Microsoft Office Macro Analysis

written by Mert SARICA | 1 December 2015

Some of you, who are the same age as me or older might remember the Melissa malware that spread through Microsoft Office Word macro in 1999 and affected millions of systems worldwide. Melissa malware was spreading by sending the first 50 people on Microsoft Outlook in the system it was infected with the help of macro support that came with Microsoft Office.

If you are asking “What is a macro ?”, Microsoft company will answer you as stated below;

A macro is a series of commands and instructions that you group together as a single command to accomplish a task automatically.You can record a sequence of actions, or you can write a macro from scratch by entering Visual Basic for Applications code in the Visual Basic Editor. However, malware can also use this functionality to download threats onto your PC. Macro malware usually hides in Microsoft Word or Microsoft Excel documents.

Throughout the years because of the misuse of macros (the abuse), Microsoft company did some security improvements on Office software. One of these improvements was new file extensions that were released with Office 2007 version. For example, if a file that was created with Office 2007 has the letter m in the file extension, this means the office file includes a macro. With this improvement, we were able to be cautious towards the files that have the letter m in their extensions and block them based on their extensions.

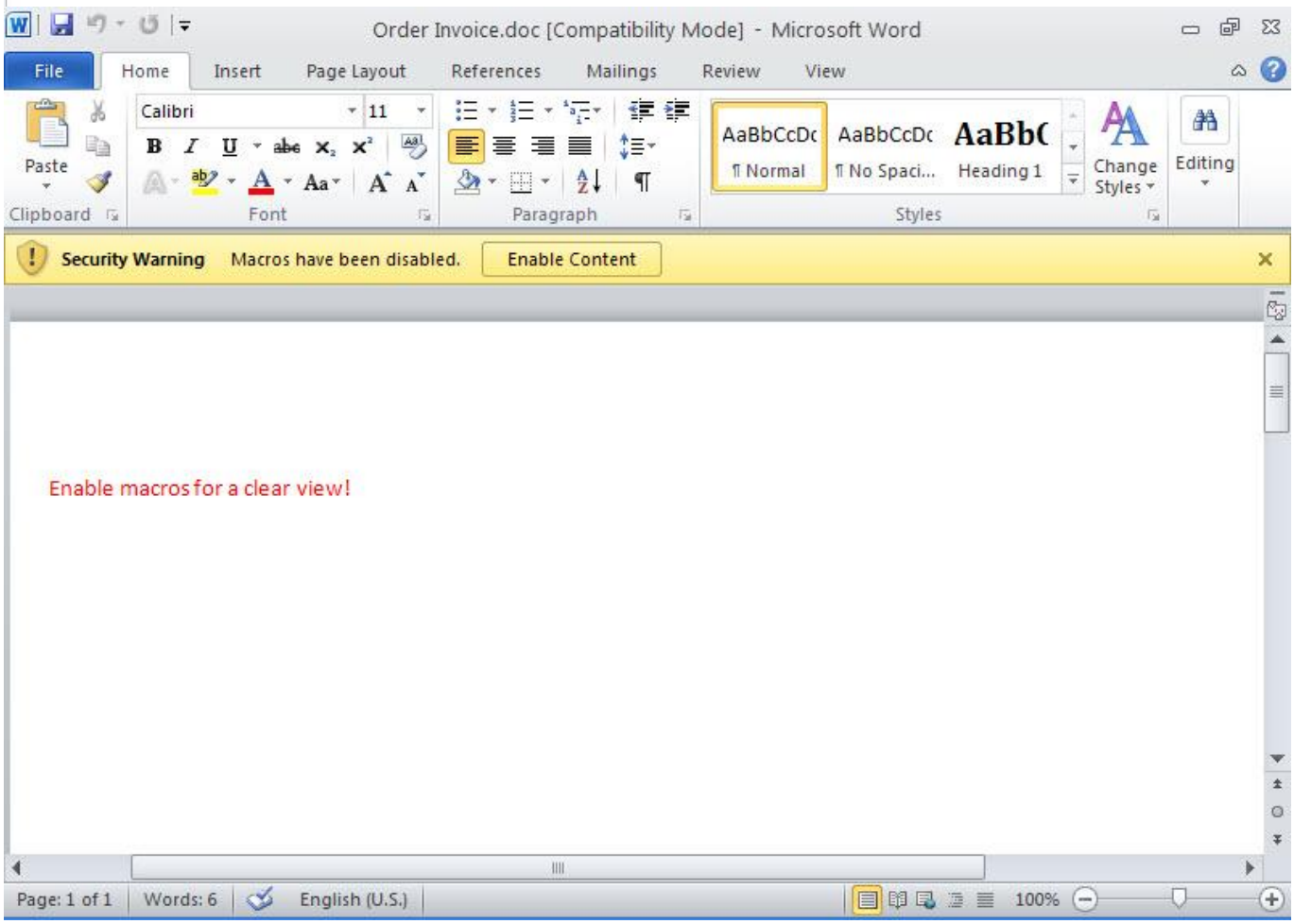
You could be saying why are you telling us all these since it’s been 20 years after Melissa virus and Microsoft did what they could about the situation. Recently we can see malicious online banking software’s and malwares like RAT trying to be spread across by using office files that include macros. Because malignant users know that the file extensions with letter m get attention, they create the macro files by using Office 2003 hence, they are able to get past the systems and informed users that do extension checks.

