天融信 TOPSEC

Darkside 勒索病毒样本分析

目录

一、 概述

6 月 1 日，从互联网中得到病毒样本，该样本为带壳的程序，启动后，通过解压的方式获取到配置信息，按照配置信息，进行相应的处理，删除回收站内的文件，在 local 文件夹下释放勒索图标，获取主机信息，拼接后向黑客后台以 post 方式发送，读取主机的 Guid，计算出勒索 ID，与勒索信的名字进行拼接，根据配置信息，对相应的目录内文件进行加密，加密后释放勒索信，删除卷影文件。

二、 程序逆向

用侦壳软件检测，使用 upx 壳，如下图所示：

脱壳后确认为 delphi，如下图所示：

静态分析，为了躲避分析，使用动态加载 API，找到回收站路径，清理回收站文件

```
67            else
68            {
69              dword_410E1A(v17);                // 找到回收站路径，将回收站里的文件清除
70            }
71          }
```

动态解密配置文件

```
sub_401472(&byte_4107E0, (_OWORD *)(v5 + 32), 0x18u);// 解密配置文件
if ( byte_4107EB )                              // $recycle.bin 等
{
  v6 = sub_402BFD(v5 + 56);
  dword_4108F8 = dword_410D56(dword_410A9E, 8, v6, a2, v21, v22);
  sub_401472((_OWORD *)dword_4108F8, (_OWORD *)(v5 + 56), v6);
}
if ( byte_4107EC )                              // autorun.inf 等
{
  v7 = sub_402BFD(v5 + 2056);
  dword_4108FC = dword_410D56(dword_410A9E, 8, v7, v23, v24, v25);
  sub_401472((_OWORD *)dword_4108FC, (_OWORD *)(v5 + 2056), v7);
}
if ( byte_4107ED )                              // 386等
{
  v8 = sub_402BFD(v5 + 4056);
  dword_410900 = dword_410D56(dword_410A9E, 8, v8, v26, v27, v28);
  sub_401472((_OWORD *)dword_410900, (_OWORD *)(v5 + 4056), v8);
}
if ( byte_4107EE )                              // backup
{
  v9 = sub_402BFD(v5 + 6056);
  dword_410904 = dword_410D56(dword_410A9E, 8, v9, v29, v30, v31);
  sub_401472((_OWORD *)dword_410904, (_OWORD *)(v5 + 6056), v9);
}
if ( byte_4107EF )                              // sql  sqlite
{
  v10 = sub_402BFD(v5 + 8056);
  dword_410908 = dword_410D56(dword_410A9E, 8, v10, v32, v33, v34);
  sub_401472((_OWORD *)dword_410908, (_OWORD *)(v5 + 8056), v10);
}
if ( byte_4107E1 )                              // vmcompute.exe 等
{
  v11 = sub_402BFD(v5 + 10056);
  dword_41090C = dword_410D56(dword_410A9E, 8, v11, v35, v36, v37);
  sub_401472((_OWORD *)dword_41090C, (_OWORD *)(v5 + 10056), v11);
}
if ( byte_4107F0 )                              // sql 等
{
  v12 = sub_402BFD(v5 + 12056);
  dword_410910 = dword_410D56(dword_410A9E, 8, v12, v38, v39, v40);
  sub_401472((_OWORD *)dword_410910, (_OWORD *)(v5 + 12056), v12);
}
if ( byte_4107F1 )                              // vss  等
```

```
if ( byte_4107E1 )                              // vmcompute.exe 等
{
  v11 = sub_402BFD(v5 + 10056);
  dword_41090C = dword_410D56(dword_410A9E, 8, v11, v35, v36, v37);
  sub_401472((_OWORD *)dword_41090C, (_OWORD *)(v5 + 10056), v11);
}
if ( byte_4107F0 )                              // sql 等
{
  v12 = sub_402BFD(v5 + 12056);
  dword_410910 = dword_410D56(dword_410A9E, 8, v12, v38, v39, v40);
  sub_401472((_OWORD *)dword_410910, (_OWORD *)(v5 + 12056), v12);
}
if ( byte_4107F1 )                              // vss  等
{
  v13 = sub_402BFD(v5 + 14056);
  dword_410914 = dword_410D56(dword_410A9E, 8, v13, v41, v42, v43);
  sub_401472((_OWORD *)dword_410914, (_OWORD *)(v5 + 14056), v13);
}
if ( byte_4107F7 )                              // catsdegree.com 、temisleyes.com
{
  v14 = sub_402BFD(v5 + 16056);
  dword_410918 = dword_410D56(dword_410A9E, 8, v14, v44, v45, v46);
  sub_401472((_OWORD *)dword_410918, (_OWORD *)(v5 + 16056), v14);
}
if ( byte_4107F2 )                              // All  of  your  files  are  encrypted!
                                                // Find  %s  and  Follow  Instructions!
{
  v15 = sub_402BFD(v5 + 17056);
  dword_41091C = dword_410D56(dword_410A9E, 8, v15, v47, v48, v49);
  sub_401472((_OWORD *)dword_41091C, (_OWORD *)(v5 + 17056), v15);
}
if ( byte_4107F3 )                              // Welcome to DarkSide 等
{
  v16 = sub_402BFD(v5 + 19056);
  dword_410920 = dword_410D56(dword_410A9E, 8, v16, v50, v51, v52);
  sub_401472((_OWORD *)dword_410920, (_OWORD *)(v5 + 19056), v16);
```

```
00402918   74 2F          je short <111111.loc_402949>
0040291A   8D43 38        lea eax,dword ptr ds:[ebx+0x38]
0040291D   50             push eax
0040291E   E8 DA020000    call <111111.sub_402BFD>
跳转未实现
00402949=<111111.loc_402949>
```

