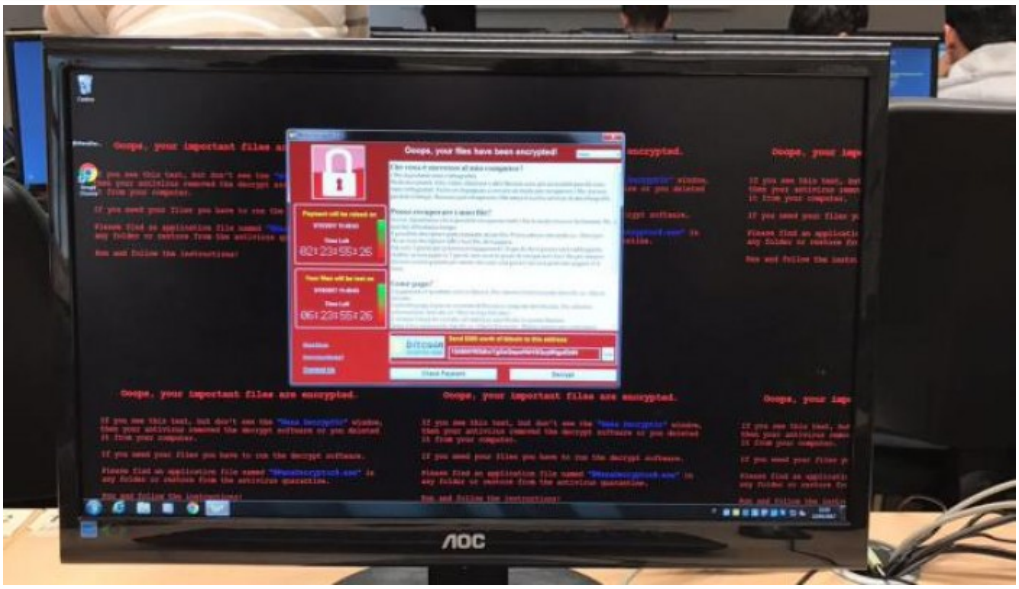
هجوم إلكتروني جديد يصيب الحواسيب



الخميس 18 مايو 2017 12:05 م

بعدما أصاب فيروس "واناكراي" المرفق بطلب فدية العالم الأسبوع الماضي، كشف خبراء المعلوماتية عن هجوم جديد واسع النطاق اخترق مئات آلاف الحواسيب في العالم عن طريق برنامج خفي يدعى "أديلكوز"، يستغل الثغرات الأمنية نفسها، لتمويل القراصنة بعملة افتراضية جديدة.

وقال الباحث نيكولا غوديبه، الخبير في الجريمة الإلكترونية في شركة الأمن المعلوماتي "بروفبوينت"، إنه بعد الهجوم الذي بدأ الجمعة "اكتشف الباحثون في الشركة هجوماً جديداً على صلة بدودة واناكراي، يسمى أديلكوز. ويستخدم (الفيروس الجديد) القادر على التواري بشكل أفضل ولغايات مختلفة، أدوات قرصنة كشفت عنها مؤخرًا وكالة الأمن القومي الأميركية ونقاط الضعف التي صححتها مايكروسوفت".

وتتمثل أعراض الهجوم بالنسبة للمستخدم في تباطؤ أداء الحاسوب ويرجح أن الهجوم بدأ في 2 أيار/مايو أو حتى في 24 نيسان/أبريل 2017 ولا يزال مستمرًا.

وأضاف روبير هولمز المسؤول في الشركة ذاتها "لا نعرف حتى الآن حجم (الأضرار) لكن مئات آلاف الحواسيب" اخترقت على الأرجح، مؤكدًا أن الهجوم "أوسع نطاقاً" من هجوم "واناكراي".

بدورها، ذكرت شركة "بروفبوينت" أنها كشفت "أديلكوز" وهي تتقصى "واناكراي" الذي شل في أوروبا خدمات الصحة العامة البريطانية، ومصانع شركة "رينو" للسيارات وغيرها.

