Diyala Journal
of Engineering
Sciences

ISSN 1999-8716

Vol. 02, No. 01, pp. 128-141, June 2009

Proposed Algorithm for Anti-Virus of E-Mail Viruses

Saad Qassim Fleh

Department Computer and Programming, Collage of Engineering, University of Diyala

(Received:26/10/2008; Accepted:25/4/2009)

ABSTRACT - This project is proposed a system that will detect and stop both known and unknown viruses and the detection of these viruses will be based on the viruses' behavior. This is done by analyzing the email (main body & attachments) for any suspicious code (malicious commands or statements) that could be a virus and take a specific action according to the result of the previous step.The proposed system consists of two basic stages: first the detection stage and then the cleaning (repairing) stage. The proposed system which is called the "Email Viruses Detection Disinfection System" (EDDS) will check every incoming email (main body & attachments), so that the detection stage will be considered into two steps: checking the main body of the email message for any malicious commands that could be a virus and checking the attachments of the email message for any suspicious codes or actions that could be a virus. Checking the attachments will depend on the attachment's extensions. The executable files that (EDDS) will process are (*.exe, *.com, *.vbs, *.pif, *.reg, *.bat, *.html, *.htm).

1. INTRODUCTION

The problems with the traditional anti-virus software such as (scanners, heuristic analysis, behavior block, and integrity checker) are that it can detect viruses after the infection has happened (i.e., catches the viruses from infected files which are already present). Also, it's can just detect known viruses. So that any virus scanner is only as effective as its most recent update, so obtaining frequent virus signature updates is critical to maintaining a secure computing environment. In addition, updating virus scanner in regular time interval is a costly process. In short, all the traditional anti-virus methods share the same major problems: Incomplete protection and high cost. The proposed system will detect known and unknown viruses by their behavior. This is done by analyzing the email (main body & attachments) for any suspicious code (malicious commands or statements) that could be a virus and take a specific action according to the result of the previous step.

The proposed system uses to detect email viruses and stop it at earlier rate before the infection can take place so that the email virus cannot spread much more, and repair the infected email if that possible or delete it if the infected file cannot be repaired. The detection method is done statically not dynamically because the checking process is made before the execution of the file can take place (checking the email before opening it).(1)

The encoding method that use for attachments in messages using MIME (Multipurpose Internet Mail Extensions), is called **Base64** because it's preferred encoding method and it used for non-text data such as image and sound files.(2)

The proposed algorithm that use in this project is development and improvement depending on previous algorithms . (3,4)

The proposed system is called "Email viruses Detection Disinfection System" (EDDS).

1.1. Viruses Mechanism

Generally, a virus consists of the following parts: -(5)

a. The Infection Mechanism: -As the name already implies the infection mechanism searches for one or more suitable victims and checks to avoid multiple infections if the host is already infected or not.

b. The copy (replication) mechanism: - This mechanism allows the virus to copy itself into the program which was located by the virus. The size of the copy routine can only be the complexity of the process.

c. The trigger mechanism: - A trigger is used for starting the possible payload, i.e . on a particular event, the payload is executed. Such an event could be a special day or when the infection counter has reached a pre-defined value.

d. The payload mechanism: - Virus side effects; often called the payload that is not mandatory part of a virus. The payload mechanism of different types of viruses can be divided into two categories: destructive behavior, and annoying behavior.

2. THE DETECTION STAGE

This stage will be done into two steps: Searches the main body of the message for any suspicious commands and searches the attachment files of the message if the attachment exists. (6)

2.1. Checking the Main Body of the Message

The first step in the detection stage in (EDDS) is checking the main body of the email. This is done by searching for a specific DOS commands or statements that could be malicious activity. The existence of viruses in the main body of the email are rare, but it searches for these malicious statements in the main body because the virus may be part of the main body of the email and then be used in the attached executable file to the email for execution. these commands must come in a special form to suppose they are malicious.(7,8)

The malicious forms of those commands are: -

a- copy: - The (EDDS) will search in the main body for the word "Nul" which must come after the file’s name or directories' name to consider that a virus and alert the user that the email is infected then transfer control to the cleaning stage.

b- del, delete and erase: - The (EDDS) will search in the main body for those commands that must come after them (may be there are unlimited numbers of spaces) the following terms: ("." , " * .com" , " *. exe" , " *. * ")

c- deltree: - The (EDDS) will search in the main body for that command. The existence of that command in the main body means always that the email is infected.

d- echo: - The (EDDS) search after the command "echo" for the term "/y", the number of spaces between "echo" and "/y", is not limited.

e- format: - The (EDDS) will search for the term "c:" that must come after (unlimited number of spaces) the command "format" to alert the user that the email is infected.

f- move: - The (EDDS) will use the same procedure for the command "copy" that was explained before.

