وزارة التنمية الاجتماعية

مديرية التطوير المؤسسي / قسم تكنولوجيا المعلومات

ورقة عمل

الفيروسات

إعـــداد

م.هبة الأشهب / م.مجد التميمي

إشـــراف

رئيس قسم تكنولوجيا المعلومات / فايزة الراميني

أيلول 2011

فهرس المحتويات

فيروس الحاسوب

فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. أي أن 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 آخر 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.

- **آلية التنفيذ** ***The Payload Mechanism***

  وهو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه.

طرق انتقال الفيروسات

1. الشبكة العنكبوتية (الإنترنت) : وسيلة سهلة لانتقال الفيروسات من جهاز لآخر ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات.
2. وسائط التخزين مثل الفلاش والأقراص الممغنطة والمرنة.
3. رسائل البريد الإلكتروني.
4. استلام ملفات أي كانت الملفات مخزنة على(أقراص مرنة أو أقراص مضغوطة أو أقراص*zip*).

ويمكن أن نميز فئتين من فيروسات الحاسوب تبعاً لآلية العدوى وانتشار الفيروس

- **فيروس العدوى المباشر*Direct Infector***

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع فإن ذلك الفيروس يبحث بنشاط عن ملف أو أكثر لينقل العدوى إليه، وعندما يصاب أحد الملفات بالعدوى فإنه يقوم بتحميله إلى الذاكرة وتشغيله وهذا النوع قليل الانتشار.

- **فيروس العدوى غير المباشر*Indirect Infector***

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع فإن ذلك الفيروس سينتقل إلى ذاكرة الحاسوب ويستقر فيها ويتم تنفيذ البرنامج الأصلي ثم يصيب الفيروس بالعدوى كل برنامج يتم تحميله إلى الذاكرة بعد ذلك إلى أن يتم قطع التغذية الكهربائية عن الحاسوب أو إعادة تشغيله.

أنواع الملفات التي يمكن أن يصيبها الفيروس

بشكل عام الفيروس تصيب الملفات التنفيذية أو الملفات المشفرة غير النصية مثل التالية:-

1. الملفات ذاتية التنفيذ مثل ملفات ذات امتداد(.EXE, .COM.).
2. سجلات الملفات والبيانات (VOLUME BOOT RECORD) في الأقراص المرنة والصلبة .
3. ملفات الأغراض العامة مثل ملفات الباتش والسكريبت (patch, script) في Windows وملفات الشل (shell) في Unix.
4. ملفات الاستخدام المكتبي في Windows التي تحتوي Microsoft office مثل (Word,excel ,power point and Accsses)
5. قواعد البيانات (Data base) وملفات الاوتولوك (Outlook) لها دور كبير في الإصابة ونشر الإصابة لغيرها لما تحويه من عناوين البريد الالكتروني.
6. ملفات الأكروبات (PDF) وبعض النصوص المهجنة HTML احتمال احتوائها على كود خبيث.
7. الملفات المضغوطة مثل RARZIP, .

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 تحميل نظام التشغيل (Booting) أو تنفيذ بعض التطبيقات، ورفض بعض التطبيقات للتنفيذ.
- عند 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 الإيميل أو إنترنت أو تبادل الأقراص المرنة.

تعمل الفيروسات بطبيعتها على تعطيل عمل الحاسوب أو تدمير ملفاته وبرامجه هناك فيروسات تعمل على خلق رسائل مزعجة وأنواع تعمل على تشغيل برامج غير مطلوبة وأنواع تعمل على إشغال المعالج بحيث تبطئ سرعة الحاسوب أو سرقة بيانات من حاسوب المستخدم مثل أرقام حسابات وكلمات السر أو أرقام بطاقات الائتمان وبيانات مهمة أخرى وهذه أهم أهداف الفيروسات الحديثة وبرامج التجسس التي يتم تطويرها يوما بعد يوم.

