أساسيات في الحاسب وحمايته

الفايروسات the viruses

تعريف الفايروسات

هي برامج يتم انتاجها خصيصا لكي تلحق نفسها ببعض البرامج المشهورة وذلك عن طريق تزييف او تعديل بسيط للتوقيع الخاص بالبرنامج الاصلي (مجموعة من الارقام الثنائية) وتتمكن هذة البرامج من تدمير البرامج والمعلومات او اصابة الاجهزة بالخلل بعد طرق فمنها ما يبدا بالعمل مباشرة عند الاصابة وبعضها عند تنفيذ بعض الاوامر والبعض الاخر عندما يحين التوقيت والتاريخ المبرمج سلفا كما تتميز هذة الفابروسات بقدرتها على التكاثر والانتقال من جهاز الى اخر عن طريق الملفات المتبادلة بين المستخدمين

انواع الفايروسات

يتم تصنيف الفايروسات على اساس طريقة هجومها (طريقة الاصابة بها) فهناك

boot sector virus

تعتبر من اقدم الفايروسات المعروفة لدى المستخدمين حيث تستطيع ان تصيب القرص الصلب والاقراص المرنة وتنتشر عن طريقها من مستخدم الى اخر وتكمن خطورة هذا النوع من الفايروسات في قدرتها على اصابة جزء اساسي من اي قرص صلب او لين وهو الجزء المخصص لتوجية الجهاز في كيفية تحميل برنامج نظام التشغيل ويقوم هذا الفيروس بتحميل نفسة للذاكرة في كل مرة يتم فيها تشغيل الجهاز

file infector virus

هذا النوع من الفايروسات يلحق نفسة كملف في اي برنامج تنفيذي ويتميز هذا النوع من الفايروسات بقدرتة على الانتشار بعدة طرق وبسرعة مهولة منها الاقراص مرنة والاقراص المدمجة ورسائل البريد الالكتروني كملف ملحق كما يمكنة الانتقال من البرامج المجانية المتوفرة في الانترنيت وتكمن خطورتة في قدرتة على الانتشار السريع واصابة بقية الملفات الموجودة في البرامج التنفيذية الاخرى

macro viruses

هذا النوع ايضا سريع الانتشار بين المستخدمين خاصة انة قادر على الانتشار بكل الطرق كالاقراص مرنة والمدمجة والبريد الالكتروني والبرامج المجانية وكذالك اثناء التحميل او تنزيل البرامج من الاجهزة الخادمة

ومن الجدير بالذكر ان هذا النوع لا يصيب الا البرامج التطبيقي التي صمم ليصيبة اساسا فمثلا لو كان هناك فيروس مصمم ليصيب برنامج تحرير الكلمات والنصوص فانة لا يستطيع الحاق الاذى ببرنامج اخر مثل برنامج قواعد المعلومات وهكذا ولكن يستطيع ان يصيب اي ملف تم انشاؤة بواسطة البرنامج المستهدف

كيفية عمل الفايروسات

يقوم من انشا او برمج الفيروس ببرمجة الفيروس وتوجية الاوامر لة حيث يقوم بتحديد الزمان و

متى وكيف يبدا الفيروس بالنشاط وعادة ما تعطى فرصة كافية من الوقت للفيروس حتى يضمن حرية الانتشار دون ان يلفت الانتباة ليتمكن من اصابة اكبر عدد ممكن من المستخدمين وتختلف الفيروسات من حيث بدا النشاط فهناك من يبدا بتاريخ او وقت محدد وهناك من يبدا بالعمل بعد تنفيذ امر معين في البرنامج المصاب وهناك من الفيروسات يبدا بالنشاط بعد التكاثر والوصول الى رقم معين من النسخ .
وبعد ان ينشط الفيروس يقوم الفيروس بعدة انشطة تخريبية حسب الغرض من انشاء ذلك الفيروس فهناك ما يقوم بعرض رسالة تستخف بالمستخدم او تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة وهناك انواع اخرى تقوم بحذف او تعديل بعض الملفات وهناك من يقوم بتكرار ونسخ نفسة حتى يشل جهازك تماما وهناك انواع اشد فتكا فتقوم بمسح كل المعلومات من قرصك الصلب

