البرمجيات الخبيثة: الدودة، وحصان طروادة، والبوت والفرق بينها

التعامل مع البرمجيات الخبيثة المعروفة باسم مالوار (Malware)، هو واقع نواجهه جميعاً عند الاتصال بالإنترنت. لا أحد يريد أن يفتح بريده الإلكتروني ليكتشف أنه قام للتو بإرسال ملف مصاب إلى جميع أصدقائه، أو أنه قد تم محو البيانات الخاصة به بسبب فيروس. على الرغم من أن معظم الناس يخشون الفيروسات، إلا أنهم على نحو مثير للدهشة أيضاً لا يدركون ما هي البرمجيات الخبيثة وكيف تقوم بعملها الخبيث. سوف نستعرض هنا بعض المستويات الأساسية للبرمجيات الخبيثة وكيف تقوم بعملها.

أساسيات البرمجيات الخبيثة

قبل أن نتعمق في الفئات والأنواع، نحن بحاجة إلى فهم واضح للبرمجيات الخبيثة. تُعرف البرمجيات الخبيثة باسم آخر، وهو الكود

الخبيث **malicious code** أو مالكود (**malcode**). وتعني كلمة "البرمجيات الخبيثة" (**malicious**) أو اختصاراً مال (**mal**) ـ المشتقة من الكلمة اللاتينية "**mallus**" والتي تعني سيءـ مهاجمة أو تدمير أو تغيير أو إتلاف الجهاز المضيف الذي تعمل عليه أو الشبكة التي يتصل بها هذا الجهاز. وباختصار، إن المالكود هو كود خطير، والمالوار هي برمجيات خطيرة.

على الرغم من أن بعض البرمجيات الخبيثة يمكن أن تدخل إلى الجهاز من خلال نقاط الضعف في نظام التشغيل أو المتصفح، إلا أن معظمها يتطلب من المستخدم تحميلها أو بطريقة أخرى تنشيطها عن طريق النقر على رابط أو فتح ملف. وما أن تصبح البرمجيات الخبيثة نشطة داخل النظام، ستعمل على تنفيذ التعليمات الواردة في الكود الخاص بها.

ليس هناك شك في أن البرمجيات الخبيثة يمكن أن تسبب الكثير من الضرر، مثل تغيير كيفية عمل التطبيقات الأخرى وتشفير أو تدمير البيانات، ولكن لديها حدود. فعلى نحو مماثل للبرمجيات المشروعة **legitimate software**، لا يمكن للبرمجيات الخبيثة إجراء أي تغييرات على مكونات الجهاز، هذا يعني أنه حتى في أسوأ السيناريوهات يمكن للمستخدم أن يفقد كل بياناته، ولكن يمكن استعادة الجهاز عن طريق إلغاء تثبيت نظام التشغيل والتطبيقات الأخرى وإعادة تثبيتها مرة أخرى.

ومع ذلك، يُفضل تجنب البرمجيات الخبيثة تماماً. إحدى الطرق لحماية مستخدمي الكمبيوتر أنفسهم هي أن يكونوا على علم بأنواع التهديدات الموجودة.

فيروسات الكمبيوتر: الإصابة بالرشح من الملفات

الفيروسات هي على الأرجح أشهر أنواع البرمجيات الخبيثة. وعلى نحو مماثل للفيروسات في العالم الطبيعي، لفيروسات الكمبيوتر غرضين رئيسيين هما: نسخ نفسها والانتشار. ويعتمد الضرر الفعلي للفيروس على من قام بتصميمه، ومن الممكن أن يكون الفيروس حميداً حيث ينتشر دون أن يتسبب بأي شيء للجهاز الذي أصابه.

لسوء الحظ، فإن معظم الفيروسات تدخل إلى برامج أخرى، وإلى السكربتات **scripts** ومجموعات أخرى من التعليمات التي تعمل على الجهاز، وتقوم بإجراء تغييرات عليها. وبهذه الطريقة يمكن للفيروسات تدمير البيانات، وإيقاف البرامج وحتى منع الكمبيوتر من الإقلاع.

