WhiteBlackCrypt 勒索病毒样本分析

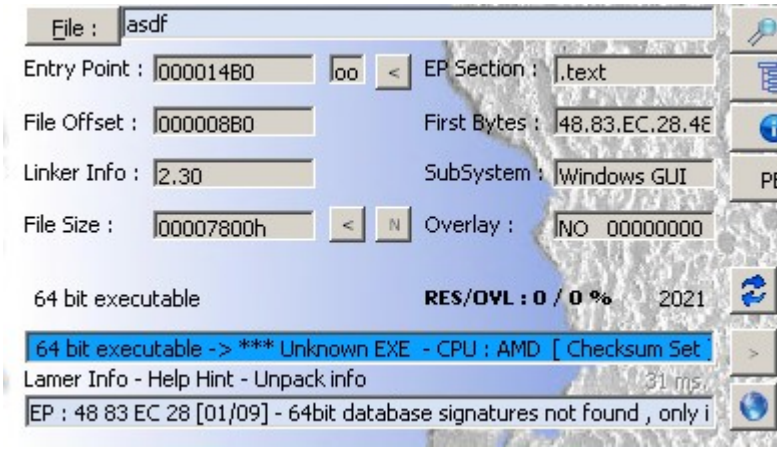
病毒概述

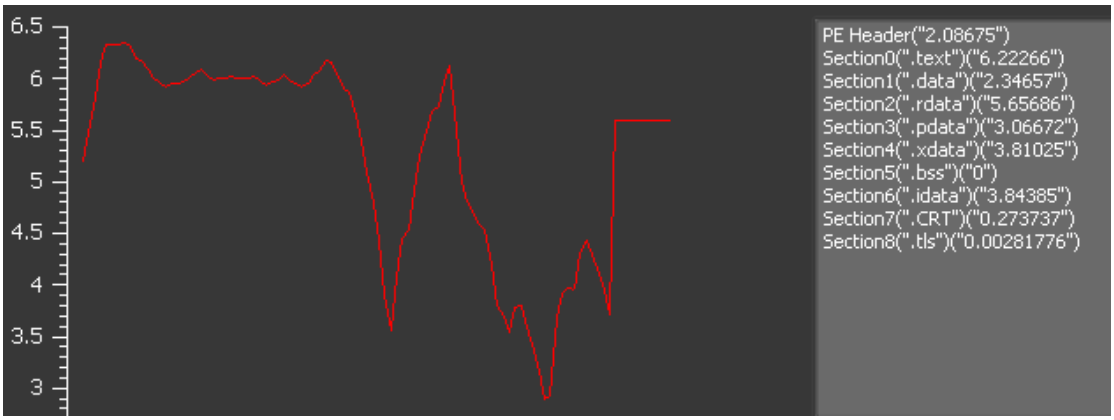
近日，天融信 EDR 安全团队捕获病毒样本。黑客利用社工方式诱骗受害人点击下载文件，点击文件后，获取操作系统信息，将自身复制到系统目录，在注册表中添加开机自启动，采用 aes 方式进行加密，根据名单中的内容，对指定的文件进行加密，加密后，弹窗提示勒索信息。

