WannaCry: الفيروس الذي أبكى الآلاف



www.nasainarabic.net
@NasaInArabic NasaInArabic NasaInArabic NasaInArabic NasaInArabic

يحتدم سباق اقتناص الفرص بين شركات الحماية الرقمية والباحثين الأمنيين حول العالم من جهة، والقراصنة والمخترقين من جهةٍ أخرى، سباق يهدف إلى اكتشاف هفوات وأخطاء الشركات والمبرمجين واستغلالها لتعود على الجهة الواصلة إليها أولاً بمكاسب مادية وأرباحٍ هائلة. وبالرغم من إنفاق الشركات الملايين في سبيل تطوير سبل الحماية وسدّ الثغرات في منتجاتها الرقمية إلا أن المخترقين لا ينفكون يجدون أبوابًا خلفيّة تمكنهم من التسلل لأعمق الأنظمة والبرامج وأكثرها سريةً وأمانًا، وتطبيق علمهم الأسود وتنفيذ خططهم الشريرة لتحقيق مكاسبهم الشخصية متجاهلين مقدار الأذى والتخريب الذي سيتسببون به.

واهمٌ من يظن أنه في مأمن في العصر السبراني، فكل ثانيةٍ تمضي تحمل معها آلاف الهجمات والاختراقات المتفرقة، (ويمكنك مشاهدة البث الحي للهجمات السبرانية باستخدام الخريطة التي يقدمها عملاق الأمن كاسبرسكي **Kaspersky**).

لكن العام الفائت شهد انتشار فيروس خطير أوقف العالم أجمع على قدمٍ واحدة لأربع أيام متتالية، ونعود في هذا المقال بجولة قصيرة إلى الفترة الماضية لنستذكر سويّةً قصّة فيروس **WannaCry** الذي يعد من أقوى وأخطر الهجمات الإلكترونية في العصر الحالي.

في منتصف ليل الثاني عشر من أيار العام الماضي تعرضت مختلف دول العالم إلى هجوم إلكتروني باستخدام فيروس الفدية، الذي أطلق عليه اسم واناكراي **Wannacry**، تسبب في تشفير بيانات الأجهزة التي هاجمها مطالبًا بدفع مبلغ مالي لقاء استعادة البيانات. وقد طالت هذه الهجمات المؤسسات، والشركات، والجامعات، والوزارات، والمستشفيات، والمصانع، والبنوك، وغيرها حول العالم، من بينها النظام الصحي الوطني في بريطانيا، وشركة الاتصالات الإسبانية تيليفونيكا **Telefónica**، ومشغل الشبكات الخلوية الروسية ميغافون **Megafon**، ومنظمات كبيرة أخرى. أي باختصار، كان أي جهاز حاسوبٍ يعمل بنظام **Windows** معرضًا للإصابة بهذا الفايروس.

ما هو فيروس الفدية وكيف يعمل؟

فيروس الفدية عبارة عن برنامج خبيث يصيب الأجهزة الذكية العاملة بنظام ويندوز وأجهزة الحاسب، فيقوم بتشفير بياناتها وقفلها بحيث لا يُمكن الوصول إليها دون دفع مبلغ مالي معين، مستغلًا ثغرة أمنية في أنظمة تشغيل ويندوز **Windows** كشفت النقاب عنها وثائق سرية خاصة بوكالة الأمن القومي الأمريكية **NSA**. وقد أكدت شركة مايكروسوفت **Microsoft** أنها قامت بتحديث أنظمة تشغيل ويندوز ومضاد الفيروسات المجاني الخاص بها، لتوفر للمستخدمين حماية من الفيروس المشفر.

كيف تمكن فيروس الفدية من اختراق الأجهزة؟

تصل رسالة أو رابط من شخص مجهول، ويكون محتوى الرابط ملفًا يتضمّن برمجيات خبيثة. يغري المرسل الضحية بتنزيل الملف عبر إيهامه بأنه ملف مهم أو شخصي. يقوم المستخدم بتحميل الملف في حاسبه أو هاتفه الذكي. عندها يقوم الفيروس بتشفير البيانات المهمة في الجهاز أو بتشفير الجهاز بأكمله، بحيث لا يستطيع المستخدم الوصول إلى بياناته، ويطلب المجرم من الضحية مبلغًا ماليًا "فدية" مقابل فك التشفير عن البيانات وإعادتها لطبيعتها.

آلية إيقاف فيروس الفدية

تمكن ماركوس هاتشينز، وهو باحث بريطاني مختص بالهجمات الإلكترونية، يبلغ 22 عامًا، من إيقاف الانتشار العالمي لفيروس الفدية واناكراي. إذ اكتشف الباحث مفتاح الإغلاق **Kill Switch** الذي منع انتشار الفيروس، وصرح عبر حسابه على تويتر: "لقد اعتمد القراصنة في هجومهم بشكل أساسي على نطاق غير مسجل، ومن خلال تسجيله استطعنا إيقاف الهجوم".