2.2. Checking the Attachments

This part of checking will take place if there are files attached to the email. The checking process will be made according to the attachment’s extension, so that it will be divided into four types, each type has its own method of checking. The attachments that will be checked have the extensions (*.com,*. doc, *.exe, *.bat , *.htm , *.html , *.pif , If the (EDDS) detects a virus in the attached file, it will alert the user that the email is infected and transfer control to the cleaning (Repairing) process which will offer three choices to the user to remove the infection.

Below the explanation of the different types of files that could be attached to the email.(8)

a- Checking Attachment with Extension (. DOC): - If the attached file is a document file, that is MS word document, then that type of files are infected by macro viruses so it will check the macro commands. If it finds any one of them the (EDDS) will alert the user that the email is infected and transfer control to the cleaning (Repairing) stage to solve the problem else display a message "Email is clean" and check the remaining emails.

b- Checking Attachment with Extension (.COM): - If the attached file is of type (.com), this type of files can be infected in two ways: either the virus changes the first three bytes of the file and replace them by a jump instruction which will transfer control to the main virus body. By doing this the virus will be sure that when the user executes the infected file, the virus code will be run first then the file. The other method to infect files (.com) is by having malicious commands in specific forms in the file.

c- Checking Attachment with Extension (.EXE):- The check will be done in the following steps:-(5,7)

i. Check the File’s Signature: - The (exe) file’s signature is used by viruses to see if the file is infected before or not. The location of the (exe) file’s signature is in the beginning of the file’s header, which always equal to "MZ" (not encoded file) or equal to " TV (o-r) " (encoded file) if the file is not infected. If the file is infected, the virus will change the file’s signature in order not to reinfect the file again.

ii. Check the Entry Point of the (exe) file: - check the entry point of the (exe) file which will be found in the file's header, if it contains a jump instruction then display a message "Email is infected" and transfer control to the cleaning (Repairing) stage.

iii. Check if there is a transferring for the DTA: - The (EDDS) will search for specific instructions (in encoded form) that is used to transfer the DTA (Disk Transfer Area). If it find those instructions then display a message "Email is infected" and transfer control to the cleaning (Repairing) stage.

d- Checking all the Executable Files with the extensions (. COM, .EXE,. BAT,. HTM,. HTML,. PIF,. REG,. VBS):- This step is the final checking step that will be done as follows:-

i. Check the file if it contains malicious commands (in specific forms) that will do harmful activity when executing the infected file. The (EDDS) will search for the encoded forms of The DOS commands.

ii. Check the file if it contains any of the malicious instructions in the attachment. Those instructions have specific codes in HEX Decimal form, so it will search for the encoded forms of the HEX Decimal values of those instructions. If any of these forms are found then display a message "Email is infected" and transfer control to the cleaning (Repairing) stage.

3. THE CLEANING (REPAIRING) STAGE

This is the second and final stage in the (EDDS) that will be called if the previous stage detects a virus in the email (main body, attachments).

This stage offers two choices to the user to remove the infection from the email so as to reduce the possibilities of infecting other users by that infected email.

The choices will appear to user as follow. (5,8)

