إسرائيل تجسست على مفاوضات نووي إيران باستخدام فيروس كمبيوتر

ترجمة من الفرنسية وتحرير نون بوست

تقرير: فلوريان رينو و مارتن أنترسنغر

إعتاد يوجين كاسبرسكي على الإعلان عن الأخبار السيئة، فرئيس الشركة الروسية التي تحمل نفس لقبه، كاسبرسكي، وهي الشركة الرائدة عالميا في أمن تكنولوجيا المعلومات، كثيرا ما تكشف عن وجود نقاط ضعف أو برامج للتجسس.

وقد صرح يوجين كاسبرسكي، يوم الأربعاء 3 مايو، في مؤتمر صحفي في لندن، بوجود ممارسات غريبة، فقد كشف النقاب عن هجوم استهدف شركته الخاصة، وقد بدأ كل شيء على كمبيوتر لأحد موظفي الشركة، المتواجدين في آسيا، في أوائل الربيع الماضي، ثم تمكن خبراء الشركة من تحديد برنامج يعمل بطريقة غير اعتيادية، وسرعان ما أدركوا أن هذا البرنامج كان ينشط في أنظمة الشركة لمدة عام تقريبا.

وعند القيام بعملية تدقيق تبين للشركة أنها ليست الوحيدة التي أصيبت بعدوى هذا البرنامج، فقد عثر عليه أيضا في نظم مئات الوحدات الموجودة "في الدول الغربية، والشرق الأوسط وآسيا". أما سيمانتيك، وهي شركة منافسة لكاسبيرسكي قامت أيضا بتحليل البرنامج، فقد قالت أنها رصدته داخل الشركات الأوروبية في قطاع الاتصالات، ولدى شركة الهاتف شمال أفريقيا ولدى شركة مصنعة للإلكترونيات في جنوب شرق آسيا.

المفاوضات حول النووي الإيراني تم التجسس عليها

أوضحت شركة كاسبيرسكي أن هذا البرنامج تم رصده في العديد من الفنادق التي جرت فيها المفاوضات حول النووي الإيراني بين الغرب وإيران. ولكن لم تستطع كاسبرسكي أن تقدم تفاصيل حول كيفية إصابة هذه الفنادق بعدوى هذا البرنامج، ولذلك لا يمكن تأكيد وجود عمليات تنصت على المشاركين دون علمهم، أو حدوث سرقة وثائق سرية، على سبيل المثال.

من يقف وراء هذا البرنامج، الذي أطلق عليه الباحثون اسم دوكو 2 (Duqu 2)؟ تم اكتشاف النسخة الأولى من هذا البرنامج في عام 2011، وكان وقتها يقوم برصد البرنامج النووي الإيراني. وهذا البرنامج في حد ذاته مستمد من رمز ستكسنت، وهو برنامج خبيث آخر سبق له مهاجمة المنشآت النووية الإيرانية، والذي تم تطويره، وفقا لاستطلاع صحفي من صحيفة نيويورك تايمز، من طرف الولايات المتحدة وبمساعدة إسرائيل.

ويعتقد باحثو كاسبيرسكي، ونظرا لتعقيد برنامج دوكو 2، أنه من تطوير أجهزة تابعة لدولة، ليس مجرد مجموعة من الهواة، نظرا لحجم الموارد التي تم استخدامها. ولكن أية دولة؟ فعدد قليل فقط من البلدان تمتلك القدرة التقنية والمالية لتطوير مثل هذه البرامج.

كل الأنظار، لا سيما في الصحافة الأميركية، تتجه حاليا نحو إسرائيل، فموضوع المحادثات النووية هو مسألة حاسمة بالنسبة لإسرائيل، زيادة على أنها من بين الدول الرائدة من حيث مهارات التجسس على أجهزة الكمبيوتر. وعلاوة على ذلك، فإن أحد أهداف دوكو 2 سبق استهدافه من قبل برنامج إيكواسيون، وهو برنامج آخر متطور ومن المحتمل أن يكون متصلا بالولايات المتحدة، وهو ما يوحي بأن هذين البرنامجين ليس لديهما نفس الجهات الراعية.

وقد ذكرت صحيفة وول ستريت جورنال، نقلا عن عدة مصادر من البيت الأبيض، أن الأمريكيين كانوا على قناعة بأن إسرائيل تجسست على المناقشات، وتمكنت من الحصول على معطيات بالغة سرية حول فحوى المفاوضات.

ومن الصعب الذهاب الى أبعد من هذا مع هذه المجموعة من الأدلة. وكالعادة، تحرص شركة كاسبيرسكي على عدم ذكر الجهة المسؤولة، لأنه لا يوجد أي دليل قاطع في الوقت الحاضر يؤكد من يقف وراء برنامج دوكو 2.

هجوم معقد للغاية

يجب أن نكون على يقين من فعالية مثل هذا البرنامج للتجسس، حتى يتم إطلاقه بهدف مهاجمة أكبر شركة مكافحة فيروسات، والأكثر تطورا في العالم. ولكن المهاجمين كانوا يدركون قوة هذا البرنامج، الذي يعلق عليه يوجين كاسبيرسكي قائلا: "هذا البرنامج معقد للغاية، ولم نتعرض لواحد بهذه الدرجة من التعقيد من قبل".

