فايروس:

فيروس الحاسوب (بالإنجليزية: Computer Virus) هو نوع من أنواع البرمجيات التخريبية الخارجية، صُنعت عمداً بغرض تغيير خصائص ملفات النظام. تتكاثر الفيروسات عن طريق توليد نفسها بنسخ شفرتها المصدرية وإعادة توليدها، أو عن طريق إصابة برنامج حاسوبي بتعديل خصائصه. إصابة البرامج الحاسوبية يتضمن، ملفات البيانات، أو قطاع البوت في القرص الصلب.

خواص الفيروسات

برنامج قادر على التناسخ Replication والانتشار.

الفيروس يربط نفسه ببرنامج أخر يسمى الحاضن host.

لا يمكن أن تنشأ الفيروسات من ذاتها.

يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

يمكن للفيروسات التخفي في عدّة ملفات

مكونات الفيروس

يتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي:

آلية التناسخ The Replication Mechanism وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.

آلية التخفي The Protection Mechanism وهو الجزء الذي يخفي الفيروس عن الاكتشاف.

آلية التنشيط The Trigger Mechanism وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس (Michelangelo) الذي ينشط في السادس من آذار من كل عام.

آلية التنفيذ The Payload Mechanism وهو الجزء الذي ينفذه الفيروس عندما يتم تنشيطه.

الوقاية من الفيروس

استخدام برامج للكشف عن الفيروسات في الجهاز.

احتفظ بنسخ احتياطية من البرامج والملفات الموجودة على الحاسب.

إجراء الفحص على البرامج المحملة (المنزلة) أو المنقولة من شبكة الإنترنت قبل تشغيلها.

استخدام برمجيات الجدار الناري .

استخدم نظام التشغيل جنو/لينكس فهو يعتبر أكثر أمانا وفيه فيروسات قليلة عكس نظام التشغيل ويندوز.

لا تشغل أي برنامج أو ملف لا تعرف ما هو بالضبط.

الحذر من رسائل البريد الإلكتروني غير معروفة المصدر وفحصها قبل الإقدام على فتحها.

تنزيل البرامج والألعاب من مواقع ومصادر موثوقة (مصادرها الأصلية).

أنواع الملفات التي يمكن أن يصيبها الفيروس

بشكل عام الفيروس تصيب الملفات التنفيذية أو الملفات المشفرة غير النصية مثل التالية:

الملفات ذاتية التنفيذ مثل ملفات ذات امتداد (.EXE ,.DLL,.COM)ضمن أنظمة التشغيل دوس وميكروسوفت ويندوز، أو (ELF) في أنظمة لينكس.

سجلات الملفات والبيانات (VOLUME BOOT RECORD) في الأقراص المرنة والصلبة والسجل رقم (0) في القرص الصلبMASTER BOOT.

ملفات الأغراض العامة مثل ملفات الباتش والسكريبت في ويندوز وملفات الشل في يونيكس.

ملفات الاستخدام المكتبي في نظام تشغيل مايكروسوفت ويندوز التي تحتوي ماكرو مثل مايكروسوفت وورد ومايكروسوفت إكسل ومايكروسوفت أكسس.

قواعد البيانات وملفات الأوتولوك لها دور كبير في الإصابة ونشر الإصابة لغيرها لما تحويه من عناوين البريد الالكتروني.

الملفات من النوع (نسق المستندات المنقولة) وبعض نصوص لغة ترميز النص الفائق احتمال احتوائها على كود خبيث.

الملفات المضغوطة مثل ZIP

ملفات إم بي 3.

أنواع الفيروسات

فيما يلي بعض أنواع الفيروسات:

الفيروسات متعددة القدرة التحويلية (المخادع): هذه الفيروسات لديها القدرة الديناميكية على تحويل وتغيير شفرتها عند الانتقال من ملف إلى أخر لكي يصعب اكتشافها.

فيروسات قطاع التشغيل: تستقر هذه الفيروسات في الأماكن التي يقراها الحاسوب بالقرص الصلب عند اقلاعه (تشغيله) ليستقر في الذاكرة وينفذ شفرته.

فيروسات الماكرو: وهو أحدث أنواع الفيروسات وهو فيروس يكتب بلغة الورد WORD ويصيب هذا الفيروس ملفات البيانات. ويصيب ملفات الأوفيس.

الفيروسات متعددة الملفات: يبدأ هذ الفيروس في الجهاز بصيغة أوليه ثم يتحول لصيغ أخرى ليصيب ملفات أخرى.

الفيروسات الخفية: تختبئ هذه الفيروسات في الذاكرة ثم تتصدى لأي طلب تشخيص وفحص قطاع التشغيل ليرسل تقريرا بأن قطاع التشغيل سليم وغير مصاب.

فيروسات الملفات التنفيذية: تلصق هذه الفيروسات نفسها مع ملفات البرامج التنفيذية مثل command.com .