أوتش! | ديسمبر (كانون الأول) ٢٠١٤

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- نظرة عامة
- كيف تعمل برامج مكافحة الفيروسات
- نصائح عامة لاستخدام برامج مكافحة الفيروسات

ما هي برامج مكافحة الفيروسات

نظرة عامة

برنامج مكافحة الفيروسات هو تطبيق يتم تثبيته على جهاز الكمبيوتر المكتبي أو المحمول لحمايته من الإصابة ببرامج خبيثة. مصطلح «البرمجيات الخبيثة» يشمل أي نوع من البرامج الضارة مثل الفيروسات والديدان الشبكية وأحصنة طروادة وبرامج التجسس. مصطلح malware يأتي من الجمع بين malicious وتعني «الخبيثة» وsoftware وتعني «البرمجيات». إذا أصبح جهازك مصاباً بأحد البرمجيات الخبيثة، فهذ يمكن مهاجمي الإنترنت من أحد وربما كل الامور لتالية: تخزين كل تتم كتابته باستخدام لوحة المفاتيح، الإطلاع على ملفات المستندات الخاصة بك، أو استخدام جهازك لمهاجمة الآخرين. على عكس ما يعتقد بعض المستخدمين، جميع أنظمة التشغيل، بما في ذلك «ماك» و «لينكس»، يمكن أن تتعرض للاصابة.

المحرر الضيف

المحرر الضيف. جيك وليامز مؤسس Rendition Infosec (www.renditioninfosec.com) وهو مدرس معتمد ومُعِد لبعض الدورات بمعهد سانز. وهو نشط على تويتر @MalwareJake وله مدونة malwarejake.blogspot.com.

يمكنك شراء برنامج مكافحة الفيروسات كبرنامج مستقل، أو في كثير من الأحيان يكون مثبتاً على الاجهزة الجديدة عندما تشتريها. المشكلة هي أن برامج مكافحة الفيروسات لم تعد قادرة على مواكبة مهاجمي الإنترنت الذين يطورون أنواع جديدة من البرمجيات الخبيثة باستمرار. هناك الكثير من الإصدارات الجديدة للبرامج الخبيثة كل يوم ولا يمكن لبرنامج مكافحة الفيروسات الكشف والحماية من كل هذه البرمجيات الخبيثة. ولذا علينا أن نعرف أنه رغم أن برامج مكافحة الفيروسات تساعد على حماية جهازك، فإنه لا يمكنها اكشاف جميع أنواع البرمجيات الخبيثة. لكى يتضح المفهوم، دعونا ننظر في كيف تعمل معظم هذه البرامج المضادة للفيروسات.

كيف تعمل برامج مكافحة الفيروسات

بشكل عام، البرامج المضادة للفيروسات تستخدم طريقتان للكشف عن البرامج الضارة. كشف التوقيع وكشف السلوك. كشف التوقيع يعمل مثل نظام المناعة البشري و يقوم بمسح جهازك و يبحث عن الخصائص أو التوقيعات المعروفة لبرامج خبيثة. هذا المسح يستخدم قائمة تحتوي على توقيعات على البرمجيات الخبيثة المعروفة، إذا كان هناك برنامج على جهازك يطابق أحد التوقيعات في هذه القائمة، فهذا البرنامج يصنف كبرنامج خبيث. مثل نظام المناعة البشري، هذه القائمة لا بد أن تحدث باستمرار، مثل لقاح الانفلونزا، للحماية ضد سلالات جديدة. كشف التوقيع يمكن أن يحمي فقط ضد ما يطابق نمط في القائمة. المشكلة هي أن المهاجمين مستمرون فى تطوير برمجيات خبيثة جديدة وبسرعة عالية مما يجعل مصممي برامج مكافحة الفيروسات غير قادرين على التماشي مع هذه السرعة. ونتيجة لذلك، حتى وإن كنت تمتلكآخر التحديثات (اقائمة الأحدث لتواقيع البرمجيات الخبيثة) ، فهناك دائما برامج خبيثة جديدة لا يمكن لبرنامج مكافحة الفيروسات كشفها.

ما هي برامج مكافحة الفيروسات

الطريقة الأخرى للكشف عن البرمجيات الخبيثة هي من خلال مراقبة سلوك البرامج المثبتة على جهازك. عندما يقوم برنامج بعمل مثير للريبة مثل محاولة الوصول إلى ملف محمي أو تعديل برنامج آخر، يقوم برنامج مكافحة الفيروسات الكاشف للسلوك بتنبيهك إلى ذلك. هذه الطريقة توفر حماية ضد الأنواع جديدة من البرمجيات الخبيثة التي لا تكون موجودة بعد في قائمة التواقيع. المشكلة مع هذا النهج هو أنه يحذرك من جميع البرامج التي تنهج سلوك معين (حتى التطبيقات الغير خبيثة) أي أن الكثير من هذه التحذيرات غير صحيحة. أنت كمستخدم للجهاز، قد تكون غير متأكد هل تسمح لبرنامج معين بتنفيذ ما يحاول فعله أم لا, وبمرورالوقت تصبح أنت غير مبالى بهذه التحذيرات. و بهذه الطريقة قد توافق لجميع البرامج للتخلص من التحذير مما قد يتسبب في اصابة جهازك. وبالإضافة إلى ذلك، في الوقت الذي يتم فيه الكشف عن سلوك برنامج خبيث، فان هذا البرنامج الخبيث قد يكون بالفعل أشتغل على جهازك وأنت لا تعرف ماذا فعل هذا البرنامج الخبيث بجهازك قبل كشفه.

