فايروس الفدية

ما هو فايروس الفدية؟

فايروس الفدية هو نوع من البرامج الخبيثه تم تصميمه لاحتجاز الملفات أو حتى نظام تشغيل الكمبيوتر كرهينة، من ثم يطالبك بدفع فديه لكي تتمكن من استعادة بياناتك. لقد أصبحت برمجيات فايروس الفدية شائعة جدًا لأنها مربحة جدًا للمجرمين.

مثل معظم البرامج الضارة، تبدأ برامج الفدية بإصابة الكمبيوتر، وهذا يحدث غالبًا عندما تفتح مرفقًا مصابًا أو تنقر على رابط ضار في بريد إلكتروني مشبوه. بمجرد إصابة حاسوبك بفيروس الفدية، فإنه يقوم بتشفيربعض الملفات الموجودة على قرص التخزين – او ربما حتى كامل قرص التخزين- أو أي شيء آخر متصل بحاسوبك وعندها لن يكون بإمكانك الوصول إلى ملفاتك. من ثم سيتم اعلامك أن الطريقة الوحيدة لاستعادة ملفاتك هي الدفع للمجرمين (من هنا جاءت تسميه فايروس الفدية). في بعض الأحيان، يهدد المجرمون أيضًا بنشر ملفاتك الخاصة للعلن إذا لم تدفع الفدية. قد يطلب المجرمون الدفع في شكل عملة رقمية لا يمكن تعقبها، مثل بيتكوين Bitcoin. عند دفعك للفدية، قد يمنحك المجرمون حق الوصول إلى ملفاتك، ولكن لا توجد هناك أي ضمانات. في بعض الأحيان سيأخذون أموالك و يتركون جهازك مصابًا دون فك التشفير أو يستمرون في طلب المزيد من المال.

الحماية من الإصابة

يمكنك حماية حاسوبك من الإصابة بفيروسات الفدية بنفس الطريقة التي تحميه بها ضد الأشكال الأخرى من البرامج الضارة. فيما يلي ثلاث خطوات رئيسية:

- **قم بتحديث الأنظمة والبرامج الخاصة بك:** غالبًا ما يستهدف مجرمو الإنترنت أجهزة الكمبيوتر من خلال الاستفادة من العيوب الغير مرقعة (المعروفة باسم الثغرات الأمنية) في البرمجيات ونظام التشغيل. وكلما كان نظام التشغيل والبرمجيات محدثة باستمرار، قل عدد نقاط الضعف المعروفة، وزادت الصعوبة على مجرمي الإنترنت لاستهدافها. لذلك، تأكد من تفعيل التحديث التلقائي لأنظمة التشغيل والتطبيقات والأجهزة الخاصة بك.

- **تفعيل برنامج مكافحة الفيروسات:** قم باستخدام أحدث برامج مكافحة الفيروسات من مصادرها الموثوقة. هذه الأدوات تم تصميمها للكشف عن البرامج الضارة وإيقافها. مع ذلك، لا يمكن لبرامج مكافحة الفيروسات حظر جميع البرامج الضارة أو إزالتها، وعادة لا يمكنها استرداد ملفاتك بعد الإصابة ببرامج الفدية. مجرمو الإنترنت

يطورون و يبتكرون باستمرار وسائل وتقنيات جديده لنشر برمجيات ضارة أكثر تعقيدا ويصعب كشفها .في المقابل، يقوم شركات انتاج برامج مكافحة الفيروسات بتحديث منتجاتهم باستمرار بإمكانيات جديدة للكشف عن .البرامج الضارة .من نواحٍ عديدة، لقد أصبح سباقًا للتسلح، بحيث يحاول الطرفان التفوق أحدهما على الآخر

- **كن يقظًا**: غالبًا ما يخدع مجرمو الإنترنت الأشخاص لحثهم على تثبيت برامج الفدية وأشكال أخرى من البرامج الضارة من خلال هجمات التصيد عبرالبريد الإلكتروني. على سبيل المثال، قد يرسل لك مجرم الإنترنت بريدًا إلكترونيًا يبدو شرعيًا ويحتوي على مرفق أو رابط. قد يبدو لك أن البريد الإلكتروني وارد من مصرفك أو حتى من صديق. مع ذلك، إن قمت بفتح الملف المرفق أو نقرت على الرابط، عندها تنشط التعليمات البرمجية الضارة لتصيب جهازك. إذا كانت الرسالة تخلق إحساسًا قويًا بالإلحاح أو تبدو جيدة جدًا لدرجة يصعب تصديقها، فقد تكون هجومًا. كن يقظًا - يلعب المهاجمون السيبرانيون على عواطفك. المنطق والفطره السليمة غالبًا ما تكون أفضل دفاع لك.

النسخ الاحتياطي للملفات الخاصة بك قبل الإصابة

من غير العملي افتراض أنك ستتمكن دائمًا من منع الإصابة، فإن أفضل دفاع لك ضد برامج الفدية هو أخذ النسخ الاحتياطية. إذا كان لديك نسخة احتياطية من المستندات المهمة والملفات الأخرى، فسيكون لديك خيار الاسترداد من النسخة الاحتياطية بدلاً من دفع الفدية. من المهم أن تستخدم أسلوب النسخ الاحتياطي التلقائي الذي يعمل على نسخ جميع ملفاتك احتياطيًا بانتظام و أيضا أن تختبر إجراءات الاستعادة للتأكد من أنه يمكنك استردادها إذا ما دعت الحاجة. هناك العديد من حلول النسخ الاحتياطي السحابية والمحلية البسيطة التي يمكنك تثبيتها على جهازك والتي ستقوم بعمل نسخ احتياطية لجميع ملفاتك بشكل آمن ومنتظم.

المحرّر الضيف

ليني زيلتسرLenny Zeltser هو مدير امن المعلومات في شركة Axonius ، وهي شركة لإدارة أصول الأمن السيبراني. كما يقوم بتدريس مكافحة البرامج الضارة والكتابة في معهد SANS ناشط على Twitter باسمlennyzeltser @ ويكتب لمدونة .zeltser.com

الموارد

هل لديك نسخة احتياطية لبياناتك؟: https://www.sans.org/security-awareness-training/resources/got-backups
عبارات المرور: https://www.sans.org/security-awareness-training/ouch-newsletter/
أهمية التحديثات: https://www.sans.org/security-awareness-training/resources/power-updating
SANS FOR610 Course - Reverse Engineering Malware: https://sans.org/for610

ترجمها للعربية: محمد سرور، فؤاد ابو عويمر، درويش الحلو، اسلام الكرد