وعملياً يتسلل هذا البرنامج الخبيث إلى حواسيب ضعيفة بسبب الخلل ذاته في نظام "ويندوز" الذي استخدمه "واناكراي"، وكشفت عنه الوكالة الأميركية للأمن القومي. وأعلنت مجموعة قراصنة "شادو بروكرز" تسريبه عبر الإنترنت في نيسان/أبريل.

وبعد اختراقه الحواسيب وتوغله فيها، يقوم البرنامج الخبيث وبشكل خفي بإنتاج وحدات من عملة افتراضية لا يمكن تتبعها تسمى "مونيرو"، شبيهة بعملة "بيتكوين". ويتم استخراج المعطيات التي تتيح استخدام هذه الأرباح وإرسالها الى عناوين مشفرة.

ورغم أن "بيتكوين" المعروفة في التداولات الافتراضية تضمن السرية لمستخدميها غير أنه يمكن تتبع مساراتها. أما "مونيرو" فهي كتيمة لأن سلسلة التحويلات فيها مشفرة تماماً وهذا ما يجعل القراصنة مولعين بها.

وأشار غوديبه إلى أنه "بالرغم من أنه أكثر مواراة وليست لديه واجهة تظهر للمستخدم، فان هجوم أديلكوز يدر عائدات أكبر على قراصنة الإنترنت. فهو يحول المستخدمين المتضررين دون إرادتهم إلى مشاركين في تمويل مهاجميهم".

أما جيروم بيلوا، الخبير في شركة "ويفستون" فأكد أن هذه الأموال الافتراضية "ليست أموالا تتم سرقتها من أحد".

وتتمثل أعراض الهجوم بالنسبة للمستخدم خصوصاً في تباطؤ أداء الحاسوب، وصعوبة الوصول إلى ملفات "ويندوز" المشتركة.

وللمفارقة، فإن "اديلكوز" وفق بيلوا "أقل ضرراً على الشركات لأنه لا يشل خدماتها ولا يركعها مثل واناكراي الذي يشفر الملفات ويطالب بفدية لفك الشيفرة".

عندما كشف عن ثغرات أمنية في نظام "ويندوز" وعن سبل استغلالها الشهر الماضي، أصيب خبراء الأمن المعلوماتي بالهلع لأنهم

يعرفون أن ذلك يفتح الباب أمام هجمات لا سابق لها وفق جيروم بيلوا

وقال خبير فرنسي آخر طلب عدم ذكر اسمه إنّ "المشكلة هي أننا لا نعرف على وجه التأكيد منشأ الهجوم" الذي لم ينفذ عبر "التصدي الاحتيالي" (فيشنك) للبريد الإلكتروني مثلما كانت عليه الحال في أكثر الأحيان

وقال نيكولا غوديه "هناك شركتان كبيرتان تستغلان الثغرات بالأدوات التي طورتها وكالة الأمن القومي الأميركية ونحن ننتظر أن تتبعها أخرى".

إلى ذلك، كشفت مدونة إعلاناً نسبته إلى قراصنة "شادو بروكرز" عن نيتهم اعتبارًا من حزيران/يونيو ومقابل مبالغ مالية "كشف معلومات كل شهر" عن نقاط ضعف تتيح قرصنة نظام "ويندوز 10" الذي كان بمنأى حتى الآن عن الهجمات

وهددت كذلك باختراق معلومات البرامج النووية والصاروخية في روسيا والصين وإيران وكوريا الشمالية وبنشر معلومات مصرفية من مختلف أنحاء العالم

في المقابل، قالت مايا هوروفيتس المحللة لدى "تشيكبوينت" في بيان إن "واناكراي يواصل انتشاره رغم تباطؤه".

وبيّنت الشركة أن القراصنة جمعوا حتى الآن 75 ألف يورو من خلال بعض الحواسيب المخترقة التي يطالبونها بالفدية

اخترق "واناكراي" أكثر من 300 ألف حاسوب في نحو 150 بلداً، بحسب توم بوسير، مستشار الأمن الداخلي للرئيس الأميركي، منذ الجمعة، وتحدث خبراء الأمن المعلوماتي عن صلة محتملة مع كوريا الشمالية