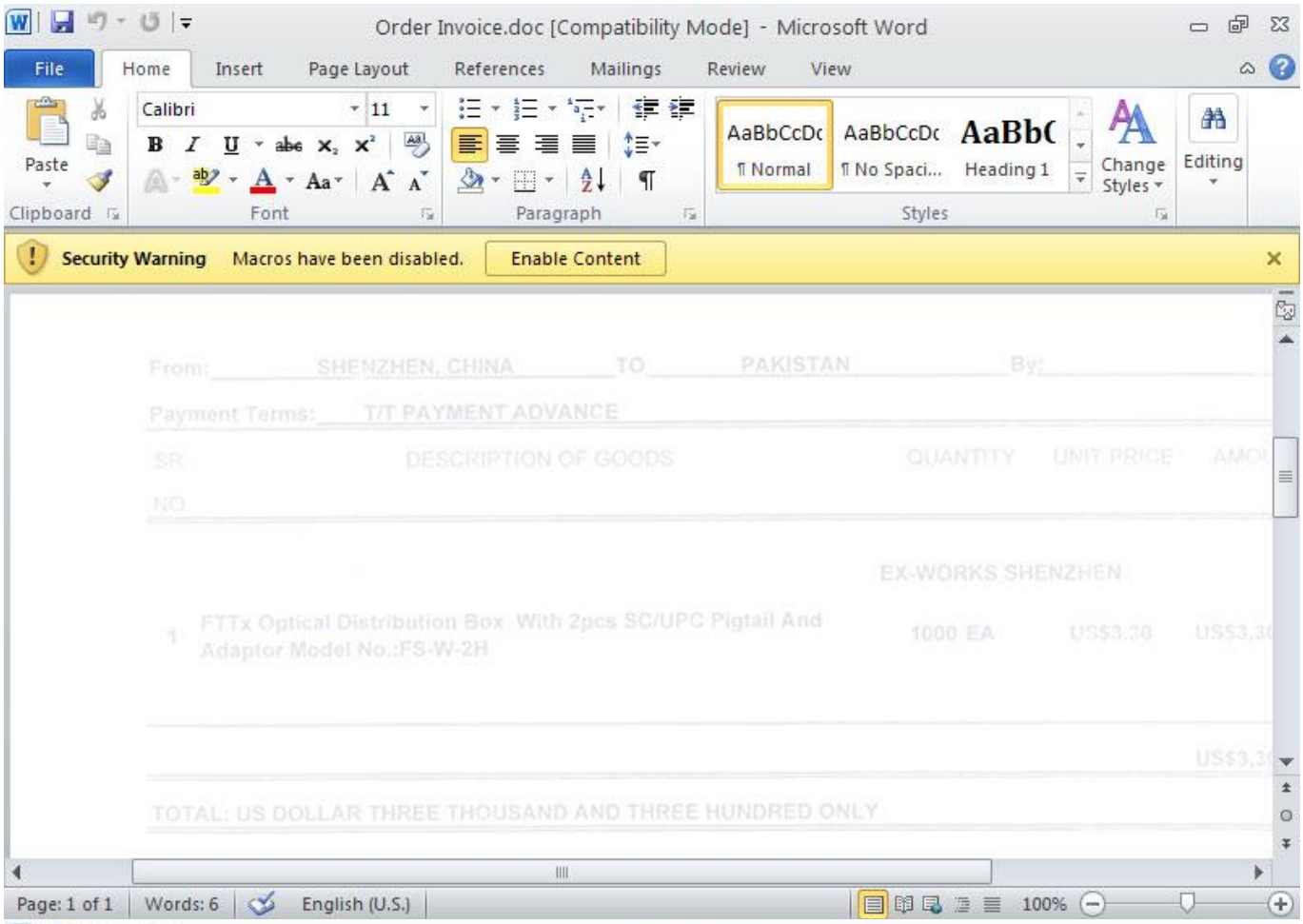
Subject: FW: urgent RE: PO/002/2015- urgent