أنواع الفيروسات

1. من حيث النوع

• **(Worms) :** فيروس ينتشر فقط عبر الشبكات والإنترنت ويعمل على الانتشار على الشبكات عن طريق دفتر عناوين البريد الإلكتروني مثلا فعند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص وهكذا... مما يؤدي إلى انتشاره بسرعة عبر الشبكة وقد اختلف الخبراء فمنهم اعتبره فيروس ومنهم من اعتبره برنامج خبيث وذلك كون Worm لا ينفذ أي عمل مؤذي إنما ينتشر فقط مما يؤدي إلى إشغال موارد الشبكة بشكل كبير.

• **(Trojan Horse) :** سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها وهكذا تكون آلية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج دون أن يعلم المستخدم.

2. من حيث السرعة

- فيروسات سريعة الانتشار.
- فيروسات بطيئة الانتشار.

3. من حيث توقيت النشاط

- فيروسات تنشط في أوقات محددة.
- فيروسات دائمة النشاط.

4. من حيث مكان الإصابة

- فيروسات مقطع التشغيل boot sector على الأقراص وهي الأكثر شيوعاً.
- فيروسات الماكرو macro التي تختص بإصابة الوثائق والبيانات الناتجة عن حزمة مايكروسوفت أوفيس (Microsoft Office) .

5. من حيث حجم الضرر

- **الفيروسات المدمرة للأجهزة** : لا يوجد فيروسات خارقه تدمر الأجهزة كما نسمع أحيانا (احترق المعالج بسبب الفيروس، تعطلت وحدة التغذية بسبب الفيروس، أو تلف الشاشة بسبب الفيروس ،... الخ) ولكن يمكن للفيروس أن يؤذي الذاكرة Rom في الحاسب كما في فيروس تشرنوبل أو أن يمحي معلومات ال ((MBR (Main Boot Record) على القرص الصلب فتعود الأقراص الصلبة كما أتت من المصنع وفي الحالتين السابقتين لا يتم إقلاع الجهاز Booting مما يوحي للبعض أن الفيروس (حرق) الحاسوب ، وهذه الفيروسات تعتبر خطيرة جدا لأنها تتسبب في إتلاف البيانات المخزنة والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤدي إلى خسائر جسيمة أو إلى توقف الحاسبات عن العمل كما في تشرنوبل مما يؤدي إلى توقف الخدمات المقدمة.

- **الفيروسات المدمرة للبرامج:** يعد تأثير هذه الفيروسات محدود طالما أن البيانات لم تتأثر حيث يمكن تخزين البيانات وإعادة تهيئة الحاسوب وإعادة البرامج المتضررة من أقراصها الأصلية.

- **الفيروسات عديمة الضرر**: وهي التي لا تقوم بأي عمل مؤذي وإنما تم برمجتها لإثبات الذات والقدرة على البرمجة من بعض المراهقين فمنها ما يرسم كرة أو أي شكل على الشاشة طوال فترة عمل الكمبيوتر ومنها ما يغير بعض الأحرف (كتغير حرف بحرف أينما وجد) أو تغيير مؤشر الماوس.

أمثلة على بعض الفيروسات

- **فيروس Brontok أو الفيروس الذي يخفي خيارات المجلد أو يفقدك التحكم في الرجستريRegistry فتصبح غير قادر على التحكم في الحاسوب:** هذا الفيروس من أبرز مهامه أنه يقوم بإخفاء خيارات المجلد من قائمة أدوات الموجودة في نظام الويندوز (Windows) وأيضا يقوم بتكرار جميع المجلدات التي يصيبها حتى أنك لا تعرف الأصل من النسخة وقد تحذف الأصل ظنا منك أنه الفيروس، وهو أيضا يقوم بفتح شاشة Internet Explorer ويقوم بفتح شاشة خضراء اللون بشكل مستمر مما يسبب بطء في النظام ومما يؤدي إلى زيادة انتشار هذا الفيروس في الكمبيوتر

- **فيروس copy :** يصيب هذه الفيروس الـ Partion للقرص الصلب ويجعله لا يفتح مباشرة وذلك بزرع ملف autorun وحينما تحاول فتح الـPartion يعطيك قائمة فتح باستخدام (Open with) ولا تستطيع الدخول إلى القسم الذي تريده إلا بطرق ملتوية مثل (استكشاف وتشغيل)، ويقوم أيضا باستمرار طلب إدخال الفلوبي دسك(Floppy desk) أو القرص المرن (CD) للكمبيوتر .

