وزارة التعليم العالي والبحث العلمي
جامعة تكريت
كلية التربية الأساسية / شرقاط

أساسيات الحاسوب

قسم اللغة الانكليزية – المرحلة الاولى

أعداد :

م. م. رند أحمد عطا

٨.فـــيروس الحاســـب الآلـــي

١,٨فيــروس الحاسب الآلي :

هو برنامج صغير ضار ينسخ نفسه ويتكاثر كالفيروس الحقيقي ، ويقوم باتلاف و تخريب البرامج والملفات في الحاسب أو يصيب نظام الحاسب بالضرر.

أن فيروسات الكمبيوتر ليست مدمرة بطبيعتها ، والميزة أو الخاصية الأساسية لبرنامج الكمبيوتر التي تجعله يصنف كفيروس ليست قدرته على تدمير البيانات ، ولكن قدرته على التكاثر ونسخ نفسه ذاتيا ، وقدرته على السيطرة على الكمبيوتر وتوظيف موارده بشكل كامل لنسخ الفيروس

2.8 مكونـــــــات الفيـــــــروس

يتكون برنامج فيروس من عدده آليات رئيسية:

1. **آلية للبحث**: حيث يقوم فيروس بتحديد البرنامج او الملفات التي ينسخ نفسة اليها.
2. **آلية النسخ**: حيث يقوم فيروس بنسخ نفسه الى موقع محدد في البرنامج او الملف. آلية النسخ الذاتي هي اهم جزء في الفيروس ، بل هي جزء إلزامي في كل فيروس ، فإذا كان هذا الجزء غير موجود ،فان البرنامج لا يعتبر فيروس بحسب التعريف الرسمي له ,وإنما يدخل في أي نوع آخر من البرامج الضارة غير الفيروسات
3. **آلية التخفي**: وهو الجزء الذي يخفي الفيروس عن الاكتشاف بحيث يظل متخفياً ولا ينطلق لتنفيذ مهامه الا في وقت وتاريخ محدد.
4. **آلية الضرر**: هو الجزء الذي ينشط بيه الفيروس حيث يقوم بمهامه التخريبية وتعرف هذه آلية ب Payload.فآلية الضرر التي يتضمنها الفيروس يمكن تقسيمها إلى مجموعتين ؛ خبيثة وغير خبيثة . الاجراءات الضارة الخبيثة مثل ؛ حذف الملفات ، محو أو تعديل البيانات ، تخريب البرامج ، الكشف عن البيانات السرية وغيرها.اما الغير خبيثة مثل ؛ اللعب بالموسيقى ، عرض صور أو رسوم متحركه على الشاشة وغيرها

٣,٨ طرق انتشـــــــــــــار الفيروسات

هناك عدد من الطرق المعروفة التي تنتقل بواسطتها الفيروسات من حاسوب إلى آخر , من أهم هذه الطرق :

1- الوسائط القابلة للإزالة :

الوسائط القابلة للإزالة مثل الأقراص الضوئية والفلاشات هي واحدة من الطرق الرئيسية التي تتيح للفيروسات الإنتقال من حاسب إلى آخر , ومن شخص إلى آخر . وعادة ما كانت الملفات المصابة بالفيروس تنسخ أولا إلى وسيط قابل للإزالة , وعندما يقوم المستخدم الضحية بتشغيل ملف البرنامج في الوسيط أو على الجهاز فإنه ينشط وينفذ مهامه التخريبية وينتشر داخل الجهاز . وتستمر الدائرة عندما يقوم الضحية الجديدة بنسخ الملفات والبرامج المصابة بالفيروس وينقلها –بعلم أو بدون علم – إلى اشخاص آخرين وهكذا ..

2- البريد الإلكتروني :

ظهور البريد الالكتروني وارتفاع شعبيته وشيوع استخدامه بين الشركات والمؤسسات والأفراد زود الفيروسات بطريقة سريعة وواسعة للإنتشار إلى كل مكان في العالم . خاصة مع تطوير الوسائل القياسية لإرسال المرفقات مع البريد الالكتروني . ويرسل الفيروس أو الملف المصاب بالفيروس إلى الضحية كمرفق مع رسالة البريد الالكتروني, وعادة ما تتضمن رسالة البريد الالكتروني التي تحمل فيروس عبارات تغري المستلم بفتح الملف المرفق بها والذي يحتوي على فيروس , مثل الفوز بجائزة أو منحة أو مساعدة , أو الوعد بالحصول على أموال أو مشاريع , أو أي شيء هام آخر يمكنه جذب وخداع المستلم , وبمجرد أن يفتح المستلم المرفقات ينشط فيروس البريد الالكتروني, وينتشر داخل الجهاز الخاص به , ثم يستولي على دفتر عناوين البريد الالكتروني الخاص بالمستلم ويرسل نسخ من نفسه إلى جميع العناوين التي حصل عليها . وبذلك ينتشر بسرعة فائقة إلى أكبر عدد من الأجهزة والحواسيب عبر العالم .

