Microsoft Office Makro Analizi

written by Mert SARICA | 1 December 2015

Hemen hemen benle aynı yaşta veya daha yaşlı olanlarınız, 1999 yılında Microsoft Office Word makrosu ile yayılan ve dünya genelindeki milyonlarca sistemi etkileyen Melissa zararlı yazılımını (virüs) hatırlayacaklardır. Melissa zararlı yazılımı, Microsoft Office ile gelen makro desteği sayesinde, çalıştırıldığı sistem üzerinde Microsoft Outlook üzerinde kayıtlı olan ilk 50 kişiye kendisini göndererek yayılıyordu.

Nedir bu makro diye soracak olursanız, Microsoft firması size aşağıdaki gibi bir yanıt verecektir;

Makrolar, tuş ve fare eylemlerinde zaman kazanmak için sık kullanılan görevleri otomatikleştirir. Pek çok makro, Visual Basic for Applications (VBA) kullanılarak oluşturulmuştur ve yazılım geliştiricileri tarafından yazılırlar. Ancak bazı makrolar olası bir güvenlik riski yaratır. Korsan olarak da bilinen kötü niyetli kullanıcılar, bir dosyaya, bilgisayarınıza veya kuruluş ağınıza virüs bulaştırabilecek zararlı bir makro yerleştirebilir.

Yıllar içinde makroların kötüye kullanımı nedeniyle Microsoft firması da boş durmayarak Office yazılımı üzerinde çeşitli güvenlik iyileştirmeleri yaptı. Bunlardan bir tanesi de Office 2007 sürümü ile sunulan yeni dosya uzantıları oldu. Örneğin Office 2007 ile oluşturulmuş bir office dosyasının uzantısında m harfi geçiyor ise bu, office dosyasının makro içerdiğini belirtir. Durum böyle olunca da uzantısında m harfi geçen office dosyalarına daha teminkinli yaklaşabilir, uzantıya göre bu dosyaları bloklayabilir olduk.

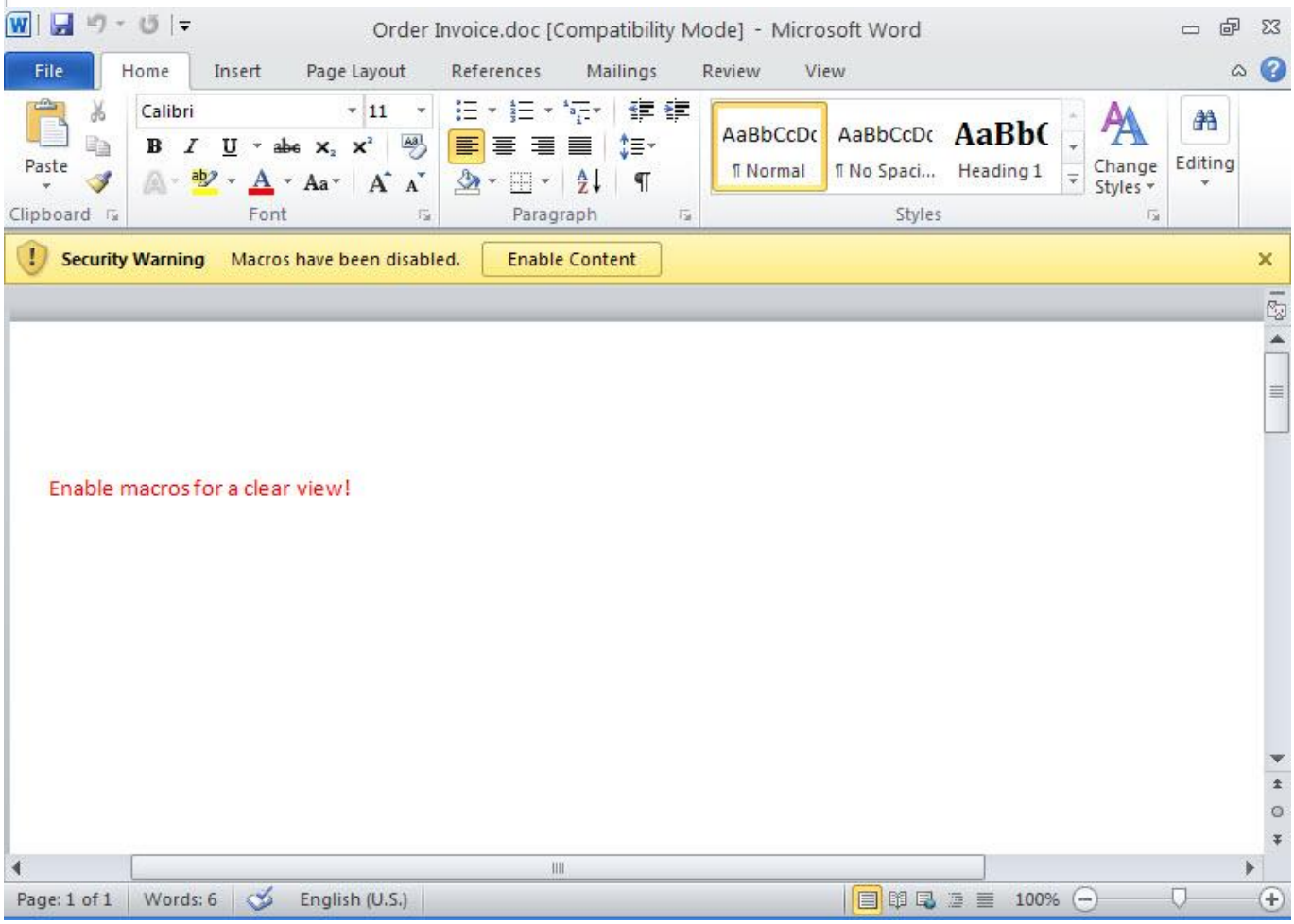
Melissa zararlı yazılımından bu yana neredeyse 20 sene geçmiş, Microsoft da üzerine düşenleri yapmış, bize bunları neden anlatıyorsun diyenleriniz olabilir. Makro içeren office dosyaları ile son zamanlarda, internet bankacılığı zararlı yazılımları ve RAT türü zararlı yazılımların yayılmaya çalıştığını görüyoruz. M harfi içeren dosya uzantılarının dikkat çektiğini bilen art niyetli kişiler de makro içeren dosyaları Office 2003 sürümü ile hazırladıkları için bilinçli kullanıcıların ve uzantı kontrolü yapan sistemlerin dikkatinden, kontrolünden geçebiliyor.