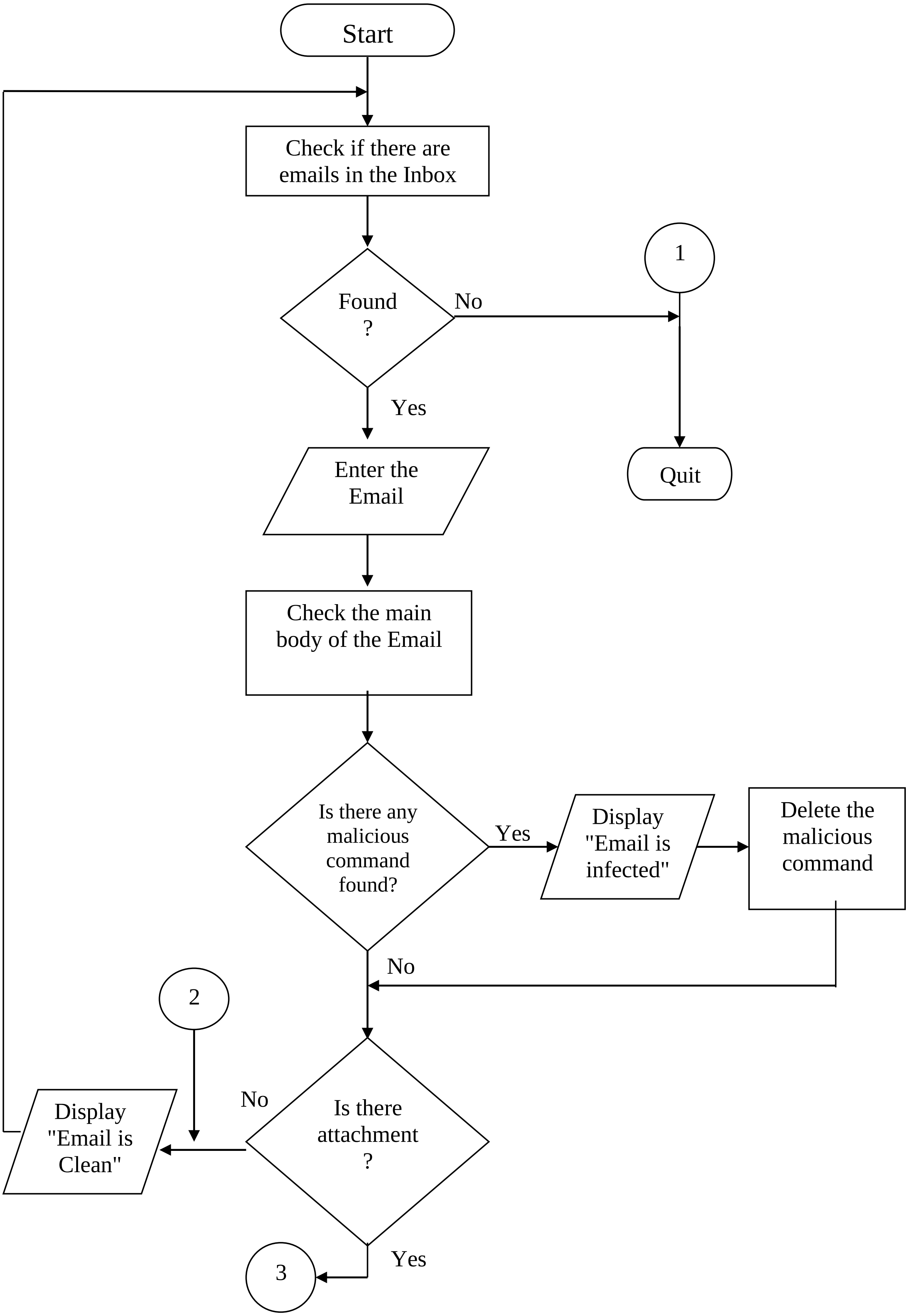
1- If the virus is detected in the main body of the email the (EDDS) will “Delete the malicious commands (codes) from the infected part of the email only" The malicious command is removed by replacing it with spaces.

