الخـــــلاصـة

إن فيروسات الحاسبة تزيد من خطورة سلامة البيانات. إنها تسبب فقدان البيانات المهمة وتكلف مبالغ ضخمة وضياع الجهود المبذولة عند إعادة البيانات المدمرة أو المفقودة الى الوضع السابق. ولزيادة مشكلة الفيروسات، جائت الحاجة إلي أدوات لاكتشافها و استئصالها من النظام.

لأجل حماية نظام الحاسبة من إصابتها بالفيروسات يضع اكثر المستخدمين برمجيات ضد الفيروس كوقاية الحاسبة منها وكمانع بينهما. لكن هذه البرمجيات تكشف فقط الفيروسات المعروفة والتي تحفظ بصمتها في قواعد البيانات الخاصة بها ولا تفعل أي شيء ازاء للفيروسات الغير معروفة بالنسبة لها والتي تشكل مشكلة حقيقية.

افترضنا في هذا البحث طريقة لاكتشاف الفيروسات الغير معروفة التي تحدث في البريد الإلكتروني(Email) لان اكثر الفيروسات الحديثة تنتقل خلال البريد الإلكتروني. سوف نحاول معالجة التهديدات بتصميم طريقة اكتشاف جديدة تستخدم لإيقاف انتشار الفيروسات في البريد الإلكتروني. النظام سمي بـ" نظام حماية البريد الإلكتروني" (EPS) يختبر الرسالة البريدية المنتقلة خلال محيط الحاسبات الشخصية نوع (PC) والتي تعمل على برمجيات النافذة (Windows) وباستخدام تطبيق (Outlook Express).

النظام المفترض يتألف من مرحلتين: الاكتشاف و الإصلاح. أول مرحلة الاكتشاف، يعتمد الاكتشاف بواسطة مراقبة السلوك والذي هو اكتشاف الجمل الخبيثة والتي تسبب فيروس.

يقوم النظام بفتح الملفات الملحقة بالرسالة (attachment file) بشكلين مختلفين: على شكل ثنائي (binary form) وشكل نص (text form). ويقوم أولا بفك الجفرة ومن ثم يحولها إما إلى ثنائي أو إلى نص عادي.

نقوم في هذا البحث بفحص محتوى الرسالة (body of the message) والملفات الملحقة بها. نبحث في محتوى الرسالة عن الإيعازات المؤذية المكتوبة بلغة (DOS) . ويتم فحص الملحقات من أنواع مختلفة من الجمل المؤذية. أولا، فحص ايعازات الماكرو (Macro) التي توجد في ملفات ألـ (Word). الفحص الثاني هو فحص عملية القفز (jump operation) في بداية الملف إذا كان الملف الملحق من نوع (COM). الفحص الثالث هو فحص الملفات

PDF created with pdfFactory trial version www.pdffactory.com

من نوع (EXE) من وجود حالتين فيها، الأول تغيير نقطة الدخول (entry point) والثاني هو نقل المنطقة المخصصة للمعلومات في الملف (DTA). أما الفحص الرابع والأخير فهو عبارة عن نوعين من الفحص. الأولى فحص الإيعازات المؤذية المكتوبة بلغة ألـ(DOS) والثانية فحص الإيعازات المكتوبة بلغة الآلة.

المرحلة الثانية من النظام هو مرحلة الإصلاح. نقوم باقتراح ثلاثة اختيارات لحل المشكلة وإزالة الفيروسات من الرسالة قبل انتشارها.

PDF created with pdfFactory trial version www.pdffactory.com

ABSTRACT

Computer viruses pose an increasing risk to computer data integrity. They cause loss of valuable data and cost an enormous amount in wasted effort in restoration/duplication of lost and damaged data. As the problem of viruses increases, we need tools to detect them and to eradicate them from our systems.

In order to protect a computer system from being infected by a computer virus, many individuals install anti-virus software assuming a shield of immunity has been put between them. But this software detects only known viruses that have a signature for it in the its database. They do nothing about unknown viruses the real problem.

In this research we proposed a method for detecting unknown viruses in electronic mail (email) because many viruses spread via email. We will attempt to process threats by designing a new detection method used to stop spreading of email viruses. The system which is called EPS (Email Protect System) checks the email message that is transmitted through PC's environment that runs windows software and uses outlook express application.

The proposed system consists of two stages: detection, and repairing. The first stage detection, depends on detection by behavior to detect the malicious statements that could cause a virus.

The EPS opens an attachment files in two different forms, binary form and text form. It first decodes the attachment file and then converts it either into binary or into text.

PDF created with pdfFactory trial version www.pdffactory.com

In this thesis the body of the message as well as the attachments is checked. It searches the body from malicious command written in DOS commands. The attachment checking is done in more than one type of malicious statement. The first is checking Macro command that is in Word document file attached to email. Second, is checking jump operation in the beginning of file if the attached file is COM file. The third is checking for changing an entry point or transferring of DTA (Disk Transfer Area), if the file is EXE file. The last check is done for all executable files. This checking consists of two checkings. The first one is checking the malicious code written in DOS commands, and the second is checking the binary form of file from malicious code written in machine code.

The second stage of the EPS is repairing stage. It suggests three options for solving the problem. It removes the virus code from the message before the virus spreads through environment.

PDF created with pdfFactory trial version www.pdffactory.com