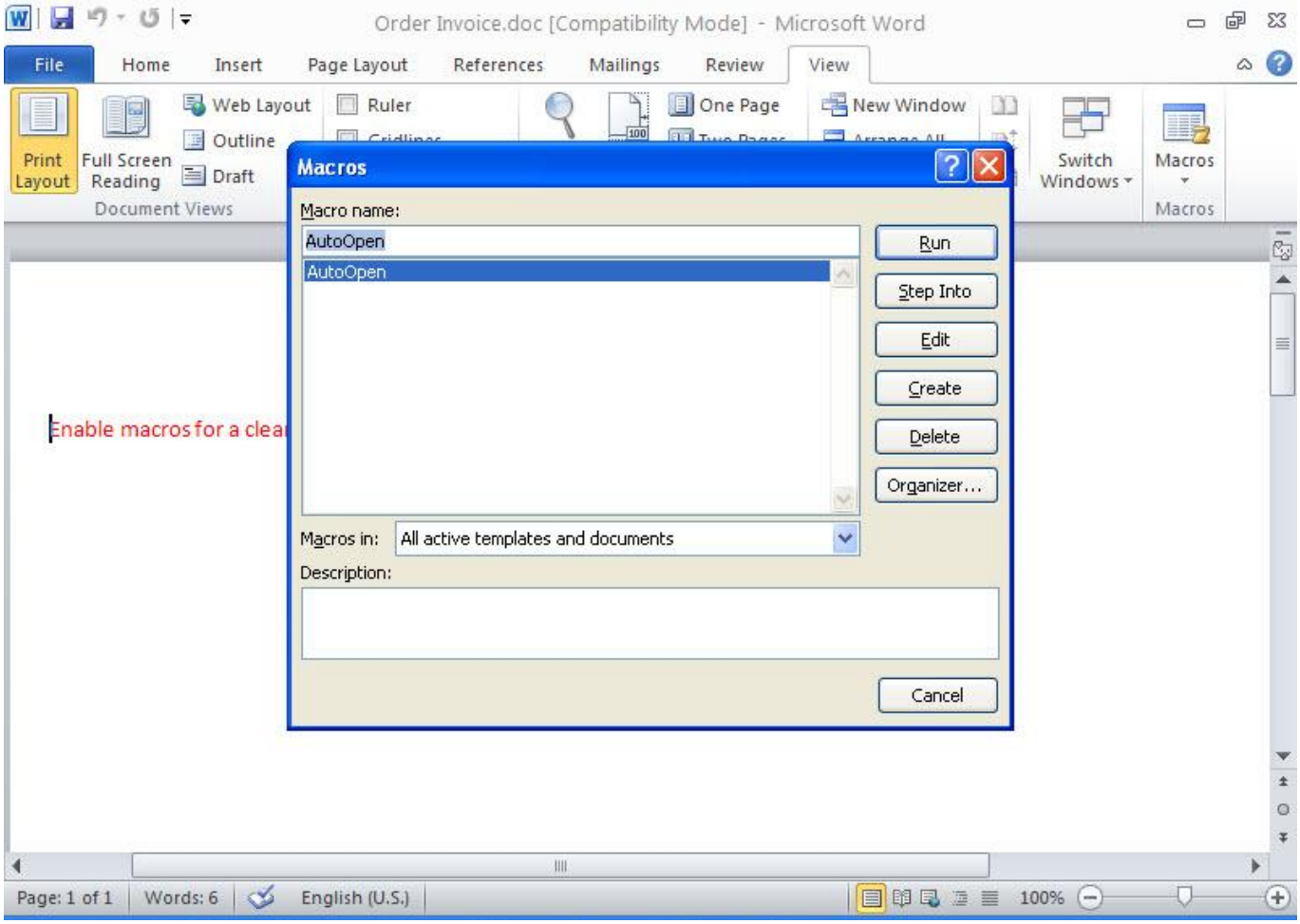
Message | Order Invoice.doc (148 KB)

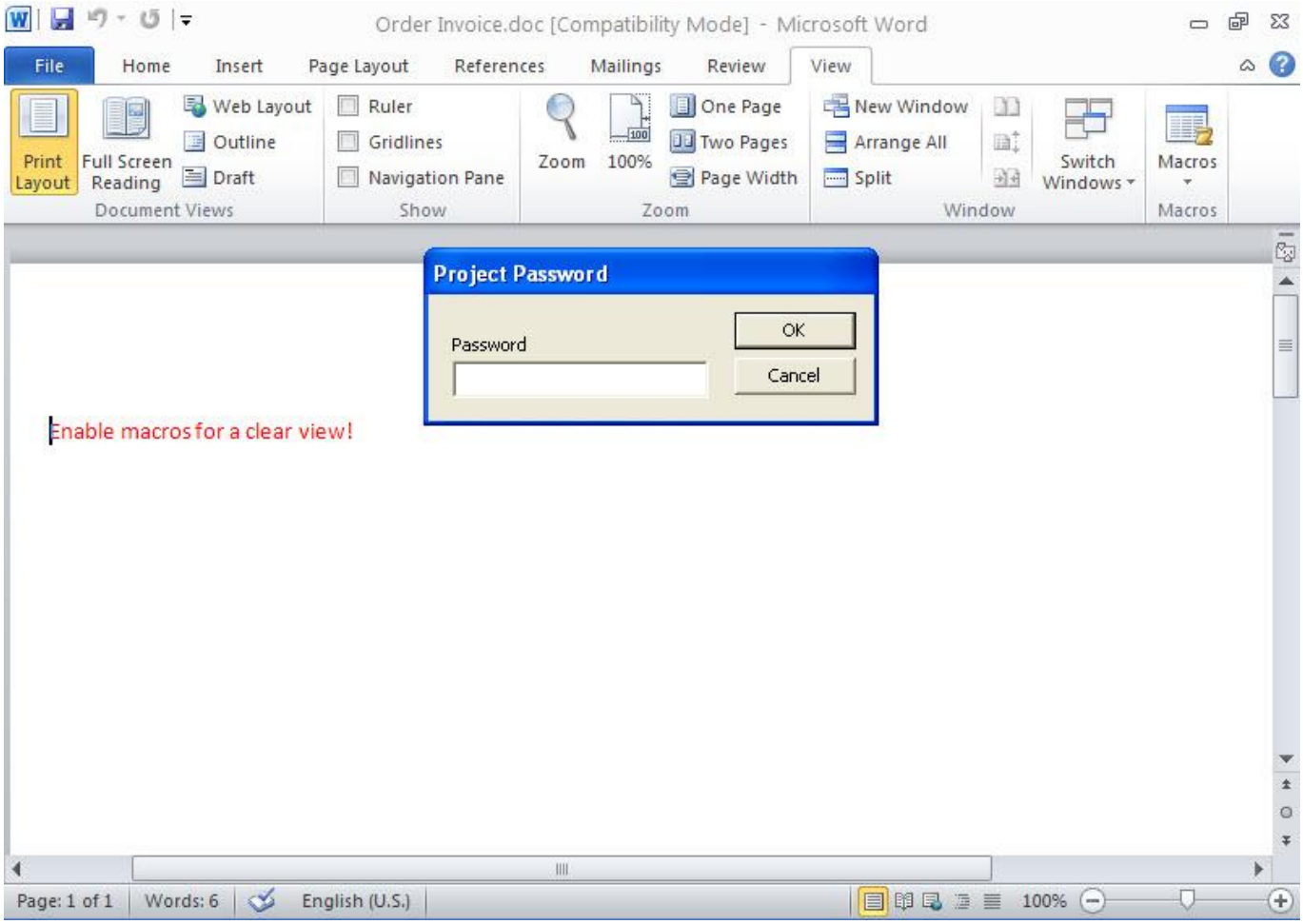
From: [redacted]
Sent: Tuesday, May 26, 2015 5:16 AM
To: [redacted]
Subject: RE: urgent RE: PO/002/2015- urgent

