

أنواع الفيروسات في الحاسب الألي

ماهي أنواع الفيروسات ؟

أشرف الدكتور القدير/

أعداد الطالب /زهير هشام المرشدي

عبدالماجد الخليدي

تخصص/هندسة اتصالات

سنخلص في هذا البحث معلومات مهمة عن أنواع
الفيروسات والفرق بين كل نوع واخر من حيث تأثيراتها
عل الحاسب الألي

أولاً : ما هي الفيروسات :

هي برنامج أو جزء في الشفرة التي تدخل إلى الحاسب الألي لهدف التخريب وتتميز بقدرتها على نسخ نفسها إلى نسخ كثيرة وقدرتها على الانتقال من مكان إلى مكان ومن حاسب إلى حاسب والاختفاء وتغطية محتوياتها .اهمية وجودها .

أسئلة متداوله:

(١) ماهي الفيروسات ؟

(٢) مما يتكون الفيروس؟

(٣) ماهي انواع

الفيروسات؟

ثانياً : مما يتكون الفيروس؟

(١) برنامج فرعي ليصيب البرامج التنفيذية .

(٢) برنامج فرعي لبدء عمل الفيروس ..

(٣) برنامج فرعي لبدء التخريب ..مكونات اللوحة الام المادية

ثالثاً: أنواع الفيروسات :

(١) يبدأ عمل الفيروس التخريبي إذا تحقق شرط معين كتاريخ - أو فتح برنامج أو انتقال من نظام إلى نظام.

(٢) يبدأ عمل الفيروس التخريبي بمجرد التشغيل الحاسب وتعمل على نسخ نفسها لإعادة تشغيلها.

(٣) يبدأ عمل الفيروس التخريبي بمجرد الانتقال ولمرة واحدة.

ملاحظات هامة :

الفيروسات هي برامج

تخريبية صممت من قبل

مبرمجين

رابعاً: مكان الإصابة بالفيروسات :

(١) فيروسات قطاع التشغيل (**Boot Sector Virus**)

(**Virus**) :وهو الذي ينشط في منطقة نظام

التشغيل وهو من اخطر أنواع الفيروسات حيث انه

يمنعك من تشغيل الجهاز

أسئله متداوله:

١- ماهي الفيروسات

من حيث مكان

الإصابة؟

(٢) فيروسات الماكرو (**Macro Virus**) :وهي

من أكثر الفيروسات انتشارا حيث أنها تضرب برامج

الأوفيس و كما أنها تكتب بالورد

(٣) فيروسات الملفات (**File Virus**) :وهي

تنتشر في الملفات وعند فتح أي ملف يزيد انتشارها

ملاحظات هامه:

تختلف انواع

الفيروسات من حيث

المكان المستهدف

(٤) الفيروسات المخفية (**Steath Virus**)

:وهي التي تحاول أن تختبئ من البرامج المضادة

للفيروسات و لكن سهل الإمساك بها

تابع : مكان الإصابة بالفيروسات :

ملاحظه هامه :

تابع مكان الإصابة

بالفيروسات:

(5) الفيروسات المتحولة (Polymorphic)

(virus) : وهي الأصعب على برامج المقاومة

حيث انه صعب الإمساك بها وتتغير من جهاز إلي

آخر في أوامرها ..ولكن مكتوبة بمستوى غير

تقني فيسهل إزالتها.

(6) فيروسات متعددة الملفات

(Multipartite Virus) : تصيب ملفات قطاع

التشغيل و سريعة الانتشار

(7) فيروسات الودودة (Worm) : وهو عبارة عن

برنامج ينسخ نفسه على الاجهزه و يأتي من

خلال الشبكة و ينسخ نفسه بالجهاز عدة مرات

حتى يبطل الجهاز وهو مصمم لإبطاء الشبكات لا

الأجهزة و بعض الناس تقول انه هذا النوع لا يعتبر

فيروس حيث انه مصمم للإبطاء لا لأزله الملفات و

تخريبها ..

ملاحظات هامه:

تختلف انواع

الفيروسات من حيث

المكان المستهدف

تابع : مكان الإصابة بالفيروسات :

ملاحظه هامه :

(١) تابع مكان الإصابة

بالفيروسات:

(٢) خطوات عمل

الفيروس:

٨)الباتشات (Trojans) : وهو أيضا عبارة عن برنامج صغير قد يكون مدمج مع ملف آخر للتخفي عندما ينزله شخص و يفتحه يصيب ال Registry و يفتح عندك منافذ مما يجعل جهازك قابل للاختراق بسهولة و هو يعتبر من أذكى البرامج فمثلا عند عمل سكان هناك بعض التورجن يفك نفسه على هيئة ملفات غير محدد فيمر عليها السكان دون التعرف عليه و من ثم يجمع نفسه مره ثانيه.

