للبرامج المقيمة في الذاكرة، بدءاً من تشغيل التطبيقات والنسخ الاحتياطي للملفات إلى مراقبة ضغطات لوحة المفاتيح ونقرات الماوس (والكثير من الأعمال الأخرى)، فيمكن برمجة الفيروس المقيم، لتنفيذ أي عمل يمكن أن يقوم به نظام التشغيل، تقريباً . يمكن تشغيل الفيروس المقيم كقنبلة، فيبدأ مهمته على جهازك عند حدث معين. ومن الأمور التي تستطيع الفيروسات المقيمة عملها، مسح (scan) قرصك الصلب وأقراص الشبكة بحثاً عن الملفات التنفيذية، ثم نسخ نفسها إلى هذه الملفات وتلويثها .

أنواع الفيروسات:

يبحث مطورو الفيروسات، بشكل دائم، عن طرق جديدة لتلويث كمبيوترك ، لكن أنواع الفيروسات معدودة عملياً، وتصنف إلى: فيروسات قطاع الإقلاع(boot sector viruses) ، وملوثات الملفات (file infectors)، وفيروسات الماكرو (macro viruses) ، وتوجد أسماء أخرى لهذه الفئات، وبعض الفئات المتفرعة عنها، لكن مفهومها يبقى واحداً.
تقبع فيروسات قطاع الإقلاع في أماكن معينة على القرص الصلب ضمن جهازك، وهي الأماكن التي يقرأها الكمبيوتر وينفذ التعليمات المخزنة ضمنها، عند الإقلاع. تصيب فيروسات قطاع الإقلاع الحقيقية منطقة قطاع الإقلاع الخاصة بنظام دوس(DOS boot record) ، بينما تصيب فيروسات الفئة الفرعية المسماة MBR viruses، قطاع الإقلاع الرئيسي للكمبيوتر .(master boot record) يقرأ الكمبيوتر كلا المنطقتين السابقتين من القرص الصلب عند الإقلاع ، مما يؤدي إلى تحميل الفيروس في الذاكرة. يمكن للفيروسات أن تصيب قطاع الإقلاع على الأقراص المرنة، لكن الأقراص المرنة النظيفة، والمحمية من الكتابة، تبقى أكثر الطرق أمناً لإقلاع النظام، في حالات الطوارئ. والمشكلة التي يواجهها المستخدم بالطبع، هي كيفية التأكد من نظافة القرص المرن، أي خلوه من الفيروسات، قبل استخدامه في الإقلاع، وهذا ما تحاول أن تفعله برامج مكافحة الفيروسات.

تلصق ملوثات الملفات (وتدعى أيضاً الفيروسات الطفيلية (parasitic viruses نفسها بالملفات التنفيذية، وهي أكثر أنواع الفيروسات شيوعاً. وعندما يعمل أحد البرامج الملوثة، فإن هذا الفيروس، عادة، ينتظر في الذاكرة إلى أن يشغّل المستخدم برنامجاً آخر، فيسرع عندها إلى تلويثه. وهكذا، يعيد هذا النوع من الفيروس إنتاج نفسه، ببساطة، من خلال استخدام الكمبيوتر بفعالية، أي بتشغيل البرامج! وتوجد أنواع مختلفة من ملوثات الملفات، لكن مبدأ عملها واحد.

تعتمد فيروسات الماكرو(macro viruses) ، وهي من الأنواع الحديثة نسبياً، على حقيقة أن الكثير من التطبيقات تتضمن لغات برمجة مبيتة ضمنها. وقد صممت لغات البرمجة هذه لمساعدة المستخدم على أتمتة العمليات المتكررة التي يجريها ضمن التطبيق، من خلال السماح له بإنشاء برامج صغيرة تدعى برامج الماكرو. تتضمن برامج طاقم أوفيس، مثلاً، لغة برمجة مبيتة، بالإضافة إلى العديد من برامج الماكرو المبيتة أيضاً، والجاهزة للاستخدام المباشر. وفيروس الماكرو ببساطة، هو برنامج ماكرو مصمم للعمل مع تطبيق معين، أو عدة تطبيقات تشترك بلغة برمجة واحدة. أصبحت فيروسات الماكرو شهيرة بفضل الفيروس المصمم لبرنامج مايكروسوفت وورد. فعندما تفتح وثيقة أو قالباً ملوثين، ينشط الفيروس ويؤدي مهمته التخريبية. وقد بُرمِج هذا الفيروس لينسخ نفسه إلى ملفات الوثائق الأخرى، مما يؤدي إلى ازدياد انتشاره مع استمرار استخدام البرنامج.

ويجمع نوع رابع يدعى الفيروس "متعدد الأجزاء (multipartite)" بين تلويث قطاع الإقلاع مع تلويث الملفات، في وقت واحد.

ستجد قائمة ضخمة بأسماء الفيروسات، مع شرح تفصيلي عن آثار كل منها، في قسم Virus Encyclopediaمن موقع مختبر مكافحة الفيروسات، الخاص بشركةSymantic ، التي تنتج برنامج نورتون أنتي فايروس الشهير