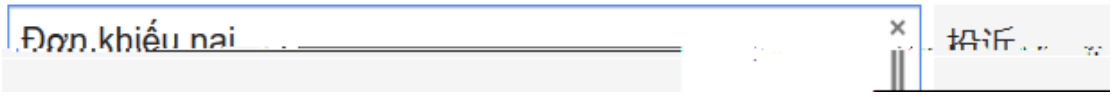
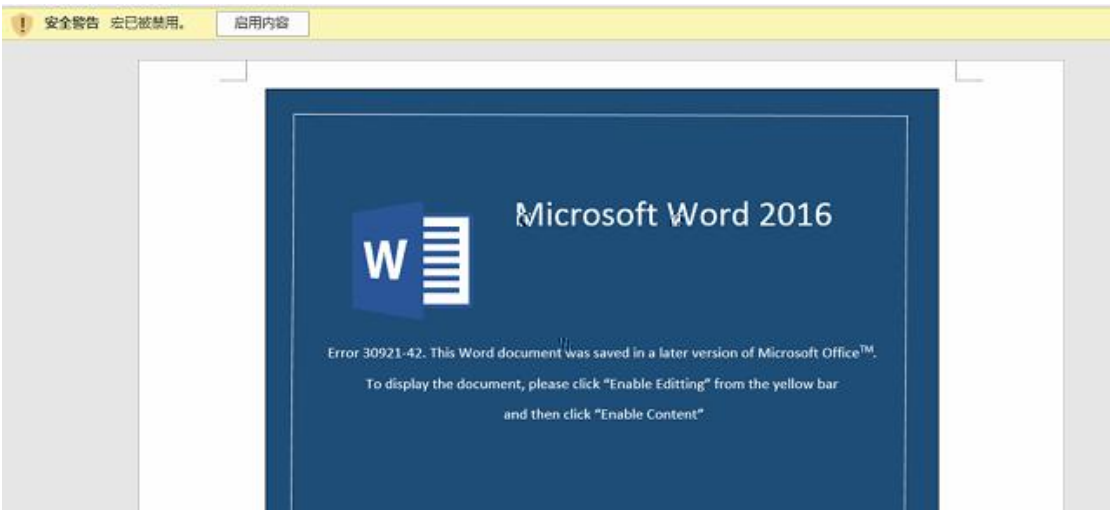