كما أكد الباحثون أن لهذا البرنامج صلات قوية مع برنامج يسمى دوكو. وهذا الأخير، وفقا لكاسبيرسكي، كان بمثابة الأساس لبناء الفيروس الذي هاجمهم مؤخرا، لذلك تمت تسميته دوكو 2. وترى شركة كاسبيرسكي أنه عبارة عن "نسخة محسنة تتضمن العديد من الأفكار الجديدة ومن البرمجيات الخبيثة الحديثة".

ويستخدم البرنامج، في عملية انتشاره، عدة عيوب تسمى "ثغرة يوم الصفر"، وهذا المصطلح يطلق على مجموع الثغرات الأمنية للكمبيوتر والتي لم يتم بعد الكشف عنها. وتعتبر هذه الثغرات مؤشر جيد لمعرفة درجة تطور البرنامج المهاجم. ووفقا لكاسبيرسكي فإن برنامج دوكو 2 يستخدم على الأقل ثلاثة ثغرات ما يجعله من بين البرامج الأكثر تعقيدا.

برنامج شبح

بعد دخوله كمبيوتر كاسبيرسكي، تمكن البرنامج من الانتشار في شبكة الشركة. ولكن كيف تمكن هذا البرنامج من تجاوز دفاعات الشركة التي يتمثل عملها في تحديد التهديدات وتطوير الدفاعات المناسبة؟

دوكو 2 هو نموذج شبح. وخلافا لما لاحظه باحثو كاسبرسكي إلى حد الآن، لا يتم تخزين البرنامج الجاسوس في أجهزة الكمبيوتر التي يصيبها، فهو ينتشر في الذاكرة المؤقتة للكمبيوتر، ما يجعل من الصعب للغاية الكشف عنه عن طريق برامج مكافحة الفيروسات التقليدية.

هذا النمط من البرامج يثير إعجاب ضحاياه بفضل درجة الابتكار الموجودة فيه، فبالنسبة لديفيد ايم، وهو باحث في كاسبيرسكي، يرى أن الذين وضعوا هذا البرنامج "كانوا على ثقة تامة من أنه لن تتم ملاحظته". هذا البرنامج، مثل برامج التجسس الأكثر تطورا، يضم مجموعة متنوعة من الأدوات القادرة على التجسس وجمع الكعلومات، مثل اعتراض الاتصالات والتقاط صور الفيديو.

هجوم غير مسبوق

من الشائع أن تهتم أجهزة الاستخبارات بالمفاوضات الحساسة حول الملف النووي الإيراني، لكن الأقل شيوعا هو أن يهاجموا مباشرة شركة رائدة على مستوى العالم في أمن تكنولوجيا المعلومات. وعلى الرغم من أن كاسبيرسكي هي شركة روسية تدير أمن مؤسسات اقتصادية لدول كبرى، وعلى الرغم من بعض الهجمات ضد شركات متواضعة الحجم، إلا أن المزودين الرئيسيين لبرامج مكافحة الفيروسات لم يتعرضوا في السابق لمثل هذه الهجمات المتطورة، فهي تعتبر الأولى من نوعها وفقا لعدة مصادر.

ويؤكد ديفيد ايم، من شركة كاسبيرسكي: "لقد شهدنا من قبل محاولات اختراق لكنها هذه هي المرة الأولى التي يتمكن فيها برنامج من اختراق شبكتنا"، مضيفا: "فمن الغباء مهاجمة شركة تعمل في تأمين الكمبيوترات!". كما بين الباحث فيتالي كاملوك في كاسبرسكي وجود "قاعدة ضمنية شائعة بعدم مهاجمة شركة كاسبيرسكي".

استهداف شركات مثل كاسبيرسكي، فيه خطر أن يتم التعرف عليك وبسرعة، بحسب ما جاء في تقرير الشركة حول برنامج دوكو 2، لكن الوضع يتغير وهو ما يقلق الشركة، حيث قال فيتالي كاملوك: "نحن نشهد ظهور سباق تسلح ينطوي على نوع من المواجهة بين جواسيس يعملون لصالح الدول ضد شركات تعمل في مجال أمن برامج الكمبيوتر. إنهم يحاولون التعدي علينا وتخريب برامج الشركة التي تعد صمام الأمان للمؤسسات والشركات، وهو ما يدعو إلى القلق الشديد بالنسبة لنا جميعا".

على أي حال، فإن أهداف الذين قاموا بمهاجمة كاسبيرسكي واضحة، فهم يريدون معرفة المزيد عن قدرة الشركة في الكشف عن برامجهم، حيث قال ايم: "إنهم مهتمون بصفة خاصة بتقنياتنا ومنتجاتنا المستقبلية". وتؤكد كاسبيرسكي أنه لم يتم اختراق أي زبون، إلا أنها تبقى مراوغة بشأن عواقب عملية القرصنة الأخيرة وتأثيرها على قدرتها على الكشف عن تهديدات مماثلة في المستقبل.

المصدر: صحيفة لوموند الفرنسية