كل ما تود معرفته عن فيروس WannaCry

الاثنين 15 مايو 2017 07:05 م

منذ بضعة أيام، بدأ هجوم واسع الانتشار لفيروس WannaCry -الذي يستخدم برنامج التشفير Trojan- وأصبح وباءً يهدد العالم كله؛ وقد أطلق عليه وباء نتيجة انتشاره الهائل الذي أسفر عن إصابة أكثر من 45,000 حالة في يوم واحد فقط، ومن المؤكد أن الرقم الفعلي أكبر من ذلك كثيراً.

ما الذي حدث؟

تعرض عدد كبير من المؤسسات الكبيرة مثل المستشفيات البريطانية لهجوم متزامن أدى إلى تعليق أعمالها. ووفقاً للبيانات الصادرة عن أطراف ثالثة، اخترق فيروس WannaCry أكثر من 100,000 جهاز كمبيوتر، الأمر الذي جعله السبب الرئيسي وراء جذب هذا الفيروس ذلك القدر الهائل من الاهتمام.

وقد جاءت روسيا في المرتبة الأولى من حيث تعرضها لهجمات الفيروس. كما عانت عدة دول مثل أوكرانيا والهند وتايوان من هذا الفيروس. وفي المجمل، بلغ عدد الدول المصابة بالفيروس 74 دولة، وكل ذلك في اليوم الأول فقط من الهجوم.

ما المقصود بفيروس WannaCry؟

بوجه عام، يهاجم فيروس WannaCry على مرحلتين: المرحلة الأولى يطلق عليها استغلال الثغرات ويهدف فيها إلى التسلل والانتشار، والمرحلة الثانية يطلق عليها التشفير ويحدث ذلك عن طريق برنامج تشفير يتم تنزيله إلى الكمبيوتر بعد إصابته بالفيروس.

وهذا هو الفرق الرئيسي بين فيروس WannaCry ومعظم برامج التشفير الأخرى. وليتمكن الفيروس من التسلل إلى جهاز كمبيوتر عبر برنامج تشفير مشترك، يجب أن يرتكب المستخدم خطأً مثل النقر على رابط مريب يسمح لبرنامج "الوورد" بتشغيل وحدة ماكرو خبيثة، أو تنزيل مرفق مريب من رسالة بريد إلكتروني. ويمكن أن تصاب النظم بفيروس WannaCry بدون القيام بأي خطأ.

فيروس WannaCry: استغلال الثغرات والانتشار

فقد استفاد مبتكرو فيروس WannaCry من ثغرة نظام Windows المعروفة باسم EternalBlue، واستغلوا نقطة ضعف عالجتها شركة مايكروسوفت في التحديثات الأمني MS17-010بتاريخ 14 مارس من العام الحالي. ومن خلال استخدام هذه الثغرة، استطاع المخربون الوصول عن بُعد إلى أجهزة الكمبيوتر وتثبيت برنامج التشفير.

إذا قمت بتثبيت التحديث، ولم تعد نقطة الضعف موجودة في جهاز الكمبيوتر الخاص بك، فلن تجدي أي هجمات لاختراق الكمبيوتر عن بُعد نفعاً. ويود فريق الأبحاث والتحليل العالمي الخاص بشركة Kaspersky Lab فريق GreAT الإشارة على وجه خاص إلى أن معالجة نقطة الضعف وتصحيحها لن يردع بأي شكل من الأشكال برنامج التشفير عن العمل. من ثم إذا ساعدت بطريقة ما على تشغيل برنامج التشفير (راجع أعلاه لمعرفة ما إذا ارتكبت خطأ أم لا) فلن تجدي المعالجة والتصحيح نفعاً.

وبعد اختراق فيروس WannaCry جهاز الكمبيوتر بنجاح، سيحاول الانتشار عبر الشبكة المحلية للوصول إلى أجهزة الكمبيوتر الأخرى، مثلما تفعل دودة الكمبيوتر. ثم يمسح برنامج التشفير أجهزة الكمبيوتر الأخرى بحثاً عن نقطة الضعف نفسها التي يمكن استغلالها بمساعدة ثغرة EternalBlue، وعندما يعثر فيروس WannaCry على آلية ضعيفة، فإنه يهاجمها ويقوم بتشفير ملفات داخلها.

وقد تبيَّن أن فيروس WannaCry يستطيع الانتشار إلى الشبكة المحلية بكاملها وتشفير كل أجهزة الكمبيوتر الأخرى المتصلة بهذه

الشبكة عند اختراقه كمبيوتر واحد؛ مما جعل الشركات الكبيرة أكثر من عانى من هجمات فيروس WannaCry – فكلما زاد عدد أجهزة الكمبيوتر الأخرى في الشبكة المحلية زاد الضرر.

فيروس WannaCry: برنامج التشفير

ولما كان فيروس WannaCry برنامج تشفير (يُطلق عليه بعضهم اسم تشفير WCrypt أو برنامج فك التشفير WannaCry حتى ولو كان من الناحية المنطقية برنامج تشفير وليس برنامج فك تشفير) فهو يعمل مثل برامج التشفير الأخرى؛ أي أنه يضع شفرة على الملفات الموجودة في أجهزة الكمبيوتر ثم يطلب فدية مقابل فك تشفيرها. وهو يعد إلى حد كبير صورة أخرى من برنامج التشفير الشهير CryptXXX Trojan السيئ السمعة.

يقوم فيروس WannaCry بتشفير ملفات مختلفة الأنواع (والقائمة الكاملة هنا) تشمل -بالطبع- المستندات المكتبية، والصور، ومقاطع الصوت، والملفات الأرشيفية، وتنسيقات الملفات الأخرى التي ربما تحتوي على بيانات شديدة الأهمية للمستخدم. ويتم إعادة تسمية امتدادات الملفات المشفرة إلى .WCRY (أي اسم برنامج التشفير) ثم تصبح الملفات غير قابلة للوصول على الإطلاق.

بعد ذلك، يُغيِّر برنامج التشفير Trojan خلفية سطح المكتب إلى صورة تحتوي على معلومات عن العدوى والإجراءات التي يجب على المستخدم فعلها لاستعادة الملفات. وينشر فيروس WannaCry إشعارات في شكل ملفات نصية تحتوي على المعلومات نفسها في كل المجلدات في الكمبيوتر حتى يضمن تسلُّم المستخدم للرسالة.

وكالعادة، تنتهي كل هذه الأمور إلى تحويل مبلغ معين بعملة البيتكوين إلى محفظة الأشرار. وبعد ذلك ربما يفكون التشفير من كل الملفات. في البداية، طلب المجرمون السيبرانيون 300 دولار أمريكي ثم قرروا زيادة السعر؛ حيث طلب آخر إصدارات من فيروس WannaCry فدية تبلغ 600 دولار أمريكي.

كما يهدد المخربون المستخدم بأن الفدية ستزداد بعد 3 أيام، وسيكون من المستحيل فك شفرة الملفات بعد 7 أيام. ونحن نوصي بعدم دفع الفدية للأشرار؛ نظراً لعدم وجود ضمان على أنهم سيفكون شفرة الملفات بعد تسلُّمهم الفدية. في الواقع، أظهر الباحثون أن مبتزين سيبرانيون آخرين -في بعض الأوقات- يحذفون ببساطة بيانات المستخدم، مما يعني أنه لا يمكن مادياً فك شفرة بقايا الملفات، رغم ذلك إلا أنهم يستمرون في طلب فدية وكأن شيئاً لم يحدث.

كيف أوقف تسجيل مجال انتشار العدوى مؤقتاً؟ ولماذا لم ينتهِ هذا الوباء بعد؟

ومن المثير للاهتمام أن هناك باحثاً يحمل اسم Malwaretech استطاع إيقاف انتشار العدوى مؤقتاً عن طريق تسجيل مجال اسمه طويل وبلا معنى على الإطلاق عبر الإنترنت.

فقد تبيَّن أن بعض إصدارات فيروس WannaCry راسلت هذا المجال نفسه، وعند عدم تسلُّمها رداً إيجابياً تقوم بتثبيت برنامج التشفير وتبدأ أعمالها القذرة. أما إذا كان هناك رد (أي تم تسجيل المجال) فيوقف البرنامج الخبيث كل أنشطته.

