كليمون باسو | نشر في ٢١ فبراير ,٢٠١٥

كاسبرسكي تتهم واشنطن بتطوير فيروس واختراق آلاف الحواسيب

ترجمة وتحرير نون بوست

أعلنت شركة برمجيات الحماية "كاسبرسكي لاب" أنها اكتشفت مؤخرًا مصدر الهجوم الفيروسي المعقد الذي ضرب الأقراص الصلبة لحواسيب تحتوي على معلومات خاصة بحكومات ووكالات وشركات مهمة، وهو برنامج تجسس قوي وفعّال يسمى "فاني" يقوم بجمع المعلومات من ملايين الحواسيب حول العالم تحت غطاء فيروسات خبيثة تتسرب لتلك الحواسيب.

"فاني" دودة جديدة من صنع وكالة الأمن القومي الأمريكية

لم يعلن التقرير الصادر عن الشركة الروسية لحماية الحواسيب كاسبرسكي صراحةً عن مصدر حملة الهجمات الرقمية والاختراقات، ولكنه أشار إلى أوجه شبه بين هذه الهجمات وفيروس Stuxnet الذي طورته الولايات المتحدة وإسرائيل لعرقلة البرنامج النووي الإيراني.

وقالت كاسبرسكي إن هذا الهجوم يُعتبر الأكثر تعقيدًا وتطورًا في عالم التجسس عبر الإنترنت وتعود بدايات استخدامه إلى سنة 2001 على يد مجموعة هاكرز "المعادلة" التي يُعتقد أنها المجموعة الأكثر تطورًا في العالم والأكثر تهديدًا في العصر الحالي.

وتتمّ عمليات التجسس عبر الدودة التي سمتها شركة كاسبرسكي "فاني" والتي تقوم بالتسلل للحاسوب عبر منفذ ناقل البيانات USB، وتستغل الثغرات في نظام الحماية لسرقة المعلومات من الحاسوب، وقد تمت أغلب هذه العمليات في الشرق الأوسط وأسيا، كما يؤكد التقرير على التشابه الكبير بين أسلوب عمل مجموعة هاكرز "المعادلة" وأسلوب فيروس Stuxnet؛ وهو ما يشير إلى وقوف الولايات المتحدة وراء هؤلاء الهاكرز وهذه الفيروسات.

وكالة الأمن القومي ترفض التعليق

رفضت وكالة الأمن القومي الأمريكية NSA التي قادت في السنوات الماضية أكبر عملية لمراقبة الإنترنت على المستوى العالمي بتعلّة حربها على الإرهاب، الإدلاء بتعليق حول ضلوعها في إنتاج هذا الفيروس،

وصرح الناطق الرسمي باسم الوكالة فاني فاينس لوكالة الأنباء الفرنسية بأنهم على علم بالتقرير وبأنهم لم يُدلوا بأي تعليق على الاتهامات الموجهة ضدهم أو بخصوص المعلومات الواردة في التقرير.

وفي نفس السياق أشار شون ساليفان من شركة برمجيات الحماية الفنلندية Secure-F إلى تطابق معلوماتهم مع تقرير شركة كاسبرسكي، وقال إن مجموعة هاكرز "المعادلة" التي يشير إليها التقرير هي في الحقيقة فريق عمل تابع لأحد أقسام وكالة الأمن القومي الأمريكية يحمل اسم ANT كانت شركتهم قد أجرت بحثًا في سنة 2013 حول قيامه بخلق الثغرات في المنتوجات التكنولوجية.

وقد تسبب الهجوم الفيروسي بمشاكل لمعدل ألفي مستخدم شهريًا في ثلاثين بلدًا وحصلت أغلب هذه الاختراقات في إيران وروسيا وباكستان وأفغانستان، كما تضررت دول أخرى مثل سوريا وكازاخستان وبلجيكا والصومال وليبيا وفرنسا واليمن والمملكة المتحدة وسويسرا والهند والبرازيل.

وشرح الباحثون إحدى الخصائص الخطيرة لهذه الهجمات وهي سهولة اختراقها لأقراص تخزين المعلومات حتى تلك التي تنتجها أفضل الشركات في العالم مثل Digital Western، Seagate، Maxtor. وSamsung فقد تم تصنيع بطريقة الفيروس بحيث نه تمكن من عملية أمام حتى الصمود من المسح الكامل وإعادة تهيئة القرص الصلب وإعادة تنزيل نظام تشغيل جديد فيه، وقد قال عنه الباحث في شركة كاسبرسكي سيرغي مالنكوفيتش إنه فيروس تجسس لا يمكن التفطن إليه ولا يمكن تدميره فهو كابوس بأتم معنى الكلمة في عالم حماية الحواسيب.

