المحاضرة الحادية عشر

البرامج الضارة التي تصيب الحاسوب

2- ديدان الحاسب الالي

- دودة الحاسب الالي هي عبارة عن برنامج مستقل بذاته وله ملف خاص به فالدودة تعد برنامجا تطبيقيا متكاملا يمكن ان يعمل لوحدة ولا يضيف نفسه لملف اخر كما الفيروسات
- الدودة ايضا تعمل بمفردها وتحمل نفسها الى ذاكرة الحاسب الالي وتبدأ بالعمل بشكل الي

الفوارق الاصلية بينها وبين الفيروسات

- الديدان تستخدم الشبكات وروابط الاتصالات لكي تنتشر على عكس الفيروسات لا تلتحم مباشرة بالملفات القابلة للتنفيذ
- الديدان لا تحتاج ان تستثيرها لكي تنتشر مثل الفيروسات كفتح ملف او تشغيل برنامج مثل الفيروسات فهي تنتقل مباشرة الى الجهاز بمجرد تصفح مواقع الانترنت او بمجرد فتح بريد الكتروني
- تنتشر اسرع واوسع من الفيروسات
- برنامج الدودة يتكون من أجزاء (رأس وجسم كما في الدودة الطبيعية) تعمل ى اجهزة متفرقة فممكن ان نجد راس البرنامج في جهاز والجسم في جهاز اخر

طرق الانتشار

- من اهم خصائص الديدان هي قدرتها على الانتشار والتكاثر عبر الاتصال بشبكات الحاسب الالي, ومن اهم طرق الانتشار ما يلي:

1) مرفقات البريد الالكتروني المصابة
2) التحميل التلقائي عند زيارة بعض مواقع الانترنت التي من خلالها تنتشر الديدان
3) التسلل عبر الثغرات الامنية في أنظمة التشغيل او برامج الحماية

أضرار الديدان

لا تقل اضرارها عن الفيروسات من ناحية التلف او فقد البيانات

- تتيح للمهاجم استخدام الحاسب الالي المصاب لمهاجمة اجهزة اخرى أو مواقع الانترنت او ارسال بريد الكتروني أو تحميل برامج ضارة اليه
- فتح باب خلفي في الجهاز المصاب فيمكن التحكم بالجهاز من خلال هذا الباب
- يمكن للديدان ان تنسخ نفسها وترسل نسخة الى كل بريد الكتروني مخزن في الجهاز المصاب

3- برامج أحصنة طروادة

- يعرف حصان طروادة بأنه جزء من برنامج(كود) قابل للتنفيذ يؤدي بعض المهام لا يتوقعها المستخدم
- طروادة يمكن ان يوضع في برنامج سليم عند تأليفه وجمعه أو اضافته للبرنامج بعد جمعه
- سبب التسمية يرجع للقصة اليونانية حصان طروادة حيث يمثل (حصان طروادة الخشبي) البرنامج السليم وأما (الجنود)بداخل الحصان هم البرنامج الضار
- تختلف عن الفيروسات او الديدان بأنها لا تتكاثر أو تتضاعف

مكافحة البرامج الضارة

- يمكن مكافحة البرامج الضارة باستخدام حزمة برامج واحدة لمكافحة كل الفيروسات والديدان واحصنة طروادة, فلا بد من تثبيت برامج جيدة وتحديثها باستمرار ,ويجب ان تشمل هذه البرامج على كشف البرامج الضارة وازالتها , ومن اشهرها
  - حزمة برنامج مكافي .(McAfee)
  - حزمة برامج سيمانتك .(Symantec)
  - حزمة برامج كاسبر سكاي .(Kasper SKY)
  - حزمة برامج نورتون .(NORTON)

الخطوات التي يجب اتباعها للحصول على مكافحة جيدة

1. تحديث برنامج المكافحة اليا ودوريا لضمان كشف البرامج الضارة
2. تحديث نظام التشغيل اليا ودوريا عن طريق تنشيط خاصية التحديث التلقائي
3. تحميل ملفات الاصلاح الامنية الخاصة بأنظمة التشغيل وبعض البرامج التطبيقية الاخرى
4. عدم فتح مرفقات البريد الالكتروني التي لها الامتدادات التشغيلية مثل (exe)(scr) ((vbs او (txt.vbs)