خامساً : خطوات عمل الفيروس :

تختلف طريقة العدوى من فايروس لآخر و من نوع لآخر و هذا شرح مختصر لكيفية عمل الفيروسات :

(١)تحدث العدوى لبرنامج تنفيذي و لن تشعر باي تغيير فيه .

(٢) عندما يبدأ البرنامج المصاب بالعمل يبدأ نشاط الفيروس كما يلي :

أنظر الى الجدول الذي يوضح الخطوات لبدأ نشاط الفيروس :

ملاحظات هامه:

تبيين لخطوات عمل

الفيروسات

عندما يبدأ البرنامج
المصاب بالعمل يبدأ
نشاط الفيروس كما يلي
:

ب- بعد ذلك
تكون حدثت
العدوى فتحدث
عملة التخريب
التي تسبب
الأخطاء عند
عمل البرنامج
المصاب .

أ- ينفذ البرنامج الفعلي
الخاص بالبحث ، فيبحث
الفيروس عن البرامج
ذات الامتداد . exe
أو com . أو أن واجد أي
منها يحضر جزء صغير
من بداية البرنامج إلى
الذاكرة و من ثم يبحث
عن علامته فان وجدها
ترج البرنامج و بحث
عن غيره و إذا لم يجدها
يضعها في أول البرنامج

ملاحظه هامه :

(١)تابع خطوات عمل

الفيروس:

(٢) هناك رسم بياني

يوضح خطوات بدأ

نشاط الفيروس

(٣) بعد ذلك يعود التحكم للبرنامج مره أخرى (بعد ان

كان الفيروس يتحكم فيه) ليبدو انه يعمل بصورة

طبيعية .

(٤) بعد ذلك تكون عملية العدوى انتهت يتم التخلص

من الفيروس الموجود في الملف التنفيذي الأول

حيث أن الفيروس قد انتشر في البرامج الأخرى .

ملاحظات هامه:

تبيين لخطوات عمل

الفيروسات

سادساً: ما هو تأثير الفيروس :

(١) تباطؤ أداء الكمبيوتر ، أو حدوث أخطاء غير معتادة عند تنفيذ البرنامج .

(٢) زيادة حجم الملفات ، أو زيادة زمن تحميلها إلى الذاكرة .

(٣) سماع نغمات موسيقية غير مألوفة .

(٤) ظهور رسائل أو تأثيرات غريبة على الشاشة .

(٥) زيادة في زمن قراءة القرص إذا كان محمياً وكذلك ظهور رسالة **FATAL/O ERROR**

(٦) تغيير في تاريخ تسجيل الملفات كما في فيروس **Vienna** الذي يكتب ٦٢ مكان الثواني .

(٧) حدوث خلل في أداء لوحة المفاتيح كأن تظهر رموز مختلفة عن المفاتيح التي تم ضغطها كما في فيروس **Haloechon** أو حدوث قفل للوحة المفاتيح كما في فيروس **Edv** .

(٨) نقص في مساحة الذاكرة المتوفرة كما في فيروس **Ripper** الذي يحتل ٢ كيلو بايت من أعلى الذاكرة الرئيسية . ويمكن كشف ذلك بواسطة الأمر **MEM** أو **CHKDSK** .

ملاحظه هامه :

(١) ماهي تأثيرات
الفيروسات على
الحاسب الآلي؟

ملاحظات هامه:

تبيين تأثيرات

الفيروسات

تابع : تأثيرات الفيروس:

٩) ظهور رسالة ذاكرة غير كافية لتحميل برنامج
كأن يعمل سابقاً بشكل عادي .

١٠) ظهور مساحات صغيرة على القرص كمناطق

سيئة لا تصلح للتخزين كما في فيروس **Italian**

وفيروس **Ping Pong** اللذين يشكلان قطاعات

غير صالحة للتخزين مساحاتها كيلوبايت واحد .

١١) تعطيل النظام ب الإقلاع **BOOT**

SECTOR

١٢) إتلاف ملفات البيانات مثل ملفات وورد واكسل

..... وغيرها .

سابعاً : ما هي مراحل العدوى ؟

١) مرحلة الكمون : حيث يختبأ الفيروس في

الجهاز لفترة ..

٢) مرحلة الانتشار : و يبدأ الفيروس في نسخ

نفسه والانتشار في البرامج وأصبتها ووضع

علامته فيها.

