فيروسات الحاسب الالى

تعريف :

فيروس الكمبيوتر هو برنامج صغير يتم إدخاله الى الحاسب الآلي دون علم المستخدم بغرض تدمير بعض أو جميع البرامج والأجهزة المكونة للحاسب الآليه و برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. اي ان فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة. يتصف فيروس الحاسب بأنه :

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

مكونات الفيروس

يتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي

- آلية التناسخ The Replication Mechanism

وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.

- آلية التخفي The Protection Mechanism

وهو الجزء الذي يخفي الفيروس عن الاكتشاف.

- آلية التنشيط The trigger Mechanism

وهو الجزء الذي يسمح للفيروس 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 الفيروس عندما يتم تنشيطه.

اللغات التي يكتب بها الفيروس

من أهم اللغات التي يكتب بها كود الفيروس هي لغة التجميع اسمبلي لسهولة الوصول لعتاد الحاسوب وهنا أيضاً اللغات الراقية مثل لغة سي ولغة سي ++ وفيجوال سي وفيجوال بيسك

تاريخ الفيروسات :

لقد بدأت الفيروسات بالإنتشار في منتصف الثمانينات من القرن الماضي و منذ ذلك الوقت تطورت وظهرت أنواع أكثر شراسة و سرعة خاصة مع نهاية عقد التسعينات و لقد وصل العدد المعروف من الفيروسات الشهيرة و النسخ المعدلة منها الىمئات الالوف من الفيروسات و هي في ازدياد كل يوم وهنالك الاف من الفيروسات الجديدة الفتاكة و المتواجدة داخل المختبرات و مراكز الأبحاث في دول عديدة وهي مخزنة كأسلحة الكترونية ضد الأعداء في حالة الحرب لتخريب أجهزة الكمبيوتر التابعة للعدو .

كيفية عمل الفيروسات :

يقوم من أنشأ الفيروس ببرمجة الفيروس و توجيه الأوامر له حيث يقوم بتحديد الزمان و متى و كيف يبدأ الفيروس بالنشاط وعادة ما تعطى فرصة كافية من الوقت للفيروس حتى يضمن حرية الإنتشار دون أن يلفت الإنتباه ليتمكن من إصابة أكبر عدد ممكن من المستخدمين ، و تختلف الفيروسات من حيث بدأ النشاط فهنالك من يبدأ بتاريخ أو وقت محدد و هنالك من يبدأ بالعمل بعد تنفيذ أمر معين في البرنامج المصاب وهناك من الفيروسات من يبدأ بالنشاط بعد التكاثر و الوصول الى رقم معين من النسخ.

و بعد أن ينشط الفيروس يقوم الفيروس بعدة أنشطة تخريبية حسب الغرض من انشاء ذلك الفيروس فهنالك من يقوم بعرض رسالة تستخف بالمستخدم أو تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة وهناك انواع اخرى تقوم بحذف أو تعديل بعض الملفات وهناك من يقوم بتكرار ونسخ نفسه حتى يشل جهازك تماما و هناك انواع اشد فتكا فتقوم بمسح كل المعلومات من القرص الصلب .

انواع الفيروسات :

1- فيروسات تعمل عند بدء التشغيل : Boot 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 الفيروسات بالتسلل إلى القطاع الخاص ببرنامج الإقلاع على القرص (Boot Sector) ، وإتلاف محتوياته والعبث بها، ما يؤدي إلى تعطل عملية الإقلاع.

2- فيروس الملفات : File 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 الفيروسات برامج التطبيقات المكتبية مثل مايكروسوفت وورد أو أكسل. وهي من أكثر أنواع الفيروسات انتشاراً واستخداماً في عمليات التسلل إلى كمبيوترك عبر التطبيقات.

4- الفيروسات المتعددة الملفات :

تنسخ هذه الفيروسات نفسها في صيغة أولية ثم تتحول إلى صيغ أخرى لتصيب ملفات أخرى.

5- الفيروسات 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- الفيروسات متعددة القدرة التحوليّة :

وهذه الفيروسات لها القدرة الديناميكية على التحول وتغيير الشفرات عند الإنتقال من ملف إلى آخر، لكي يصعب اكتشافها.

من خصائص الفيروسات

1- الإنتشار :

يتميز الفيروس أيضاً بقدرة هائلة على الإنتشار .. وقد سبق وأن قدمت العوامل التي تساعده في ذلك ..