تدمير الأقراص المضغوطة CD

أشار باحثو شركة كاسبرسكي أيضًا إلى أن هذا الفيروس تسرب في سنة 2009 إلى الأقراص المضغوطة التي تم توزيعها على ضيوف منتدى علمي عالمي وهو ما سبب مشاكل واختراقات لحواسيب العشرات من العلماء من كافة أنحاء العالم.

وقال الباحثون إنه يصعب القول متى بدأت مجموعة هاكرز "المعادلة" عملها، ولكن عينات الفيروس التي تمت مراقبتها تعود لسنة 2002، كما أن مصدر إطلاقها تأسس ربما في سنة 2001 أما المجموعة في حد ذاتها فربما يعود تاريخ تكوينها إلى سنة 1996.

ورغم أن الولايات المتحدة ترفض التعليق على فيروس Stuxnet فإن الأبحاث تشير إلى أن الفيروس الذي يعود أول ظهور له إلى سنة 2007 صنعته هذه المجموعة لحساب إسرائيل والولايات المتحدة بهدف احتواء البرنامج النووي الإيراني.

هجمات إلكترونية على البنوك تسبب خسائر فادحة

كشفت شركة كاسبرسكي أيضًا في تقرير صدر يوم الإثنين الماضي في موسكو أن موجة من الهجمات الإلكترونية ضربت بنوك العالم وخاصة روسيا منذ سنة 2013 متسببة في خسائر قدرت بمليار دولار، وقالت الشركة إن هذه الهجمات التي لاتزال متواصلة تُبرز بوضوح أننا دخلنا في عصر جديد من الجريمة الإلكترونية، وأشارت صحيفة نيويورك تايمز في نفس السياق إلى أن مئات البنوك تعرضت للهجوم وتكبدت نصفها خسائر مالية هامة ويوجد أغلب الضحايا في روسيا والولايات المتحدة وألمانيا والصين وأوكرانيا.

ورغم أن بعض العلامات تُشير إلى ضلوع الصين في هذه الهجمات على البنوك، فإن كاسبرسكي حذّرت في تقريرها من أن بعض الآثار التي يخلفها الفيروس تم تصميمها عن دراية لمغالطة المحققين في مصدر الهجوم، ورغم تزايد الهجمات الإلكترونية التي تحمل أهداف سياسية فإن هذا الهجوم على ما يبدو كان فقط بغرض سرقة المال وليس للتجسس بما أن منفذي العملية لديهم خبرة في برمجيات وشبكات عمل البنوك، وقد استعمل الهاكرز في تلك العمليات برنامجًا يُسمى Carbanak يستهدف

مباشرة موظفي البنوك للإيقاع بهم عند تحميلهم لملفات حاملة للفيروس الذي يقوم بدوره باصطياد المعلومات وإرسالها لمصدر الهجمة، ويتسرّب هذا الفيروس إلى داخل شبكات اتصال البنوك ويخترق عمليات تحويل الأموال والحسابات المصرفية وآلات سحب النقود، وعند حدوث الاختراق يقوم منفذو الهجمة فورًا بتحويل مبالغ مالية كبيرة لحسابات تابعة لهم أو يقومون بسحب الأموال مباشرة، ووصلت جرأة هؤلاء الهاكرز إلى درجة اختراق كاميرات المراقبة في البنوك والتجسس على الموظفين المستهدفين لتسهيل إيقاعهم في الفخ، وتقول كاسبرسكي أن الأموال التي تم الاستيلاء عليها تقدر بمبالغ ضخمة وقد تم تحويلها لحسابات في الصين والولايات المتحدة ، وقد سجل أحد البنوك خسارة بأكثر من سبعة مليون دولار وسجل آخر خسارة بعشرة مليون دولار بسبب عمليات سحب وتحويلات تمت عبر الإنترنت.

وحذر التقرير من أن هؤلاء الهاكرز يحاولون في الوقت الحالي توسيع نطاق هجماتهم واستهداف دول أخرى في وسط أوروبا والشرق الأوسط وأسيا وأفريقيا.

المصدر: مدونة ويكيسترايك