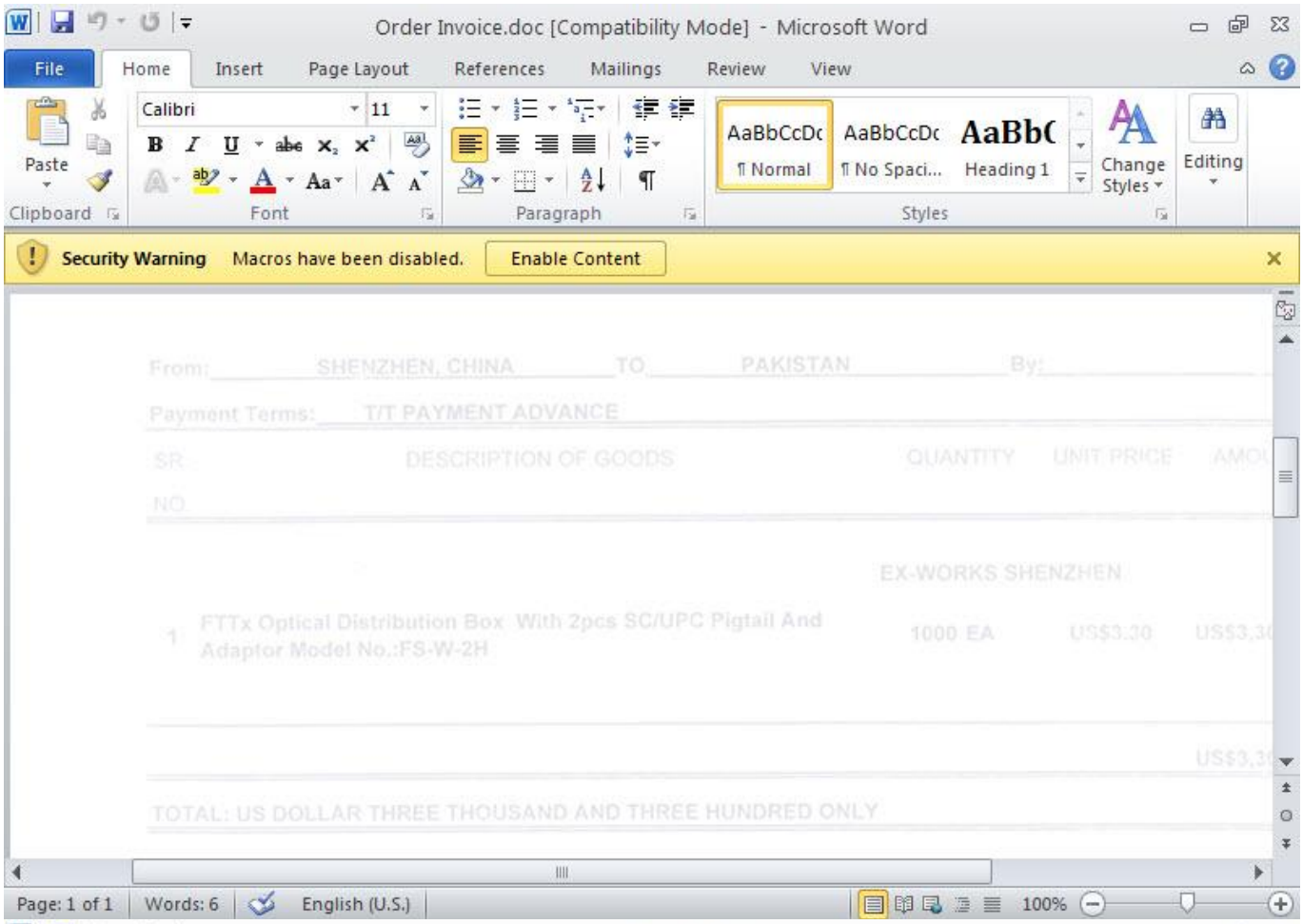
Subject: FW: urgent RE: PO/002/2015- urgent

