



b. ملفات التجسس (Spywares): هي برامج مصممة لجمع المعلومات الشخصية مثل المواقع الإلكترونية التي يزورها المستخدم وسجل بياناته وكلمة المرور للحسابات الإلكترونية، وكذلك تستطيع الحصول على أمور مهمة للمستخدم مثل رقم بطاقة الائتمان دون علمه.

c. ملفات دعائية (Adware) هي برامج مصممة للدعاية والإعلان وتغيير الإعدادات العامة في أجهزة الحاسوب، مثل تغيير الصفحة الرئيسية للمتصفح وإظهار بعض النوافذ الدعائية أثناء اتصالك بالإنترنت وتصفحك للمواقع الإلكترونية.

d. قلة الخبرة في التعامل مع بعض البرامج: مع ازدياد استخدام الإنترنت من عامة الناس غير المتخصصين، واستخدامهم وتعاملهم مع برامج متطورة الخاصة بخدمة تطبيقات الإنترنت وبشكل مستمر وبدون خبرة كافية لكيفية التعامل مع تلك البرامج، قد يفتح ثغرة في جهاز الحاسوب تمكن الآخرين من اختراق الجهاز.

e. أخطئه عامة: مثل سوء اختيار كلمة السر أو كتابتها على ورقة مما يمكن الآخرين من قراءتها، أو ترك الحاسوب مفتوح مما يسمح للآخرين (خاصة غير المخولين أو الغرباء) بالدخول لملفات الحاسوب أو تغيير بعض الإعدادات.

3-10 برامج خبيثة Malware:

Malware هي اختصار لكلمتين **Malicious Software** وهي برامج مخصصة للتسلل لنظام الحاسوب أو تدميره بدون علم المستخدم. وما إن يتم تثبيت البرمجية الخبيثة فإنه من الصعب إزالتها. وبحسب درجة البرمجية من الممكن أن يتراوح ضررها من إزعاج بسيط (بعض النوافذ الإعلانية غير المرغوب بها خلال عمل المستخدم على الحاسوب متصلاً أم غير متصلاً بالشبكة) إلى أذى غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. من الأمثلة على البرامج الخبيثة هي الفيروسات وأحصنة طروادة

3-10-1 فايروسات الحاسوب:

هي برامج صغيرة خارجية صممت عمداً لتغيير خصائص الملفات التي تصيبها وتقوم بتنفيذ بعض الأوامر إما بالحذف أو التعديل أو التخريب وفقاً للأهداف المصممة لأجلها. ولها القدرة على التخفي، ويتم تخزينها داخل الحاسوب بإحدى طرق الانتقال لإلحاق الضرر به والسيطرة عليه.



3-10-2 الأضرار الناتجة عن فايروسات الحاسوب

1. تقليل مستوى أداء الحاسوب
2. إيقاف تشغيل الحاسوب وإعادة تشغيل نفسه تلقائياً كل بضع دقائق أو إخفائه في العمل بعد إعادة التشغيل.
3. تعذر الوصول إلى مشغلات الأقراص الصلبة والمدجة (وحدات التخزين) وظهور رسالة تعذر الحفظ لوحدة التخزين.
4. حذف الملفات أو تغيير محتوياتها.
5. ظهور مشاكل في التطبيقات المنصبة وتغير نوافذ التطبيقات والقوائم والبيانات.
6. تكرار ظهور رسائل الخطأ في أكثر من تطبيق.
7. إفشاء معلومات وأسرار شخصية هامة.

3-10-3 صفات فايروسات الحاسوب

1. القدرة على التناسخ والانتشار Replication
2. ربط نفسها ببرنامج آخر يسمى الخاضع (المضيف Host)
3. يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

3-10-4 مكونات الفايروسات

يتكون برنامج الفايروس بشكل علم من أربعة أجزاء رئيسة تقوم بالآتي:

1. آلية التناسخ The Replication Mechanism تسمح للفايروس أن ينسخ نفسه.
2. آلية التخفي The Hidden Mechanism تخفي الفايروس عن الاكتشاف.
3. آلية التنشيط The Trigger Mechanism تسمح للفايروس بالانتشار.
4. آلية التنفيذ The Payload Mechanism تنفيذ الفايروس عند تنشيطه.

3-10-5 أنواع الفايروسات

تقسم الفايروسات إلى ثلاثة أنواع، كما في الشكل (3-2):

1. الفايروس (Virus): برنامج تنفيذي (ذات الامتداد com, exe, bat, pif, scr). يعمل بشكل منفصل ويهدف إلى إحداث خلل في الحاسوب، وتراوح خطورته حسب المهمة المصمم لأجلها، فمنها البسيطة ومنها الخطيرة، وينتقل بواسطة نسخ الملفات من حاسوب بحوي ملفات مصابة إلى حاسوب آخر عن طريق الأقراص المدجة (CD) والذاكرة المتحركة (Flash Memory).
2. الدودة (Worm): تنتشر فقط عبر الشبكات والإنترنت مستفيدة من قائمة عناوين البريد الإلكتروني (مثل تطبيق برنامج التحدث الماسنجر Messenger)، فعند إصابة الحاسوب

يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في قائمة العناوين ويرسل نفسه إلى كل الأشخاص في القائمة، مما يؤدي إلى انتشاره بسرعة عبر الشبكة.

3. حصان طروادة (Trojan Horse): فايروس تكون آلية عمله مرفقاً (ملحقاً) مع أحد البرامج، أي يكون جزءاً من برنامج دون أن يعلم المستخدم. سمي هذا البرنامج بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة، إذ اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها.



الشكل (2-3) أشكال مختلفة من الفايروسات

3-11 أهم الخطوات اللازمة للحماية من عمليات الاختراق:

الحفاظ على جهاز الحاسوب ضد هذه الملفات بشكل كامل صعب جداً مادام الجهاز مربوط بشبكة الإنترنت، لكن يمكن حماية الحاسوب بنسبة كبيرة وتقليل خطر الإصابة بالاختراقات الالكترونية والبرامج الضارة باتباع الخطوات الآتية:

1. استخدام نظم تشغيل محمية من الفايروسات كنظم يونكس ولينكس ومشتقاتها. وتم بناء هذه النظم بحيث لا يمكن أن يدخل إليها أي برنامج خارجي إلا بموافقة وعلم المستخدم بشكل واضح وصريح، كما أن ملفات النظام الأساسية تكون محمية من أي تغير أو تلاعب حتى عن طريق الخطأ غير المتعمد.
2. تثبيت البرامج المضادة أو المكافحة للفايروسات (Antivirus) مثل (Norton, Kaspersky, McAfee, Avira) وبرنامج مكافحة ملفات التجسس (Antispyware) مثل AVG Anti-Spyware ذات الإصدارات الحديثة وتحديث النسخة.
3. الاحتفاظ بنسخ للبرامج المهمة مثل نظم التشغيل ويندوز وحزمة أوفيس ونسخة من ملفات المستخدم.
4. عدم فتح أي رسالة أو ملف ملحق بريد إلكتروني وارد من شخص غير معروف للمستخدم، أو الملفات ذات امتدادات غير المعروفة.