

الهجمات الإلكترونية تجتاح العالم أكثر من 75 ألف هجوم في 99 بلداً



السبت 13 مايو 2017 11:05 م

حذرت السلطات الأميركية والبريطانية، الجمعة 12 مايو، من موجة هجمات إلكترونية استهدفت بصورة متزامنة "العديد من دول العالم" بواسطة برنامج خبيث لابتزاز الأموال، مناشدة ضحايا هذه الهجمات عدم الدفع للقراصنة

ويبدو أن القراصنة استغلوا ثغرة في أنظمة التشغيل "ويندوز" كشفت في وثائق سرية لوكالة الأمن القومي الأميركية "إن إس إيه" تمت فرصتها

وقالت الوكالة البريطانية للأمن المعلوماتي في بيان: "شهدنا اليوم سلسلة هجمات إلكترونية استهدفت آلاف المؤسسات والأفراد في عشرات الدول".

وأوصت الوكالة بتحديث برامج أمن المعلومات وبرامج مكافحة الفيروسات الإلكترونية

من جهتها قالت وزارة الأمن الداخلي الأميركي في بيان: "لقد وردتنا تقارير عدة عن برنامج معلوماتي يطالب الضحايا بدفع فديات نحض الأفراد والمنظمات على عدم الدفع لأن ذلك لا يضمن استعادة البيانات مجدداً".

وتشير هذه الموجة من الهجمات الإلكترونية "على مستوى عالمي" قلق خبراء أمن المعلوماتية الذين لفتوا الى أن البرنامج الخبيث يقفل ملفات المستخدمين المستهدفين ويرغمهم على دفع مبلغ من المال على هيئة بيتكوينز مقابل إعادة فتحها

ومساء أمس الجمعة (قراءة الساعة 20:00 ت غ) كتب جاكوب كروستيك، المسؤول في شركة أفاست لأمن المعلوماتية، على مدونة: "لقد رصدنا أكثر من 75 ألف هجوم في 99 بلداً".

من جهتها قالت شركة "فورسبوينت سيكيوريتي لابس" المتخصصة أيضاً في أمن المعلوماتية إنها رصدت "حملة كبيرة من الرسائل الإلكترونية المصابة" بالفيروس المعلوماتي الخبيث، مؤكدة أن وتيرة الهجوم بهذه الرسائل المصابة بالفيروس ناهزت خمسة ملايين رسالة في الساعة

إلا أن باحثاً في شركة لأمن المعلوماتية قال إنه بالإمكان وقف انتشار برنامج "واناكري" للفدية مؤقتاً من خلال تسجيل اسم مجال يستخدمه البرنامج

وقال الباحث الذي يستخدم اسم "@مالوير_تيك_بلوغ" في رسالة خاصة على تويتر لوكالة فرانس برس إن القراصنة "كانوا يعتمدون بشكل خاص على اسم مجال لم يتم تسجيله، وعندما قمنا بذلك أوقفنا انتشار البرنامج الخبيث".

لكن هذا الحل الذي توصل إليه الباحث صفة لا يفيد الأجهزة التي أصيبت وشدد الباحث على ضرورة أن يقوم المستخدمون "بتحديث أنظمتهم بأسرع ما يمكن" لتفادي تعرضها لهجمات

بلبله في مستشفيات بريطانية

قال محللون إن الهجمات استهدفت منظمات في إسبانيا وأستراليا وبلجيكا وفرنسا وألمانيا وإيطاليا والمكسيك في الولايات المتحدة أقرت شركة "فيديكس" للبريد السريع بتعرضها لهجوم

وفي موسكو، أعلنت وزارة الداخلية الروسية، مساء الجمعة، أن أجهزة الكمبيوتر التابعة لها تعرضت لـ"هجوم فيروسي"، لكن دون أن توضح ما إذا كان الأمر يتعلق بالهجوم نفسه

واستهدفت الهجمات الإلكترونية كذلك خدمة الصحة العامة في بريطانيا "إن إتش إس" مما شلّ عمل أجهزة الكمبيوتر في العديد من مستشفيات البلاد

وحاولت إدارة "إن إتش إس" طمأنة السكان بالقول: "في هذه المرحلة ليس لدينا عناصر توحى بأنه تم الوصول الى بيانات المرضى".

إلا أن الهجمات أحدثت بلبلة في عشرات المستشفيات التي اضطرت إلى إلغاء إجراءات طبية وإرسال سيارات إسعاف الى مستشفيات أخرى

وأعلن المركز الوطني للأمن الإلكتروني البريطاني: "نحن مدركون أن هذه الهجمات على خدمات الطوارئ لها تأثير كبير على المرضى وأسرهم ونقوم بكل الجهود من أجل إعادة العمل في هذه الأجهزة الحيوية".

وتناقلت شبكات التواصل الاجتماعي صور لشاشات كمبيوتر تابعة لخدمة الصحة العامة عليها مطالب بدفع 300 دولار فدية على هيئة بيتكوينز مع عبارة "لقد تم تشفير ملفاتكم".

ويطالب القراصنة بدفع الفدية في غضون ثلاثة أيام وإلا فإن المبلغ سيزداد الى الضعف، أما إذا لم يتم الدفع بعد سبعة أيام فسيتم محو الملفات

لا ينتقل عبر البريد الإلكتروني

نشرت "مايكروسوفت" تصحيحاً أمنياً قبل بضعة أشهر لسد هذه الثغرة، لكن العديد من الأجهزة لم يتم تحديثها

وتقول شركة "كاسبيرسكي" للأمن المعلوماتي إن البرنامج الخبيث نشرته مجموعة "شادو بروكز" للقراصنة في نيسان/أبريل الماضي، وتضيف أنها اكتشفت هذه الثغرة من وثائق مقرصنة من وكالة "إن إس إيه".

وأوضح لانس كوتريل، المدير العلمي لمجموعة "إنتربييد" الأميركية التكنولوجية: "خلافاً للفيروسات العادية، هذا الفيروس ينتقل من كمبيوتر الى آخر عبر الخوادم المحلية وليس العناوين الإلكترونية"، مضيفاً: "هذا البرنامج يمكن أن ينتقل دون أن يقوم أحد بفتح رسالة إلكترونية أو النقر على رابط ما".

وتابع كوتريل: "هذه البرامج مؤذية بشكل خاص عندما تصيب مؤسسات كالمستشفيات إذ تعرض حياة المرضى للخطر".

وفي تغريدة علّق إدوارد سنودن، المتعاقد السابق مع "إن إس إيه" الذي كشف عمليات المراقبة على نطاق واسع التي تقوم بها هذه الوكالة في عام 2013: "لو تباحثت (إن إس إيه) في هذه الثغرة المستخدمة لمهاجمة المستشفيات عند (كشفها) وليس عند سرقة الوثائق التي ترد فيها لكان من الممكن تفادي ما يحدث".