2- القدرة على التخفي :

للفيروسات قدرة عجيبة على التخفي والخداع عن طريق الإرتباط ببرامج أخرى كما تم أيضاً تزويد الفيروسات بخاصية التوميه والتشبّه حيث أن الفيروس يرتبط ببرنامج يقوم بأعمال لطيفة أو له قدرة عرض أشياء مثيرة، وعند بداية تشغيله يدخل إلى النظام ويعمل على تخريبه.

وللفيروسات عدة وسائل للتخفي منها ارتباطه بالبرامج المحببة إلى المستخدمين .. ومنها ما يدخل النظام على شكل ملفات مخفية بحيث لا تستطيع ملاحظة وجوده عن طريق عرض ملفات البرنامج.

وبعض الفيروسات تقوم بالتخفي في أماكن خاصة مثل ساعة الحاسب وتنتظر وقت التنفيذ.

كما أن بعضها تقوم بإخفاء أي أثر لها حتى أن بعض مضادات الفيروسات لا تستطيع ملاحظة وجودها ثم تقوم بنسخ نفسها إلى البرامج بخفة وسرية..

3- القدرة التدميرية :

تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل كأن يكون تاريخ معين (كفيروس تشرنوبل).

أعراض الإصابة

- تكرار رسائل الخطأ في أكثر من برنامج.
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
- تكرار اختفاء بعض الملفات التنفيذية.
- حدوث بطء شديد في إقلاع[نظام التشغيل]أو تنفيذ بعض التطبيقات. رفض بعض التطبيقات للتنفيذ.
- فعند تشغيل البرنامج المصاب فإنه قد يصيب باقي الملفات الموجودة معه في قرص صلب أو المرن, لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر, بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الايميل أوإنترنت أو تبادل الاقراص المرنة.

البرامج المضادة للفيروسات:

هي البرامج التي تقوم بحماية الاجهزة من هجمات الفيروسات و بقية البرامج التي تشكل تهديدا امنيا على معلوماتك وتستطيع أن تحدد هذه الملفات الضارة القادمة من

أي مصدر مثل الأقراص المدمجة و الأقراص اللينة و الرسائل الإلكترونية و كذلك يمكنها رصد هذه البرامج في القرص الصلب وتتمكن هذه البرامج من مسح أو تعطيل عمل البرامج المهددة لسلامة الجهاز و ملفات البرامج الموجودة على جهازك و يتكون برنامج مضاد الفيروسات من جزئين مختلفين

1- التشغيل المباشر عند الدخول :

وهذا الجزء يعمل تلقائيا عند تشغيل(الدخول) البرامج أو تنزيل الملفات من الإنترنت وهو ما يعرف ب On Access element .

2- التشغيل عند الطلب :

وهذا الجزء يعمل عندما تطلب أنت منه ذلك و هو متخصص بالكشف عن الفيروسات و أحصنة طروادة (TORJAN) في القرص الصلب و الأقراص اللينة و الأقراص المدمجة وهو مايعرف ب Demand element .

كيفية عمل البرامج المضادة للفيروسات :

ان البرامج المضادة للفيروسات عبارة عن تقنية مسح و رصد للبرامج المشبوهه التي تتميز بخصائص معينة أو تحتوي على صيغة معينة من البرمجة عبارة عن مجموعة من الأرقام الثنائية وهي التي تعرف ب (التوقيع) و يتم ذلك بالطريقة التالية

- يقوم البرنامج المضاد بالنظر الى كل الملفات و البرامج ذات الطبيعة التنفيذية
- تتم مقارنة التوقيع الموجود على كل ملف بالتواقيع المخزنة في قاعدة المعلومات الخاصة بالبرنامج المضاد للفيروسات

الجدير بالذكر أن كل برنامج مضاد للفيروسات يحتوي على توقيع أكثر من 40000 نوع من الفيروسات و أكثر من عشرة الاف من تواقيع أحصنة طروادة و الديدان كما أن كل شركة منتجة للبرامج المضادة للفيروسات تقوم بتحديث و اضافة المزيد من هذه التواقيع كل يوم .

- بعد عملية المقارنة يقوم البرنامج المضاد بإكتشاف الفيروس أو حصان طروادة و يقوم بإعلام المستخدم عنه .
- يقوم البرنامج المضاد بتخيير المستخدم بين مسح أو تعطيل الفيروس أو بإصلاح الخلل بطريقة آلية .