Dear Mohamed,
Kindly see see the see the attached invoice for the order and do the needful. We have confirmed the last payment in our account and the original documents will be sent through Aramex today .
Please do the needful in respect to the the attached invoice and also forward to your accounts.
Regards
Ahmed
APAM.

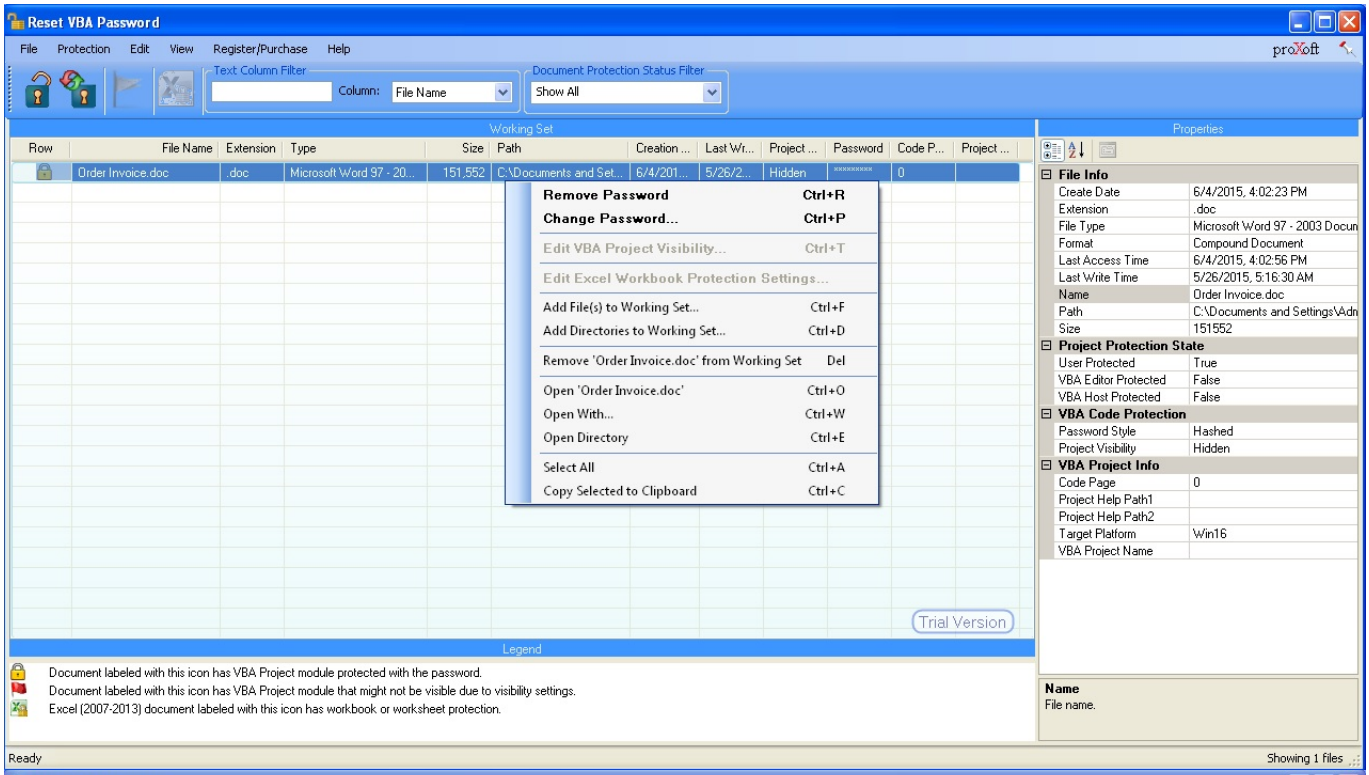


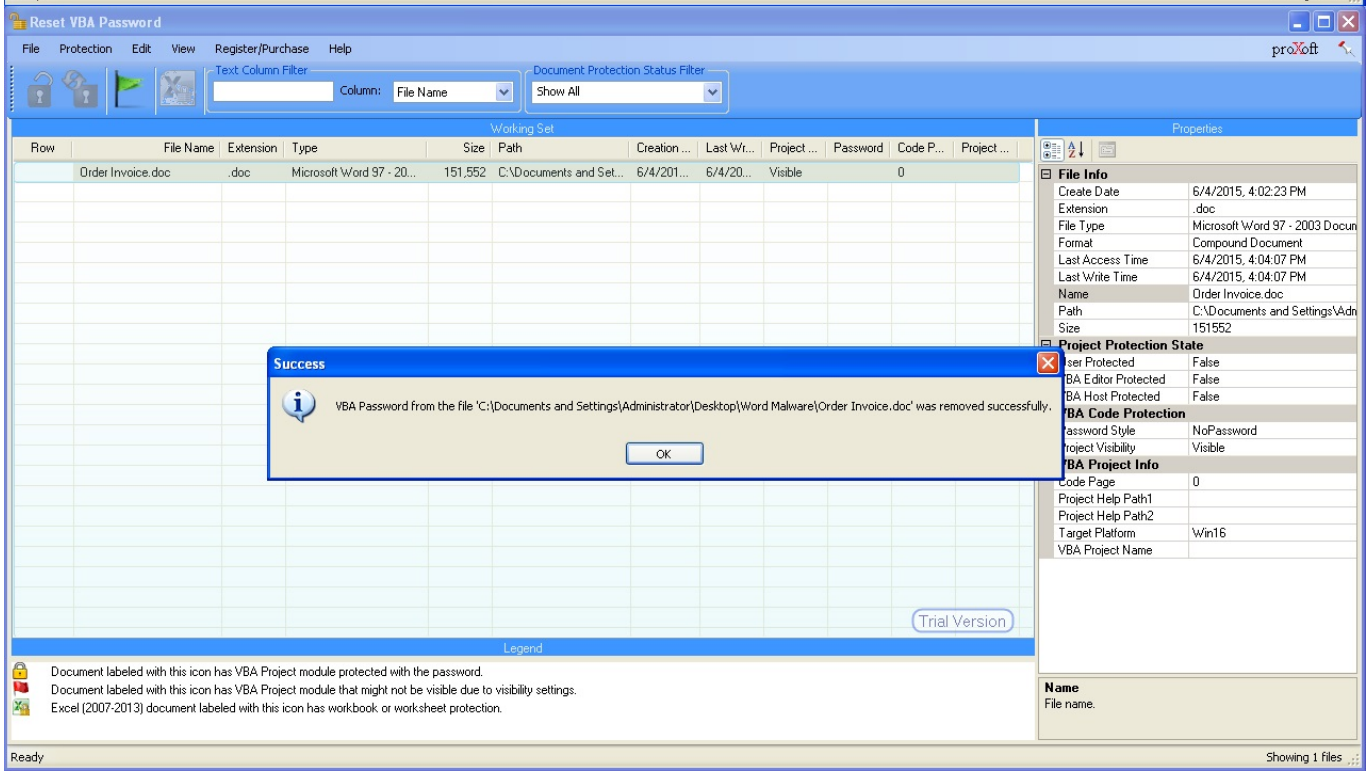

Order Invoice.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Security Warning
Macros have been disabled.
Enable Content
From: SHENZHEN, CHINA TO PAKISTAN By:
Payment Terms: T/T PAYMENT ADVANCE
DESCRIPTION OF GOODS
QUANTITY
UNIT PRICE
EX-WORKS SHENZHEN
FTTx Optical Distribution Box With 2pcs SC/UPC Pigtail And Adaptor Model No.:FS-W-2H
1000 EA
US$3.30
TOTAL: US DOLLAR THREE THOUSAND AND THREE HUNDRED ONLY
Page: 1 of 1
Words: 6
English (U.S.)
100%