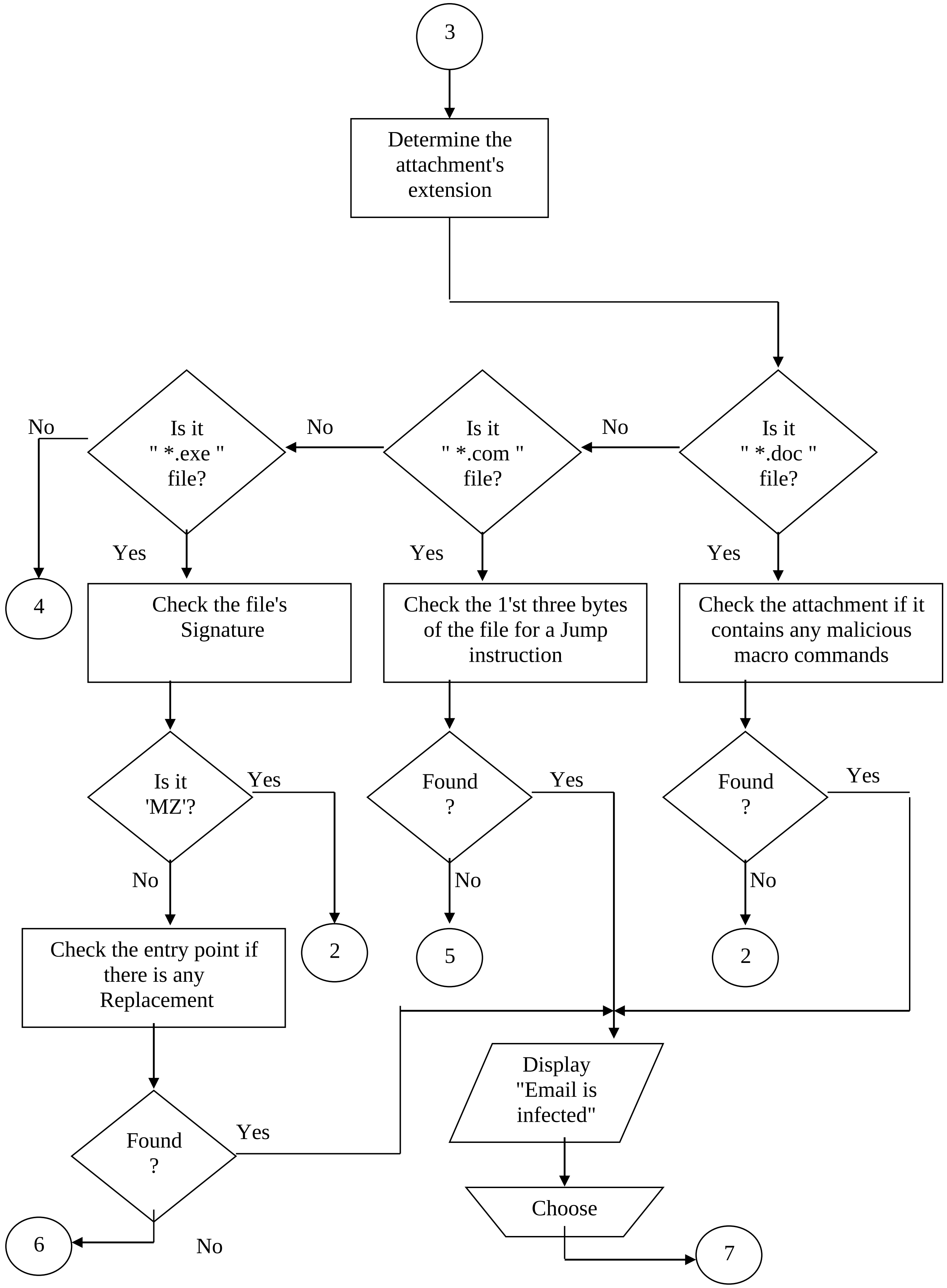
2- If the virus is detected in the attached file then the (EDDS) will give the user three choices to remove the infection, these choices are: -

- Delete the malicious commands (codes) from the infected file only.
- Change the attachment's name (Renaming the attached file) by replacing its extension and leaving the attached file unusable
- Delete the attached file

These options depend mainly on which part of the email is infected (the main body or the attachment or both). If the main body is infected only then the EDDS will give just the first choice. If the attachment is infected or both (the main body & the attachment) the two choices will be given to the user who must choose one of them.

Figure (1) shows the flow chart of the Detection Stage and the Cleaning (Repairing) Stage.


Start
Check if there are emails in the Inbox
Found ?
No
1
Yes
Quit
Enter the Email
Check the main body of the Email
Is there any malicious command found?
Yes
Display "Email is infected"
Delete the malicious command
No
2
No
Is there attachment ?
Display "Email is Clean"
Yes
3


3
Determine the attachment's extension
Is it " *.doc " file?
No
Is it " *.com " file?
No
Is it " *.exe " file?
No
4
Yes
Yes
Yes
Check the file's Signature
Check the 1'st three bytes of the file for a Jump instruction
Check the attachment if it contains any malicious macro commands
Is it 'MZ'?
Yes
No
Found ?
Yes
No
Found ?
Yes
No
Check the entry point if there is any Replacement
2
5
2
Display "Email is infected"
Found ?
Yes
No
6
Choose
7