地址	HEX 数据																ASCII
005FA198	24	00	72	00	65	00	63	00	79	00	63	00	6C	00	65	00	$.r.e.c.y.c.l.e.
005FA1A8	2E	00	62	00	69	00	6E	00	00	00	63	00	6F	00	6E	00	..b.i.n...c.o.n.
005FA1B8	66	00	69	00	67	00	2E	00	6D	00	73	00	69	00	00	00	f.i.g...m.s.i...
005FA1C8	24	00	77	00	69	00	6E	00	64	00	6F	00	77	00	73	00	$.w.i.n.d.o.w.s.
005FA1D8	2E	00	7E	00	62	00	74	00	00	00	24	00	77	00	69	00	..~.b.t...$.w.i.
005FA1E8	6E	00	64	00	6F	00	77	00	73	00	2E	00	7E	00	77	00	n.d.o.w.s...~.w.
005FA1F8	73	00	00	00	77	00	69	00	6E	00	64	00	6F	00	77	00	s...w.i.n.d.o.w.
005FA208	73	00	00	00	61	00	70	00	70	00	64	00	61	00	74	00	s...a.p.p.d.a.t.
005FA218	61	00	00	00	61	00	70	00	70	00	6C	00	69	00	63	00	a...a.p.p.l.i.c.
005FA228	61	00	74	00	69	00	6F	00	6E	00	20	00	64	00	61	00	a.t.i.o.n. .d.a.
005FA238	74	00	61	00	00	00	62	00	6F	00	6F	00	74	00	00	00	t.a...b.o.o.t...
005FA248	67	00	6F	00	6F	00	67	00	6C	00	65	00	00	00	6D	00	g.o.o.g.l.e...m.
005FA258	6F	00	7A	00	69	00	6C	00	6C	00	61	00	00	00	70	00	o.z.i.l.l.a...p.
005FA268	72	00	6F	00	67	00	72	00	61	00	6D	00	20	00	66	00	r.o.g.r.a.m. .f.
005FA278	69	00	6C	00	65	00	73	00	00	00	70	00	72	00	6F	00	i.l.e.s...p.r.o.

不加密以下文件夹、文件、后缀名的文件

```
$recycle.bin
config.msi
$windows.~bt
$windows.~ws
windows
appdata
application
data
boot
google
mozilla
program
files
program
files
(x86)
programdata
system
volume
information
tor
browser
windows.old
intel
msocache
perflogs
x64dbg
public
all
users
default
```

```
autorun.inf
boot.ini
bootfont.bin
bootsect.bak
desktop.ini
iconcache.db
ntldr
ntuser.dat
ntuser.dat.log
ntuser.ini
thumbs.db
```

```
386 adv
ani bat
bin cab
cmd com
cpl cur
deskthemepack diagcab
diagcfg diagpkg
dll drv
exe hlp
icl icns
ico ics
idx ldf
lnk mod
mpa msc
msp msstyles
msu nls
nomedia ocx
prf psl
rom rtp
scr shs
spl sys
theme themepack
wpx lock
key hta
msi pdb
```