ويمكن ان تعمل برامج المكافحة بإحدى الطرق الاتية او جميعها

I. باستخدام جدول زمني معين يحدد من خلاله عمل البرنامج ليبدأ بفحص جميع المكونات مثلا في منتصف الليل من كل يوم

II. عند الطلب من قبل المستخدم ويمكن ان يكون في أي وقت

III. عند تشغيل البرامج أو فتح الملفات أيا كان نوعها

برامج التجسس

- هو أي برنامج يحصل سرا على معلومات عن المستخدم عن طريق الربط بالإنترنت وخاصة بدعوي دعائية واعلانية
- هي برامج مشاركة يمكن تنزيلها من الانترنت وبمجرد تركيبه يبدأ بمراقبة حركة المستخدم على الانترنت وينقل المعلومات من وراء الكواليس لجهة اخرى
- يمكن تصنيف برامج التجسس الى نوعين: برامج رصد وتسجيل وبرامج تتبع
- برامج الرصد والتسجيل: تقوم برصد كل حركة للماوس او ضغطة لوحة المفاتيح بحيث يعيد ترتيب وتكوين ما يفعله المستخدم
- أما المتتبعات: فتراقب عادات الاستخدام وأنماطه وتخزها كبيانات احصائية بهدف اعداد التقارير

طريقة عمل برنامج التجسس

- فنيا لا تصنف برامج التجسس كفيروسات لذلك لا يمكن مكافحته بشكل كامل من خلال برامج مكافحة الفيروسات
- برامج التجسس تعمل خلسة ولا تتلف البيانات بل تتجسس عليها
- لدى برنامج التجسس مكونان اساسيان: ففي الواجهة هو برنامج عادي يعمل في العلن ومفيد بينما هو في الخلف برنامج تجسس ينقل ويراقب المعلومات
- يمكن لبرامج التجسس البقاء في أي صورة او اشكال البرامج القابلة للتنفيذ بما في ذلك التطبيقات (ActiveX, Plug-in), أو أكواد (Applets)

اعراض وجود برامج تجسس

- نشاط اعلى من الحد المعتاد: ويتضح ذلك عندما يرسل الحاسب الالي ويستقبل كميات كبيرة من البيانات عبر شبكة الانترنت ويمكن ملاحظة ذلك بمراقبة جهاز المودوم
- طلب الاتصال بالإنترنت تلقائيا: وتظهر هذه الحالة في الاجهزة التي لا يوجد بها جهاز مودوم (Digital Subscriber Line-DSL)
- ظهور أشرطة أدوات غير مألوفة تضاف الى متصفح الانترنت
- اختيار صفحة بداية لمتصفح الانترنت غير الصفحة التي تم ضبطها من قبل المستخدم

مكافحة برامج التجسس

ليس هناك برنامج يحمي من برامج التجسس بدرجة كاملة ولكن يمكن اخذ بعض التدابير الوقائية منها:

- [illegible] ما يسمى بملفات الكوكي (Cookie Files)
- [illegible] (Pop-UP Blockers) ومنع نوافذ الظهور التلقائي
- استخدام مضادات برامج التجسس

هي برامج شبيهة ببرامج الفيروسات (Antispyware Scanners) حيث يعمل عملية مسح للبرامج بحثا عن برامج التجسس لإزالتها

- استخدام جدار النار الشخصي وبرامج كشف التطفل

تثبيت برامج الجدار الناري (Personal Firewall) قد يوفر بعض الحماية ويمكن للجدار الناري تنبيه المستخدم الى محاولات للدخول للجهاز اثناء تصفح الانترنت

- تأمين متصفح الانترنت

وهي ضبط اعدادات الامان متصفح الانترنت لدرجة مقبولة من الامان

- تأمين ادخال كلمات المرور

وذلك من خلال لوحة مفاتيح افتراضية على الشاشة بدلا من لوحة الاصلية لمنع أي عملية رصد وتسجيل لازار المضغوط عليها من قبل المستخدم