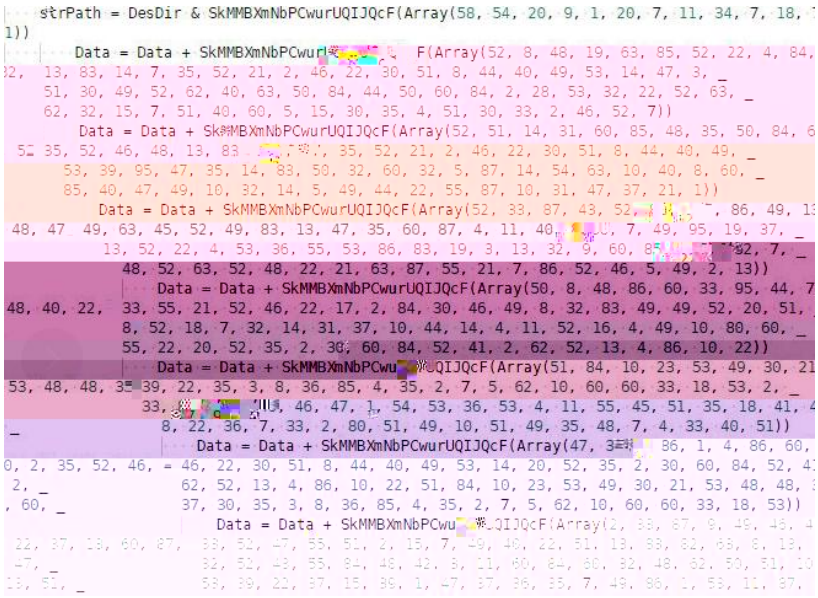
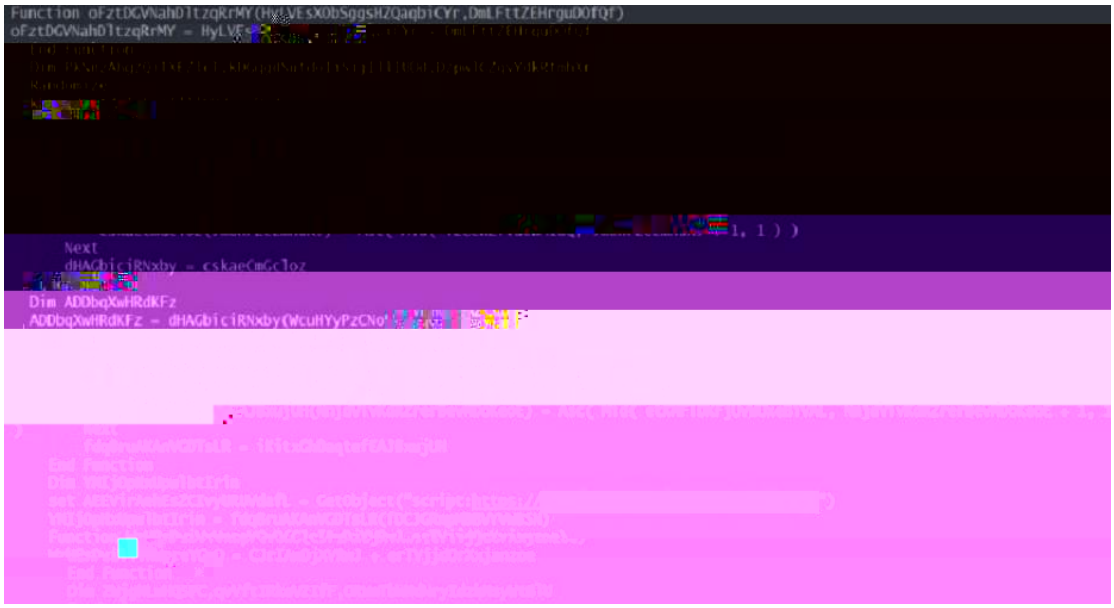
u n i “ ”