تكنولوجيا الكشف:

يقوم مصنعي و مبرمجي الفيروسات عادة بتعديل أو تحريف التوقيع الأصلي لبعض البرامج الشهيرة و ذلك لتضليل المستخدم و البرنامج الأصلي و تقوم تكنولوجيا الكشف عن هذا التزوير و التعدبل بواسطة المقارنة السريعة بين التواقيع الأصلية و المزيفة

مدى الإعتمادية على هذه البرامج :

ليس هنالك برنامج مضاد للفيروسات قادر على حمايتك مائة في المائة و لكن اذا قمت بالتحديث المستمر لبرنامجك كل اسبوع فإنك سوف تحصل على حماية تصل الى 95% و ذلك لأن هنالك أكثر من ستمائة من الفيروسات الجديدة و أحصنه طروادة تظهر كل شهر

مفاهيم خاطئة عن برامج الحماية من الفيروسات:

لعل من أكثر المفاهيم الخاطئة بين المستخدمين على مستوى العالم هي الإعتقاد بأن اقتناء برنامج مضاد للفيروسات يمنع و يحمي من هجوم الهاكرز و المخترقين وهذا طبعا ليس صحيح حيث أن هذه البرامج تحميك فقط من الفيروسات و الديدان و تستطيع التعرف على معظم أحصنه طروادة و لكن لا تقوم بغلق المنافذ و المعابر الموجودة في جهازك و التي تمكن المخترقين من الوصول الى جهازك ومعلوماتك و لذلك فإنه من الضروري أن تقوم بالحصول على برنامج متخصص يعرف بجدران اللهب .

أمثلة برامج الحماية من الفيروسات

توجد العديد من برامج الحماية من الفيروسات لكن أفضلها وأشهرها على الإطلاق هما هذان البرنامجان :

- **برنامج النورتون أنتي فايرس Norton Antivirus**
- **برنامج مكافي Mcafee**

وهذان البرنامجان هما الأفضل والأقوى في دنيا مكافحة الفيروسات وخصوصاً مع التحديث الدائم لهما ولتعريفات الفيروسات من خلال الإنترنت لأن التحديث الدائم للبرنامج يتيح له الفرصة في التعرف على الفيروسات الجديدة ومن ثم منعها من إحداث أي ضرر بالجهاز .. وكنصيحة شخصية أنصح الأصدقاء الأعزاء باستخدام برنامج .

كيفية حمـــــاية الحاسب :

1- من الضروري تركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز. إن هذا يتيح لهذه البرامج البحث عن الفيروسات 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 للفيروسات، بشرط أن يكون مصدر الرسالة معروفاً، و أن تكون تتوقع وصول هذا الملف لأن بعض الفيروسات ترسل نفسها بأسماء أشخاص آخرين عن طريق دفتر العناوين .. لذا احذر من ذلك .

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

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

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

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

7- تشغيل برامج مستكشف الفيروسات، 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 الفيروسات تختبئ داخل القرص المرن حتى تجد الفرصة الملائمة للتشغيل عندها.

9- تحميل البرامج عن طريق المواقع الموثوق فيها.

نماذج من الفيروسات :

1-هناك فيروس من نوع الدودة Worm
يحمل هذا الفيروس الاسم " بنتاغون Pentagon" ، ولعل أخطر ما في هذا الفيروس هو سرعة انتشاره عبر الإنترنت ، وذلك عن طريق برنامج

مايكروسوفت أوتلوك ونظام إرسال الرسائل آي سي كيو، ما أدى إلى إصابة الآلاف من أجهزة الكمبيوتر حتى الآن.
ويصيب فيروس البنتاغون برنامج مكافحة الفيروسات بالعجز، ومن ثم يرسل نفسه بصورة تلقائية إلى جميع عناوين البريد الإلكتروني وعناوين الرسائل المستعجلة الموجودة ضمن الكمبيوترات المصابة.
والملف المصاب هو عبارة عن ملف من المفترض أنه تطبيق لحفظ الشاشة Screen Saver، أما الرسالة فتأتي معنونة بعبارة " هاي" ويتضمن نصها عبارة: كيف حالك؟ إنني في عجلة من أمري أعد بأنك ستحبها".
ويقول أحد خبراء مركز أبحاث الفيروسات لدى شركة مكافي أن الفيروس الجديد ينتشر بسرعة كبيرة جداً، وقد ألحق بالشركات والأفراد من مستخدمي الكمبيوتر أضراراً جسيمة نظراً للفترة الزمنية القصيرة التي ينتقل خلالها من مكان لآخر.

