فيروس الكمبيوتر وفرص التحوّل إلى قاتلٍ حقيقيّ

كتبه برين بوسي | 4 مايو ,2019

ترجمة وتحرير: نون بوست

في مرحلة ما من حياتي، لم أكن أؤمن بوجود برامج الكمبيوتر الضارة. وخلال السنوات التي سبقت 1991، لم أتعرض، لا أنا ولا أحد من معارفي، إلى حادثة لها علاقة بهذه البرامج. لقد كنت أعتقد أن فيروسات الكمبيوتر موجودة في أفلام هوليوود فحسب.

في نهاية المطاف، أدركت أن هذه الفيروسات أمر واقع، ولكنها لم تكن مثلما صوّرتها الأفلام. وقد كان أول فيروس واجهته في حياتي يُدعى "يانكي دودل"، حيث أصاب ملفات كانت موجودة في نظام تشغيل الحواسيب "إم إس-دوس" وامتدادات الملفات "إي اكس إي". ومن المرجّح أن هذا الفيروس يُعرف بسبب تشغيله لأغنية "يانكي دودل" في وقت محدّد خلال اليوم.

> لم تكن هذه الفيروسات بشكل خاص، إلى جانب بعض الفيروسات الأخرى التي ظهرت في ذلك الوقت، ضارة إلى حد ما، على الأقل مقارنة بالمعايير المعتمدة في الوقت الراهن

بعد ذلك بوقت قصير، تعرّض حاسوبي إلى فيروس آخر يحمل اسم "كوكي مونستر"، الذي يعمل على تعطيل أي نشاط أقوم به من خلال عرض صورة "كوكي مونستر" على الشاشة مرفقة برسالة تقول "أعطني ملف تعريف ارتباط". وفي حال كتبت كلمة "كوكي"، في إشارة إلى ملف تعريف ارتباط، فستختفي لفترة من الزمن، ويمكنك حينها استئناف ما كنت بصدد القيام به. وبمرور الوقت، تظهر هذه الصورة من جديد وبشكل مستمر. ولكن، بإمكانك حظر ظهورها نهائيًا من جهاز الكمبيوتر عن

طريق كتابة كلمة "أوريو".

لم تكن هذه الفيروسات بشكل خاص، إلى جانب بعض الفيروسات الأخرى التي ظهرت في ذلك الوقت، ضارة إلى حد ما، على الأقل مقارنة بالمعايير المعتمدة في الوقت الراهن. وفي حين أن بعض سلالات فيروس "يانكي دودل" قادرة على تعطيل النظام بشكل كامل، يمكن لأي برنامج مضاد للفيروسات في ذلك الوقت التخلص منها وإعادة الأمور إلى طبيعتها.

البرامج الضارة تصبح خبيثة

بمرور الوقت، أضحت البرامج الضارة خبيثة على نحو متزايد. وعلى الرغم من أنه يمكن وصف هذه البرامج، التي ظهرت في أواخر الثمانينيات وأوائل تسعينيات القرن الماضي، بأنها مضرة وغريبة الأطوار، إلا أن البرامج الضارة في الوقت الحالي يمكن أن تكون عدائية للغاية. على سبيل المثال، وقع استخدام برنامج الفدية لاحتجاز بيانات مهمة كرهائن مقابل دفع الفدية المطلوبة.

في تناقض صارخ، أصبح الهدف من العديد من البرامج الضارة اليوم (التي

> يُعتقد أن الكثير منها مرتبط بالجريمة المنظمة أو الدول المارقة) يتمثل في الحصول على المال

كان ظهور برامج الفدية مؤشرًا واضحًا على حدوث تحوّل كبير في الأهداف التي وضعها مؤلفو البرامج الضارة. وفي وقت مبكر، كان مؤلفو هذه البرامج مهتمين بشكل أساسي بإلحاق بعض الأذى من خلال الاشتراك فيما يسمى "التخريب الإلكتروني". وفي وقت لاحق، أصبح هؤلاء المؤلفين مهتمين باكتساب سمعة سيئة عن طريق إنشاء برامج ضارة تتميز بقدرات غير مسبوقة، على غرار "فان لوف" و"كود ريد" و"ميدوم" و"سلامر"، التي حظيت باهتمام كبير من قبل وسائل الإعلام.