اشهر الهجمات الفيروسية

لقد بدا الفيروس بالانشار في منتصف الثمانينات من القرن الماضي ومنذ ذلك الوقت تطورت وظهرت انواع اكثر شراسة وسرعة خاصة مع نهاية عقد التسعينات ولقد وصل العدد المعروف من الفيروسات الشهيرة والنشخ المعدلة منها الى اكثر من خمسين الف فيروس وهي في ازدياد كل يوم وهناك الاف من الفيروسات الجديدة الفتاكة المتواجدة داخل المختبرات ومراكز الابحاث في دول عديدة وهي مخزنة كاسلحة الكترونية ضد الاعداء في حالة الحرب لتخريب اجهزة الكمبيوتر التابعة للعدو اشهر الفيروسات التي انتشرت بطريقة وبائية وبسرعة فائقة لتصيب الملايين من الاجهزة حول العالم

melissa virusفيروس ميليسا

وهي من اسرع الفيروسات التي انتشرت في عام 1999 وهي من نوع ماكروفيروس متخصص في اصابة البريد الالكتروني وهي تقوم بالانتشار عن طريق الالتصاق في برامج النصوص كملحق في رسالة البريد الالكتروني وما ان يقوم المستخدم بفتح الملف الملحق بالرسالة ال ويبدا الفيروس بالعمل حيث يستطيع الوصول الى قائمة المراسلة الخاصة بالمستخدم ليقوم بارسالة نفس الرسالة الى اول خمسين عنوان دون علمك وتستمر على نفس المنوال

explore zip

وهوة فيروس مشابة للسابق ولكنة مدمر اكثر حيث يقوم بمسح كل الملفات التي انشات بواسطة برنامج لتحرير النصوص

bubble boy: مشابة للسابق

cih virus

وهوة من اخطر الفيروسات لانة قادر على مسح القرص الصلب واصابة البرنامج الاساسي المسؤول عن المخرجات والمدخلات للجهاز مما قد يتسبب في تلف اللوحة الام

love virusفيروس الحب

وهوة مشابة لفيروس مليسا ولكنة متخصص في اصابة برنامج مايكروسوفت اوت لوك لادارة البريد الالكتروني ولقد اثار الرعب في بداية هذا العام نتيجة لسرعة انتشارة

كيفية الوقاية

طبعا ليس هناك افضل من الحصول على برنامج متخصص ضد الفيروس مع متابعة تحديث البرنامج كل شهر وكذلك الحذر من فتح الملفات الملحقة في الرسائل الالكترونية ولمزيد من

المعلومات يرجى الاطلاع على المقالة الخاصة بهذا الخصوص

البرامج المضادة للفيروس

هي البرامج التي تقوم بحمايتك من هجمات الفيروسات وبقية البرامج التي تشكل تهديدا امنيا على معلوماتك وتستطيع ان تحدد هذة الملفات الضارة القادمة من اي مصدر مثل الاقراص المدمجة و الاقراص مرنة والرسائل الالكترونية وكذلك يمكنها رصد هذة البرامج في القرص الصلب وتتمكن هذة البرامج من مسح او تعطيل عمل البرامج المهددة لسلامة الجهاز وملفات البرامج الموجودة على جهازك ويتكون برنامج مضاد للفيروسات من جزئين مختلفين :

التشغيل المباشر عند الدخول

وهذا الجزء يعمل تلقائيا عند تشغيل (الدخول) البرامج او تنزيل الملفات من الانترنيت وهو ما يعرف ب

on access element

التشغيل عند الطلب

وهذا الجزء يعمل عندما تطلب انت منة ذلك وهو متخصص بالكشف عن الفيروسات واحصنة طروادة في القرص الصلب والاقراص مرنة والاقراص المدمجة وهو ما يعرف ب(on demand element

كيفية عملها

ان البرامج المضادة للفيروسات عبارة عن تقنية مسح ورصد للبرامج المشبوهة التي تتميز بخصائص معينة او تحتوي على صيغة معينة من البرمجة عبارة عن مجموعة من الارقام الثنائية وهي تعرف ب(التوقيع) ويتم ذلك بالطريقة التالية

يقوم البرنامج المضاد بالنظر الى كل الملفات والبرامج ذات الطبيعة التنفيذية

تتم مقارنة التوقيع الموجود على كل ملف بالتواقيع المخزنة في قاعدة المعلومات الخاصة بالبرنامج المضاد للفيروسات

والجدير بالذكر ان كل برنامج مضاد للفيروسات يحتوي على توقيع اكثر من 40000 نوع من الفيروسات واكثر من عشرة الاف من تواقيع احصنة طروادة ويقوم باعلام المستخدم عنة

يقوم البرنامج المضاد بتخيير المستخدم بين مسح او تعطيل الفيروس او باصلاح الخلل بطريقة الية

