## Lesion 3 : Computer Protection & Maintenance

### تعريف الفايروس :

عن كود برمجي (شفرة) الغرض منها إحداث أكبر قدر من الضرر .ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى عن طريق التوالد والانتشار بين برامج الحاسب وكذلك مواقع مختلفة من الذاكرة حتى يحقق أهدافه التدميرية

يتصف فيروس الحاسب بأنه :

1. برنامج قادر على التناسخ Replication والانتشار.
2. الفايروس يربط نفسه ببرنامج أخر يسمى الحاضن host.
3. لا يمكن أن تنشأ الفايروس ات من ذاتها.
4. يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

### مكونات الفايروس :

يتكون برنامج الفايروس بشكل عام من أربعة أجزاء رئيسية وهي

- آلية التناسخ The Replication Mechanism
  وهو الجزء الذي يسمح الفايروس أن ينسخ نفسه.
- آلية التخفي The Protection Mechanism
  وهو الجزء الذي يخفي الفايروس عن الاكتشاف.
- آلية التنشيط The trigger Mechanism
  وهو الجزء الذي يسمح للفايروس 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 ينفذ الفايروس عندما يتم تنشيطه.

### أسباب ظهور الفايروس:

أ- أهداف شخصية:
1- الرغبة في التحدي
2- الرغبة في إبراز الذات
3- الرغبة في الانتقام
ب- أهداف إجرامية ( سرقة البيانات وأرقام الحسابات البنكية )

ج- أهداف تجارية ( التسويق لشركات مكافحة الفايروس ات )
د- أهداف عسكرية ( التجسس والحرب الإلكترونية )
هـ- أهداف سياسية واقتصادية واجتماعية أخرى ( مثال: chernobyl الذي ينشط بتاريخ 26 أبريل )

## أنواع الفايروس ات:

**1- فيروسات تعمل عند بدء التشغيلBoot Sector Virus :**
يحتاج الكمبيوتر عند تشغيله إلى تعليمات خاصة داخلية لمعرفة مكونات الجهاز ، وهي توجد عادة في ملفات تدعى ملفات النظام (System Files) ، التي تحتوي على البرامج الخاصة ببدء التشغيل ويقوم هذا النوع من الفايروس ات بالتسلل إلى القطاع الخاص ببرنامج الإقلاع على القرص (Boot Sector)، وإتلاف محتوياته والعبث بها، ما يؤدي إلى تعطل عملية الإقلاع .

**2- فيروس الملفاتFile Infector Virus :**
يهاجم هذا النوع نظام التشغيل، وأي برامج أخرى موجودة على الكمبيوتر، كالتطبيقات المكتبية والألعاب وغيرها، ويعمل على العبث بمحتويات الملفات التي تنتهي بامتداد bin, com sys, exe,وتدميرها .

**3- فيروسات الماكرو Macro Viruses :**
تصيب هذه الفايروس ات برامج التطبيقات المكتبية مثل مايكروسوفت وورد أو أكسل. وهي من أكثر أنواع الفايروس ات انتشاراً واستخداماً في عمليات التسلل إلى كمبيوترك عبر التطبيقات .

**4- الفايروس ات المتعددة الملفات :**
تنسخ هذه الفايروس ات نفسها في صيغة أولية ثم تتحول إلى صيغ أخرى لتصيب ملفات أخرى .

**5- الفايروس ات الخفية ( الأشباح ):**
وهذه فيروسات مخادعة.. إذ أنها تختبئ في الذاكرة ثم تتصدى لطلب تشخيص وفحص قطاع التشغيل، ثم ترسل تقرير مزيف إلى السجل بأن القطاع غير مصاب .

**6- الفايروس ات متعددة القدرة التحوليّة :**
وهذه الفايروس ات لها القدرة الديناميكية على التحول وتغيير الشفرات عند الانتقال من ملف إلى آخر، لكي يصعب اكتشافها .

7- **الفايروس ات متعددة الأجزاء:**
يجمع هذا النوع الذي يدعى الفايروس متعدد الأجزاء بين تلويث قطاع الإقلاع مع تلويث الملفات في وقت واحد.

