جـامعة البعث
كـلـية العلوم
قسم الرياضيات

دراسة تحليلية للبرامج الضارة وطرق الوقاية منها

رسالة قُدّمت لنيل درجة الماجستير في المعلوماتية

إعداد

فدوى صافيه

بـإشـراف

الدكتور
محسن حسين

الدكتور
أحمد الخضر

١٤٣٤ هجري
٢٠١٣ ميلادي

الملخص:

يعتبر موضوع فيروسات الحاسوب من أكثر المواضيع أهمية بالنسبة لمستخدمي الحاسوب و ذلك بسبب الانتشار السريع لاستخدام الحاسوب و الشبكات و دخولها في جميع مجالات الحياة. و لهذا السبب قمنا في هذا البحث بدراسة فيروسات الحاسوب و ذلك من خلال تعريف الفيروس و آلية عمله و كذلك أنواع الفيروسات و دراسة عامة لفيروسات الملفات و كذلك وضع خوارزمية تقوم بتصميم فيروس يلتحق بالملفات بنوعيها الـ Exe و Com و بعد ذلك وضع خوارزمية تقوم بتصحيح الملفات المصابة بهذا الفيروس.

و قيمنا إمكانية توظيف هذه الخوارزمية في عملية تصحيح الملفات المصابة بالفيروسات و اعتمدنا في التقييم على مدى الاستفادة من هذه الخوارزمية من خلال إمكانيتها في تصحيح كلا الملفات أي Exe و Com معاً. و قد كانت النتائج أن الخوارزمية السابقة تستطيع تصحيح الملفات التنفيذية معاً و تقوم بإعادة الملف إلى وضعه السابق قبل الإصابة و ذلك بالكشف عن شيفرة الفيروس.

لهذا نرجو أن تكون نتائجنا هذه نقطة انطلاق نحو تطوير هذه الخوارزمية و إيجاد خوارزميات ذات أداء أفضل و أسرع و تستطيع اكتشاف أنواع أكثر من الفيروسات و بشكل يتناسب مع التطورات التي تمر بها الفيروسات و مع أشكالها المتنوعة و أهدافها المختلفة.

مقدمة:

بداية الفيروسات:

بدأ الفيروس في الظهور سنة ١٩٧٨ أو قبل هذا التاريخ بقليل حيث أن البداية الحقيقة يصعب تحديدها بدقة. ثم بدأ يأخذ طابع المشكلة المعقدة حديثاً خاصة مع انتشار وسائل الاتصالات، كما تسبب استخدام البريد الالكتروني في انتشار الفيروس بدرجة كبيرة حيث أنه من خلال البريد الالكتروني يمكن إرسال الرسائل إلى آلاف المستخدمين الذين يشتركون في نظام الحاسوب و بالتالي انتشار أسرع للفيروس أي أصبحت وسائل الاتصالات التي تقدمت تقدماً كبيراً في الفترة الأخيرة وسيلة من وسائل انتقال الفيروس إلى مسافات بعيداً جداً، و من هنا ظهرت المشكلة و قامت الشركات بإنشاء برامج تقوم بفحص الملفات و التنبيه إلى وجود فيروسات و إصلاح الملفات المصابة. في هذا البحث سنقوم:

أولاً: إجراء دراسة عن الفيروسات من خلال تعريفها و أسباب كتابة الفيروسات.

ثانياً: سنقوم بشرح أنواع الفيروسات فيروسات نظام تشغيل Dos .

ثالثاً : سنقوم بشرح أنواع الفيروسات فيروسات نظام تشغيل Windows .

رابعاً : فيروسات الماكرو البرامج التطبيقية.

خامساً: فيروسات الشبكات والبريد الالكتروني.

سادساً: الثغرات الأمنية لأنظمة التشغيل و بعض البرامج التطبيقية.

سابعاً: دراسة عن عمل الفيروس بشكل عام و كذلك آلية عمله ثم إعداد خوارزمية خاصة لبرنامج يقوم بإنشاء فيروس ملف.

ثامناً: شرح آلية عمل برنامج مضاد الفيروس و إعداد خوارزمية تقوم بفحص الملفات بشكل عام ثم تقوم بفحص الفيروس من الملف المصاب.

تاسعاً: التطبيق.

عاشراً: تحليل النتائج، الخلاصة و المقترحات.

نرجو أن يكون بحثنا هذا نبتة صغيرة تسعى نحو النمو في عصر الحاسوب و المعلوماتية و أرجو أن يكون حجر أساس لمواضيع جديدة تفيد هذا البحث و تقوم بتصميم برنامج مضاد للفيروسات بأيدي عربية و يستخدمه جميع مستخدمي الحاسوب و ذو وثوقية عالية و يكون لنا الفخر أن نقدم هذا البرنامج للناس جميعاً.

Computer virus subject is considered one of the most import subjects for the user's computer , due to the fast spread to use computer and nets and their interface in very life fields , because of that we in this research studied virus of computer by identify virus and its work machinery also the kinds of virus a general study for files virus , putting a table to design a virus joining the files in its both kinds Com and Exe , after that putting a tabulate to correct the damaged files with this virus .

We evaluated the possibility of hiring this table in correcting damage files with virus process , we depend in evaluating on how much would be the useful of this table , through its possibility correcting both files Com and Exe together.

The results were , that the previous tabulate can correct the executive files together and return the files to its previous position , before get damage by discovering the virus code .

So , we hope that our results could be a begging toward developing this table and to find tabulates have better and faster performance and can discover much more kinds of virus in a form that suits the development which virus

are going through and with their various form and different aims.

Introduction :

Beginning of virus :

Virus began to appear in 1978 or just before this date , where the true beginning is difficult to be limited exactly. Then it began to be a complicated problem recently especially with the spreading communications methods , using e-mail causes spreading virus very much , were by e-mail we can send messages to thousands of users

Who participate in computer system . as a result ; fast spreading for virus , that's to say , communications methods , which made great progress in the final era , became a mean from means of transforming virus to very far distance .

From here the problem showed up , companies established programs checking files and alerting for the existence of virus and fixing damage files.

In this research we'll :

1: Perform a research about virus through identifying it and the reasons of writing virus.

2: Explain the kinds of virus : Dos virus.

3: Explain the kinds of virus : Windows virus.

4: Macro virus and practical programs.

5: Network virus and Email virus.

6: Security opening for operation system and practical programs.

7: A research a bout virus working generally , also its work machinery , then prepare a special tabulate to a program which did the establish virus file .

8: Explain the work machinery of an anti- virus program , prepare a table checking files generally , then checking virus from the damage files .

9: Application.

10: Analysis results, Summary and suggestions.

We hope that our research is a small plant seeking for growing up in computer and informatics age , and hope to be a basic store for new subjects , make use this research and design an anti-virus program in Arabic hands , and hiring it by every user's computer.

Who have high trust . We'll be proud to produce this program to all people.