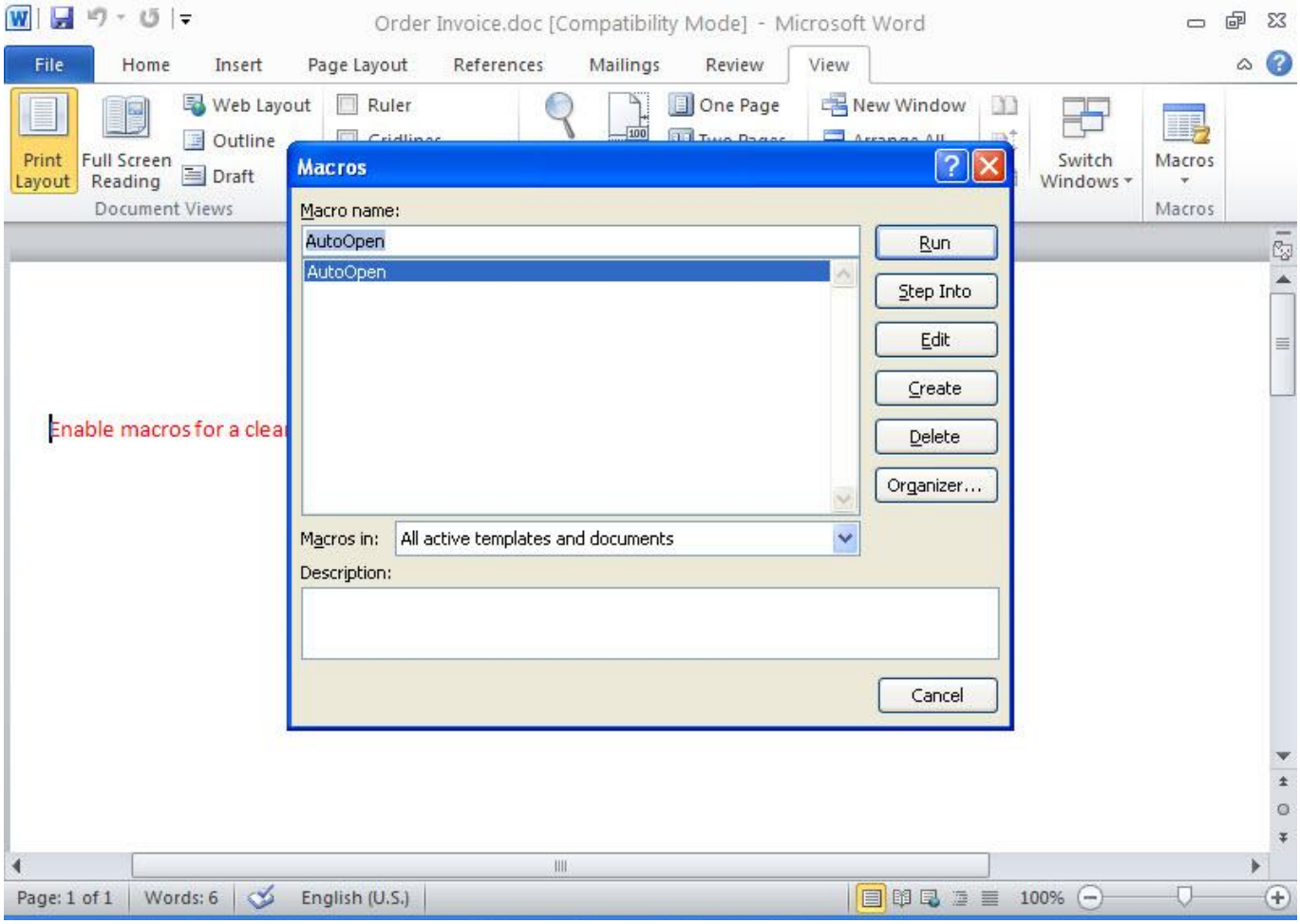
Message | Order Invoice.doc (148 KB)