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，没有壳，查看文件熵值，判断可能存在加密数据





读取系统信息，整理后如下

```
ALLUSERSPROFILE=C:\\ProgramData
APPDATA=C:\\Users\\sjz\\AppData\\Roaming
CLIENTNAME=DESKTOP-T1MJ91T
CommonProgramFiles=C:\\Program Files\\Common Files
CommonProgramFiles(x86)=C:\\Program Files (x86)\\Common Files
CommonProgramW6432=C:\\Program Files\\Common Files
COMPUTERNAME=SANDBOX-PC
ComSpec=C:\\Windows\\system32\\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\\Users\\sjz
LOCALAPPDATA=C:\\Users\\sjz\\AppData\\Local
LOGONSERVER=\\\\SANDBOX-PC
NUMBER_OF_PROCESSORS=4
OS=Windows_NT
Path=C:\\Windows\\system32;C:\\Windows;C:\\Windows\\System32\\Wbem;C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\;C:\\Users\\sjz\\Desktop
xE2\xD7\xA8\xD3\xC3\xB0\xE6Ollydbg\\\xCE\xE1\xB0\xAE\xC6\xC6\xBD\xE2\xD7\xA8\xD3\xC3\xB0\xE6Ollydbg
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 63 Stepping 2, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=3f02
ProgramData=C:\\ProgramData
ProgramFiles=C:\\Program Files
ProgramFiles(x86)=C:\\Program Files (x86)
ProgramW6432=C:\\Program Files
PSModulePath=C:\\Windows\\system32\\WindowsPowerShell\\v1.0\\Modules\\
PUBLIC=C:\\Users\\Public
SESSIONNAME=RDP-Tcp#0
SYMSRV_DBGOUT=1
SystemDrive=C:
SystemRoot=C:\\Windows
TEMP=C:\\Users\\sjz\\AppData\\Local\\Temp
TMP=C:\\Users\\sjz\\AppData\\Local\\Temp
USERDOMAIN=sandbox-PC
USERNAME=sjz
USERPROFILE=C:\\Users\\sjz
windir=C:\\Windows
```

将自身复制到系统目录

```
00000000004020F0   75 3A           jnz asdf.40212C
00000000004020F2   48 8D 05 BD 41 00 00   lea rax,qword ptr ds:[4062B6]      4062B6:"C:\\ProgramData\\CheckServiceD.exe"
00000000004020F9   48 8B 4C 24 78   mov rcx,qword ptr ss:[rsp+78]
00000000004020FE   41 B9 01 00 00 00   mov r9d,1
0000000000402104   45 31 C0        xor r8d,r8d
```

在注册表中添加开机自启动

```
0000000000402077   48 C7 C1 01 00 00 80   mov rcx,FFFFFFFF80000001
000000000040207E   48 89 44 24 30         mov qword ptr ss:[rsp+30],rax
0000000000402083   48 8D 15 D0 41 00 00   lea rdx,qword ptr ds:[40625A]      40625A:"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
000000000040208A   48 C7 44 24 20 00 00 00   mov qword ptr ss:[rsp+20],0
0000000000402093   FF 15 FF 82 00 00   call qword ptr ds:[<&RegGetValueA>]
0000000000402099   80 BC 24 B0 01 00 00 00   cmp byte ptr ss:[rsp+1B0],0
00000000004020A1   48 8B 35 B8 84 00 00   mov rsi,qword ptr ds:[<&_time64>]
```

调用 aes 算法加密文件

```
000000000040159C   44 0F B6 49 0C   movzx r9d,byte ptr ds:[rcx+C]      使用aes算法
00000000004015A1   44 0F B6 41 0D   movzx r8d,byte ptr ds:[rcx+D]
00000000004015A6   0F B6 51 0E      movzx edx,byte ptr ds:[rcx+E]
00000000004015AA   0F B6 41 0F      movzx eax,byte ptr ds:[rcx+F]
00000000004015AE   75 1E            jnz checkserviced.4015CE
00000000004015B0   43 8A 34 03      mov sil,byte ptr ds:[r11+r8]
00000000004015B4   45 8A 04 13      mov r8b,byte ptr ds:[r11+rdx]
00000000004015B8   41 8A 14 03      mov dl,byte ptr ds:[r11+rax]
00000000004015BC   43 8A 04 0B      mov al,byte ptr ds:[r11+r9]
```

遍历读取文件，根据列表中的内容排查，如果在列表中，那么加密

```
0000000000401DD6    48 83 EC 28              sub rsp,28
0000000000401DDA    48 8D 2D 5F 32 00 00     lea rbp,qword ptr ds:[405040]
0000000000401DE1    31 DB                    xor ebx,ebx
```