يذكر أن آخر الفيروسات التي انتشرت بسرعة هائلة كانت فيروس خطاب الغرام الذي أصاب الملايين من أجهزة الكمبيوتر العام الماضي.

2- فيروس ميليسا Melissa Virus

و هي من أسرع الفيروسات التي أنتشرت في عام 1999 و هي من نوع ماكرو فيروس متخصص في اصابة البريد الإلكتروني وهي تقوم بالإنتشار عن طريق الإلتصاق في برامج النصوص كملحق في رسالة البريد الإلكتروني وما أن يقوم المستخدم بفتح الملف الملحق بالرسالة الا و يبدأ الفيروس بالعمل حيث يستطيع الوصول الى قائمة المراسلة الخاصة بالمستخدم ليقوم بإرسال نفس الرسالة الى أول خمسين عنوان دون علمك و تستمر على نفس المنوال.

3- فيروس الحبLove Virus

و هو مشابه لفيروس مليسا و لكنه متخصص في إصابة برنامج مايكروسوفت أوت لوك لإدارة البريد الإلكتروني و لقد أثار الرعب في بداية هذا العام نتيجة لسرعة انتشاره

4- وفيروس ينتشر ضمن ملفات أدوب أكروبات.

"استطاع قسم مكافي المتخصص في أبحاث الفيروسات لدى شركة نيتورك أسوسيتس، التعرف على فيروس جديد يحمل اسم بيتشي Peachy، وهو يعتمد على مستندات بي دي إف للتنقل والانتشار"، حسب ما ذكره فينسينت غولوتو، مدير مجموعة مكافي لمكافحة الفيروسات.

ولكن لحسن الحظ، فإن أولئك الذين يقومون فقط بتصفح هذا النوع من الملفات لن يكونوا عرضة لمخاطر فيروس بريتشي، فالفيروس ينتشر فقط عن طريق برنامج أدوب أكروبات، البرنامج الذي يقوم بإنشاء مستندات بي دي إف، وليس من خلال برنامج أكروبات ريدر المجاني الذي تنحصر مهمته فقط في استعراض هذا النوع من المستندات.

يستغل هذا الفيروس خاصية متوفرة في برنامج أدوب أكروبات تسمح للمستخدم بدمج ملفات أخرى ضمن ملحقات بي دي إف والتي لا يمكن لأحد فتحها إلا إذا كان لديه برنامج أكروبات.
(يمكننا القول بأن خطورة هذا الفيروس قليلة إلى حد ما، حيث لم يردنا إلى الآن أي تقرير عن وجوده لدى أحد من عملائنا) و يضيف غولوتو : ولكن مما لا شك فيه أن فيروس بريتشي هذا سيثير قلقاً عارماً بين أوساط مستخدمي الكمبيوتر والإنترنت، فظهوره يعني إمكانية أن تتحول مستندات بي دي إف ذات الانتشار الواسع بين مستخدمي البريد الإلكتروني والإنترنت إلى قناة جديدة لتسرب الفيروسات وانتشارها.

يرتبط اسم هذا الفيروس الجديد بلعبة صغيرة موجودة ضمن مستندات بي دي إف تدور فكرتها حول البحث عن الخوخ Peach ، وذلك حسب ما جاء على لسان شخص اسمه زولو يدعي أنه هو الذي صمم هذا الفيروس.

وفي حال قامت شركة أدوب مستقبلاً بتعديل إصداراتها الجديدة من أكروبات ريدر بحيث تغدو قادرة على قراءة الملفات المرفقة داخل مستندات من نوع بي دي إف، فإن هذا البرنامج سيصبح عرضة لفيروس بريتشي أيضاً.

ولدى وصول الفيروس إلى جهاز ما، فإنه يقوم تلقائياً بإرسال نفسه إلى الآخرين بعد أن يجمع كافة العناوين البريدية من برنامج آوتلوك وعقب عقد اتفاقية مع شركة أدوب في يونيو/ حزيران الماضي، أصبح برنامج مكافحة الفيروسات مكافي قادراً على إجراء مسح وقائي على مستندات بي دي إف، ولكن ومع ذلك فإن هذه العملية لن توفر الحماية الشاملة من أنواع أخرى مماثلة من الفيروسات، سيما أن البرنامج لا يستطيع التعرف على الفيروسات وإثباط نشاطها ما لم يتم تحديث بياناته باستمرار غير أن التحديث الأخير الذي تم إجراؤه على برنامج مكافي لمكافحة الفيروسات سيجعل البرنامج قادراً على كشف الفيروس بريتشي في حال وجوده ..