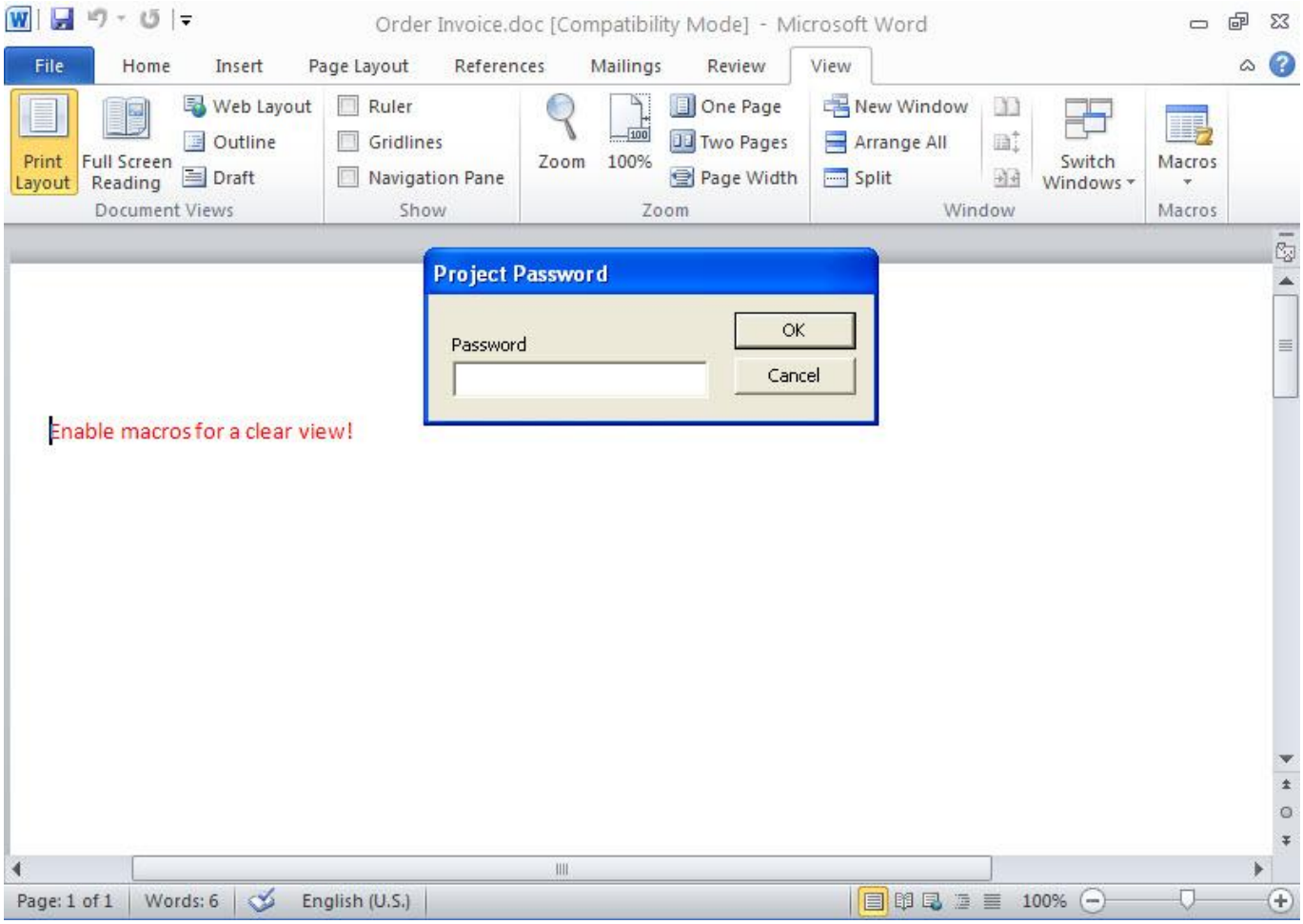
From: [redacted]
Sent: Tuesday, May 26, 2015 5:16 AM
To: [redacted]
Subject: RE: urgent RE: PO/002/2015- urgent

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.