ووفقًا لمدونة الباحث فقد حصل على عينة من البرمجية الخبيثة بمساعدة صديق له. وعند تشغيل العينة في بيئة تحليل، لاحظ على الفور استعلامها عن نطاق غير مسجل (وهو عبارة عن موقع غير مفعل على الإنترنت يقوم الفيروس بالاتصال به آلاف المرات كل ثانية)، فقام بتسجيله سريعًا وشرائه بمبلغ 10.69 دولار. وبينما كان النطاق ينتشر قام الباحث بتشغيل العينة مرة أخرى في بيئة افتراضية، إلا أن ما أثار دهشته هو أنه بعد تشفير الملفات الوهمية وتركها كاختبار، بدأ الفيروس بالاتصال بعناوين IPعشوائية على المنفذ 445 (وهو منفذ يستخدمه البروتوكول **SMB** الخاص بمشاركة الملفات في ويندوز).

ويتابع الباحث في تدوينته أنه قام بربط النطاق بخادم يُسمى **Sinkhole**، وتأكد من حصوله على البيانات المتوقعة من النطاق الذي سجله، ووجد أن هناك آلاف محاولات الاتصال بالخادم كادت تستهلك كامل قدرته، وسرعان ما كان قادرًا على إعداد خريطة تتبع

للفيروس ونشرها عبر تويتر. إلا أن ذلك برأيه لم يكن ليعني أننا أصبحنا بأمان، إذ يمكن لصاحب الهجوم أن يطلق نسخة أخرى باسم آخر مجهول، أو حتى بهجوم يتطلب طريقة إيقاف مختلفة. وبالفعل هذا ما حصل. وبعد نحو الشهر انتشر نوع جديد من فيروس الفدية في العالم يحمل اسم بيتيا **Petya**، مستغلًا ثغرة **SMBv1** نفسها التي استخدمها الفيروس السابق، واستطاع من خلالها تشفير بيانات نحو 300 ألف جهاز خلال شهر ونصف.

وقد ضرب الفيروس بنوكًا، وشركات اتصالات، وشركات مزودة للطاقة في دول عدة مثل روسيا، وأوكرانيا، وإسبانيا، وفرنسا، والهند، والمملكة المتحدة مطالبًا إياها بمبلغ 300$ بعملة البتكوين كفدية.

عمل الفيروس على إعادة تشغيل حواسيب الضحايا وتشفير جدول الملفات الرئيسية MFT في القرص الصلب، وتقييد الوصول إلى النظام بشكل كامل عن طريق الاستيلاء على معلومات تتعلق بأسماء الملفات، وأحجامها، وأماكن تخزينها على القرص. وقد حذر الخبراء الضحايا من دفع الفدية خوفًا من عدم قدرتهم على استرداد ملفاتهم أبدا، بعد أن قام مزود خدمة الإيميل بحذف الإيميل الذي يستخدمه المخترقون للتواصل مع الضحية.

ومن سخرية القدر، أنه وفي أيار/مايو اعتُقل ماركوس هاتشينز، الباحث الشاب الذي أنقذ العالم وأوقف الانتشار الخطير لفيروس الفدية، بتهمة تورطه في برمجيات تستهدف حسابات مصرفية. وذلك وفقًا للائحة اتهام أصدرتها وزارة العدل الأمريكية أشارت إلى تورطه بست جرائم تتعلق بإنشاء ونشر فيروس حصان طروادة **trojan Kronos** بين عامي 2014 و2015.

وبالرغم من إفشال مخطط القراصنة العام الفائت، إلا أننا لا نستطيع التنعم بالراحة والأمان لفترةٍ طويلة، فمرحلة الخطر لم تنتهِ بعد، ولن تنتهي في وقت قريب، فالفيروسات تبقى كامنة في أجهزة الضحايا لفترةٍ طويلةٍ حتى تحين ساعة الصفر، ووحدهم القراصنة يختارونها.

- التاريخ: 2018-05-11
- التصنيف: تكنولوجيا

#wannacry #فيروس الفدية #كاسبرسكي #الهجمات الإلكترونية #الاختراقات

المصادر

- ناسا بالعربي
- ناسا بالعربي
- ناسا بالعربي
- The Guardian

المساهمون

- إعداد
  - علي مرعي
  - حنان مشقوق
- تحرير
  - رأفت فياض
- تصميم
  - أحمد أزميزم

- نشر
  - روان زيدان