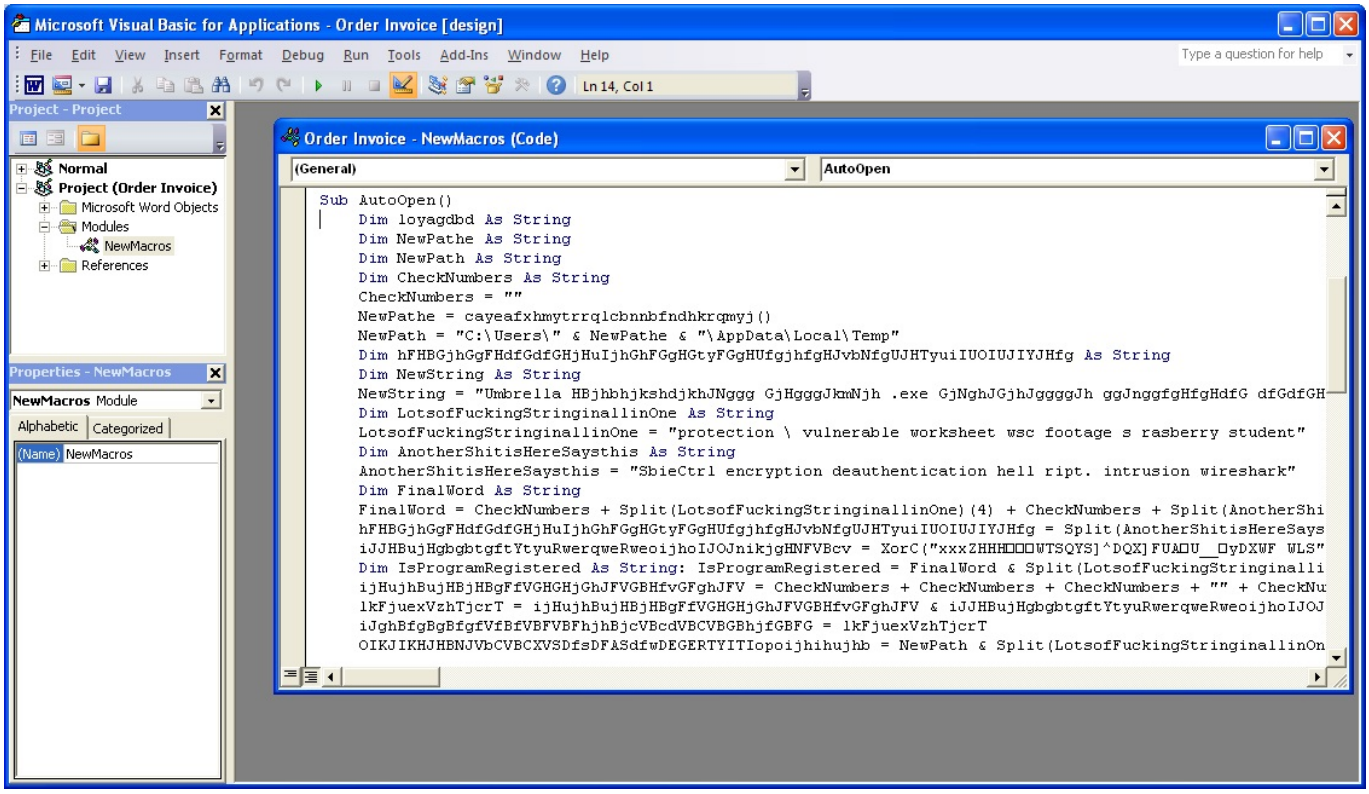

Order Invoice.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Print Layout
Full Screen Reading
Web Layout
Outline
Draft
Document Views
Ruler
One Page
New Window
Switch Windows
Macros
Macros
Macro name:
AutoOpen
AutoOpen
Run
Step Into
Edit
Create
Delete
Organizer...
Macros in:
All active templates and documents
Description:
Cancel
Enable macros for a clea
Page: 1 of 1
Words: 6
English (U.S.)
100%



Well then, how can we analyze a file that we thing has a macro? We can open the office file with Microsoft Office software in a virtual machine then we can display the contents from the Macro menu (view -> macros -> view macros). However, malicious users that know this way usually put password protection to the macro. To be able to solve this password you can use Reset VBA Password tool.

