Prepared by Assist . Prof . Imad Matti
Computer Science Department

الفصل السابع

(الجزء الاول)

فايروسات الحاسوب Computer Viruses

البرامج الخبيثة:

خلال فترة الثمانينيات والتسعينيات كانت الفكرة عن البرامج الخبيثة انها برمجياتتم انشائها بهدف التخريب او المزاح. ولكن وفي الاونة الاخيرة فان معظم البرمجيات الخبيثة قد تمت كتابتها بدافع ربحي. الرغبة من كاتبي هذه البرامج هو السيطرة على الانظمة المصابة وتحويل هذه السيطرة لتعود عليهم بعائد مادي. ومنذ حوالي عام 2003 اصبحت اكثر البرمجيات الخبيثة كلفة من حيث المال والوقت اللازم لاستعادة الانظمة هي برامج التجسس Spyware.

تنقسم البرامج الخبيثة Malware من حيث الاداء والعمل الى عدة اصناف اهمها:

1- **دودة الحاسوب (Worm)** التي هي عبارة عن برامج صغيرة قائمة بذاتها صنعت عام 2001 للقيام باعمال تدميرية او لغرض سرقة البيانات الخاصة اثناء التصفح عبر الانترنيت, تنتشر دائما من خلال البريد الالكتروني, فعند اصابتها للجهاز تبحث عن دفتر عناوين البريد الالكتروني وترسل نفسها الى كل الاشخاص, هذه الديدان استهدفت مواقع كثيرة من الشركات العالمية اشهرها Microsoft Office .

2- **حصان طروادة (Trojan Horse)** سمي هذا البرنامج بحصان طروادة لانه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبا الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها, وبالتالي الية عمل هذا البرنامج يكون مرفقا مع احد البرامج اي جزء منه دون علم المستخدم.

3- **فيروس الحاسوب (Computer Virus)** هو نوع من انواع البرمجيات الخبيثة الخارجية, صنعت عمدا بغرض تغيير خصائص ملفات النظام.

تتكاثر الفايروسات عن طريق توليد نفسها بنسخ شفرتها المصدرية واعادة توليدها او عن طريق اصابة برنامج حاسوبي بتعديل خصائصه.

فريد كوهين (Fred Cohen) مهندس و عالم كمبيوتر امريكي وهو المخترع الاول لفيروس الكمبيوتر والذي تسبب في اتلاف الملايين من الاجهزة الحاسوبية لملايين من الاشخاص. ولقد اخترع اول فيروس كمبيوتر في عام 1985 عندما تحدث عن الفيروسات خلال مشروع تخرجه حيث ناقش في مشروع تخرجه برمجيات الاستنساخ الذاتي التي كانت بداية لاختراع الفيروسات التي تنسخ نفسها على كمبيوتر الضحايا وكان اول فيروس كمبيوتر اخترعه يسمى (Parasitic Application) والذي يستطيع ان يسيطر على اي حاسب شخصي, وكان بامكانه ان يدمره بالكامل.

والغريب في حياة هذا الشخص انه يمتلك الان شركة تعمل في مجال حماية المعلومات على الحاسبات الشخصية.

مكونات الفايروس

يتكون برنامج الفايروس بشكل عام من اربعة اجزاء رئيسية وهي:

- ألية التناسخ Replication Mechanism

وهو الجزء الذي يسمح للفيروس ان ينسخ نفسه.

- ألية التخفي Protection Mechanism

وهو الجزء الذي يخفي الفيروس من الاكتشاف.

- ألية التنشيط Trigger Mechanism

وهو الجزء الذي يسمح للفيروس بالانتشار قبل ان يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس Michelangelo الذي ينشط في السادس من اذار من كل عام.

- ألية التنفيذ Payload Mechanism

وهو الجزء الذي ينفذه الفيروس عندما يتم تنشيطه.

طرق انتقال الفيروسات

1- فيروس العدوى المباشر Direct Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع, فان ذلك الفيروس ينشط في ملف او اكثر لينقل العدوى اليه, وعندما يصاب احد الملفات بالعدوى فانه يقوم بتحميله الى الذاكرة وتشغيله وهذا النوع قليل الانتشار.

2- فيروس العدوى غير المباشر Indirect Infector

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع فان ذلك الفيروس سينتقل الى ذاكرة الحاسوب ويستقر فيها, ويتم تنفيذ البرنامج الاصلي ثم يصيب الفيروس بالعدوى كل برنامج يتم تحميله الى الذاكرة بعد ذلك الى ان يتم قطع التغذية الكهربائي عن الحاسوب او اعادة تشغيله

طرق الانتقال

اهم طرق الانتقال الان هي الشبكه العنكبوتية (الانترنيت)

حيث تكون وسيلة سهلة لانتقال الفيروسات من جهاز لاخر ما لم تستخدم أنظمة الحماية من الفيروسات مثل برامج الجدران النارية.