الديدان Worms: تحفر طريقها لشبكتك

تُشبه الديدان الفيروسات بشكل كبير فهي على الأغلب تنسخ نفسها وتنتشر، لكنها تستخدم آلية وصول مختلفة. بدلاً من الانتشار عبر الملفات المصابة، تستخدم الديدان نقاط الضعف في الشبكة للانتقال من جهاز مضيف إلى آخر. وهذا يعني أن الديدان لا تتطلب من المستخدم فتح أي شيء أو تفعيلها على أي حال، فهي تخترق شبكة المستخدم من خلال ثغرة في نظام أمانها.

وفور دخولها إلى الشبكة، تبدأ الدودة بالبحث عن مكان آخر لتنتشر. بينما تتحرك بين الأجهزة المضيفة في الشبكة، يمكن للدودة التسبب بنفس أنواع الضرر الناتج عن الفيروس. تحمل معظم الديدان أيضاً حمولة **payload**، والتي هي في جوهرها فيروس كمبيوتر تنقله الدودة لكل جهاز جديد تصله. على سبيل المثال، حملت دودة بلاستر **Blaster Worm** ـالتي ظهرت في عام 2003– الفيروس الذي تسبب بإعادة إقلاع أجهزة الكمبيوتر التي تعمل بنظام التشغيل ويندوز عدة مرات. ومع ذلك، يمكن للديدان الخالية من الحمولة والتي تبدو غير ضارة أن تتسبب بحمل زائد على الشبكة، أو تطلق "هجمات حجب الخدمة" **denial-of-service attack**.

أحصنة طروادة Trojans: مهتمة في السيطرة على على جهازك أكثر من اختطاف هيلين من طروادة

مثل الحصان الخشبي الأسطوري الذي تم استخدامه لخداع الناس في طروادة حتى يدخل اليونانيين إليها، تسمح أحصنة طروادة الخبيثة للناس الآخرين بالدخول إلى الأجهزة الخاصة بك. ومثل الفيروس أو الدودة، يمكن لحصان طروادة تشغيل الكود الذي سيُدمر أو يُغير جهازك والبيانات الخاصة به. ومع ذلك، يتم تصميم معظم أحصنة طروادة لفتح باب خلفي **back door** في نظام يمكن أن يستخدمه القراصنة للسيطرة والتحكم بالجهاز.

وعلى عكس الفيروسات والديدان، أحصنة طروادة لا تنسخ نفسها أو تحاول الانتشار إلى أجهزة كمبيوتر متعددة، فهي توجد بشكل عام في ملف متخفٍ يعتمد على المستخدم لتنشيطه.

البوتات:Bots عندما تحكم الروبوتات العالم

هي برامج مؤتمتة تقوم بعملية معينة. هناك العديد من البوتات المشروعة التي تساعد في عمل الإنترنت بسلاسة، مثل برنامج **Googlebot**. ومع ذلك، يمكن أيضاً استخدام البوت لتنفيذ العديد من العمليات المشكوك بها، مثل إصابة أجهزة الكمبيوتر غير المحمية وإضافتها إلى شبكة بوت خبيثة (**botnet**).

يمكن أن ينفذ الشخص المسؤول عن تشغيل "البوت نت" العديد من أنواع الهجمات المختلفة، عن طريق التحكم عن بُعد بعدد من أجهزة الكمبيوتر. وعلى سبيل المثال، يمكن للبوت سرقة البيانات من جهاز الكمبيوتر المصاب، بما في ذلك جهات الاتصال الخاصة بالمستخدم وكلمات السر وغيرها من المعلومات الخاصة. وقد تصبح أجهزة الكمبيوتر المصابة من قبل البوت أيضاً نقاط لنشر البريد المزعج والبرمجيات الخبيثة وغيرها من المفاجآت السيئة لمستخدمين آخرين.