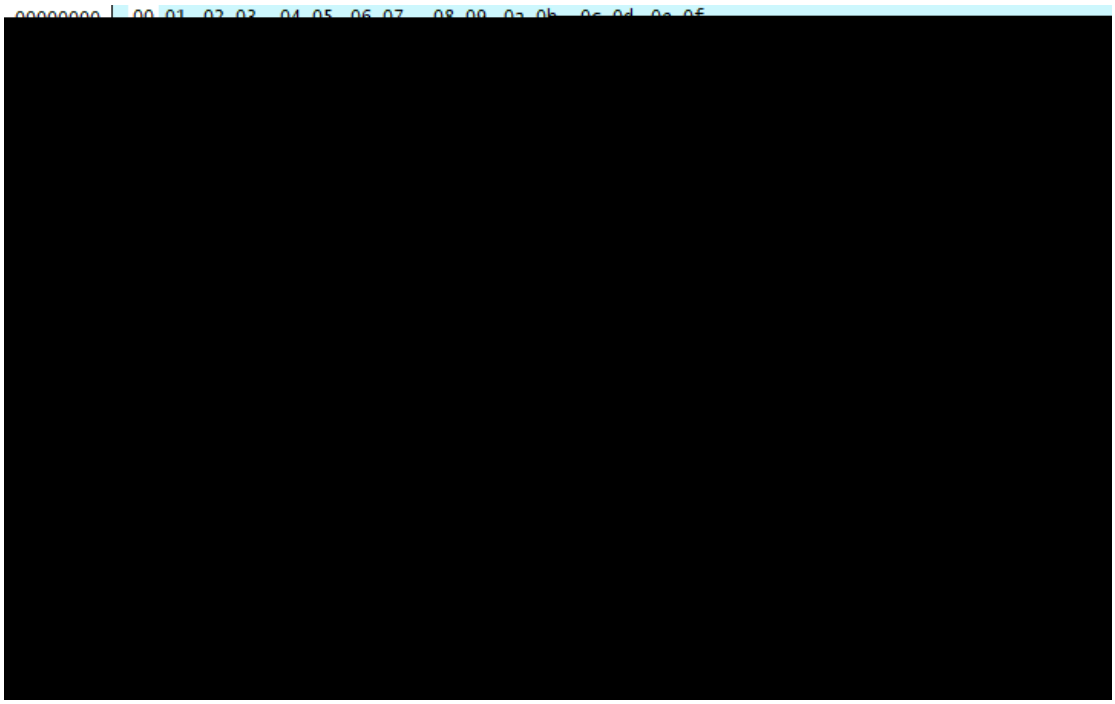

安全警告 宏已被禁用。
启用内容
Microsoft Word 2016
Error 30921-42. This Word document was saved in a later version of Microsoft Office™.
To display the document, please click "Enable Editting" from the yellow bar
and then click "Enable Content"

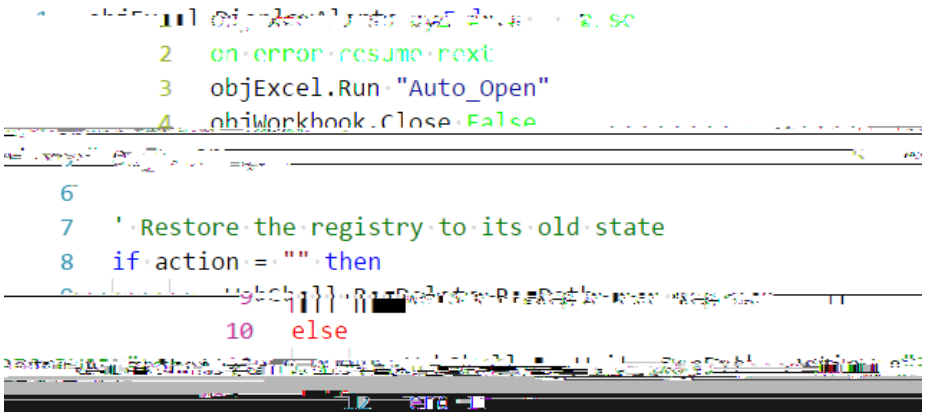


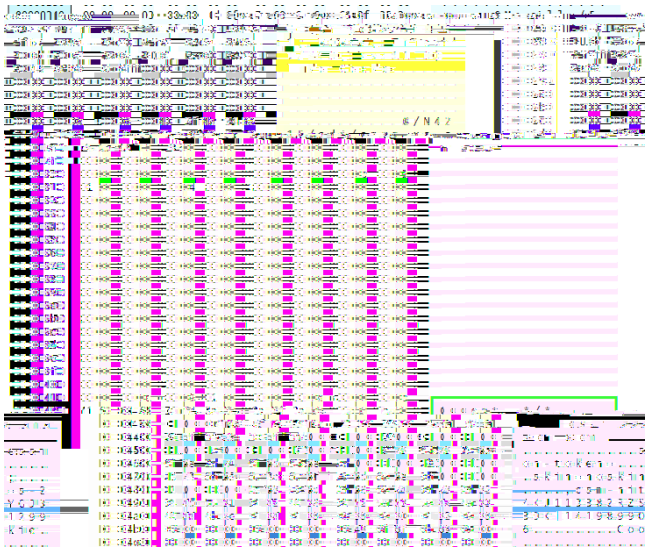


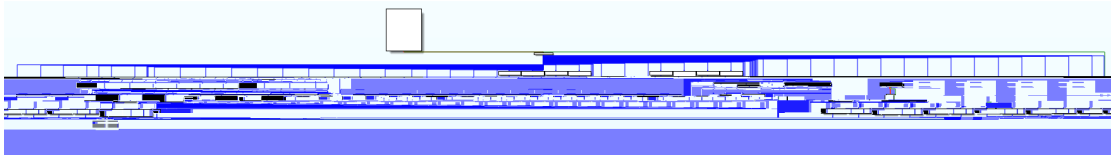


VBS Loader




on error resume next
objExcel.Run "Auto_Open"
objWorkbook.Close False
' Restore the registry to its old state
if action = "" then
else