ياتي ثانيا وسائط التخزين مثل ذواكر الفلاش والاقراص الضوئية والمرنة و ياتي ايظا ضمن رسائل البريد الالكتروني وايظا تنتقل الفيروسات الى نظامك عند استلامه ملفات سواء كانت الملفات مخزنة على اقراص مرنة او أقراص مضغوطة.


4GB


CD
VS
DVD

اعراض اصابة الجهاز بالفيروسات

- تكرار رسائل الخطأ في اكثر من برنامج.
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
- تكرار اختفاء بعض الملفات التنفيذية.
- حدوث بطء شديد في بدء تشغيل(نظام التشغيل) او تنفيذ بعض التطبيقات.
- رفض بعض التطبيقات للتنفيذ.

الوقاية من الفيروسات

1- استخدام برامج للكشف عن الفيروسات في الجهاز.

2- احتفظ بنسخ احتياطية من البرامج والملفات الموجودة على الحاسب.

3- اجراء الفحص على البرامج المحملة (المنزلة) او المنقولة من شبكة الانترنيت قبل تشغيلها.

4- استخدام برمجيات الجدار الناري.

5- استخدام نظام التشغيل لينكس فهو يعتبر اكثر امانا وفيه فيروسات قليلة عكس نظام التشغيل ويندوز.

6- لا تشغل اي برنامج او ملف لا تعرف ما هو بالضبط.

7- الحذر من رسائل البريد الالكتروني غير معروفة المصدر وفحصها قبل الاقدام على فتحها.

أخطر 10 فيروسات في تاريخ الإنترنت

إليكم قائمة بعشرة من هذه الفيروسات الأخطر في التاريخ، وفق تصنيف صحيفة " تيليغراف ":"

دودة موريس: في عام 1998 أطلق الطالب الجامعي، روبيرت موريس، دودة فيروسية أطاحت بـ 10 في المائة من كل الحواسيب المرتبطة بالإنترنت عالمياً. وهو اليوم أستاذ مساعد بمعهد ماساتشوستس للتكنولوجيا

فيروس The Concept: تم وضعه عن طريق الخطأ في الأقراص التي كانت تقدمها "مايكروسوفت" عام 1995. وهو أول فيروس يضرب ملفات "وورد". وفي غضون أيام، بات الفيروس الأكثر انتشاراً في العالم، و قد اعتمد في انتقاله على تبادل الملفات عبر البريد الإلكتروني.

فيروس CIH: و هو اختصار لعبارة The Chernobyl virus فيروس تشرينوبل إشارة إلى الكارثة النووية الشهيرة. ويتم إطلاقه كل سنة بمناسبة الذكرى السنوية للكارثة، و يعمل على شل أجهزة الكومبيوتر، و قد تم اعتقال مصممه، شين إنغ هو في تايوان.

دودة آنا كورنيكوفا: يتسبب هذا الفيروس في ظهور صورة للاعبة التنس التي تحمل هذا الاسم. و هو عبارة عن فيروس، صممه معجب هولندي مهووس بها يدعى جان دي ويت. و قد قُبض عليه و حكم عليه بأداء الخدمة المدنية.

فيروس ILOVEYOU: عام 2000 اجتاح هذا الفيروس الإنترنت العالمي، و قد صُمّم لاقتراح نفسه أوتوماتيكياً على كل العناوين في قوائم الاتصال و سرقة كلمة سر الحسابات.

فيروس ميليسا: صممه دافيد إل سميث لتكريم فنانة استعراضية. و هو أول فيروس ينجح في اختراق البريد الإلكتروني. و تم اعتقال المصمم و محاكمته بتهمة التسبب بخسائر بلغت 80 مليون دولار.

دودة The Blaster: لم يتم العثور على مصمم هذا الفيروس. تم إطلاقه عام 2003 ليخترق موقع "مايكروسوفت"، ليصيب الملايين من الحواسيب مستغلاً ثغرة في برنامج الشركة.

دودة Netsky and Sasser: وجدت المحكمة المراهق، سفين جاشن، مذنباً في تصميم هذه الدودة الفيروسية. كما كشفت التحقيقات أنه كان المسؤول عن 70 في المائة من البرمجيات الخبيثة المنتشرة في الإنترنت في تلك الفترة. إلا أنه نجا من السجن و تعاقد مع شركة أمنية كقرصان أخلاقي.

حصان طروادة OSX: عرف العالم عام 2007 هذا الفيروس الذي كان أول برمجية خبيثة تخترق أجهزة "ماك" المحصنة لغرض مالي. و تسبب الاختراق في زيادة المخاوف من تعرض أجهزة "آبل" إلى مزيد من هجمات القراصنة و هو برنامج صغير تمت برمجته لبرنامج رئيسي كبير ليقوم ببعض المهام الخفية منها تعطيل برامج الحماية لدى المستخدم و تعطيل بعض خصائص النظام وتغييرها ليصبح اختراق الجهاز أسهل.

دودة العاصفة: اخترق الفيروس ملايين الحواسيب سنة 2007، و بسببه سيطر القراصنة على هذه الحواسيب و استخدموه لنشر الرسائل الضارة و سرقة بيانات الضحايا.