查找并杀死以下服务和进程

```
sql
oracle
ocssd
dbsnmp
synctime
agntsvc
isqlplussvc
xfssvccon
mydesktopservice
ocautoupds
encsvc
firefox
tbirdconfig
mydesktopqos
ocomm
dbeng50
sqbcoreservice
excel
infopath
msaccess
mspub
onenote
outlook
powerpnt
steam
thebat
thunderbird
visio
winword
wordpad
notepad
```

```
vss
sql
svc$
memtas
mepocs
sophos
veeam
backup
GxVss
GxBlr
GxFWD
GxCVD
GxCIMgr
```

访问黑客后台

```
if ( byte_4107F7 )                              // catsdegree.com 、temisleyes.com
{
  v14 = sub_402BFD(v5 + 16056);
  dword_410918 = dword_410D56(dword_410A9E, 8, v14, v44, v45, v46);
  sub_401472((_OWORD *)dword_410918, (_OWORD *)(v5 + 16056), v14);
}
```

勒索信内容

```
00402B7E   74 58          je short <111111.loc_402BD8>
00402B80   8D83 704A0000  lea eax,dword ptr ds:[ebx+0x4A70]
00402B86   50             push eax
00402B87   E8 71000000    call <111111.sub_402BFD>
00402B8C   8BF0           mov esi,eax
00402B8E   56             push esi
00402B8F   6A 08          push 0x8
地址=005FEBD0, (ASCII "----------- [ Welcome to DarkSide ] ------------->
eax=005FEBD0, (ASCII "----------- [ Welcome to DarkSide ] ------------->
```

地址	HEX 数据																ASCII
005FEBD0	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	20	5B	20	57	65	----------- [We
005FEBE0	6C	63	6F	6D	65	20	74	6F	20	44	61	72	6B	53	69	64	lcome to DarkSid
005FEBF0	65	20	5D	20	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	e] ------------
005FEC00	2D	3E	20	0D	0A	20	20	0D	0A	20	57	68	61	74	20	68	-> .. .. What h
005FEC10	61	70	70	65	6E	64	3F	20	0D	0A	20	2D	2D	2D	2D	2D	append? .. -----
005FEC20	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	----------------
005FEC30	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	----------------
005FEC40	2D	2D	2D	2D	2D	2D	2D	2D	2D	20	0D	0A	20	59	6F	75	---------- .. You
005FEC50	72	20	63	6F	6D	70	75	74	65	72	73	20	61	6E	64	20	r computers and
005FEC60	73	65	72	76	65	72	73	20	61	72	65	20	65	6E	63	72	servers are encr

```
----------- [ Welcome to DarkSide ] ------------->

What happend?
---------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
---------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2.onion/OBB5DDMR8RB9DI2RYYF376YGBJAV2J4F2NXFEWPBSXY709MAA0MY7PMBBQJ0HVG3

When you open our website, put the following data in the input form:
Key:


5l5BZPnhuDEYAVqJR4MgValoWwML2OjDOtYwubDXeXGefcJDd4otfGdb9pJPrHW7Rt0XqdwabTWl9I5xhiHBsW6mg5BoqR4M2LZ0TIlhN4ifY7RVgRakjxxhhyImncWtgNb8LWtJlhn6cwtDLl
sIjq0wAn8s7YsdzgTPPreHXEyFiFHlozVIpZXVlmO5QXMZul6DNkFcXVIfdw5gPeSYjd3VAa7VlIH8IXgwCuza7YprCeDIOmvRqYKljBH4s4nn0VyEHnWRndP7jNNUmat6FMhNzeKnLYGbMDRw
mZR6iFdFX0Y3lhEWenDamVRchRSE5YwiL9LqTfkrnrswflssAB0SOcodZXRxG5HNItcitj3ZalNzC5fmBpdKN4jV01hMBG98ZEN8HMKeOdVxKtbAZP86K9IfBy8QcNrWLQ2hAeup6DD6KsG8R0
Jj8czKTu4MDlGaxQMtPSycA0B6IzpPVV0Tbn9yWIIFH6y4mir7lzDWbcPH3p5Hnr80gTnOFHXGzkGfrdylbjn5H99zniLFFjchV8EEPMtgG2PwKF7NVQ9dTdlMBHWQpGc

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!
```

readme 文件名

地址	HEX 数据																ASCII
0040B5AC	52	00	45	00	41	00	44	00	4D	00	45	00	25	00	73	00	R.E.A.D.M.E.%.s.
0040B5BC	2E	00	54	00	58	00	54	00	00	00	0E	00	00	00	34	84	..T.X.T...▮...4Q