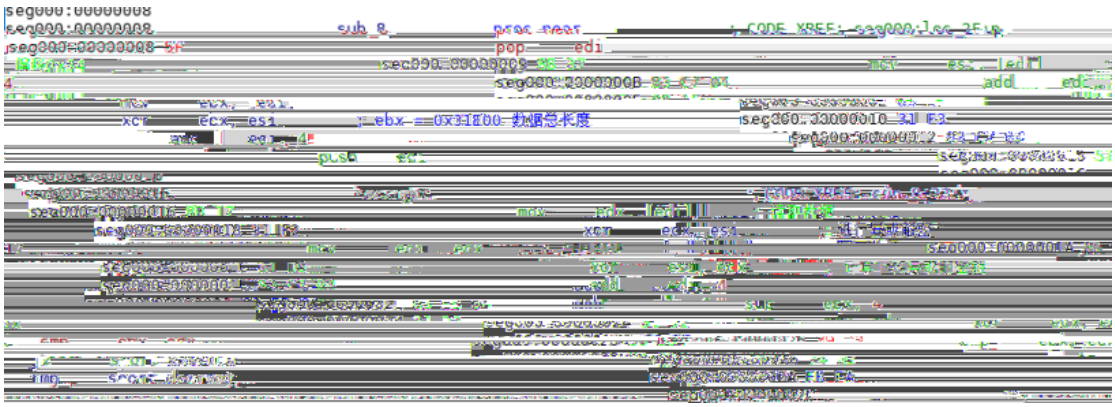


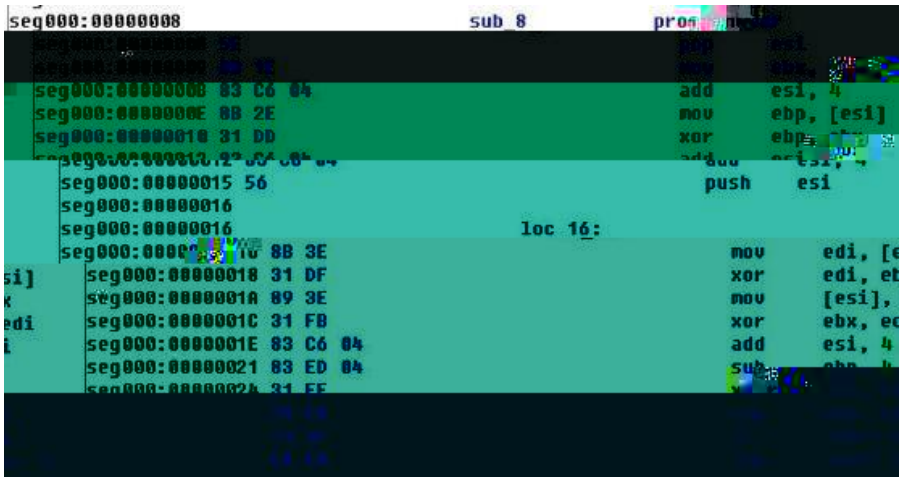


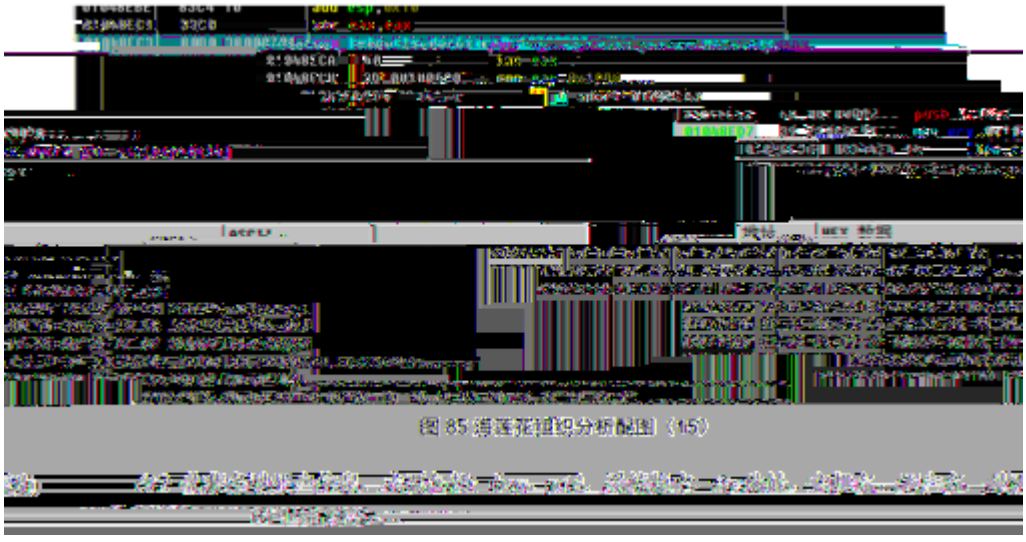
```
{
  int v3; // edi

  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;
```