!ed6335fb5dda08f57f00e9dc809d4f138428\asdf.i64

Help

No debugger

External symbol Lumina function

udocode-C | Pseudocode-B | Pseudocode-A | Strings window

```
00405028                align 20h
00405040 off_405040     dq offset aDoc          ; DATA XREF: sub_401DD2+8↑o
00405040                                        ; ".DOC"
00405048                dq offset aDocx         ; ".DOCX"
00405050                dq offset aXls          ; ".XLS"
00405058                dq offset aXlsx         ; ".XLSX"
00405060                dq offset aPpt          ; ".PPT"
00405068                dq offset aPptx         ; ".PPTX"
00405070                dq offset aPst          ; ".PST"
00405078                dq offset aOst          ; ".OST"
00405080                dq offset aMsg          ; ".MSG"
00405088                dq offset aEml          ; ".EML"
00405090                dq offset aVsd          ; ".VSD"
00405098                dq offset aVsdx         ; ".VSDX"
004050A0                dq offset aTxt          ; ".TXT"
004050A8                dq offset aCsv          ; ".CSV"
004050B0                dq offset aRtf          ; ".RTF"
004050B8                dq offset aWks          ; ".WKS"
004050C0                dq offset aWk1          ; ".WK1"
004050C8                dq offset aPdf          ; ".PDF"
004050D0                dq offset aDwg          ; ".DWG"
004050D8                dq offset aOnetoc2      ; ".ONETOC2"
004050E0                dq offset aSnt          ; ".SNT"
004050E8                dq offset aJpeg         ; ".JPEG"
004050F0                dq offset aJpg          ; ".JPG"
004050F8                dq offset aDocb         ; ".DOCB"
00405100                dq offset aDocm         ; ".DOCM"
00405108                dq offset aDot          ; ".DOT"
00405110                dq offset aDotm         ; ".DOTM"
00405118                dq offset aDotx         ; ".DOTX"
00405120                dq offset aXlsm         ; ".XLSM"
00405128                dq offset aXlsb         ; ".XLSB"
00405130                dq offset aXlw          ; ".XLW"
00405138                dq offset aXlt          ; ".XLT"
00405140                dq offset aXlm          ; ".XLM"
00405148                dq offset aXlc          ; ".XLC"
```

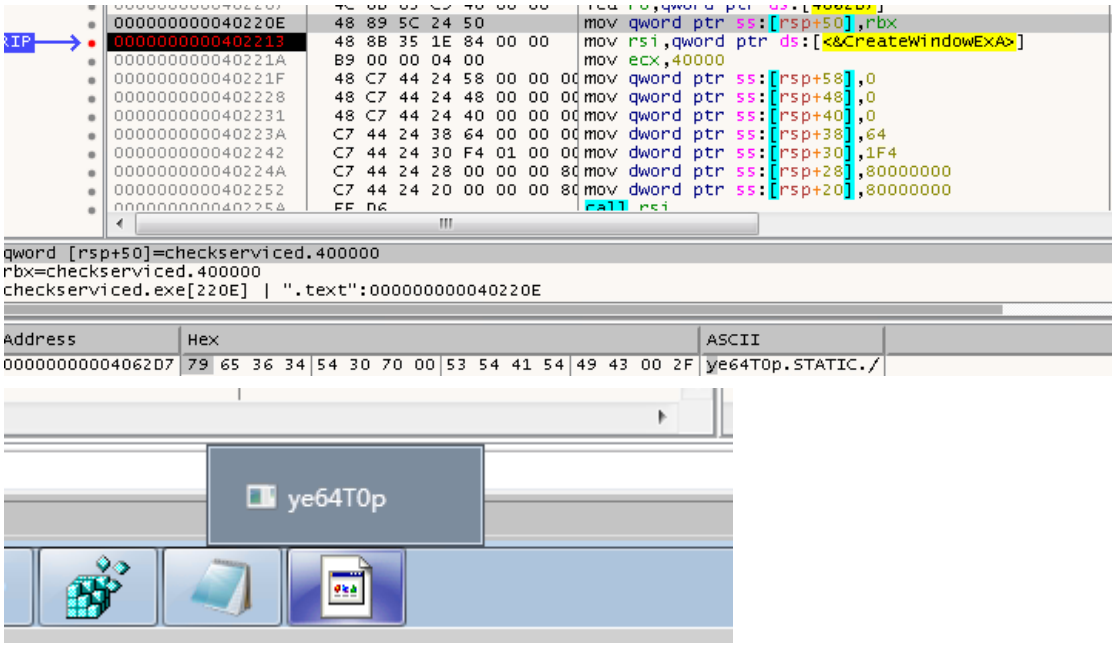
被加密的后缀名整理后如下

```
.DOC .DOCX .XLS .XLSX .PPT .PPTX .PST .OST .MSG .EML .VSD .VSDX .TXT .CSV .RTF .WKS .WK1 .PDF .DWG .ONETOC2 .SNT
.JPEG .JPG .DOCB .DOCM .DOT .DOTM .DOTX .XLSM .XLSB .XLW .XLT .XLM .XLC .XLTX .XLTM .PPTM .POT .PPS .PPSM .PPSX .PPAM
.POTX .POTM .EDB .HWP .602 .SXI .STI .SLDX .SLDM .VDI .VMDK .VMX .GPG .AES .ARC .PAQ .BZ2 .TBK .BAK .TAR .TGZ .GZ .7Z
.RAR .ZIP .BACKUP .ISO .VCD .BMP .PNG .GIF .RAW .CGM .TIF .TIFF .NEF .PSD .AI .SVG .DJVU .M4U .M3U .MID .WMA .FLV
.3G2 .MKV .3GP .MP4 .MOV .AVI .ASF .MPEG .VOB .MPG .WMV .FLA .SWF .WAV .MP3 .SH .CLASS .JAR .JAVA .RB .ASP .PHP .JSP
.BRD .SCH .DCH .DIP .PL .VB .VBS .PS1 .BAT .CMD .JS .ASM .H .PAS .CPP .C .CS .SUO .SLN .LDF .MDF .IBD .MYI .MYD .FRM
.ODB .DBF .DB .MDB .ACCDB .SQL .SQLITEDB .SQLITE3 .ASC .LAY6 .LAY .MML .SXM .OTG .ODG .UOP .STD .SXD .OTP .ODP .WB2
.SLK .DIF .STC .SXC .OTS .ODS .3DM .MAX .3DS .UOT .STW .SXW .OTT .ODT .PEM .P12 .CSR .CRT .KEY .PFX .DER .HTML .CSS
.PY .GO
```

