هجوم فدية "لم يسبق له مثيل" يضرب أوروبا ويتجه إلى الأمريكيتين

الثلاثاء 27 يونيو 2017 08:06 م

وقع اليوم الثلاثاء هجوم إلكتروني من نوع انتزاع الفدية، وصف بأنه الأول من نوعه ولم يسبق له مثيل، على أجهزة الحاسب في أكبر شركة نفط روسية ومصارف في البلاد، بالإضافة إلى مطار أوكرانيا الدولي، وكذلك شركة الشحن العالمي "أي بي مولر مايرسك" A.P. Moller-Maersk.

وقالت شركة الأمن السيبراني "جروب آي بي" Group IB، التي تتخذ من موسكو مقرًا لها، إن القراصنة استغلوا الشيفرة التي طورتها وكالة الأمن القومي الأمريكية NSA والتي تم تسريبها على الإنترنت ثم استُخدِمت في هجوم الفدية الشهير "وانا كراي" WannaCry الذي تسبب فى اضطراب عالمي في شهر أيار/مايو الماضي.

وقال أحد ضحايا الهجوم السيبراني اليوم الثلاثاء، وهي شركة إعلامية أوكرانية، إن أجهزة الحاسب الخاصة بها قد تم حظرها وأنها تلقت طلبًا بقيمة 300 دولار أمريكي من العملة المشفرة بيتكوين لاستعادة إمكانية الوصول إلى ملفاتها.

ووفقًا للقطات شاشة نُشرت من قبل قناة أوكرانيا 24، جاء في رسالة القراصنة: "إذا كنت ترى هذا النص، فإن ملفاتك لم تعد متاحة، لأنها قد شُفرِّت. ربما أنت مشغول الآن في البحث عن وسيلة لاستعادة ملفاتك، ولكن لا تضيع وقتك. لا أحد يستطيع استعادة ملفاتك دون خدمة فك التشفير خاصتنا".

يُذكر أن ذات الرسالة ظهرت على أجهزة الحاسب في مكاتب ميرسك في روتردام، وذلك وفقًا للقطات شاشة نشرت على وسائل الإعلام المحلية. وقالت شركة الشحن الدنماركية إنها قد تأثرت في مناطق متعددة بسبب انقطاع الخدمة الحاسوبية. وقالت المتحدثة باسم الشركة: "يمكننا تأكيد أن الانهيار ناجم عن هجوم سيبراني".

وشملت قائمة الشركات الأخرى التي قالت إنها تعرضت لهجوم إلكتروني مفترض كلًا من شركة صناعة المعادن الروسية "ايفراز" Evraz، وشركة مواد الإنشاءات الفرنسية "سانت غوبين" Saint Gobain وأكبر وكالة إعلان عالمية WPP، ومع ذلك ليس من الواضح ما إذا كانت مشكلاتها ناجمة عن نفس الفيروس.

وسارعت شركات الأمن السيبراني لفهم نطاق تأثير الهجمات، والسعي لتأكيد شكوك بأن القراصنة قد استغلوا نفس النوع من أداة القرصنة الخاصة بوكالة الأمن القومي الأمريكية واستُغلت من قبل وانا كراي، وتحديد سبل وقف الهجوم.

وأطلق باحثون من شركات متعددة اسم "بيتيا" Petya على برمجية انتزاع الفدية، وهي برمجية خبيثة تجعل أجهزة الحاسب غير صالحة للتشغيل عن طريق تشفير محركات الأقراص الصلبة وتطالب بفدية في مقابل مفتاح رقمي لاستعادة الوصول.

ويقول ميكو هيبونين، رئيس قسم الأبحاث في شركة "إف-سيكيور" F-Secure: "إنها مثل وانا كراي مرة أخرى ومن البداية". وأضاف أنه من المحتمل جدًا أن يكون الهجوم قد استغل أداة القرصنة التي طورتها وكالة الأمن القومي الأمريكية، وتوقع أن يتم الإبلاغ عن تفشي الفيروس في الأمريكتين قريبًا، حيث تحول العمال إلى أجهزة ضعيفة، مما يسمح للفيروس بالهجوم.

وأردف هيبونين قائلًا: "لا شيء يوقف بيتيا الآن، وهذا قد يصيب الولايات المتحدة على نحو سيء للغاية".

وظهرت التقارير الأولى عن الاضطراب من روسيا وأوكرانيا، مع وصف رئيس الوزراء الأوكراني فولوديمير غروسمان الهجمات على بلاده بأنها "لم يسبق لها مثيل". وقال مستشار لوزير الداخلية الأوكراني أن الفيروس دخل إلى أنظمة الحاسب عن طريق رسائل "تصيد" كُتبت باللغتين الروسية والأوكرانية بهدف جذب الموظفين لفتحها.

وفى روسيا، قالت روزنيفت، وهي أحد أكبر منتجي النفط في العالم، أن إنتاجها الخام لم يتأثر بالانقطاع وتوقف موقع الشركة لمدة ساعتين على الأقل، لكنه عاد للعمل في تمام الساعة 14:50 بتوقيت جرينتش وقالت الشركة على موقع تويتر: "إن هجوم القرصنة قد يؤدي الى عواقب وخيمة ولكن الشركة انتقلت إلى نظام تجهيز الإنتاج الاحتياطي ولم يتم وقف إنتاج النفط ولا تكريره".

وفي أوكرانيا، قال يفهن ديخن، مدير مطار بوريسبيل في العاصمة، إن المطار تعرض للهجوم أيضًا وذكر في منشور له على موقع فيس بوك: "فيما يتعلق بالوضع غير النظامي، فإن بعض التأخير فى الرحلات ممكن الحدوث". وقال نائب رئيس الوزراء الأوكراني بافلو روزينكو إن شبكة الحاسب الحكومية قد توقفت ونشر صورة على تويتر لشاشة حاسب مع رسالة خطأ

وقال البنك المركزي الأوكراني إن عددًا من البنوك والشركات، بما فى ذلك الشركة الوطنية للطاقة الكهربائية، أُصيب بهجوم سيبراني عطل بعض العمليات وذكر البنك في بيان: "نتيجة لهذه الهجمات السيبرانية، تواجه هذه البنوك صعوبات في خدمات العملاء والقيام بعمليات مصرفية".