**8- الفايروس ات الطفيلية :**
الطفيلية Parasitic Viruses نفسها بالملفات التنفيذية وهي أكثر أنواع الفايروس ات شيوعا

وعندما يعمل أحد البرامج الملوثة فإن هذا الفايروس عادة ينتظر في الذاكرة إلى أن يشغل المستخدم برنامجا آخر فيسرع عندها إلى تلويثه وهكذا يعيد هذا النوع من الفايروس إنتاج نفسه ببساطه من خلال استخدام الكمبيوتر بفعالية أي بتشغيل البرامج وتوجد أنواع مختلفة من ملوثات الملفات لكن مبدأ عملها واحد

**أسباب الإصابة بالفايروس ات:**

1. تحميل البرامج من الانترنت دون التأكد منها.
2. تحميل البرامج من أقراص الليزر المحشوة بالبرامج غير الموثوقة.
3. نقل البيانات من أجهزة أخرى عبر الشبكة .
4. فتح الرسائل الالكترونية دون معرفة مصدرها.

أعراض الإصابة بالفايروس :

1- نقص شديد في الذاكرة.
2- بطء تشغيل النظام بصورة مبالغ فيها.
3- عرض رسائل الخطأ بدون أسباب حقيقية.
4- تغيير في عدد ومكان الملفات وكذلك حجمها بدون أي أسباب منطقية
5- الخطأ في استخدام القرص الصلب بطريقة عشوائية وتستطيع أن تلاحظ ذلك من إضاءة لمبة القرص الصلب حتى وإن كان لا يعمل.
6- الخطأ في استخدام لوحة المفاتيح عن طريق إظهار أحرف غريبة أو خاطئة عند النقر على حرف معين
7- توقف النظام بلا سبب
8- اختلاط أدلة القرص أو رفض النظام العمل منذ البداية.

**كيفية حمـــــاية الكمبيوتر من الفايروس ات :**

1- من الضروري تركيب البرامج المضادة للفايروس ات على الجهاز وتشغيلها طوال فترة استخدام الجهاز. إن هذا يتيح لهذه البرامج البحث عن الفايروس ات وتدميرها سواء كان أسبوعياً أو يومياً أو عند التشغيل

2- عدم فتح أي ملف مرفق ضمن أي رسالة بريد إلكتروني أو أي برنامج آخر كالماسنجر، مهما كان مصدرها، إلا بعد أن تفحصها باستخدام برنامج مضاد للفايروس ات، بشرط أن يكون مصدر الرسالة معروفاً، و أن تكون تتوقع وصول هذا الملف لأن بعض الفايروس ات ترسل نفسها بأسماء أشخاص آخرين عن طريق دفتر العناوين .. لذا احذر من ذلك .

3- متابعة أخبار الفايروس ات وطرق تغريرها بالمستخدم ، عبر مواقع الأخبار التقنية أو الصحف اليومية أو النشرات الإخبارية بهدف أخذ الاحتياطات اللازمة وعدم الوقوع في فخ هذا الفايروس الجديد .

4- التأكد من مصدر أي برنامج تقوم بإنزاله عبر إنترنت وفحصه بواسطة برنامج مضاد الفايروس ات الذي تستخدمه قبل تثبيته في جهازك .

5- تعطيل خاصية تحميل الجهاز من مشغل الأقراص المرنة (Floppy drive)

6- من الضروري أيضاً تحديث برامج مستكشف الفايروس ات بصورة دورية، من خلال الحصول عليها من الشركة المنتجة، أو من مواقع إنترنت المختلفة، كي تضمن حصولك على آخر المعلومات والأعراض الخاصة بالفايروس ات الجديدة، وطريقة الوقاية منها .

7- تشغيل برامج مستكشف الفايروس ات، وتفحّص أي ملفات أو برامج جديدة تصلك عبر البريد الإلكتروني، والإنترنت، والأقراص المرنة ، وعدم السماح بإدخال وتشغيل أي ملفات أو برامج مجهولة المصدر وبدون الفحص مسبقاً .

8- الانتباه إلى عدم تشغيل أو إعادة تشغيل الكمبيوتر بوجود القرص المرن في موقعه، حيث أن بعض هذه الفايروس ات تختبئ داخل القرص المرن حتى تجد الفرصة الملائمة للتشغيل عندها .

9- تحميل البرامج عن طريق المواقع الموثوق فيها.