على الرغم من أن برامج مكافحة الفيروسات هي وسيلة ضرورية لحماية جهازك ضد الهجمات. فهذه البرامج لا يمكنها الكشف عن جميع البرامج الخبيثة. في النهاية فأنت صاحب الدور الأساسي في حماية جهازك.

مكافحة الفيروسات جزء مهم لتأمين جهازك، كلما أمكن ذلك نحن ننصحك بتثبيتها واستخدامها. ومع ذلك، فإن النقطة الرئيسية هي ان نتذكر أنه بغض النظر عن الكيفية التي يعمل بها برنامج مكافحة الفيروسات، فإنه لا يمكن أبدا حمايتك من جميع أنواع البرمجيات الخبيثة. في نهاية المطاف، هذه البرمجيات لا تستطيع وحدها حمايتك، فأنت صاحب الدور الأساسي في حماية جهازك ضد مهاجمين الانترنت.

نصائح عامة لاستخدام برامج مكافحة الفيروسات

١. الحصول على برنامج مكافحة الفيروسات فقط من مصادر معروفة و موثوق بها. هناك حيلة منتشرة يستخدمها مهاجمين الانترنت بتوزيعهم برامج مكافحة فيروسات وهمية هي في الواقع برامج خبيثة.

٢. تأكد من أن لديك أحدث نسخة من برنامج مكافحة الفيروسات وأن برنامج مكافحة الفيروسات يتم تحديثه تلقائياً. إذا لم تتصل بالانترنت من جهازك لفترة من الوقت، ولم تحدث برنامج مكافحة الفيروسات فمن المهم جداً تحديث برنامج مكافة الفيروسات بمجرد جهازك بشبكة الأنترنت.

٣. تأكد من أن برنامج مكافحة الفيروسات يقوم بفحص وسائط التخزين الخارجية مثل وصلة USB بمجرد توصيلها بالجهاز.

٤. انتبه إلى التحذيرات التي تظهر على الشاشة والتنبيهات التي يتم يصدرها برنامج مكافحة الفيروسات. تشمل معظم التنبيهات خيار الحصول على مزيد من المعلومات أو توصية حول ما يجب القيام به. إذا كنت تستخدم الجهاز الخاص بجهة عملك فعليك الاتصال بمكتب الدعم الفني لمساعدتك في اتختذ القرار عند ظهور رسالة التحذير.

٥. لا تعطل أو تلغى تثبيت برنامج مكافحة الفيروسات لأنك تشعر أنه يبطئ جهازك ويمنعك من الوصول الى موقع ما على شبكة الانترنت

ما هي برامج مكافحة الفيروسات

أو يمنعك من تثبيت تطبيق أو برنامج معين. تعطيل برنامج مكافحة الفيروسات يعرض جهازك لمخاطر عديدة و يمكن أن يؤدي إلى وقوع أختراق أمني خطير لجهازك. إذا لاحظت وجود مشكلات مستمرة على الجهاز الخاص بجهة عملك فعليك التواصل مع مكتب الدعم الفني لمساعدتك. أما إذا ا لاحظت وجود مشكلات مستمرة على جهاز الخاص بجهة عملك فعليك التواصل مع مكتب الدعم الفني لمساعدتك ستمرت التحذيرات على جهازك لحاص عليك الاتصال بالشركة الموردة لبرنامج مكافحة الفيروسات الذي تستخدمه أو زيارة موقعهم على الانترنت لمزيد من المعلومات أو استبدال برنامج مكافحة الفيروسات ببرنامج آخر.

٦. لا تثبت أكثر من برنامج لمكافحة الفيروسات على جهازك في نفس الوقت. القيام بذلك على الأرجح يسبب تعارض ويمكن أن يقلل من أمن جهازك.

٧. تعلم كيفية التعرف على التحذيرات التي تصدر من برنامج مكافحة الفيروسات الذي تستخدمه. المهاجمون قادرون على انشاء مواقع خبيثة تصدر تحذيرات مماثلة لما تصدره برامج مكافحة الفيروسات وتتوي هلى رابط لحل المشكلة واقع الأمر أن هذا الرابط سيأخذك لموقع به برمجيات خبيثة يمكنها مهاجمة جهازك بمجرد زيارتها.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول الى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة http://www.securingthehuman.org.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة المتخصصين في أمن المعلومات بكلية علوم وهندسة الحاسب الآلي بجامعة الملك فهد للبترول والمعادن.

مصادر إضافية

موقع لتقييم برامج مكافحة الفيروسات والمقارنة بينها (باللغة الانجليزية):	http://www.av-test.org/en/
عدد أوتش حول الهندسة الاجتماعية:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_aa.pdf
عدد أوتش حول هجمات تصيد المعلومات عبر البريد الإلكتروني:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_aa.pdf
عدد أوتش حول "تم اختراق جهازي، ماذا أفعل الآن:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-2014-05_aa.pdf

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين.