باحث في أمن الإنترنت يوقف فيروس الفدية "بدون قصد"

الأحد 14 مايو 2017 08:05 م

كشف باحث بريطاني في أمن الإنترنت لـ بى بى سى كيف أنه أوقف "عن طريق الصدفة" انتشار فيروس "الفدية" رانسوموير الخبيث الذي ضرب مئات المنظمات، بما في ذلك خدمة هيئة الرعاية الصحية البريطانية.

وكان الرجل، البالغ من العمر 22 عاما، والمعروف بالاسم المستعار مالويرتك، قد حصل على أجازة لمدة أسبوع من العمل، لكنه قرر التحقيق في رانسوموير بعد سماعه عن الهجوم السيبراني العالمي.

وقد تمكن من وقف انتشاره عندما وجد ما يبدو أنه "مفتاح قتل" في تعليمات البرمجيات الخبيثة.

وقال لـ بى بى سى "في الواقع تم الأمر جزئيا عن طريق الصدفة"، بعد قضاء الليلة في التحقيق، "فأنا لم يغمض لي جفن".

وعلى الرغم من أن اكتشافه لم يصلح الأضرار التي سببها رانسوموير، فإنه منعها من الانتشار إلى أجهزة كمبيوتر جديدة، وتمت الإشادة به باعتباره "بطل الصدفة."

وقال لـ بي بي سي "أعتقد أن ذلك صحيحا"، مشيرا إلى أن رئيسه منحه أسبوعا أجازة للتعويض عن أجازته.

ما الذي اكتشفه بالضبط؟

في البداية لاحظ الباحث أن البرامج الضارة تحاول الاتصال بعنوان ويب معين في كل مرة تصيب جهاز كمبيوتر جديد.

ولكن عنوان الويب الذي كان يحاول الاتصال به خليط طويل من الحروف ولم يتم تسجيله.

فقرر مالويرتك تسجيله وقام بشرائه بمبلغ 10.69 دولار (8 جنيهات إسترلينية). فسمح له امتلاكه لعنوان الويب أن يرى أين أجهزة الكمبيوتر التي تتصل به، مما أعطاه فكرة عن مدى انتشار رانسوموير.

وتسبب بذلك وبشكل غير متوقع في كشف جزء من تعليمات البرمجة الخاصة برانسوموير، مما مكنه من وقف انتشاره.

هل ذلك يعني هزيمة رانسوموير؟

في حين يبدو أن تسجيل عنوان الويب قد أوقف انتشار رانسوموير من جهاز إلى جهاز، فإنه لا يصلح أجهزة الكمبيوتر المصابة بالفعل.

وحذر خبراء الأمن أيضا من ظهور أشكال جديدة من البرامج الضارة التي تتجاهل ظهور "مفتاح القتل".

ويقول مالويرتك: "لقد أوقفنا هذا الفيروس، ولكن سيأتي آخر لن يمكننا إيقافه، فهناك الكثير من المال في هذا الأمر، وليس لديهم سبب للتوقف، ولن يبذلوا الكثير من الجهد لتغيير تعليمات البرمجة والبدء من جديد."