جامعة تكريت

كلية التمريض

علوم التمريض الاساسية

المرحلة الثانية 2023-2024

المادة: حاسوب

عنوان المحاضرة

(الفايروسات)

المحاضرة التاسعة

أستاذ المادة:م.عثمان عواد محمد

الفايروسات

اولا:ماهية فيروسات الحاسب :

الفيروس في حقيقته هو برنامج من برامج الحاسب ولكن تم تصميمه بهدف إلحاق الضرر بنظام الحاسب , وحتى يتحقق ذلك يلزم ان تكون لهذا البرنامج القدرة على ربط نفسه بالبرامج الأخرى وكذلك القدرة على إعادة تكرار نفسه بحيث يتوالد ويتكاثر مما يتيح له فرصة الإنتشار داخل جهاز الحاسب في أكثر من مكان في الذاكرة ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز .

وتكمن خطورة الفيروس في أنه مثله مثل الفيروس الذي يصيب الجسم الإنساني قادر على الانتقال من جهاز إلى آخر بسرعة كبيرة والسبب في ذلك التقدم الكبير الذي وصلت إليه وسائل الاتصال وشبكات الحاسب مما أدى الى سهولة الاتصال بين أجهزة الحاسب والتي ربما تكون في قارات متباعدة , كما أدى توافق نظم التشغيل واتباعها للمعايير الى زيادة انتشار الفيروسات حيث يستطيع البرنامج الواحد الآن أن يعمل على انواع مختلفة من الحاسبات ونسخ مختلفة من نظم التشغيل, والعامل الثالث الذي أدى الى زيادة انتشار الفيروسات هو قرصنة البرامج التي جعلت نسخ البرامج غير الأصلية موضع التداول بين الكثير من الأجهزة ,مما أوجد ثغرة كبيرة تنفذ من خلالها البرامج الملوثة بالفيروسات .

ثانيا:أنواع الفيروسات

تأخذ الفيروسات أشكالا عديدة فقد تشبه الدودة في توالدها وتكاثرها , وقد يتم إدخالها الى النظام لتحدث التخريب المطلوب في توقيت معين أو عند حدوث واقعة معينة. وفيما يلي بعض أشكال الفيروسات :

1-حصان طروادة (esroH najorT):

هو جزء صغير من الكود يضاف الى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات ولكنه يؤدي عملا تخريبيا للنظام , وتكمن خطورته في أن النظام لا يشعر بوجوده حتى تحين اللحظة المحددة له ليؤدي دوره التخريبي .

2-القنابل المنطقية

(sbmoB cigoL)القنبلة المنطقية هي أحد أنواع حصان طراودة وتصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين, فقد تصمم بحيث تعمل عند بلوغ عدد الموظفين في الشركة عددا معينا من الموظفين مثلا أو إذا تم رفع إسم المخرب (واضع القنبلة) من كشوف الراتب, وتؤدي القنبلة في هذه الحالة الى تخريب بعض النظم او الى مسح بعض البيانات أو تعطيل النظام عن العمل .

3-القنابل الموقوتة

(sbmoB emiT)القنبلة الموقوته هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين كأن تحدث مثلا عندما يوافق اليوم الثالث عشر من الشهر يوم الجمعة .

4-باب المصيدة (roodparT)

هذا الكود يوضع عمدا بحيث يتم- لدى حدوث ظرف معين – تجاوز نظم الحماية والأمن في النظام . ويتم زرع هذا الكود عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل كامننا غير مؤذ حتى يقرر المخرب استخدامه، وكمثال على ذلك إقحام كود في في نظام الحماية والأمن يتعرف على شخصية المخرب ويفتح له الابواب دون إجراء الفحوص المعتادة .

5-الديدان (smroW)

الدودة هي عبارة عن كود يسبب أذى للنظام عند استدعائه, وتتميز الدودة بقدرتها على إعادة توليد نفسها , بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث , وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة وهكذا تنتشر الدودة وتتوالد.

ثالثا:كيفية عمل الفيروسات

يقوم من أنشأ أو برمج الفيروس ببرمجة الفيروس) توجيه الأوامر له) حيث يقوم بتحديد الزمان ومتى يبدأ الفيروس بالنشاط , وعادة ما تعطى فرصة كافية من الوقت حتى يضمن حرية الانتشار دون أن يلفت الانتباه ليتمكن من إصابة أكبر عدد ممكن من الملفات في النظام, تختلف الفيروسات من حيث بدأ المستخدمين والنشاط, فهنالك من يبدأ بتاريخ أو وقت محدد , وهنالك من يبدأ العمل بنشاط بعد تنفيذ آمر معين في

البرنامج بالانتشار بعد التكاثر المصاب وهناك بعض من الفيروسات يبدأ بالوصول الى رقم معين من النسخ ثم يقوم بدوره التخريبي .