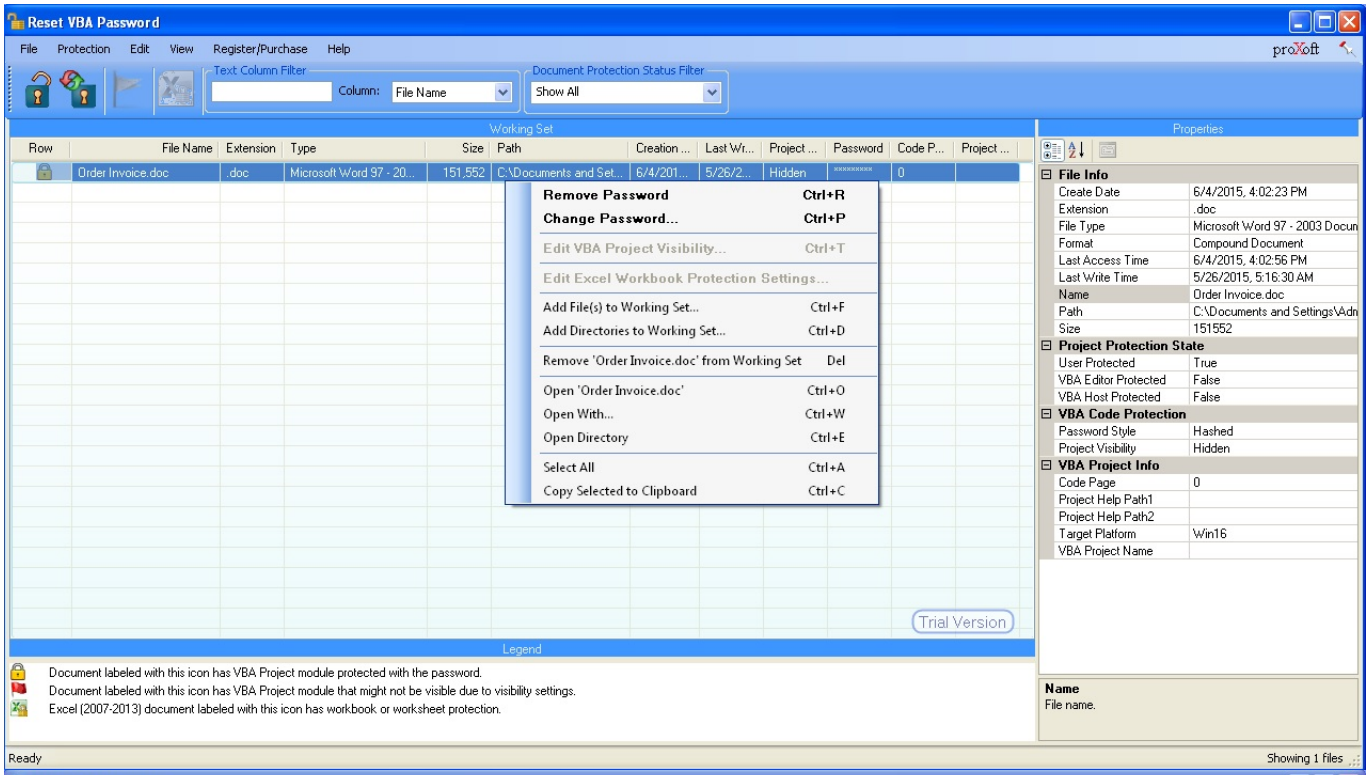


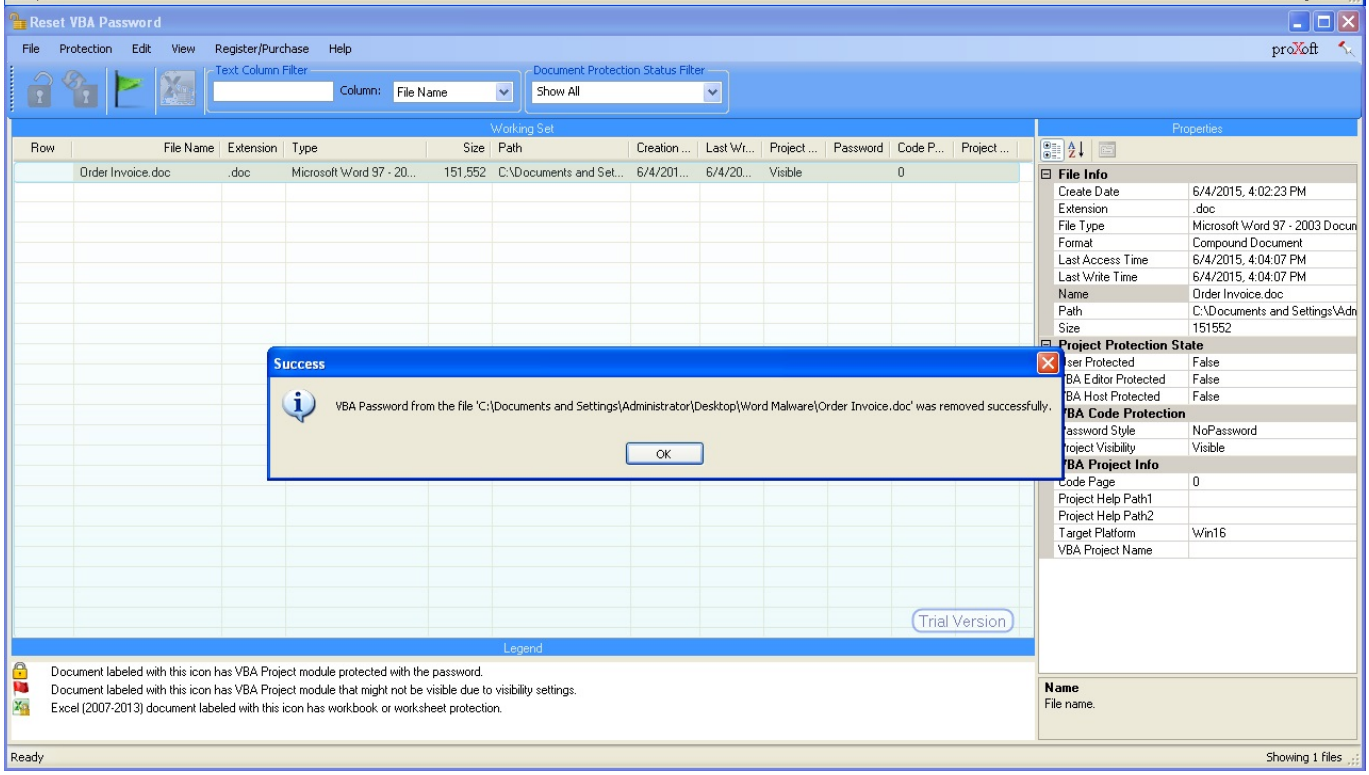

Order Invoice.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Security Warning
Macros have been disabled.
Enable Content
From: SHENZHEN, CHINA TO PAKISTAN By:
Payment Terms: T/T PAYMENT ADVANCE
DESCRIPTION OF GOODS
QUANTITY
UNIT PRICE
EX-WORKS SHENZHEN
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%