في تناقض صارخ، أصبح الهدف من العديد من البرامج الضارة اليوم (التي يُعتقد أن الكثير منها مرتبط بالجريمة المنظمة أو الدول المارقة) يتمثل في الحصول على المال. ولا يعد ذلك مرتبطًا بالضرورة ببرامج الفدية فحسب، على الرغم من أن جزءًا كبيرًا يتعلق بها. فضلًا عن ذلك، ظهر معدّنو العملات الرقمية، الذين يسعون إلى الاستيلاء على كمبيوتر الضحية، ثم سرقة العملة الرقمية الموجودة فيه.

تجدر الإشارة إلى أن البرامج الضارة تطوّرت بشكل كبير لدرجة أن آثارها لم تعد مقتصرة على العالم الرقمي فحسب. وفي فترة من الفترات، كان أسوأ شيء يمكن أن يحدث نتيجة إصابة الكمبيوتر بإحدى البرامج الخبيثة هو فقدان البيانات. ولكن، اليوم أصبحت آثار هذه البرامج تمتد إلى العالم الواقعي، حيث يمكنها أن تسعى إلى سرقة هويتك وتصفية حسابك المصرفي، وابتزازك، إلى غير ذلك. ولكن، لسائل أن يسأل: إلى أي مدى يمكن أن تمتد قدرات هذه البرامج الضارة؟ وهل يمكن تصميم برامج ضارة لارتكاب جريمة قتل؟

> على الرغم من أنني لم أعني أن أصيب منزل أيّ شخص بفيروس، إلا أن الفكرة التي كنت أحاول إثارتها هي أن الأتمتة تنطوي على تحديات أمنية كامنة لم يسبق وأن تطرّق إليها أحد في ذلك الوقت

ظاهريًا، يبدو أن فكرة البرامج الضارة القاتلة مثيرة للسخرية. ففي نهاية المطاف، لا يمكن لجهاز الكمبيوتر حمل سلاح بشكل فعلي وإطلاق النار على شخص ما. ومع ذلك، يوجد العديد من الطرق الأخرى لإنجاز هذه المهمة. ولفهم ما ذُكر آنفًا بشكل أفضل، يجدر بنا العودة بالزمن إلى الوراء والحديث عن بعض الطرق التي يمكن لأجهزة الكمبيوتر التفاعل من خلالها مع العالم المادي.

في سنة 2001، اعتدتُ على الكتابة لصالح مجلة لم تعد موجودة الآن، كانت تُعنى بالمواضيع المتعلّقة بأتمتة المنزل. وفي أحد الأعمدة التي كنت أكتب فيها، كتبت مازحًا أن أحد طموحاتي هو أن أكون أول شخص يكتب عن فيروس يصيب أنظمة أتمتة المنزل. وعلى الرغم من أنني لم أعني أن أصيب منزل أيّ شخص بفيروس، إلا أن الفكرة التي كنت أحاول إثارتها هي أن الأتمتة تنطوي على تحديات أمنية

كامنة لم يسبق وأن تطرّق إليها أحد في ذلك الوقت. وبصراحة، لن يكون من الصعب للغاية السيطرة على إحدى الأنظمة الأولى لأتمتة الأجهزة المنزلية.

ضرر غير مؤذٍ أو برامج قاتلة؟

لكن، فكر فيما قد يحدث في حال تمكّن شخص ما من الاستيلاء على نظام أتمتة المنزل. وإذا كان هذا الشخص شقيًّا، فقد يتلاعب بالأضواء أو قد يقوم بإيقاف تشغيل مكيف الهواء. ولكن، في حال كان هذا الشخص يملك نية سيئة حقًا، فيمكنه اقتحام المنزل من خلال فتح الأبواب. وبقدر ما تبدو هذه الفكرة مثيرة للقلق، إلا أنه ينبغي على المرء أن يدرك أنه في العصر الحالي لم تعد المنازل فحسب مرتبطة بالإنترنت. لقد أصبحت جميع أنواع الأجهزة الإلكترونية تقريبا متّصلة بالإنترنت.

على سبيل المثال، أصبحت معظم السيارات الجديدة التي يقع بيعها اليوم متصلة بالإنترنت أيضًا، وكذلك العديد من أجهزة إنترنت الأشياء وأجهزة الأتمتة الصناعية. لذلك، ومع أخذ ذلك بعين الاعتبار، لنعد إلى إمكانية ارتكاب البرامج الضارة جرائم قتل أم لا.