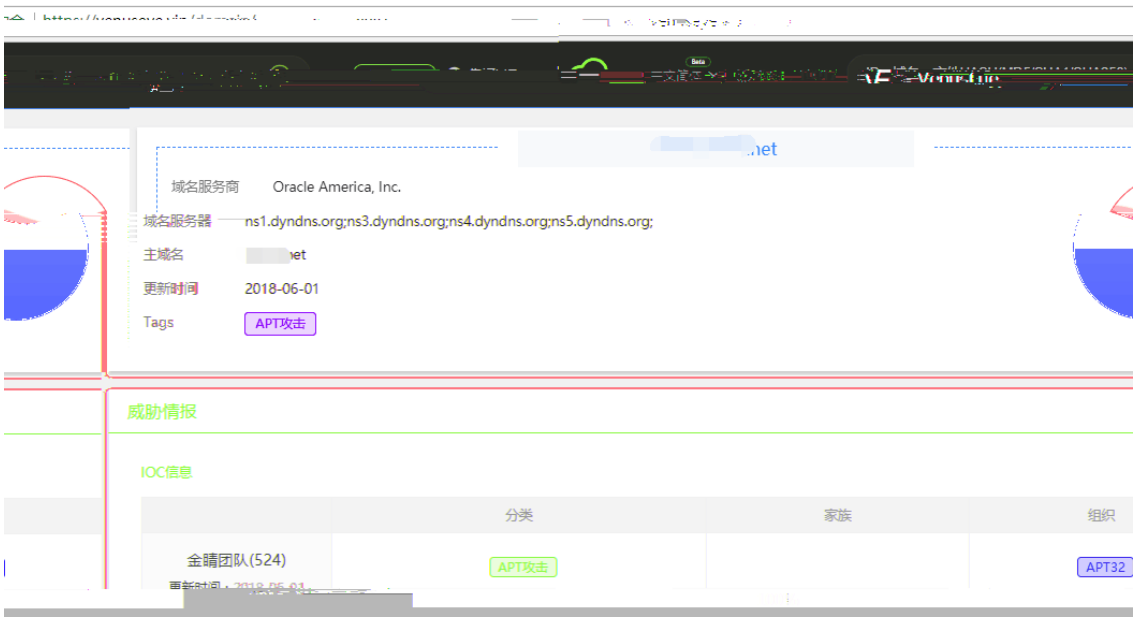
Shellcode




seg000:00000008 sub_8 proc
seg000:0000000B 83 C6 04 add esi, 4
seg000:0000000E 8B 2E mov ebp, [esi]
seg000:00000010 31 DD xor
seg000:00000015 56 push esi
seg000:00000016
seg000:00000016 loc_16:
seg000:00000018 31 DF xor edi,
seg000:0000001A 89 3E mov [esi],
seg000:0000001C 31 FB xor ebx,
seg000:0000001E 83 C6 04 add esi, 4
seg000:00000021 83 ED 04




GET /s/ref=nb_sb_noss_1/167-3294888-0262948/field-keywords=books HTTP/1.1
Host: www.amazon.com
Accept: */*


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
更新时间 2018-06-01
Tags APT攻击
威胁情报
IOC信息
分类
家族
组织
金睛团队(524)
APT攻击
APT32



Venuseye www.venuseye.com.cn