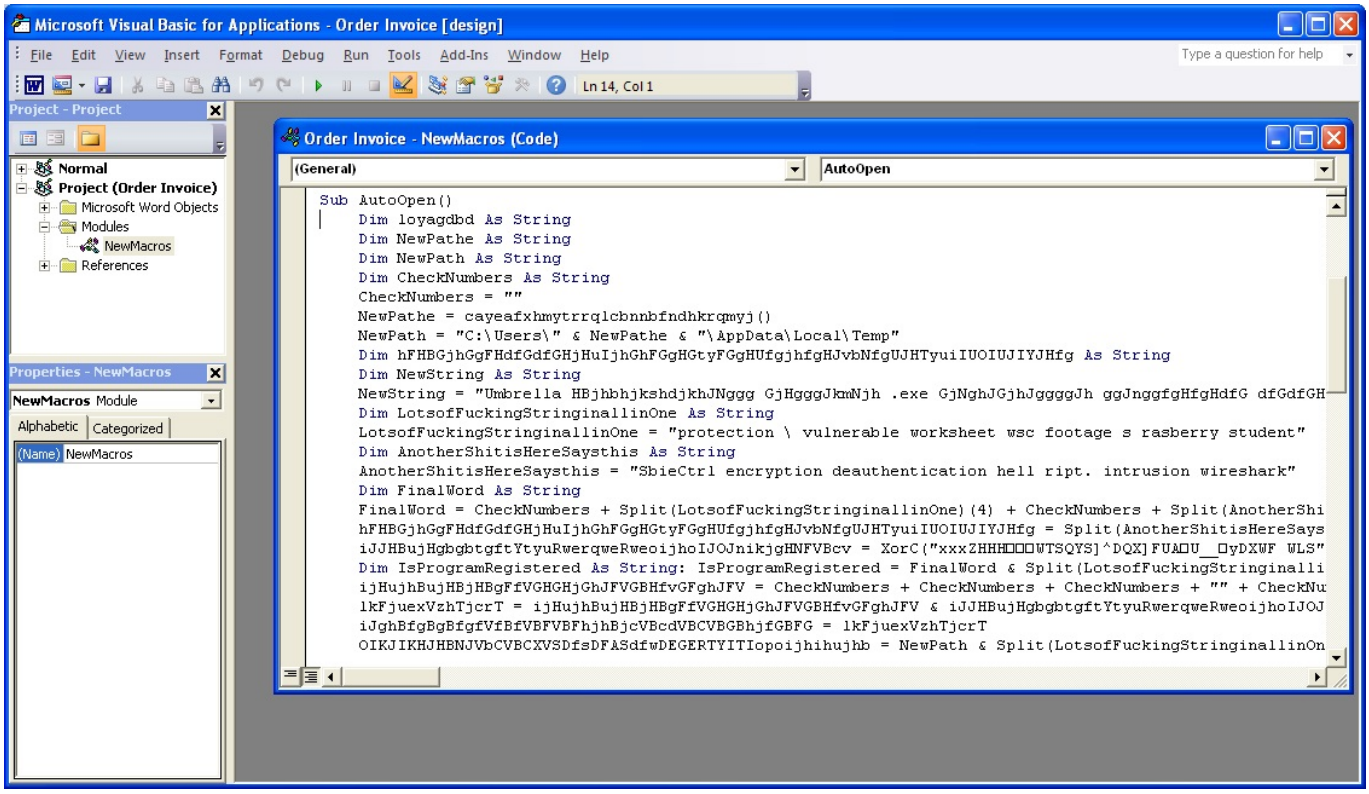

Order Invoice.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Print Layout
Full Screen Reading
Web Layout
Outline
Draft
Document Views
Ruler
One Page
New Window
Switch Windows
Macros
Macros
Macro name:
AutoOpen
AutoOpen
Run
Step Into
Edit
Create
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%



Peki makro içerdiğini düşündüğümüz bir office dosyasını nasıl analiz edebiliriz ? Office dosyasını sanal bir makine içinde Microsoft office yazılımı ile açtıktan sonra Macro (view -> macros -> view macros) menüsünden içeriğini görüntüleyebiliriz ancak bunu bilen art niyetli kişiler çoğunlukla makroya şifre koruması koymaktadırlar. Bu şifreyi çözmek için Reset VBA Password aracından faydalanabilirsiniz.