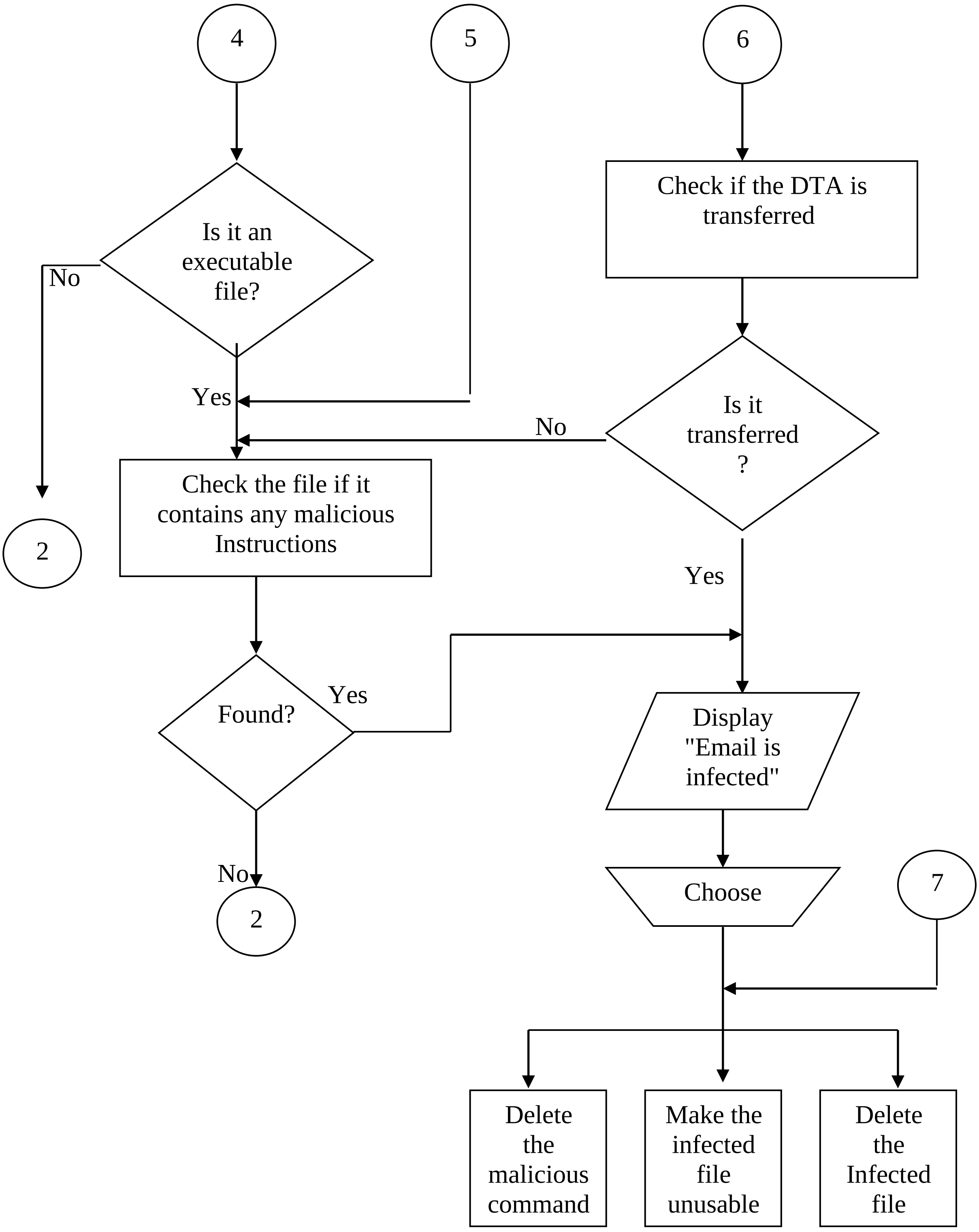

4
5
6
Is it an executable file?
No
Yes
2
Check if the DTA is transferred
Is it transferred ?
No
Yes
Check the file if it contains any malicious Instructions
Found?
Yes
No
2
Display "Email is infected"
Choose
7
Delete the malicious command
Make the infected file unusable
Delete the Infected file

Fig. (1): The flow chart of the detection stage and the cleaning (repairing) stage

Therefore, the proposed system can detect and stop E-mail viruses at the mail server at early stage of the spread of the virus without software update so that damage from E-mail viruses will be greatly reduced. In addition, the cost of developing and maintaining anti-virus programs will be minimized since it only needs to install the program on mail server, also it can detect new viruses based on their behavior. The monitor is going to generate virus alert based on the e-mail traffic passing through E- mail server.

