالة "رويترز": "لا يملك جهاز الأمن العام هذه القدرات ونتمنى أننا نملكها".

ويبين ويدل أنه "تم الكشف عن عملية بيروت عندما عثر الباحثون في (راقب) و(مؤسسة الجبهة الإلكترونية) على بيانات مسروقة حجمها 80 غيغابايت، وتحتوي على مئات الآلاف من الرسائل الهاتفية القصيرة، وبيانات للمكالمات الهاتفية، وقائمة الأرقام، على محرك غير مؤمن، وعندما حدد الباحثون مكان المحرك بدأوا بالتكهن ومحاولة فك أسماء الملفات ذات الأحرف الثلاثة: (دبليو بي7، دبليو بي 8، دبليو بي 9)، حيث قال كوينتين: (كنا نقوم بالبحث على الإنترنت لم تكن هناك عملية قرصنة)، ووجد الباحثون أن الحملة ركزت على أجهزة الهاتف المحمول، بشكل يجعلها مختلفة عن جهود التجسس الأخرى".

ويفيد الكاتب بأن الباحثين وصفوا هذه العملية بأنها "واحدة من أوسع العمليات التي كشف عنها حتى اليوم"، فعندما فكروا بسرقة بيانات الهواتف النقالة فإنهم اعتقدوا أنه كنز يمثل جزءا من عملية الرقابة التي يشرف عليها "السنور الأسود"، حيث يقول كوينتين: "ألمح لنا بعض الباحثين أن هناك زبائن آخرين" غير السنور أو كازاخستان، حيث كان حذرا في كلامه

ويشير ويدل إلى أن النكات انتشرت على "تويتر" بعد نشر التقرير ساخرة من عجز الأمن العام اللبناني، و"لا يعرف من قام بالخطأ بحيث حرق عملية القرصنة كلها، وربما كانوا هم جماعة (السنور الأسود)، بحسب كوينتين، وقد يكون عملا رخيصا قام به بائع متجول لخدمات القرصنة".

ويبين الكاتب أنه "من خلال غربلة الملفات التي عثروا عليها في المحرك، عثر الباحثون على عدد من الأشكال التي ظلت تظهر مرة تلو الأخرى، وظنوا أنهم كانوا يبحثون عن أدوات المقرصن، لكنهم نظروا بطريقة أقرب على شبكات (الواي- فاي) التي كانت كل واحدة منها مرتبطة بها، وكان واحدة مشتركة بينها واسمها (بي أل دي3 أف6)، التي حدد الباحثون مكانها في نقطة قريبة من مبنى جهاز الأمن العام في بيروت".

ويختم ويدل مقاله بالإشارة إلى أن مراسلا لوكالة "أسوشيتد برس" مر قريبا من المبنى يوم الأربعاء، وجد أن الشبكة لا تزال تبث، مستدركا بأنه عندما حاول المرور قرب المبنى يوم الجمعة فإنه "لم تعد هناك شبكة وربما خبئت أو أعيد تسميتها أو حذفت".