تصنيف الفيروسات حسب خطورتها

- **العادي: Trivial**

لا يفعل الفيروس العادي شيئا سوى التكاثر replication ولا يسبب أي ضرر أو تخريب للمعلومات مثل فيروس stupid

- **الثانوي: Minor**

يصيب الملفات التنفيذية فقط executable file (.exe) ولا يؤثر على البيانات

- **المعتدل: Moderate**

يقوم بتدمير جميع الملفات الموجودة على القرص إما باستبدال المعلومات بمعلومات لا معنى لها أو عن طريق إعادة التهيئة Reformatting مثل فيروس Disk killer الذي يقوم بإعادة تهيئة القرص، ويمكن حل مشكلة هذه الفيروسات عن طريق استخدام النسخ الاحتياطي (Backup file)

- **الرئيسي: Major**

يؤدي الفيروس إلى تخريب المعلومات بإجراء تغيرات ذكية وبارعة للبيانات دون أن يترك أثرا يشير إلى التغيير الحاصل كأن يقوم بتبديل كتل المعلومات المتساوية في الطول بين الملفات كما أن تأثيره يكون على المدى الطويل ولن يكون من الممكن اكتشاف الإصابة إلا بعد بضعة أيام وبذلك لا يمكن الوثوق بالنسخة الاحتياطية أيضا.

- **اللامحدود: Unlimited**

يستهدف الشبكات والملفات المشتركة وتمضي أكثر الوقت في محاولة معرفة كلمة السر للمستخدمين الأكثر فاعلية وعند معرفتها يقوم بتمريرها إلى أحد أو أكثر من مستخدمي الشبكة على أمل أنهم سيستخدمونها لأغراض سيئة.

- **ميليسا : Melissa**

أعطى هذا الفيروس فاعلية كبيرة جدا حيث أجبر شركة Microsoft والعديد من كبرى الشركات الأخرى على إطفاء مخدمات البريد بشكل كامل حتى تمكنوا من القضاء عليه.

من يقوم بعمل الفيروسات وما هي أهدافهم

فيروس الحاسوب لا ينشأ من لا شيء ولا يأتي من مصدر مجهول ولا ينشأ بسبب خلل بسيط حدث في الحاسوب، فيروس الحاسوب يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمه بشكل متقن. والمبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرما وصناعة الفيروس جريمة يحاسب عليها حسب قانون الدولة الموجود بها.

يعمل المبرمجون على برمجة الفيروسات وذلك لأهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية وإجرامية، فبعض المبرمجين الهواة يعتبرون أن عمل الفيروس نوع من الفن والهواية التي يمارسونها.

الهدف التجاري

يعد من أهم الأهداف لعمل فيروس الحاسوب، وذلك عن طريق عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات لأنه بعمل الفيروس يصبح المستخدمون بحاجة إلى برامج مضادة للفيروسات ويضطرون للشراء ومعظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات من قبل المبرمجين وتقوم بعمل مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكمبيوتر.

الهدف العسكري

هو محاولة الدخول لأنظمة الطرف الآخر لكشف أسرار واخذ بيانات عن طريق برامج التجسس.

الهدف الإجرامي

يهتم بسرقة البيانات وأرقام الحسابات أو أرقام بطاقات الائتمان وكلمات السر لمحاولة الدخول لحسابات المشتركين في البنوك وسرقة أموالهم ، أو سرقة بيانات من أجهزتهم.

طرق الوقاية من الفيروسات من قبل المؤسسة

هناك عدة إجراءات وقائية تحمي المؤسسة عند تطبيقها 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- على المستخدم عدم تحميل أي برنامج من الخارج في حاسوبه الشخصي، فهذا هو أوسع الأبواب لإدخال الفيروسات إلى النظم والتي عند دخولها ربما تصيب جميع الأقراص وجميع الأجهزة بالشبكة، مثال عليها البرامج 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.