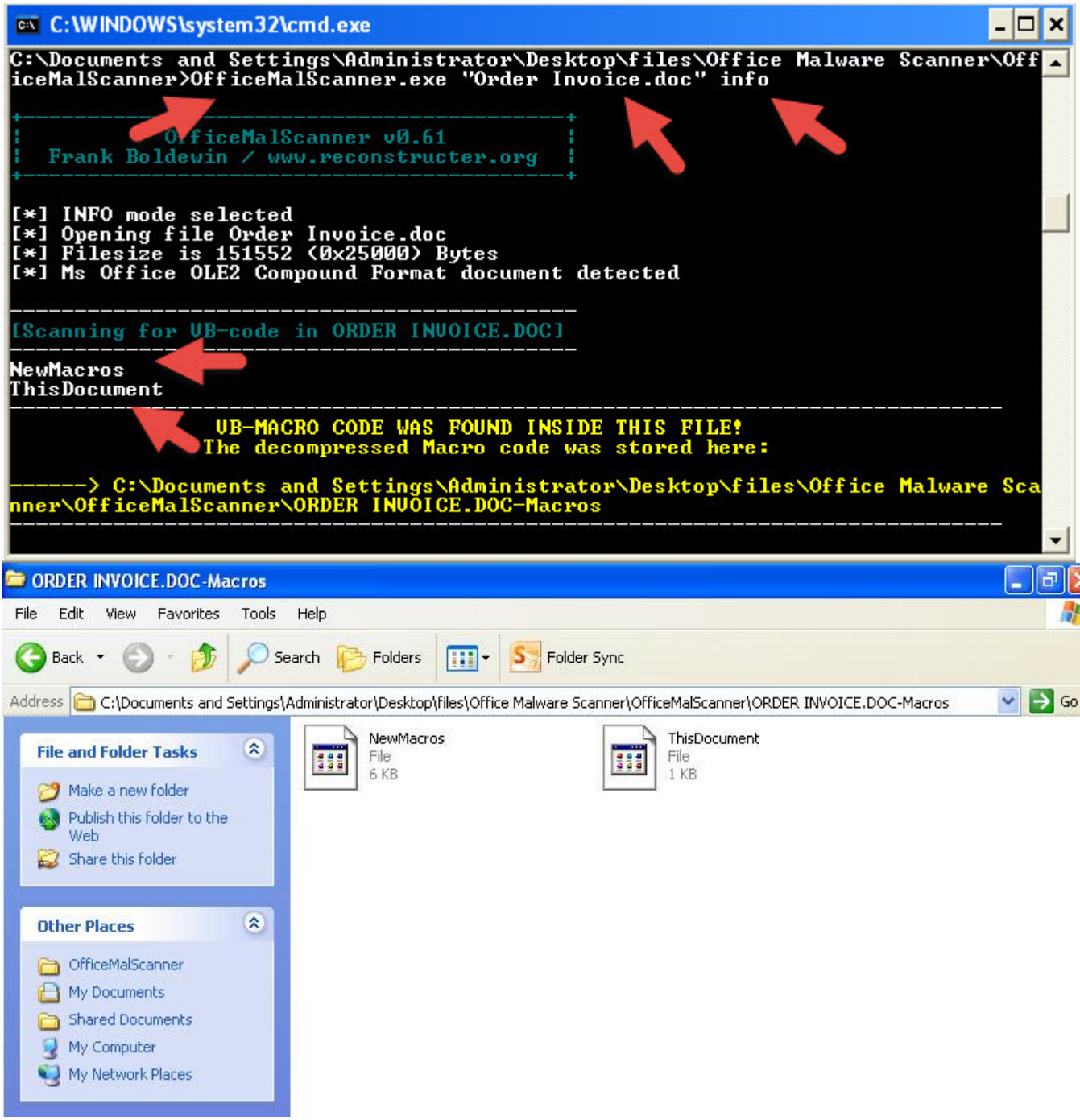

Reset VBA Password
File Protection Edit View Register/Purchase Help
proXoft
Text Column Filter
Column: File Name
Document Protection Status Filter
Show All
Working Set
Row File Name Extension Type Size Path Creation ... Last Wr... Project ... Password Code P... Project ...
Order Invoice.doc .doc Microsoft Word 97 - 20... 151,552 C:\Documents and Set... 6/4/201... 5/26/2... Hidden 0
Remove Password Ctrl+R
Change Password... Ctrl+P
Edit VBA Project Visibility... Ctrl+T
Edit Excel Workbook Protection Settings...
Add File(s) to Working Set... Ctrl+F
Add Directories to Working Set... Ctrl+D
Remove 'Order Invoice.doc' from Working Set Del
Open 'Order Invoice.doc' Ctrl+O
Open With... Ctrl+W
Open Directory Ctrl+E
Select All Ctrl+A
Copy Selected to Clipboard Ctrl+C
Trial Version
Properties
File Info
Create Date 6/4/2015, 4:02:23 PM
Extension .doc
File Type Microsoft Word 97 - 2003 Docun
Format Compound Document
Last Access Time 6/4/2015, 4:02:56 PM
Last Write Time 5/26/2015, 5:16:30 AM
Name Order Invoice.doc
Path C:\Documents and Settings\Adn
Size 151552
Project Protection State
User Protected True
VBA Editor Protected False
VBA Host Protected False
VBA Code Protection
Password Style Hashed
Project Visibility Hidden
VBA Project Info
Code Page 0
Project Help Path1
Project Help Path2
Target Platform Win16
VBA Project Name
Legend
Document labeled with this icon has VBA Project module protected with the password.
Document labeled with this icon has VBA Project module that might not be visible due to visibility settings.
Excel (2007-2013) document labeled with this icon has workbook or worksheet protection.
Name
File name.
Ready
Showing 1 files


Reset VBA Password
File Protection Edit View Register/Purchase Help
proXoft
Text Column Filter
Column: File Name
Document Protection Status Filter
Show All
Working Set
Row File Name Extension Type Size Path Creation ... Last Wr... Project ... Password Code P... Project ...
Order Invoice.doc .doc Microsoft Word 97 - 20... 151,552 C:\Documents and Set... 6/4/201... 6/4/20... Visible 0
Success
VBA Password from the file 'C:\Documents and Settings\Administrator\Desktop\Word Malware\Order Invoice.doc' was removed successfully.
OK
Trial Version
Properties
File Info
Create Date 6/4/2015, 4:02:23 PM
Extension .doc
File Type Microsoft Word 97 - 2003 Docun
Format Compound Document
Last Access Time 6/4/2015, 4:04:07 PM
Last Write Time 6/4/2015, 4:04:07 PM
Name Order Invoice.doc
Path C:\Documents and Settings\Adn
Size 151552
Project Protection State
User Protected False
VBA Editor Protected False
VBA Host Protected False
VBA Code Protection
Password Style NoPassword
Project Visibility Visible
VBA Project Info
Code Page 0
Project Help Path1
Project Help Path2
Target Platform Win16
VBA Project Name
Legend
Document labeled with this icon has VBA Project module protected with the password.
Document labeled with this icon has VBA Project module that might not be visible due to visibility settings.
Excel (2007-2013) document labeled with this icon has workbook or worksheet protection.
Name
File name.
Ready
Showing 1 files