يقوم الفيروس بعدة أنشطة تخريبية حسب الغرض من إنشاء ذلك الفيروس فهناك ما يقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة أو رسالة تستخف بالمستخدم وهناك أنواع أخرى تقوم بحذف أو تعديل بعض ملفات جهازك وهناك من يقوم بتكرار ونسخ نفسه حتى يشل تماما وهناك أنواع أشد فتكا فتقوم بمسح كل المعلومات من قرصك الصلب .

رابعا:طرق الوقاية من الفيروسات

هناك عدة إجراءات وقائية يعفي تطبيقها المؤسسة من كثير من العواقب الوخيمة التي قد تترتب على الإصابة بالفيروسات مثل :

1- تجهيز عدة نسخ من البرمجيات وحفظها بحيث يمكن استرجاع نسخة نظيفة (غير ملوثة بالفيروس) من البرنامج عند الحاجة .

2- الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل جميع وقائع نقل البرامج المعدلة إلى البيئة الإنتاجية, وبخاصة تلك البرامج المجلوبة من خارج المؤسسة .

3- يجب توعية المستخدمين بعدم تحميل أي برنامج مجلوب من الخارج في حاسباتهم الشخصية, فهذا هو أوسع الأبواب لإدخال الفيروسات إلى النظم والتي عند دخولها ربما تصيب جميع الأقراص وجميع الأجهزة بالشبكة. والبرامج المجانية التي تنتقل من يد إلى يد أو يتم توزيعها بواسطة مجلات الكمبيوتر المتخصصة يجب دائما الحذر في التعامل معها. حتى تلك البرامج التي تأتي من مصادر لا يرقى إليها الشك يجب فحصها جيدا .

4- عند فحص البرمجيات أو اختبارها قبل السماح بنشرها في المؤسسة للاستخدام العام, يجب ان يتم ذلك على جهاز مستقل غير مرتبط بالشبكة. ويجب أن يتضمن الاختبار البحث عن أي سلوك غير مفهوم في البرنامج كأن يخرج رسائل لا داعي لها على الشاشة مثلا، ولو أن خلو البرنامج من مثل هذا السلوك غير المفهوم لا يعني بالضرورة نظافة البرنامج فالفيروسات تظل كامنة ولا تكشف عن سلوكها إلا في اللحظة المناسبة .

5- تركيب برنامج للتحقق من وجود فيروسات ويفضل ان يكون هذا البرنامج دائم الوجود في الذاكرة, وهذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة لها, ولذلك فهي تكون عديمة الفائدة في مواجهة الفيروسات الجديدة, وبعض هذه البرامج يقوم بمقارنة محتويات بعض مناطق القرص (الصلب او اللين) أو

بعض مناطق الذاكرة بمحتوياتها المتوقعة والمفترض أن توجد بها والإبلاغ عن أي تغيير فيها مما قد ينبئ عن وجود فيروس .

-6ويجب عدم إجازة البرامج للاستخدام العام في المؤسسة إلا بعد اجتيازها بنجاح هذه الاختبارات.

خامسا:نصائح للمستخدم من أجل تأمين الكمبيوتر الشخصي_

-1احتفظ بنسخة احتياطية من البرامج والبيانات مأخوذة على فترات متقاربة .

-2احتفظ بهذه النسخ في مكان آمن بعيدا عن الحاسب الشخصي .

-3احتفظ بسرية كلمة المرور وقم بتغييرها من وقت لآخر .

-4لا تترك البيانات معروضة على الشاشة وتغادر المكان .

-5اغلق الجهاز قبل أن تترك مكانك أمامه .

-6احتفظ لديك بالرقم المتسلسل للجهاز وللقرص الصلب .

-7لا تقم بتحميل أي بيانات شخصية دون التنسيق مع مسؤل أمن المعلومات .

-8عند حدوث مشكلة اتصل فورا بمسؤل مساندة المستفيدين .

-9ضع شريط الحماية أو اغلق فتحة التأمين للأقراص المرنة بعد الانتهاء من استخدامها لمنع الكتابة عليها بشكل غير مقصود.