

The Function Mechanism for a Selected Group of Macro Viruses

Hassan M. Wahahat, TakiAlddin Alsmadi and Yasir Khalil Ibrahim

Computer Science Department, Jerash Private University, Jordan

Summary

The current study aimed to investigate the mechanism of a selected punch of Macro Viruses spread in the field of Personal Computers with a concentration on virus called "Concept" in order to determine the needed methods to diagnosis the infection by such kind of virus and selecting procedural steps to prevent its damaging effects on software and its files.

Inspections on the structure of this kind of virus reveled a physical development in the algorithm used to prepare it that requires a certain degree in the process of discovering it then preventing its damaging effects. The current study resulted in clarifying the most important aspects associating to the existence of an active macro virus in the personal Computer with suggesting some changes on the routines used in software macro applications to prevent the infection of personal files or executing it to the limit.

Key words:

Viruses, macro, algorithm, programming style.

1. Introduction

Computer Occupy a great position in our daily life as it has a permanent position in all fields of human knowledge due to its high potentials in processing and analyzing Data, however, working in the rich computer environment has its own risks and consequences; one of the most dangerous consequences is computer's infection with a virus.

Word Processing, Spread Sheets, and Macro were introduced and provided users with ability to make many application tasks in those kinds easily. These technical characters were found to enable the user from writing the Document Auto processing System that considered being a wide field for many applications as well as a rich field for virus makers to sneak through it to make harmful damages in the files of the programming system.

Macro Virus is not more than a special copy made by Virus makers to fulfill a series of programming tasks inside the programming environment of Word Processing, and Spread Sheets as it generates a copy infecting documents or Work Books after being attached with the file Normal Dot known as Word's Global Template File through, using the orders of the macro that been loaded automatically when the user opens the Document.

The current study aimed to investigate the mechanism of this kind of virus that spread widely recently in order to prevent its damaging effect on software used by national and information Sectors.

2. Traditional Macro: Structure and Mechanism

MS-Office had enabled the user to make applications in order to fulfill a series of frequent activities inside the system by registering it a punch of key strokes or writing it through the Macro language that based on environments like visual Basic, visual C, and Word basic. There are many orders and algorithm for the macro enabling the user to produce his Macro. Refer to Table (1)

Table.1: Kinds of Macro

Macro	Activation Phase
Auto	When initiating word or loading a
Auto	New file
Auto	Opening A file or using " find file"
Auto	Closing File
Auto	Executing A file

Macro sartworking when receiving certain orders as the existence of File AveAs gives the ser the ability to save a new file under a fixed name. Thus, stroking keysd Alt+F+A will activate the macro routine in he

comprehensive template, that traditionally consists of the following:

```
Sub main
Dim dIgh File save As
GetCurValue DIg
Dialog dlg
End Sub
```

Generally, all kinds of macro routines start to intimate Sub Main and other intimations can be added in order to change the nature of tasks it perform if we added the following line Sub Main the message we want appears (For example)

```
Sub Main
Msg Box " Take Care You Will Save Files"
Dim dIgh FileSaveAs
FileSaveAs DIG
End Sub
```

This slight change will appear when the message " Take Care You Will Save Files" when initiating the macro File Save As if we are in need to save a file, this goes for all macro subs entered. However, if we started to modify on the automatic Macro we will grant its work automatically without the need of using keys on the Key board.

3. Structure of Macro Virus

Macro Viruses are specialized ones capable of self-replicate inside files and documents or spread sheets in order to achieve the aims they are produced for and making sure that it will spread widely. These viruses can enter to the circle of Word Processing, and spread sheet by linking its routines with the execution of the Document (Ole Object) and directly replacing the commands of the Traditional macro with new ones to pave the way in front of its damaging effects,

Commands of Micro Virus are written in order to infect some or all Auto Commands provided by logos such as Word Basic or Visual Basic in order to invest the character of automatic execution done by those commands when opening or making files which may leads that the file will be infected without any attention from the user.

When opening an infected file it starts to copy its routines pasting it with Ms-word Normal Dot that effect all created, opened and new files through this template.

Virus moves with the infected document through the media of data storage, or e-mail or when moving the files form one computer to another on the net, and starts its damaging effects when users deal with the Document using the macro that can infect MS-word, Ms-Excel, Ms-power point, however the ability of infection is differ from one program to another (Refer to Table2). This virus has no ability to control the sources of the system as its depend son word Basic that is classified as High level language with occupying a huge space in the memory while being activated which makes the system rather slow in computers that haven't enough memory

Table 2: Programming System possibility of infection by Macro Virus

Infection Possibility	Programing System
>75%	MS-Word
60-75%	MS-Excel
<30%	MS-Power Point
<20%	MS-Access

The effects differ between issuing a message to the user from the virus maker or making suspected activities may cause a partial or total damage to the document, on the other hand, its effect may increase to affect the programming environment totally.