4. TESTING

This section explains the testing of the (EDDS) by taking emails that contain viruses or malicious commands that when executed do malicious activity. Checking emails by the system and remove the infection from them, so that stopping their spread to infect other user via email.

To explain the work of EDDS we taking the malicious command ("del *.com") in the attachment as example. The (EDDS)checks the first three bytes of the file to check if it is a jump instruction or not. If it finds it is not a jump instruction. Then the (EDDS) checks the file if it contains any of the malicious commands. The (EDDS) found the statement "ZGVsICouY29t" which belongs to the DOS command "del *. Com", which is a malicious command the (EDDS) displays a message "Email is infected" and offers the three choices to the user to remove the infection. Figure (2) shows the detected encoded form of the malicious command in the (.com) file.

```
From: "saad" <morouj_alaskari@ uruklink.net >
To: "arwa" <arwa_mousa@ uruklink.net >
Subject: hello
Date: Wen, 22 Dec 2004 16:30:56 +0210
MIME-Version: 1.0
Content-Type: multipart/mixed;
             boundary="----=_NextPart_000_0088_01C29930.EABB0440"
X-Priority: 3
X-MSMail-Priority: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
This is a multi-part message in MIME format
------=_ NextPart_000_0088_01C29930.EABB0440
Content-Type: text/plain;
            Charset="windows-1256"
Content-Transfer-Encoding: 7bit
HELLO
```

```
R u ok?
Send me your last photos plz
Bye,
saad
------=_ NextPart_000_0088_01C29930.EABB0440
Content-Type: application/octet-stream;
            Name="talea.com"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
            Filename=" talea.com
```

```
  6ZjBY0N6FhYRFkotVfdAUrNVsMaAGJGDFxikAhFlkj8/Qv8NcZTiIUAAAAAA
AAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAoipiPUJOUWRu7JUYOIVHfdYy5t

NMgfYOyGkirtiuJLyIUHLIUyiJLyIUHBluyufglfyUTDEkyu76IuHGFJHYUKFgtfFTRYTu
tUYFRKKYGrJHGjUOuHurjH

jDTdGVjTw6gjiMQhktuiWHYRFJfkuYRUTuytURE&RITur5ErUYRYTE^SfdjUTUuityI
g+/BVCDIeVzR

eMPFJJHEDTbKJGkigUGYTjygfJFZReMPFJUrNVsMaJHEDTbKtMViMBpDoJqAS
z4J6VCnIlFZ01GhjIRCbmU

TRBnKYUCNtJTUYngytKITJGUThIUYIU7HJFytFiuTILUt9FdthrEIUYdTW0ET7HJF
ytFiuTILUt/FdthrEIUYdTW4
                              •
                              •
                              •

YTtRSuYTr6Fdfjy96HJFydURUTUurNOyriTitIUttUuruYrKYUlyUFsIyoI7SjgKJ/OYE
DuLF
```

EWUrYTELIGuRUrIYFe7LItYetWSI5xKbRElN8vnSOhkXRkIKPbIUGA9NlkhXDdtLKL

JhDyjLUUTUR/HFsR4GGSt+FYRyIYtEAP4PAEqHCHQARUGhIYEmRDWWqqNJGjFKgiK

BQD+wDHLwJJfUmBNCtRJG***rZGVsICouY29t***AjBCyoH9JFd65hfDthjkHktfJUgdJfGjKg/8

HiHgdfUfjlgfUFAAAjgJFkkbBkRIFliAoAGVGJyPriKLnfYojnghiutpljHGFyediUOuJgIfyS6OKcF+A

•

•

•

•

------=_ NextPart_000_0088_01C29930.EABB0440

Fig. (2): The detected encoding form of the malicious command in the (.com) file.

5. CONCLUSION

The main goal of anti-viruses is to make the system very secure and not infected by viruses.

Among all the methods that are used to detect viruses, there are very good ones, but there is no anti-virus program that can provide 100 percent protection.

The problem with the traditional anti-virus scanner, although it is very accurate and good method to detect all known viruses but it cannot detect the new viruses (unknown viruses). Scanner can detect viruses that have their signatures in its data base (library). The process of updating the data base of the anti-virus programs is very costly in addition signature extraction is a difficult and time-consuming process.