قبل بضعة أشهر، كتبتُ مقالًا تحدثت فيه عن سيارة كنت أمتلكها. وقد أصيبت الأجهزة الإلكترونية فيها بخلل تقني، حيث كانت السيارة في بعض الأحيان تُشغَّل بصفة تلقائية أثناء تواجدي في موقف السيارات. لحسن الحظ، تمكنت من الضغط على الفرامل قبل أن تصطدم السيارة بأي شيء. وإذا تسبب خلل عشوائي أصاب الكمبيوتر في حدوث هذا النوع من الحوادث، فلك أن تتخيل الضرر الذي قد ينجم عن إصابة الأجهزة بأحد البرامج الضارة.

في حال كانت فكرة إصابة جهاز كمبيوتر السيارة بأحد البرامج الضارة بعيدة المنال، فهناك إعلان

تجاري حديث "لأون ستار" يوضح أن هذه الخدمة الإلكترونية قد تمكّنت من إبطال عملية سرقة سيارة عن بُعد. ويمكن أن يُستغل هذا النوع من روابط الاتصالات في محاولة لإصابة سيارة بفيروس أو التحكم فيها، حيث يمكن أن يستهل فيروس بسهولة التحكم في مدخلاتها الخاصة للتسبّب في وقوع حادث خطير.

> في عالم متصل بالإنترنت أكثر، سيكون من المهم اتخاذ إجراءات تمنع البرمجيات الخبيثة من إصابة الأنظمة الحساسة

مؤخرًا، نشرت مجلة "إم آي تي تكنولوجي ريفيو" مقالًا حول برنامج ضار، يدعى "ترايتون"، واعتبرته أكثر برامج الحاسوب الضارة فتكًا في العالم. ووفقًا لما ورد في هذا المقال، نشر قراصنة الإنترنت هذا الفيروس القاتل في محطة البتروكيماويات في المملكة العربية السعودية. وسمح هذا البرنامج الخبيث لقراصنة الإنترنت بالسيطرة على جميع أنظمة المحطة. وعلى الرغم من أنه لم يقع تفعيل هذا الفيروس الخبيث أبدًا، إلا أنه كان من الممكن أن يُستخدم للتسبّب في حدوث خلل كبير وتعطيل أنظمة الحماية، ما يعرض حياة الإنسان للخطر.

أقرّ بأن مثال سيارتي الذي اعتمدته هو مثال نظري، وأن فيروس "ترايتون" في محطة البتروكيماويات وقع إبطال مفعوله قبل أن يتسبب في أي ضرر. ومع ذلك، هناك بعض الحوادث التي تسببت فيها البرمجيات الخبيثة في ضرر كبير لحياة البشر. من جهة أخرى، أثر برنامج الفدية الإلكتروني، "واناكراي"، على عدد من المستشفيات خلال 2017، مما أدى إلى شلّ الأنظمة المستخدمة في علاج المرضى. ولحسن الحظ، لم يتسبب هذا الفيروس في وفاة أي مريض، لكن وفقا لبرالاكس، تسبب هذا الفيروس في تأخير رعاية المرضى، مما أثر بشكل سلبي على نتائج فحوصاتهم.

البرمجيات الخبيثة القاتلة: أمر ينبغي أخذه بعين الاعتبار

على حد علمي، لم تقع حتى الآن أي حادثة وقع فيها ربط البرامج الضارة مباشرة بإزهاق أرواح بشرية. ومع ذلك، كان هذا الأمر وشيك الحدوث. ويبدو أنه من المحتم أن البرمجيات الخبيثة ستكون مسؤولة في النهاية عن وفاة شخص ما. ويمكن أن تؤدي البرمجيات الخبيثة القاتلة إلى وقوع خسائر جسيمة. وعليك فقط أن تتخيل ما كان يمكن أن يحدث لو أن فيروس "ترايتون" تسلّل إلى محطة للطاقة النووية.

في عالم متصل بالإنترنت أكثر، سيكون من المهم اتخاذ إجراءات تمنع البرمجيات الخبيثة من إصابة الأنظمة الحساسة. وسيتعين على الشركات المصنعة الاعتماد على النوع ذاته من ممارسات حماية أجهزة إنترنت الأشياء المستخدمة للتحكم في الوصول إلى خوادم الشبكة.

المصدر: تاك جينكس

رابط المقال : https://www.noonpost.com/27603/