3- المستندات , الوورد والأكسل والانواع الأخرى :

4- مواقع الويب :

هناك العديد من مواقع الانترنت التي تحتوي على برامج وملفات مصابة بالفيروسات , خاصة البرامج المجانية والتجريبية , وعندما يقوم المستخدم بتحميل هذه البرامج والملفات فإن الفيروسات تنتقل إلى حاسوبه معها .

5- البرامج المقرصنة :

البرنامج المقرصن هو برنامج ينشر ويوزع بشكل غير قانوني مما يؤدي إلى حرمان صانع البرنامج الأصلي من الدخل أو الربح الذي يحصل عليه بواسطة بيعه , و البرامج المقرصنة يتم توزيعها بدرجة منخفضة من الشروط والمعايير الأمنية مما يسمح للفيروسات بالتسلل إليها , كما أن بعض الأشخاص الذين يقومون بتوزيع البرامج المقرصنة يتعمدون وضع الفيروسات فيها بقصد إلحاق أضرار بالأشخاص الذين يشترونها .

٤,٨ أشهـــــــر فيروسات الحاســـــب الآلي

١-**الفيروس الاسرائيلي** : اكتشف هذا الفيروس لاول مرة طالب في الجامعة العبرية في القدس , وقد وضع هذا الفيروس بحيث ينفذ في تاريخ ١٣ من كل شهر اذا صادف هذا التاريخ يوم جمعة , وعندما يتوافر هذان الشرطان , أي ١٣ + يوم جمعة , فإن الفيروس ينفذ ويدمر كل ما تحتويه اسطوانة الاقراص الصلبة من برامج وبيانات او يدمر البرنامج الذي يتم تشغيله .

٢-**فيروس ميليسا Melissa** : وقد تميز هذا الفيروس بأنه يقوم بالبحث عن دفتر عناوين البريد الالكتروني الخاص بك , ثم يقوم بارسال نسخة من نفسه الى عناوين اصدقائك ومعارفك الموجودة في هذا الدفتر , وعندما يفتح احد الاصدقاء او المعارف الرسالة فإنه ينتقل الى معارفه واصدقائه وهكذا . وقد ساعدت هذه الطريقة الفيروس على الانتشار الى انحاء العالم اكثر من أي فيروس اخر , ومع ان هذا الفيروس لا يسبب اضرارا تدميرية للبرامج والبيانات , إلا أنه تسبب في ارسال مئات الآلاف من رسائل البريد الالكتروني التي ادت الى بطء الخدمة واغلاق انظمة البريد الالكتروني , كما كلفت ازالته والتخلص منه خسائر مادية باهضة .

٣-**فيرس تشرنوبل ١٩٩٨** : وهو واحد من أشد الفيروسات تدميرا ، وسمي "تشرنوبل" نسبة إلى "حادثة تشرنوبل" التى وقعت فى أوكرانيا عام ١٩٨٦ بسبب انفجار فى أحد المفاعلات النووية يصيب فيرس تشيرنوبيل القرص الصلب فيجعل الجهاز غير قادر على الإقلاع. ويقوم في نفس الوقت بمحاولة مسح البيوس مما يتطلب إعادة تنصيب البيوس ، وهو امر صعب لذلك فإن الناس الذين أصيبوا بهذا الفيروس قاموا بتغيير أجهزتهم.

٤-**فيرس مايكل أنجلو – ١٩٩١** : تم اكتشاف فيرس مايكل أنجلو لأول مرة فى أبريل ١٩٩١ فى نيوزلندا ، انتشر فيرس مايكل أنجلو على الأجهزة التى تعمل بنظام MS Dos لكنه يبقى ساكنا فى الجهاز غير محدث لأية أضرار حتى مجيء يوم ٦ مارس – ذكرى ميلاد الفنان مايكل أنجلو – حيث يحدث أكبر قدر ممكن من التدمير.

٥-**دودة سانتي Santy ٢٠٠٥** م : تطلب دودة سانتي من محرك البحث مثل جوجل وياهو إنشاء قائمة بأسماء المواقع الموجودة بها الثغرة التى تنفذ من خلالها ، ثم تدمر جميع محتويات الموقع ، تاركة رسالة تفيد بأن الموقع قد تم تشويهه بواسطتها . وقد قامت بتدمير أكثر من ٤٠ ألف موقع فى أقل من ٢٤ ساعة فقط !.

6- **دودة ستاكس نت Stuxnet ٢٠١٠ م** :ضربت دودة ستاكس نت Stuxnet عدة منشآت صناعية هامة كمفاعل بوشهر النووى بإيران فضلا عن ١٥ مؤسسة صناعية أخرى ، الجدير بالذكر أن إيران تحملت ٦٠% من إجمالى الخسائر التى سببها Stuxnet مما يبين أن الهدف من وراء Stuxnet كانت أهداف سياسية تقف وراءها قوى دولية.