وبعد العثور على مرجع هذا المجال في رمز برنامج التشفير Trojan، سجَّل الباحث المجال مما أدى إلى توقف الهجوم مؤقتاً. وعلى مدار الفترة المتبقية من اليوم، تمت مراسلة هذا المجال عشرات الآلاف من المرات مما يعني إنقاذ عشرات الآلاف من أجهزة الكمبيوتر من التعرض للعدوى.

هناك نظرية ترى أن هذه الوظيفة المبنية في فيروس WannaCry تعمل وكأنها "قاطع دائرة" في حال حدوث خطأ ما، وترى نظرية أخرى يساندها الباحث نفسه أن هذه إحدى الطرق المستخدمة لتعقيد تحليل سلوك البرنامج الخبيث. في بيئات الاختبار المستخدمة في البحث، غالباً ما كان يُرسل الرد الإيجابي عن عمد من أي مجال، وكان برنامج التشفير Trojann -في هذه الحالة- لا يفعل أي شيء في بيئة الاختبار.

ولكن للأسف، يكفي للأشرار تغيير اسم المجال المشار إليه سابقاً بوصفه "قاطع دائرة" في الإصدارات الجديدة من برنامج التشفير "Trojan" حتى يستأنف الفيروس هجومه. لذا من المرجح جداً ألا يكون اليوم الأول لهجوم فيروس WannaCry هو اليوم الأخير.

كيف أواجه فيروس WannaCry؟

لسوء الحظ، لا يجود شيء يمكن فعله الآن لفك شفرة الملفات التي اخترقها فيروس WannaCry وقام بتشفيرها (ولكن يعمل باحثونا من أجل إيجاد حل). وهذا يعني أن الطريقة الوحيدة لمواجهة الاختراق هي عدم التعرض للاختراق في المقام الأول.

<u>إليك بعض النصائح حول كيفية الوقاية من الاختراق وتقليل الضرر:</u>

إذا كنت تملك بالفعل حلاً أمنياً من Kaspersky Lab مثبتاً في نظامك، فإننا ننصحك بالقيام بما يلي: ابدأ بعملية مسح يدوية للأجزاء الشديدة الأهمية بالنسبة لك، وإذا كشف الحل الأمني عن وجود برنامج خبيث مثل MEM:Trojan.Win64.EquationDrug.gen (هذه هي الطريقة التي تقوم بها حلولنا الأمنية المضادة للفيروسات بكشف فيروس WannaCry)، فأعد تشغيل النظام الخاص بك.
إذا كنت عميلاً حالياً لدينا، فحافظ علىوحدة "System Watcher" في وضع التشغيل، فمن الضروري مكافحة الأنواع الجديدة لهذا الفيروس التي قد تظهر.

تثبيت تحديثات البرامج. يدعو هذا الوباء بكل جدية إلى تثبيت تحديثات النظام الأمنية MS17-010من جانب كل مستخدمي نظام Windows، خاصة عندما تصدر شركة مايكروسوفت تحديثات للنظم التي لم تعد تدعمها رسمياً مثل: نظام Windows XP، أو نظام Windows 2003. أحدثكم بمنتهى الجدية، قوموا بتثبيت هذه التحديثات الآن! فالآن هو ما يُطلق عليه الوقت المهم للغاية.
أنشأ نسخاً احتياطية من الملفات بانتظام وخزِّن النسخ في أجهزة تخزين غير متصلة دائماً بالكمبيوتر. إذا كان لديك نسخة احتياطية حديثة، فلن تكون الإصابة بالفيروس كارثة، ولكنها ستكون مضيعة لساعات عديدة في إعادة تثبيت النظام. إذا لم تكن ترغب في إنشاء نسخ احتياطية بنفسك، فبإمكانك الاستفادة من خدمة النسخ الاحتياطي المدمجة في برنامجKaspersky Total Security التي يمكنها تنفيذ هذه العملية بصورة آلية.
استخدم برنامجاً موثوقاً لمكافحة الفيروسات. يستطيع برنامج Kaspersky Internet Security الكشف عن فيروس WannaCryy عند محاولته اختراق الجهاز، وعند محاولته الانتشار عبر الشبكات. وعلاوة على هذا، تملك وحدة System Watcher المدمجة مزية إلغاء جميع التغييرات غير المرغوب فيها، مما يعني أنها ستمنع تشفير الملفات حتى مع تلك الفيروسات الخبيثة غير المدرجة بعد في قواعد بيانات برامج مكافحة الفيروسات.