The routine used copy the macro virus to the automatic commands does not need deep experience in programming languages, as employing the following routine paves the way to copy the command Auto close in the comprehensive template carrying whatever side effects it wants aimed by the maker.

```
Sub Main
Macro Copy WindowName$0+":Auto close",1
End Sub
```

Putting number one at the end of the command makes the macro Execute only, which prevent modifying the content of the Virus by others.

Table 3: Presents the symptoms related to macro virus infection

Side Effects	Degree of infection Possibility
Warning message appears when any related document-macro activity happens	40-50%
Inability to save the Document as a template	80-90%
The feature of the Icon change to a template instead of a file	30-40%
A dialog box appears containing number(1) when opening the infected file	15-30%
More than one macro names appear in the macro list available in the system	40-50%
Un expected messages appear when opening the Document or the template or doing any activity	60-70%

3.1 Analyzing Concept Virus

This virus is considered one of the most famous and widespread viruses all around the world; moreover it has many names in the circle of anti-Virus programs. Its names are Concept, Pranko, **WM-Concept, WW6, Word Macro, and WinWord Concept.**

The first version of this virus was prepared by using Word Basic related to Ms-Word and it has the ability to spread in more than one programming environment such as: Windows 3x, windows 95/98, and windows-NT.

Analyzing the structure of this virus through infected files shows that it has three kinds of macro the first and the second are related to the procedural functions of the system, while the Third occupying a position in the programming environment. The First and the second macro are copied within two phases of infection and the number of active macros becomes (5) as follows:

The First Macro: Auto open

Opposite Macro: AAAZAO

The Second Macro: FildeSaveAs

Opposite Macro: AAAZFS

Third Macro: Pay Load

It is clear as seen above that macro copies one and two are starting with letters AAAZ that counterpart the transformation of the functional action while Ao stands for Auto open and Fs = file Save As. Following the routine used in Concept Virus as we took it from an infected file.

Sub Main

On Error Goto Abort

iMacroCount=Count Macros(0.0)

Fori=1 to iMacroCount

If MacroName\$(i.0)="Pay load"then

bInstalled=1

End If

If MacroNames\$(I,0,0)= "File Save As"then

B too Much trouble=-1

End If

NextI

iWW6Instancw=Val(Get

document Var\$("WW6infecto")

sMe\$-FileName\$0

sMacro\$=sMe\$+":Payload"

```

Macrocopy sMacro$,"Global:Payload"
sMacro$=sMe$+AAAZFs
sMacro$=sMe$+":AAAZAO"
Macro Copy sMacro$" Global:AAAZAO
Set Profilestring " WW6I",Str$(iWW6IInstance+1)
Msg box str$(iWW6IInstance+1)
End if
Abort:
End Sub
Sub Main
Dim dIg As File save As
On Error Goto bail
GetCur Values dIg
Dialo dIg
If dIg.format=0 Then dIG.format=1
sMe$-FileName$0
sTmacros4=sMe$+":Auto open"
sTmacros$+":AAAZAO
s1Nacro$=sme$+AAAZFS"
Macro Copy " Global:AAASFS">STmacro$
sT macro$=sMe$+": Payload"
Macrocopy" Global:Payload",sTmacro$
File save AsDIG
Goto done
Bail:
If Err<>102Then
File Save As Dig
End if
Done:
End Sub
Payload
Sub main
REF That's Enough to prove my Point
(This is the message of the Virus)
End Sub

```

The mechanism of its work consists of two essential phases:

Phase one: Primary infection of the system

When opening an infected file with Concept is starts to check Normal Dot template in MS-Word to make sure that macros of File Save As and Pay load are existed if they are so the self replicate process stopped, if they aren't existed or one of them the copy process starts and this dialogue box appear on the screen (dialogue box contains number 1 with the button OK).

This box is planned to work as a scale to count times of infection but the programming structure of the virus maker suffered form many mistakes and didn't do this task leaving number (1) attached to it so this box appears one time at the time of the first infection, this malfunction is caused by macro modification to the variable WW6 infector and storing it by mistake on a new name WW6I losing its aim.

The virus starts copying the four macros mentioned in Table(4) to the virtual template (Comprehensive template) increasing the value of the scale (Zero) by (1) and this value is saved on INI of NS-word but the defect of the virus doesn't occur when activating WW6Infector so the value remains Zero and saved the value of the variable WW6I equal to (1) without any change.

Table 4: cases of Concept Macro Virus

Infected Template	Infected File
AAAZAO	AAAZAO
AAAZFS	AAAZFS
File Save As	Auto Open
Pay load	Pay load

Second Phase: Spread Phase

This virus spread when starting the process of storing a file with one of the two commands, File Save As or File Save with the Macro copied in the comprehensive template, in its two copies AAZFS and File Save As when executing the command Auto open adding its functions to the dialogue Box of File save As, so functions are transformed in the light of the four added macros, and the file becomes a tool of the concept virus as Auto open doesn't effect open files unless they are not infected.