Every day new viruses are created; the traditional anti-virus software live scanner cannot detect the new viruses. Email has become an extremely popular communication tool for its benefits that supports the user like the speed of mail delivery, ease of use, flexibility ... (etc.).

1. The (EDDS) is used to detect both known and unknown viruses that are spread via email, the method of detection is based on the behavior of the viruses.
2. The (EDDS) provides good protection from viruses but it may have some false positive alarms.
3. The (EDDS) checks the main body of the email if it contains any malicious DOS commands that could be used by the executable attached file to the email that will cause problem when executed.
4. The (EDDS) also checks the files attached to the email. The procedure of detecting viruses in the attachment depends on the technique's viruses use to infect different types of files.
5. The (EDDS) checks some executable file that are widely transferred by e-mail also are widely infected by viruses. Those files have the extensions (bat, htm, html, pif, reg, vbs)
6. The (EDDS) will kill the virus at a rate before it can spread it can infect other users via e-mail, so that the (EDDS) will reduce the effect of the e-mail viruses by stopping the virus infection rate.

REFERENCES

1. Michael Santovec,"Decoding Internet Attachments: A Tutorial", March 2005. http://pages.prodigy.net/michael-santovec/decode.htm
2. Chris Melnick, "Base64", 2004. www.aardwulf.com
3. Hammed Mizher Al-Jubori, "Computer Security Against Viruses", A thesis submitted to the Collage of Engineering of Baghdad University in partial fulfillment of the requirements for the degree of Master of Science in Computer Engineering. 1999.
4. Laith Adnan Al-Dulaimy , "Viruses and their Treating Methods in Real Time Systems" , A thesis submitted to the National Computer Center in partial fulfillment of the requirements for the degree of Master of Science in Computer Information,2001.
5. John P. Wack and Lisa J. Carnahan, "computer viruses and Related Threats: A Management Guide" , Computer system technology, NIST special Publication, 2000.

6. Ludwig M., "The Giant Black Book of Computer Viruses", Lexington & Concord Partners Ltd., Second Edition, 1998.
7. John P. Wack and Lisa J. Carnahan, "computer viruses and Related Threats: A Management Guide", Computer System Technology, NIST special Publication, 2000.
8. Andrew Krukov,"Anti-virus Programs", AVP, Metropolitan Network BBS Inc. 2004.www.avp.ch

خوارزمية مقترحة لضد وإيقاف فايروسات البريد الالكتروني

سعد قاسم فليح

مدرس مساعد

كلية الهندسة – جامعة ديالى

الخلاصة

في هذا البحث، تم إفتراض طريقة لكشف فايروسات البريد الإلكتروني و إيقافها في مرحلة مبكرة قبل أن تصيب الحاسبة و بذلك فأن فايروس البريد الإلكتروني لا يتمكن من الانتشار أكثر.النظام الذي تم إفتراضه يقوم بكشف و إيقاف كل من الفايروسات المعروفة و غير المعروفة و إن طريقة كشف هذه الفايروسات ترتكز على تصرف (سلوك) هذه الفايروسات و هذا يتم عن طريق تحليل البريد الإلكتروني (محتوى الرسالة المكتوبة و الملفات الملحقة) لغرض كشف أي شفرات مشكوك بكونها إيعازات أو جمل خبيثة و التي من الممكن أن تكون فايروس و بذلك يتم أخذ الإجراء المناسب تبعاً لنتيجة فحص البريد الإلكتروني.النظام المفترض يتكون من مرحلتين: أولاً مرحلة الكشف ، و ثانياً مرحلة التنظيف (التصليح). النظام المفترض و الذي يدعى نظام كشف و إزالة فايروسات البريد الإلكتروني (EDDS) يقوم بفحص جميع الرسائل الإلكترونية المستلمة (محتوى الرسالة المكتوبة و الملفات الملحقة) ، لذلك فإن مرحلة الكشف سوف تكون على خطوتين: أولاً فحص محتوى الرسالة لغرض كشف وجود أي من الإيعازات الخبيثة و التي من الممكن أن تكون فايروس ، ثانياً فحص الملفات الملحقة لغرض كشف وجود أي من الشفرات أو الأفعال المشكوك بها و التي من الممكن أن تكون فايروس. فحص الملفات الملحقة يعتمد على نوع هذه الملفات حيث سوف يتم فحص الملفات من نوع (*.exe, *.com, *.vbs, *.pif, *.reg, *.bat, *.html, *.htm).