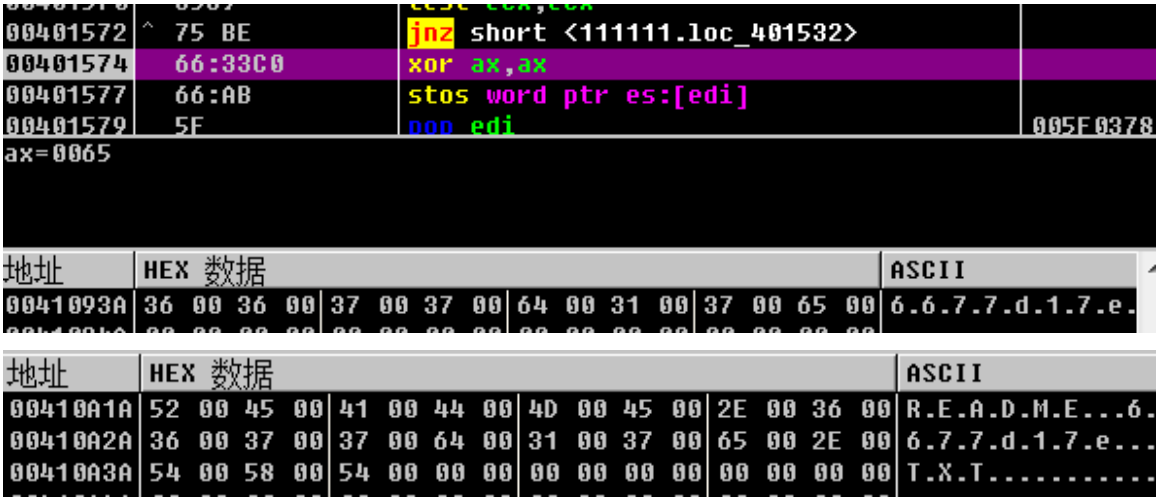
从注册表获取当前主机的 GUID，得出勒索 ID

```
0018FE6C   005F0378  UNICODE "MachineGuid"
0018FE70   005F1948  UNICODE "SOFTWARE\Microsoft\Cryptography"
```

```
10  HIBYTE(v6) = 0;
11  do
12  {
13    v7 = *a1++;
14    v8 = v7;
15    LOBYTE(v6) = v7 >> 4;
16    v9 = v8 & 0xF;
17    if ( (unsigned __int8)v6 <= 9u )
18      LOBYTE(v6) = v6 + 48;
19    if ( (unsigned __int8)v6 >= 0xAu && (unsigned __int8)v6 <= 0xFu )
20      LOBYTE(v6) = v6 + 87;
21    if ( v9 <= 9u )
22      v9 += 48;
23    if ( v9 >= 0xAu && v9 <= 0xFu )
24      v9 += 87;
25    *a3 = v6;
26    v10 = a3 + 1;
27    LOBYTE(v6) = v9;
28    *v10 = v6;
29    a3 = v10 + 1;
30    --a2;
31  }
32  while ( a2 );
33  result = 0;
34  *a3 = 0;
35  return result;                                // 从注册表获取Guid开始计算，得到最终的勒索ID
36}
```

```
strcpy(v4, "kernel32");
strcpy(v5, "LoadLibraryA");
strcpy(v6, "LoadLibraryExA");
strcpy(v2, "VirtualAlloc");
strcpy(v3, "VirtualProtect");                   // 将相关函数填充
v7 = (*(int (__stdcall **)(char *))a1)(v4);
*(_DWORD *)(a1 + 8) = (*(int (__stdcall **)(int, char *))(a1 + 4))(v7, v5);
*(_DWORD *)(a1 + 12) = (*(int (__stdcall **)(int, char *))(a1 + 4))(v7, v6);
*(_DWORD *)(a1 + 16) = (*(int (__stdcall **)(int, char *))(a1 + 4))(v7, v2);
*(_DWORD *)(a1 + 20) = (*(int (__stdcall **)(int, char *))(a1 + 4))(v7, v3);
memset(v4, 0, 9u);
memset(v5, 0, 0xDu);
memset(v6, 0, 0xFu);
memset(v2, 0, 0xDu);
result = 0;
memset(v3, 0, 0xFu);
return result;
```