We would like to mention here that this virus has no damaging effect on files or system as macro Payload has no code except the comment (That is enough to prove My Point).

The most common and easy ways to discover this Virus lies in using the available anti-virus programs in the field (Update). The most common symptoms related to the infection of this virus is a message box generated when activating the infected file and we can use the tools of macro available in the program so the five active macros emerge.

4. Ways used to prevent the activity of Macro Virus

Making the macro virus in the environment of word Visual Basic makes the process of discovering it needs a great deal of accuracy and the effort of preventing it from infecting our files must be personal far from anti-virus Programs especially to those who are working in information Sector who face new infections with no anti-virus at that moment to deal with it and that of course threats their systems and files.

Generally, MS-Office offers warning tools to alert the user when a macro activity occurs related to any of its files without distinguishing between what is legal and what is suspected, in turn Ms-Word contains tools to discover Concept and processing it only so these tools don't provide a comprehensive protection to the user in front of other macro viruses

5. Conclusions

The fundamental Core of facing virus infection – whatever its kind was- lies in adopting a procedural protective way to limit its effect in the infected file and treating it as soon as possible. Generally those procedures depend to one of these steps or a punch of them according to the nature of the infection and the mechanism of the virus,. Those:

1. Pressing shift when opening the suspected file in order to make sure that Auto open that holds the virus is not activated. In turn, we press the same key to close the file in order not to activate Auto Close.

2. when make sure of the infection or there is a great possibility for this to happen we can follow the following procedures:

- (a) After opening the file all Macro kinds can be chosen inside the file then copying the content of the file and pasting it in another file and storing it in another name.
- (b) . After opening the file all Macro kinds can be chosen inside the file then copying the content of the file and pasting it in another file and storing it in another name.

- 3 Using a new method in storing files warning the user to s dialogue store or modify Normal. Dot However, this procedure does not fit previous infected files but it prevents new ones.

- 1) Using a Macro contains the command Disable Auto Macros to stop the activity of all macros and any automatic activity some goes to stop all activities associated to files whatever its kind was.
- 2) Creating a new macro structured as follows:


```
Sub Main
Disable Auto Macros1
End Sub
```

That enables the infected file without activating Auto open, which prevents the infection of the comprehensive template. This thing is as two-edge weapon. The First Edge holds the ability of stopping the effect of some kinds of macro viruses that available functions can deal with.. On the other hand, this side resulted in stopping automatic macro collection from working which stands as an obstacle in front of many activities used by the user when working on the programming system. We see that the best and easiest solution is transferring the characters of the Normal Dot to Read only state by suggesting a password through the Tool list in order to prevent any infection.

References

- [1] Bozo, Word Macro Viruses, An Electronic Document available on: <http://www.xs4all.nl/~cicatrix/index.html>.
- [2] Chengi Jimmy Kuo, Free Macro Anti Virus Technique, An Electronic Document available on: <http://www.xs4all.nl/~cicatrix/index.html>
- [3] Joe Wells, Concept : Understanding The Virus and Its Impacts, An Electronic Document available on: <http://www.xs4all.nl/~cicatrix/index.html>
- [4] McAfee, Macro Viruses, An Electronic Document available on: <http://www.xs4all.nl/~cicatrix/index.html>
- [5] Method for emulating an executable code in order to detect maliciousness, document available on <http://www.freepatentsonline.com/20040133796.html>

Dr. Hassan M. Wahahat, received the B.S. and M.S. degrees in Electrical Engineering from Shibaura Institute of Technology in 1997 and 1999, respectively. During 1997-1999, he stayed in Communications Research Laboratory (CRL), Ministry of Posts and Telecommunications of Japan to study digital beamforming antennas, mobile satellite communication systems, and wireless access network using stratospheric platforms. He now with DDI Tokyo Pocket Telephone, Inc.

TakiAlddin Alsmadi received the B.S. and M.S. degrees in Electrical Engineering from Shibaura Institute of Technology in 1997 and 1999, respectively. During 1997-1999, he stayed in Communications Research Laboratory (CRL), Ministry of Posts and Telecommunications of Japan to study digital beamforming antennas, mobile satellite communication systems, and wireless access network using stratospheric platforms. He now with DDI Tokyo Pocket Telephone, Inc.

Dr. Yasir Khalil Ibrahim received the B.S. and M.S. degrees in Electrical Engineering from Shibaura Institute of Technology in 1997 and 1999, respectively. During 1997-1999, he stayed in Communications Research Laboratory (CRL), Ministry of Posts and Telecommunications of Japan to study digital beamforming antennas, mobile satellite communication systems, and wireless access network using stratospheric platforms. He now with DDI Tokyo Pocket Telephone, Inc.