勒索后缀名

```
call    malloc
mov     rdx, rbp        ; Source
mov     rcx, rax        ; Destination
call    strcpy
lea     rdx, Source     ; ".encrpt3d"
```

建立勒索界面，并且起名为 ye64T0p



勒索信内容如下

```
000000000040632C 21 57 41 52 4E 49 4E 47 21 0A 59 6F 75 72 20 66 !WARNING!.Your f
000000000040633C 69 6C 65 73 20 68 61 73 20 62 65 65 6E 20 45 4E iles has been EN
000000000040634C 43 52 59 50 54 45 44 21 20 4E 6F 77 2C 20 79 6F CRYPTED! Now, yo
000000000040635C 75 20 63 61 6E 74 20 61 63 63 65 73 73 20 74 68 u cant access th
000000000040636C 65 6D 2C 20 62 75 74 20 74 68 65 79 20 61 72 65 em, but they are
000000000040637C 20 6E 6F 74 20 64 65 6C 65 74 65 64 2E 20 57 65  not deleted. We
000000000040638C 20 6E 65 65 64 20 74 6F 20 67 65 74 20 31 30 20  need to get 10
000000000040639C 42 54 43 20 61 74 20 74 68 65 20 73 70 65 63 69 BTC at the speci
00000000004063AC 66 69 65 64 20 61 64 64 72 65 73 73 3A 0A 2D 2D fied address:.--
00000000004063BC 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D ----------------
00000000004063CC 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D ----------------
00000000004063DC 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D ----------------
00000000004063EC 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D ----------------
00000000004063FC 2D 2D 2D 2D 2D 2D 2D 0A 31 39 42 35 42 74 31 31 -------.19B5Bt11
000000000040640C 6F 55 71 59 6E 77 53 58 66 42 67 52 70 77 77 44 oUqYnwSXfBgRpwwD
000000000040641C 47 67 35 41 6A 69 72 62 6A 6E 0A 2D 2D 2D 2D 2D Gg5Ajirbjn.-----
000000000040642C 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D ----------------
```

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