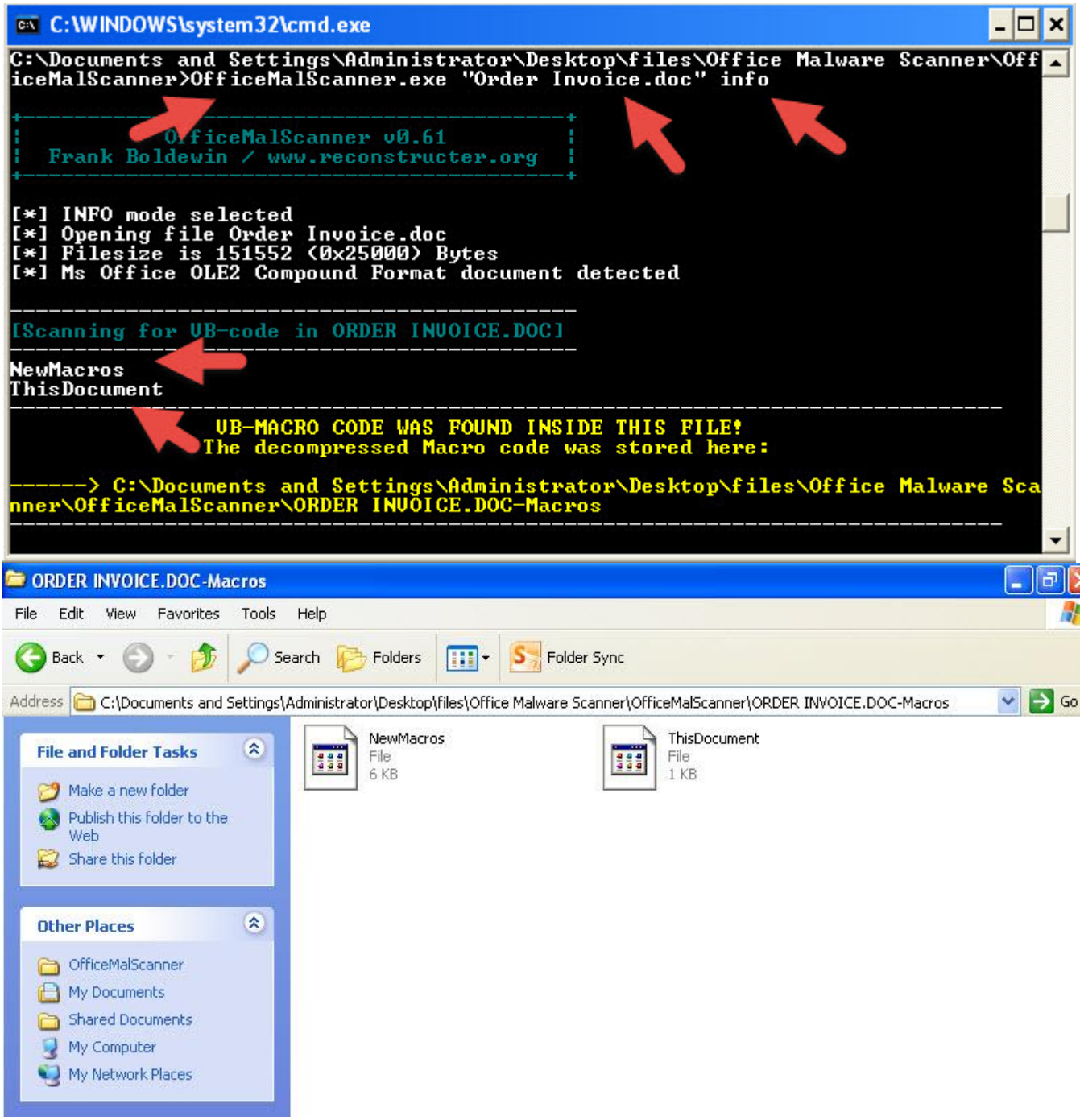

Reset VBA Password
File Protection Edit View Register/Purchase Help
proXoft
Text Column Filter
Column: File Name
Document Protection Status Filter
Show All
Working Set
Row File Name Extension Type Size Path Creation ... Last Wr... Project ... Password Code P... Project ...
Order Invoice.doc .doc Microsoft 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