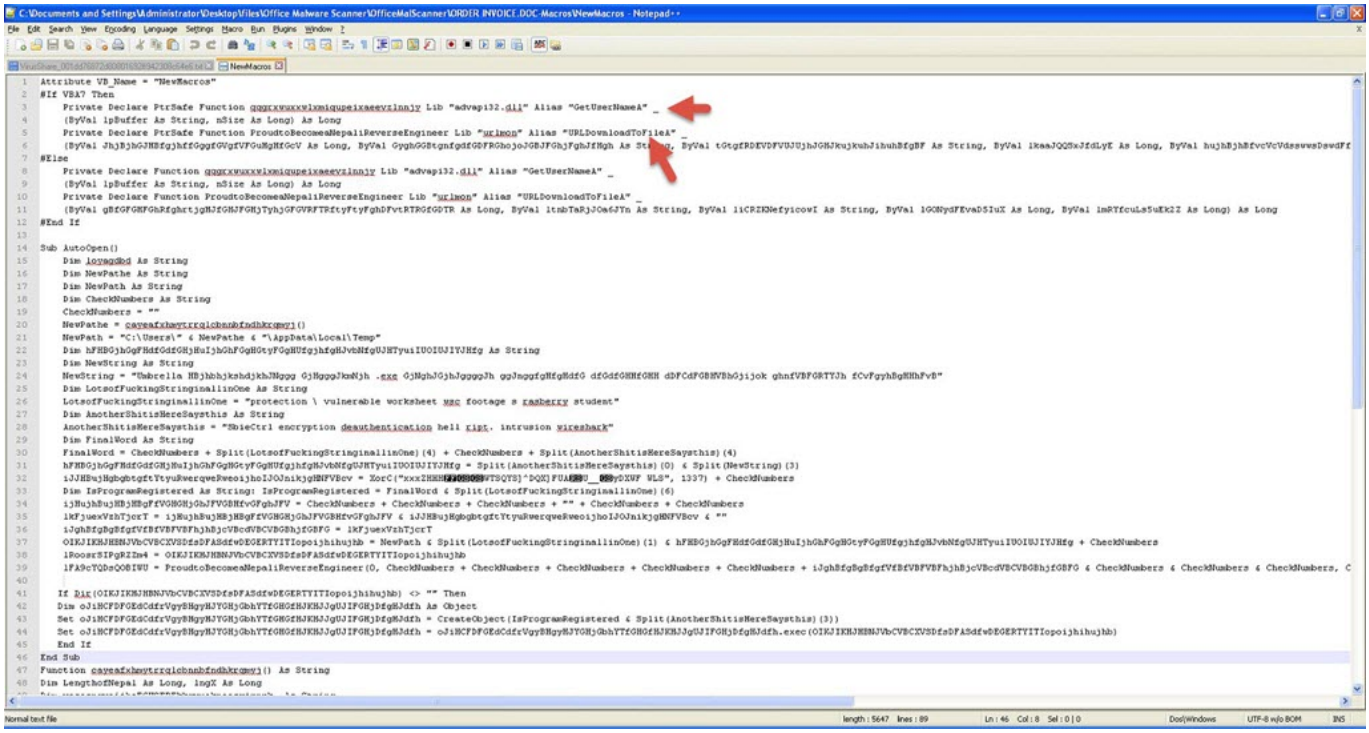


It is also possible to analyze an office file that you think has a macro without Microsoft Office and this is possible with OfficeMalScanner tool. OfficeMalScanner is a very beneficial tool that helps us analyze suspicious (shellcode, PE detection) office files and also help us extract the macro code it found inside the office file for us to analyze.

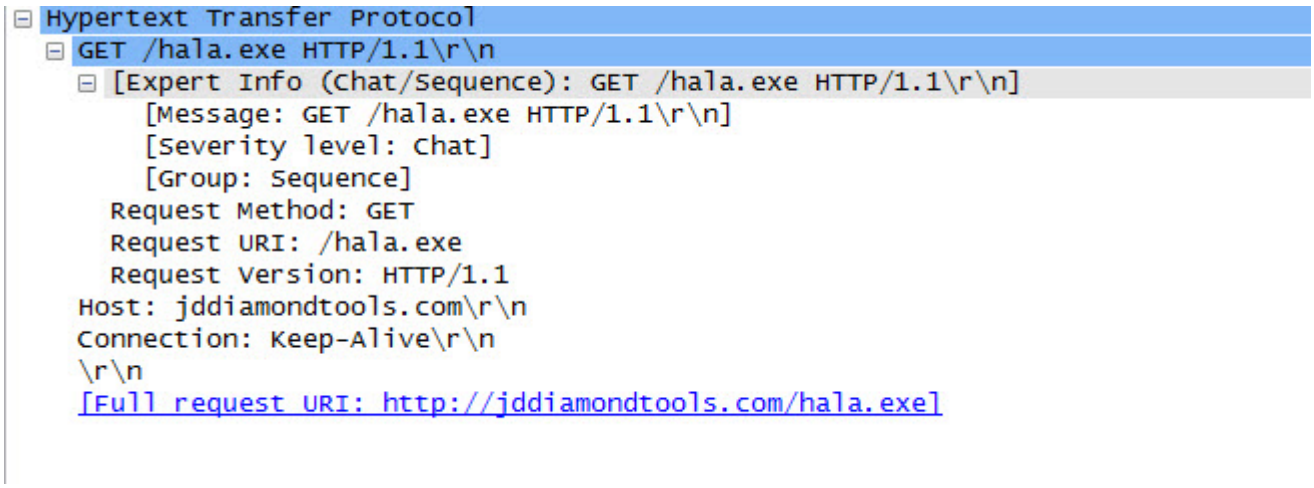
For example, if we have a suspicious file that we think was created using Microsoft Office 2003 like I mentioned above, you can give this tool info command as a parameter and let the tool analyze the file and extract the macro code for us. If the file in hand is created with Microsoft Office 2007 or later, we can use the inflate command (actually no different than changing the office file extension to .zip then opening it with winzip/winrar) to make the tool open the file and extract the macro code inside the file with once again info command.


C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator\Desktop\files\Office Malware Scanner\OfficeMalScanner>OfficeMalScanner.exe "Order Invoice.doc" info
OfficeMalScanner v0.61
Frank Boldewin / www.reconstructer.org
[*] INFO mode selected
[*] Opening file Order Invoice.doc
[*] Filesize is 151552 (0x25000) Bytes
[*] Ms Office OLE2 Compound Format document detected
[Scanning for VB-code in ORDER INVOICE.DOC]
NewMacros
ThisDocument
VB-MACRO CODE WAS FOUND INSIDE THIS FILE!
The decompressed Macro code was stored here:
------> C:\Documents and Settings\Administrator\Desktop\files\Office Malware Scanner\OfficeMalScanner\ORDER INVOICE.DOC-Macros

ORDER INVOICE.DOC-Macros
File Edit View Favorites Tools Help
Back Search Folders Folder Sync
Address C:\Documents and Settings\Administrator\Desktop\files\Office Malware Scanner\OfficeMalScanner\ORDER INVOICE.DOC-Macros
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
OfficeMalScanner
My Documents
Shared Documents
My Computer
My Network Places
NewMacros
File
6 KB
ThisDocument
File
1 KB



When we analyze the macro code that came up, we can see that it is a downloader that downloads RAT type malware by inspecting the used API’s.



Hope that this post will be helpful for you to analyze suspicious office files. See you on the next post and have a secure day.

Original Article: Microsoft Office Makro Analizi
Translated to English by: Hüseyin Fatih Akar | Twitter: @thehakar)