生成勒索 ID，将之前解密出的文件名进行拼接，得到完成的勒索信文件名

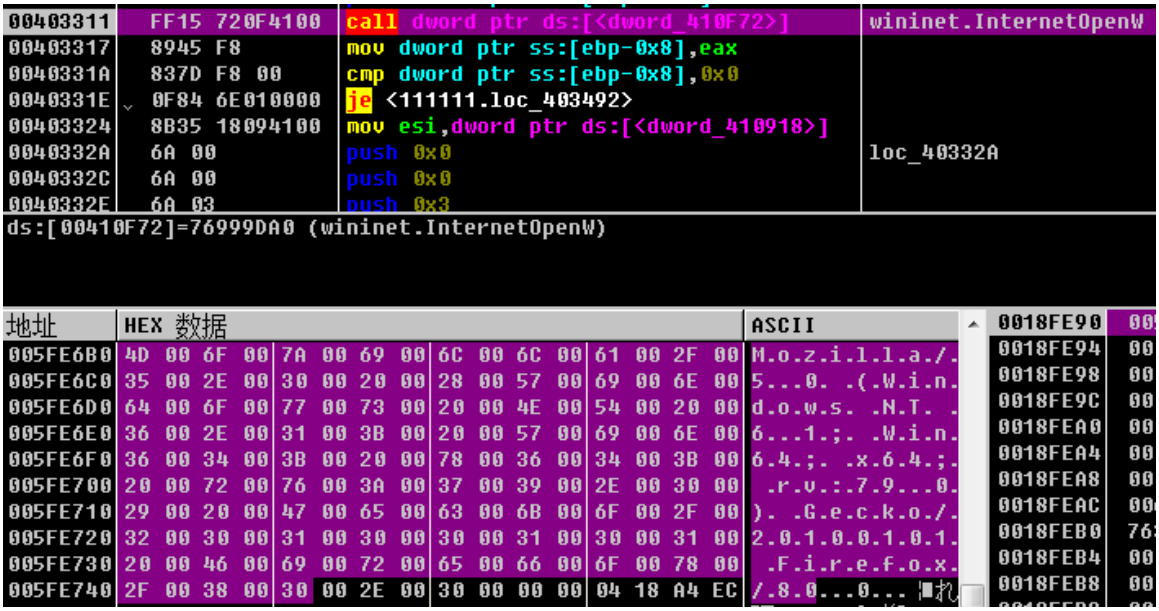


获取当前主机信息

```
  v3 = a2 / 0xFF;
  v4 = a2 % 0xFF;
  if ( a2 / 0xFF )
  {
    v5 = a2 / 0xFF;
    do
    {
      LOBYTE(v3) = sub_4017AA(a1, 255);
      a1 += 255;
      --v5;
    }
    while ( v5 );
  }
  if ( v4 )
    LOBYTE(v3) = sub_4017AA(a1, v4);
  return v3;                                    // 提取受害者信息
}
```

```
"os":{

"lang":"zh-CN",

"username":"sjz",

"hostname":"SANDBOX-PC",

"domain":"WORKGROUP",

"os_type":"windows",

"os_version":"Windows7Ultimate",

"os_arch":"x64",

"disks":"C:37/59",

"id":"9415d568434a3042c67a"

}
```

伪装浏览器头，向黑客服务器发送受害者信息



调用加密模块进行加密文件

```
    if ( v2 )
    {
      switch ( v2 )
      {
        case 1:                                         // 加密模块
          sub_40209C(v8 + 13, v8 + 65, v8 + 65, v7);
          if ( v1[9] )
          {
            *(_QWORD *)(v1 + 5) += 0x80000i64;
            --v1[9];
            v1[12] = 0;
          }
          else
          {
            v4 = *(_QWORD *)(v1 + 7);
            if ( v4 == -1 )
            {
              v1[12] = 2;
            }
            else
            {
              *(_QWORD *)(v1 + 5) += v4;
              v1[9] = v1[10];
              v1[12] = 0;
            }
          }
```

附录

文中涉及样本 SHA256：

4d9432e8a0ceb64c34b13d550251b8d9478ca784e50105dc0d729490fb861d1a