وأخيراً، يمكن للبوت استخدام الشبكة المصابة لإطلاق هجمات حجب الخدمة وغيرها من الهجمات على نطاق واسع. ربما يكون البوت أقوى أنواع البرمجيات الخبيثة فهو قادر على الانتشار بأساليب مختلفة والقيام بالهجوم بطرق عديدة.

برامج التجسس Spyware

لا تهاجم برامج التجسس جهاز الكمبيوتر الخاص بك، لكنها لا تزال ضمن تعريف البرمجيات الخبيثة. يقوم برنامج التجسس بجمع المعلومات من جهاز الكمبيوتر الخاص بك وإعادة إرسالها إلى منشئ البرنامج، لذلك سيكون بمقدوره على نحو محتمل تسجيل الدخول إلى حسابك المصرفي أو بيع المعلومات الشخصية الخاصة بك. وغالباً ما يتخفّى برنامج التجسس كبرنامج مجاني لتنفيذ وظيفة أخرى، أو قد يكون مع حزمة برمجيات مشروعة.

كيفية التعامل معها: المنطق السليم يصنع الكثير

الآن وبعد أن تعرفت إلى كل هذه التهديدات، كيف يمكنك حماية نفسك؟

إن قليلاً من التعليم والمنطق السليم هما الجانبان الأكثر أهمية. الأمر بسيط جداً: لا تفتح مرفقات البريد الإلكتروني من أشخاص لا تعرفهم، ولا تنقر على روابط من الغرباء. إن قصور الفيروسات يكمن في أنها تعمل عن طريق انتشارها بواسطة الملفات المصابة. في الغالبية العظمى من الحالات، يجب على المستخدم فتح ملف لتنشيط الفيروس.

والشيء الآخر الذي يمكن القيام به هو التحديث المستمر لبرنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك. إن مصطلح "مكافحة الفيروسات" أصبح قديماً بعض الشيء. ستقوم معظم الحزم بحمايتك ليس فقط من الفيروسات، ولكن أيضاً من تهديدات أخرى مثل الديدان وأحصنة طروادة، وأيضاً من برامج التجسس. هناك العديد من الخيارات لبرامج الحماية سواء مجانية أو غير مجانية، من شأنها أن تعطيك حماية قوية من معظم التهديدات.

وأخيراً، إن إبقاء نظام التشغيل ونظام مكافحة الفيروسات الخاصين بك محدثين يكون كافياً في كثير من الأحيان لإبقاء البرمجيات الخبيثة بعيدة عنك. تعمل شركات مثل مايكروسوفت جاهدة لحماية أنظمة التشغيل التي توفرها من أي تهديدات جديدة. قد لا تلاحظ شيئاً مختلفاً أثناء استخدام الكمبيوتر بعد تحديث الويندوز، ولكن عليك أن تعلم أنه تم إجراء تحديثات كبيرة لسد الثغرات الأمنية التي تم اكتشافها.

الخلاصة

لن تذهب البرمجيات الخبيثة بعيداً. في الواقع، كلما زاد عدد الأشخاص الذين يستخدمون الأجهزة المتصلة بالإنترنت، فإن عدد وأنواع البرمجيات الخبيثة من المرجح أن يزداد أيضاً. إن معرفة البرمجيات الخبيثة هي الخطوة الأولى لحماية نفسك من الهجمات. يمكن تجنب معظم البرمجيات الخبيثة من خلال تطبيق بعض المنطق السليم عند تحميل وفتح الملفات من مصادر مختلفة. ومع ذلك، للحصول على الأمان الكامل، عليك ببرنامج ضد الفيروسات موثوق وجدار حماية **firewall** مناسب، فذلك لا يمكن هزيمته!

- التاريخ: 2017-03-16
- التصنيف: تكنولوجيا

#الانترنت #البرمجيات الخبيثة #فيروسات الكمبيوتر #أحصنة طروادة الخبيثة #الكمبيوتر

المصادر

- techopedia
- الصورة

المساهمون

- ترجمة
  - دانا أسعد
- مُراجعة
  - شريف دويكات
- تحرير
  - روان زيدان

- تصميم
  - هادي أبو حسون
- نشر
  - مي الشاهد