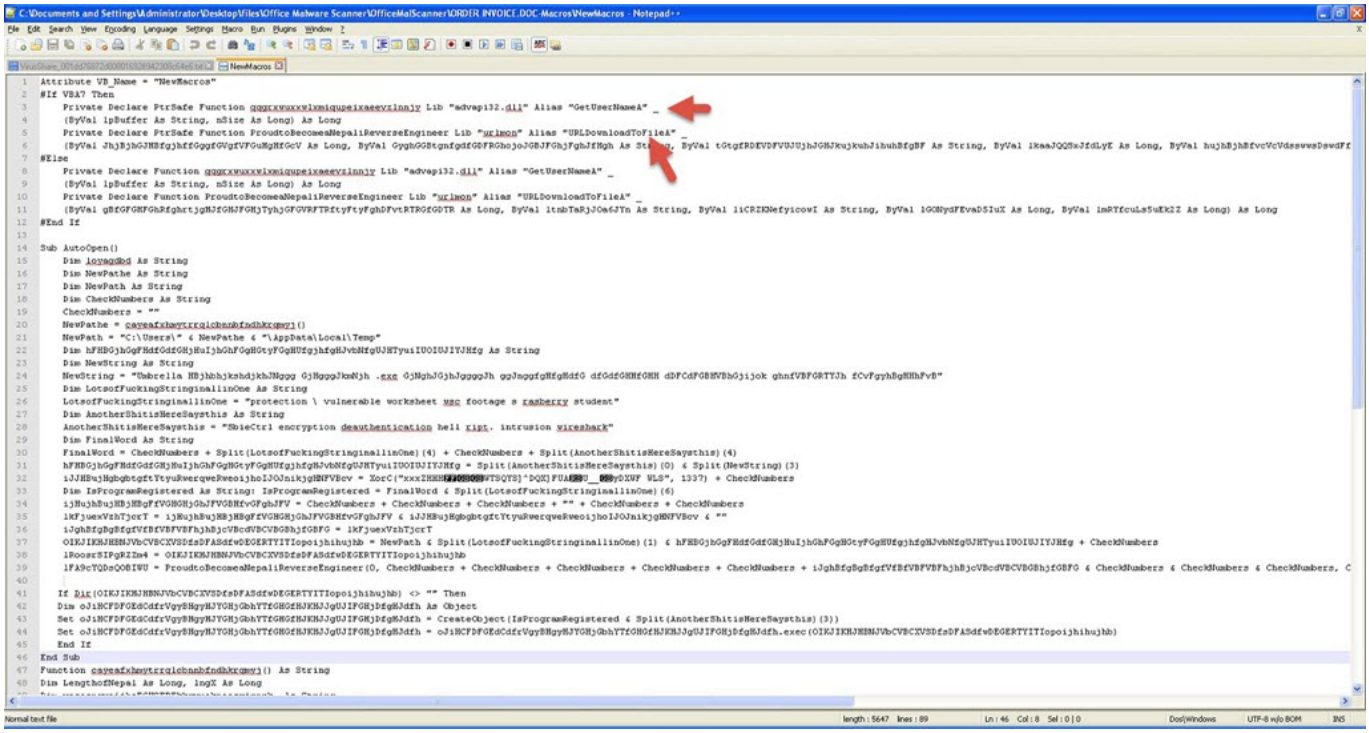


Makro içerdiğini düşündüğümüz bir ofis dosyasını Microsoft Office yüklü olmadan analiz etmenin bir yolu yok mu derseniz, OfficeMalScanner aracı sayesinde onun da mümkün olduğunu söyleyebilirim. OfficeMalScanner aracı, şüpheli (kabukkodu, PE tespiti gibi) ofis dosyalarını analiz etmemize yardımcı olan ve ofis dosyası içinde tespit ettiği makro kodunu analiz için çıkarmamıza yardımcı olan oldukça faydalı bir araçtır.

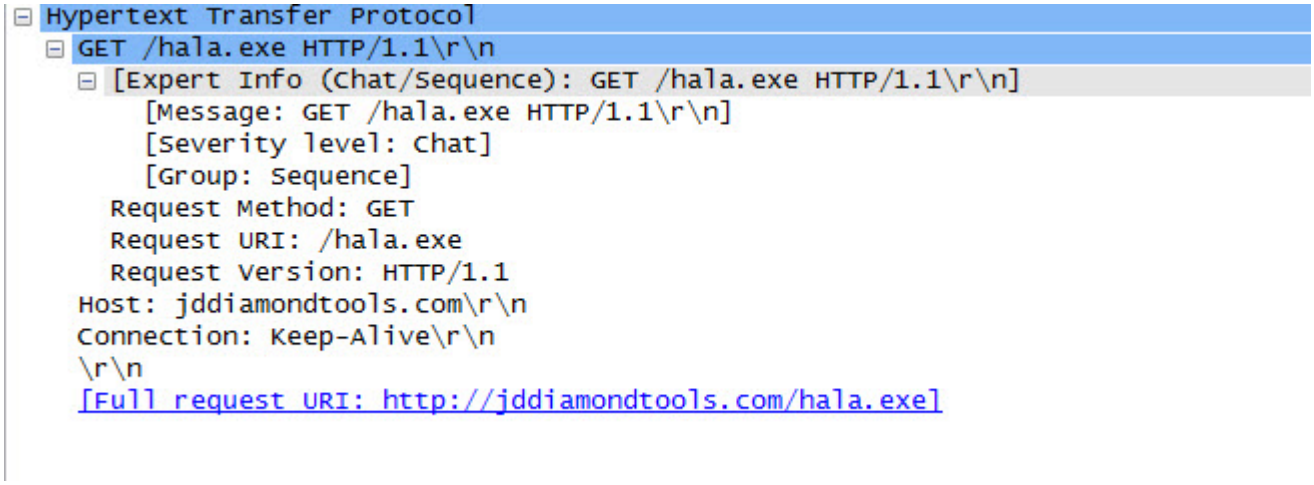
Örneğin elimizde Microsoft Office 2003 ile oluşturulduğunu düşündüğümüz yukarıdaki gibi şüpheli bir ofis dosyası var ise bu araca parametre olarak info komutunu vererek aracın bizim için dosyayı analiz etmesini ve makro kodunu çıkartmasını sağlayabiliyoruz. Eğer elimizdeki ofis dosyası Microsoft Office 2007 ve sonrası ile oluşturulmuş ise bu defa inflate komutunu kullanarak (aslında ofis dosyasının uzantısını .zip olarak değiştirip winzip/winrar ile açmaktan pek farkı yok) ofis dosyasını açmasını ve içinde yer alan makro kodunu tekrar info komutu ile çıkartmasını sağlayabiliyoruz.


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



Ortaya çıkan makro kodunu analiz ettiğimiz zaman, kullanılan APIler'den de yola çıkarak bunun RAT türü zararlı yazılım indiren bir indirici (downloader) olduğunu rahatlıkla görebiliyoruz.



Bu yazının şüphelendiğiniz ofis dosyalarını analiz etmenizde siz yol göstermesi ümidiyle, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.