ملاحظه هامه :

تابع

١) ماهي تأثيرات

الفيروسات على

الحاسب الآلي؟

٢) ماهي مراحل

العدوى؟

ملاحظات هامه:

تابع

تبيين تأثيرات

الفيروسات

تابع : مراحل العدوى :

(٢) مرحلة جذب الذناب : و هي مرحلة الانفجار في

تاريخ معين او يوم. مثل فيروس تشرنوبيل .

(٤) مرحلة الأضرار : و يتم فيها تخريب الجهاز .

ثامناً: كيف تنتقل أو تصيب الأجهزة :

(١) تشغيل الجهاز بواسطة اسطوانة مرنة مصابه.

(٢) تنفيذ برنامج في اسطوانة مصابه .

(٣) نسخ برنامج من اسطوانة مصابة بالفيروس

إلى الجهاز .

(٤) تحميل الملفات أو البرامج من الشبكات أو

الإنترنت .

(٥) تبادل البريد الإلكتروني المحتوي على

الفيروسات (attachments) .

(٦) فلاشات الميمورى والميمورى كاردس.

ملاحظه هامه :

(٢) ماهي مراحل

العدوى؟

ملاحظات هامه:

تبيين تأثيرات

الفيروسات

تاسعاً : الإجراءات الواجبة عند اكتشاف

الإصابة بالفيروسات :

(١) تصرف بهدوء وبدون استعجال لئلا تزيد الأمر سوءاً ولا تبدأ بحذف الملفات المصابة أو تهيئة الأقراص .

(٢) لا تباشر القيام بأي عمل قبل أعداد وتدقيق خطة العمل التي تبين ما ستقوم به بشكل منظم .

(٣) أعد إقلاع جهازك من قرص نظام مأمون ومحمي وشغل أحد البرامج المضادة للفيروسات التي تعمل من نظام دوس ومن قرص لين ولا تشغل أي برنامج من قرصك الصلب .

(٤) أفحص جميع الأقراص اللينة الموجودة لديك مهما كان عددها لعزل الأقراص المصابة من السليمة .

ملاحظه هامه :

٣) ماهي الاجراءات

الواجبه عند

أكتشاف الأصابه

بالفيروسات؟

ملاحظات هامه:

هذه الإجراءات مهمه

للحفاظ على الحاسب الألي

عاشراً: الوقاية من الإصابة بالفيروسات :

ملاحظه هامه :

(١) كيفية الوقايه من

الأصابه

بالفيروسات؟

(١) فحص جميع الأقراص الغريبة أو التي

استخدمت في أجهزة أخرى قبل استعمالها .

(٢) تهيئة جميع الأقراص اللينة المراد استخدامها

على جهازك .

(٣) عدم تنفيذ أي برنامج مأخوذ من الشبكات

العامة مثل إنترنت قبل فحصه .

(٤) عدم إقلاع الكمبيوتر من أي قرص لين قبل

التأكد من خلوه من الفيروسات .

(٥) عدم ترك الأقراص اللينة في السواعة عند ما

يكون الجهاز متوقفا عن العمل .

(٦) التأكد من خلو سواعة الأقراص اللينة قبل

إعادة إقلاع الجهاز .

(٧) عدم تشغيل برامج الألعاب على الجهاز ذاته

الذي يتضمن البيانات والبرامج الهامة .

(٨) استخدام برامج أصلية أو مرخصة .

(٩) استخدام كلمة سر لمنع الآخرين من العبث

بالكمبيوتر في غيابك .

ملاحظات هامه:

الوقايه خير من العلاج

(مهمه)

تابع الوقاية من الإصابة بالفيروسات :

١. الاحتفاظ بنسخ احتياطية متعددة من جميع ملفاتك قبل تجريب البرامج الجديدة .

١١) تجهيز الكمبيوتر ببرنامج مضاد للفيروسات واستخدامه بشكل دوري .

١٢) تحديث البرامج المضادة للفيروسات بشكل دائم لضمان كشف الفيروسات الجديدة .

١٣) الاحتفاظ بنسخة DOS نظيفة من الفيروسات ومحمية ضد الكتابة لاستخدامها عند الإصابة.

١٤) الانتباه للأقراص اللينة الواردة من المعاهد والكيانات (الأماكن التقليدية للفيروسات) .

١٥) حماية الأقراص اللينة ضد الكتابة لمنع الفيروسات من الانتقال إليها .

١٦) إغلاق الجهاز نهائياً وإعادة تشغيله عند ظهور عبارة **non bootable diskette**.

تم بحمد الله

تحت اشراف الدكتور القدير /

عبد الماجد الخليدي

ملاحظه هامه :

٢) تابع كيفية الوقايه

من الأصابه

بالفيروسات؟

ملاحظات هامه:

الوقايه خير من العلاج

(مهمه)