تكنلوجا الكشف يقوم مصنعي ومبرمجي الفيروسات عادة بتعديل او تحريف التوقيع الاصلي لبعض البرامج الشهيرة و ذلك لتضليل المستخدم والبرنامج الاصلي وتقوم تكنلوجا الكشف عن هذا التزوير والتعديل بواسطة المقارنة السريعة بين التواقيع الاصلية والمزيفة

مدى الاعتمادية على هذا البرنامج

ليس هناك برنامج مضاد للفيروسات قادر على حمايتك مائة في مائة ولكن اذا قمت بالتحديث المستمر لبرنامجك كل اسبوع فانك سوف تحصل على حماية تصل الى 95% وذلك لان هناك اكثر من ستمائة من الفيروسات الجديدة واحصنة طروادة كل شهر

تكاليف البرامج المضادة للفيروسات واشهرها

ان البرامج المتخصصة في الحماية من الفيروسات رخيصة الثمن ولذلك احرص على اقتناء واحد لحمايتك من الفيروسات واحصنة طروادة

نصائح عامة بخصوص برامج الفيروسات
دائما قم بشراء برنامج من شركة متخصصة تقوم بخدمة التحديث الدائم مجانا عبر شبكة الانترنيت لمدة عام على الاقل من تاريخ شراؤك للبرنامج وقم بتجديد البرنامج لديك كل اسبوعين او كل شهر على الاكثر لان هناكالكثير من الفيروسات الجديدة كل فترة والطريقة الوحيدة لتجنب الاصابة بالفيروسات هي استمرارية التحديث لبرامجك مع اجراء الكشف الكامل لكل الملفات الموجودة في جهازك بعد كل تحديث

مفاهيم خاطئة عن برامج الحماية من الفيروسات
لعل من اكثر المفاهيم الخاطئة بين المستخدمين على مستوى العالم هي الاعتقاد بان اقتناء برنامج مضاد للفيروسات يمنع ويحمي من هجوم الهاكرز والمخترقين وهذا طبعا ليس صحيح حيث ان هذة البرامج تحميك فقط من الفيروسات والديدان وتستطيع التعرف على معظم احصنة طروادة ولكن لا تقوم بغلق المنافذ والمعابر الموجودة في جهازك والتي تمكن المخترقين من الوصول الى جهازك ومعلوماتك و لذلك فانة من الضروري ان تقوم بالحصول على برنامج متخصص يعرف بجدران اللهب fire wall

طرق العدوى بالفيروسات

تعتبر الرسائل الالكترونية اكبر مصدر للفيروسات وذلك لسهولة اضافتها كملفات ملحقة وسرعة انتشارها على الشبكة في زمن قصير جدا وتعتبر نسخ البرامج المقلدة مصدرا اخر للفيروسات . اما المصدر الاقل انتشار فهي الاقراص مرنة ولكنها اخطر بكثير من المصادر الاخرى وذلك لتعاملها المباشر مع نظام بدء التشغيل لجهازك
اما احصنة طروادة وديدان الانترنيت فهي شبيهة جدا بالفيروسات ولكنها تختلف في الهدف فمثلا الديدان تقوم بمسح او تدمير المعلومات من البرامج التطبيقية كبرامج المحاسبة وقواعد المعلومات فقط كما ان بمقدور هذة الديدان التكاثر حتى تملا الذاكرة وتعطل الجهاز الضحية اما احصنة طروادة فهي لا تدمر ولا تسمح المعلومات ولكنها تتجسس وتقوم بجمع المعلومات والبيانات ومن ثم ارسالها لمصدرها (مرسل برنامج حصان طروادة) وهو عادة ما يكون فرد او موقع او منظمة لجمع المعلومات

hackingالاختراق

هو قيام شخص او اكثر بمحاولة الوصول الى جهازك او الشبكة الخاصة بشركتك عن طريق شبكة الانترنيت وذلك باستخدام برامج متخصصة (سكانرز) في فك الرموز والكلمات السرية وكسر الحواجز الامني واستكشاف مواطن الضعف في جهازك او شبكة معلوماتك وعادة ما تكون المخارج (بوابات العبور للمعلومات) الخاصة بالشبكة المحلية وهذة اسهل الطرق للوصول الى جميع ملفاتك وبرامجك وبالنسبة للمخترقين اصبحت المهمة عسيرة بعض الشيء وذلك في اختراق المؤسسات والمواقع الكبيرة بعد تطور نظم الدفاع وبرامج الحماية ولكن بالنسبة لاجهزة الافراد ما زالت الابواب مفتوحة .