3- فحص البرمجيات أو اختبارها قبل السماح بنشرها في المؤسسة للاستخدام العام، يجب أن 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، كما 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 .

4- تركيب برنامج للتحقق من وجود فيروسات ويفضل أن يكون هذا البرنامج دائم الوجود في الذاكرة، وهذا البرنامج يقوم بالتأكد من عدم وجود الفيروسات المعروفة له، ولذلك فهو يكون عديم الفائدة في مواجهة الفيروسات الجديدة، ما لم يتم تحديث هذا البرنامج بشكل مستمر .

برامج مكافحة الفيروسات

مضاد الفيروسات (أو برنامج *مضاد للفيروسات)* هو برنامج يستخدم لمنع واكتشاف وإزالة البرمجيات الخبيثة، بما فيها فيروسات الحاسوب، والديدان، وأحصنة طروادة.

مهما كانت برامج مكافحة الفيروسات مفيدة، في بعض الأحيان يمكن أن تكون لها عيوب، فيمكن لبرامج مكافحة الفيروسات أن تؤثر على أداء الحاسوب إذا لم تكن مصممة بكفاءة، وقد يواجه المستخدمين غير الخبراء مشكلة في فهم الأوامر والقرارات التي تقدمها برامج الحماية من الفيروسات ويؤدي القرار غير الصحيح إلى الإخلال بالأمن.

يمكن القول أن هناك عدة أسباب تؤدي إلى حدوث مشاكل بسبب الفيروسات بالرغم من وجود برامج الحماية منها:-

1- عدم تحديث برامج الحماية بشكل دوري مما يعني ظهور فيروسات جديدة لا تستطيع تلك البرامج اكتشافها.

2- جهل المستخدم بطريقة استعمال برامج الحماية، واعتقاد البعض أن برامج الحماية كفيلة بتقديم الحماية المطلوبة وبالتالي يهمل الجوانب الأخرى، مثل عمل النسخ الاحتياطي بشكل دوري لجميع المعلومات الهامة وحفظها في أماكن آمنة بعيدة عن المخاطر التي يمكن أن تتعرض لها.

3- عدم تحديث معلومات خبراء المعلوماتية بالمستوى الذي يتطلبه أداء أعمالهم.

من الأمثلة على برامج مكافحة الفيروسات :-

Kaspersky, MacAfee, Norton , Avira

نصائح للمستخدم من أجل تأمين الكمبيوتر الشخصي

1. تحميل برنامج مكافح الفيروسات على الجهاز، ومعرفة كيفية استعماله ومتابعة تحديثه.
2. احتفظ بنسخة احتياطية من البرامج والبيانات مأخوذة على فترات متقاربة، وضعها في مكان آمن بعيدا عن الحاسب الشخصي .
3. احتفظ بسرية كلمة المرور وقم بتغييرها من وقت لآخر .
4. لا تترك البيانات معروضة على الشاشة وتغادر المكان .
5. أغلق الجهاز قبل أن تترك مكانك أمامه.
6. عدم استعمال أي فلاش أو قرص بدون فحصه من قبل برنامج مكافح الفيروسات.
7. عدم فتح رسائل مجهولة المحتوى أو في حال عدم معرفة مرسلها بواسطة البريد الالكتروني وعدم فتح مواقع وصفحات انترنت غير موثوق بها.
8. عند حدوث مشكلة اتصل فورا بمسؤول مساندة المستخدمين.

المصادر

- http://www.moheet.com/show_news.aspx?nid=114396&pg=10.
- http://www.mafhoum.com/press4/136T45.htm.
- http://ar.wikipedia.org/wiki/%D9%81%D9%8A%D8%B1%D9%88%D8%B3_%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D9%88%D8%A8 .
- http://www.nwtechusa.com/pdf/kaspersky_vs_mcafee.pdf
- http://www.isoftland.com/docs/kaspersky/info/Kaspersky_vs_Microsoft.pdf