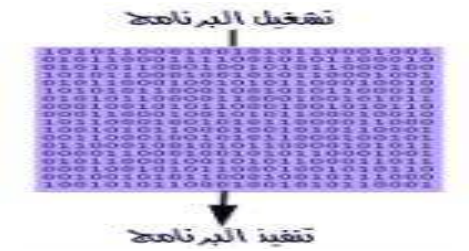
5.8 الادوات اللازمة لبرمجـــــــــة الفيروســـــــات

فأن اهم الادوات اللازمة لعمل ذلك:

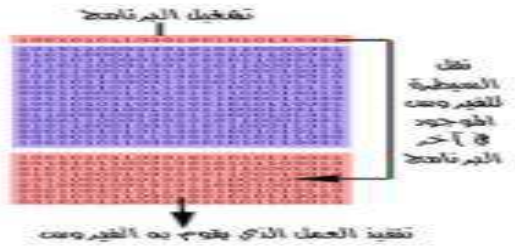
1) المعرفة الجيدة بنظام التشغيل.
2) المعرفة الجيدة بلغة البرمجة
3) مترجم خاص بلغة البرمجة
4) برنامج لتشفير وحماية الفيروس

6.8 كيف يعمل الفيروس

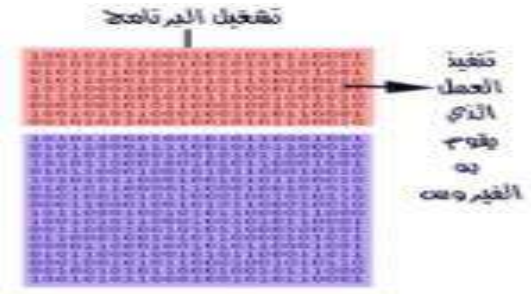
في الواقع يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن يقوم فعلياً بأي تغيير في مكونات الملف الأصلية. لننظر للصورة التالية التي توضح شكل البرنامج غير المصاب بفيروس.



نلاحظ أنه عند استدعاء البرنامج فإنه يعمل بشكل طبيعي . والآن لنتصور أنه تم إصابة البرنامج بفيروس. في الواقع يقوم الفيروس بلصق نفسه في البرنامج كما أسلفنا دون أن يغير في محتويات الملف شيئاً. و طريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه :



وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب ، و يضع علامة في بدايته هكذا:



إن هذا الفيروس يختبئ في نهاية الملف المصاب، و يضع في مقدمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحول السيطرة للفيروس بدلاً من تشغيل البرنامج . وفي الحالتين قد يعود الفيروس بعد الانتهاء من تنفيذ عمله المؤذي لتشغيل البرنامج و لكنه قد لا يعود أيضاً و يسبب أضراراً جسيمة للجهاز . ويحاول كل فيروس تقريباً أن يقوم بنفس الشيء .. وهو الانتقال من برنامج إلى آخر ونسخ الشفرة إلى الذاكرة ومن هناك تحاول الشفرة نسخ نفسها إلى أي برنامج يطلب العمل أو موجود بالفعل قيد العمل، كما تحاول هذه الشفرة أن ت غير من محتويات الملفات ومن أسمائها أيضاً دون أن تعلم نظام التشغيل بالتغيير الذي حدث، مما يتسبب في فشل البرامج في العمل.

7.8 اعراض الاصابـــــــــة بالفيروس الحاسـب

1- تكرار رسائل الخطأ في أكثر من برنامج.

2- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.

3- تكرار اختفاء بعض الملفات التنفيذية.

4- حدوث بطء شديد في تشغيل نظام التشغيل او تنفيذ بعض التطبيقات. رفض بعض التطبيقات للتنفيذ.

8.8 الوقايـــــــــــة من الفيروســـــات

1- لابد من موجود برنامج حماية من الفيروسات في جهاز الحاسوب.

2- لابد أن من تحديث برنامج حماية بشكل دوري، وإلا فلا فائدة من وجوده .

3- لا تشغل اي مرفقات في أي إيميل لا تعرف مرسله .

4- لا تشغل اي مرفقات في إيميلات أصدقائك إذا وجدتها تنتهي بـ exe أو bat أو أي امتداد لا تعرفه .

5- لا تقبل ملف من شخص لا تعرفه أبداً . إذا قبلت ملفاً من شخص تعرفه، افحصه أيضاً ببرنامج الحماية، فقد يكون صديقك نفسه ضحية .

6- حرص على فحص جميع البرامج التي تقوم بتنزيلها من الإن ترنت، أو تشغيلها من قرص مرن أو سي دي. قبل أن تشغّلها

7- لا تدخل إلى مواقع الهاكرز المنتشرة خاصةً إذا كنت غير متمكن ولم تتخذ الاحتياطات اللازمة، فبعضها ينسخ الفيروس مع الملفات المؤقتة. و لتجنّب مثل هذه الحالات يمكنك تفعيل خيار الحماية في التصفّح في برنامج الحماية الذي يقدم مثل هذه الخدم