أخر يسمى البرنامج الحاضن HOST بحيث أن أي تنفيذ لذلك البرنامج سيضمن تنفيذ الفيروس، هذا ما يميز الفيروس عن الديدان worms التي لا تحتاج إلى ذلك.

(آلية عمل الفيروس و أنواعه)

آلية عمل الفيروسات:

للفيروس أربعة آليات أثناء انتشاره في الكمبيوتر الضحية:

1- آلية التناسخ Replication

وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه و بدونه لا يمكن للبرنامج أن يكرر ذاته وبالتالي فهو ليس فيروساً.

2- آلية التخفي The Protection Mechanism

وهو الجزء الذي يخفى الفيروس عن الاكتشاف ويمكن أن يتضمن تشفير الفيروس لمنع البرامج الماسحة التي تبحث عن نموذج الفيروس من اكتشافه.

3- آلية التنشيط Activate

وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة كما في فيروس MICHELANGELO الذي ينشط في السادس من آذار من كل عام وهنالك فيروسات تنتظر حتى تنفذ برنامج ما عددا معين من المرات كما في فيروس ICELAND ،و كما في فيروس TAIWAN الذي يسبب تهيئة القرص الصلب بعد (90) إقلاع للكمبيوتر ،وفيروس MANCHU الذي ينشط عند الضغط على مفاتيح CTRL+ALT+DEL .

تعمل الفيروسات بطرق مختلفة، وسنعرض فيما يلي للطريقة العامة التي تنتهجها كافة الفيروسات. في البداية يظهر الفيروس على جهازك، ويكون قد دخل إليه مختبئاً في ملف برنامج ملوث (مثل ملفات COM أو EXE أو قطاع الإقلاع). وكانت الفيروسات في الماضي تنتشر بشكل أساسي عن طريق توزيع أقراص مرنة ملوثة. أما اليوم، فمعظمها يأتي مع البرامج المنقولة عبر الشبكات (ومن بينها إنترنت)، كجزء من برنامج تركيب نسخة تجريبية من تطبيق معين، أو ماكرو لأحد التطبيقات الشهيرة، أو كملف مرفق (attachment) برسالة بريد إلكتروني.

ويجدر التنويه إلى أن رسالة البريد الإلكتروني نفسها لا يمكن أن تكون فيروساً، فالفيروس برنامج، ويجب تشغيله لكي يصبح نشطاً. إذاً الفيروس المرفق برسالة بريد إلكتروني، لا حول له ولا قوة، إلى أن تشغّله. ويتم تشغيل فيروسات المرفقات عادة، بالنقر عليها نقرة مزدوجة بالماوس .ويمكنك حماية جهازك من هذه الفيروسات، بالامتناع عن تشغيل أي ملف مرفق برسالة بريد إلكتروني، إذا كان امتداده COM أو EXE ، أو إذا كان أحد ملفات بيانات التطبيقات التي تدعم الماكرو، مثل برامج أوفيس، إلى ما بعد فحصه والتأكد من خلوه من الفيروسات. أما ملفات الرسوميات والصوت ، وأنواع ملفات البيانات الأخرى القادمة كمرفقات، فهي آمنة، ولا يمكن للفيروس أن ينشط من خلالها، ولذلك فهو لا يهاجمها.

إذاً يبدأ الفيروس دورة حياته على الجهاز بشكل مشابه لبرنامج حصان طروادة، فهو يختبئ في ثنايا برنامج أو ملف آخر، وينشط معه. في الملفات التنفيذية الملوثة، يكون الفيروس قد أضاف شيفرته إلى البرنامج الأصلي، وعدل تعليماته بحيث ينتقل التنفيذ إلى شيفرة الفيروس .وعند تشغيل الملف التنفيذي المصاب، يقفز البرنامج عادة إلى تعليمات الفيروس، فينفذها، ثم يعود ثانية لتنفيذ تعليمات البرنامج الأصلي. وعند هذه النقطة يكون الفيروس نشطاً، وجهازك أصبح ملوثاً ،وقد ينفذ الفيروس مهمته فور تنشيطه ويطلق عليه فيروس العمل المباشر direct-action أو يقبع منتظراً في الذاكرة، باستخدام وظيفة " الإنهاء والبقاء في الذاكرة terminate and stay resident, TSR التي توّمنها نظم التشغيل عادة .

وتنتمي غالبية الفيروسات لهذه الفئة، ويطلق عليها الفيروسات" المقيمة". ونظراً للإمكانيات الكبيرة المتاحة