Andromeda僵尸病毒样本分析

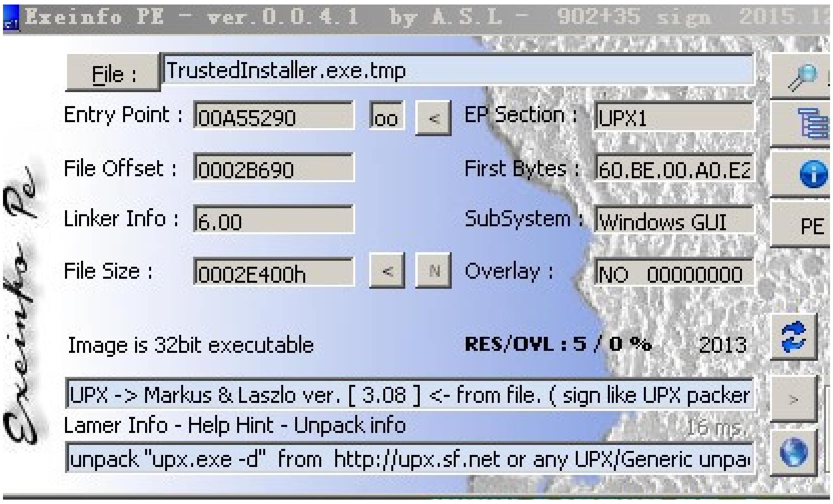
病毒概述

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，将自身设置为隐藏文件，把自身复制到指定的目录下，判断操作系统的位数，注入到相应的进程中，注册表设置开机自启动，根据名单内的地址向黑客后台发出连接请求。

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，发现是UPX壳


Exeinfo PE - ver.0.0.4.1 by A.S.L - 902+35 sign 2015.1

File : TrustedInstaller.exe.tmp

Entry Point : 00A55290 oo < EP Section : UPX1

File Offset : 0002B690 First Bytes : 60.BE.00.A0.E2

Linker Info : 6.00 SubSystem : Windows GUI

File Size : 0002E400h < N Overlay : NO 00000000

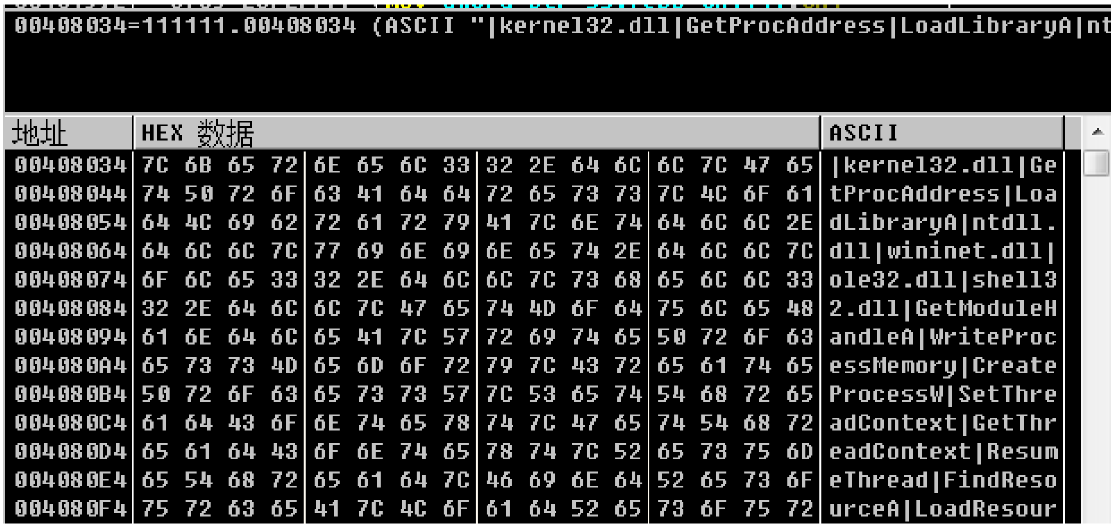
Image is 32bit executable RES/OVL : 5 / 0 % 2013

UPX -> Markus & Laszlo ver. [3.08] <- from file. (sign like UPX packer

Lamer Info - Help Hint - Unpack info 16 ms.

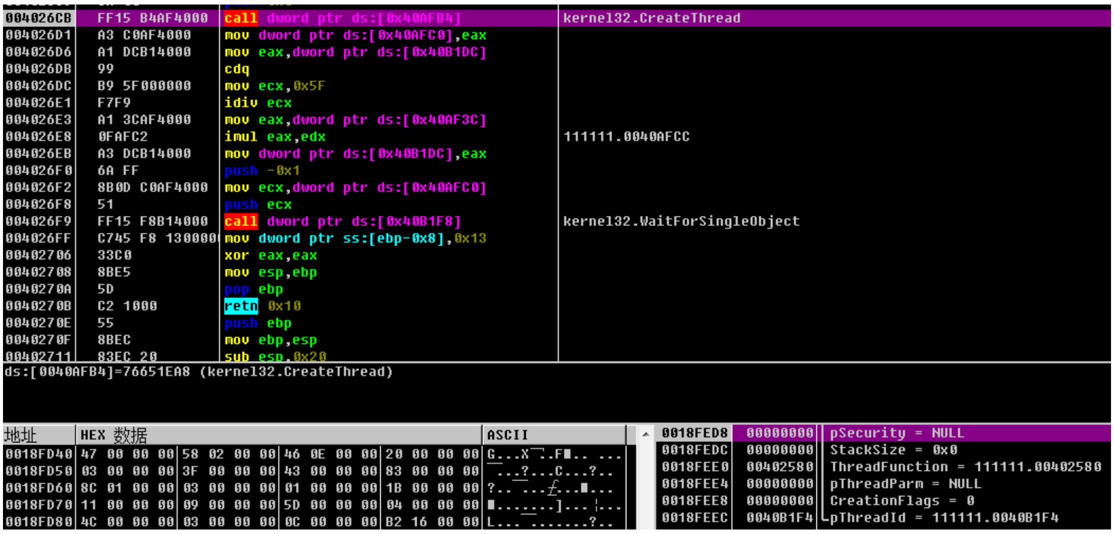
unpack "upx.exe -d" from http://upx.sf.net or any UPX/Generic unpa

脱壳后，程序动态加载函数，躲避静态分析



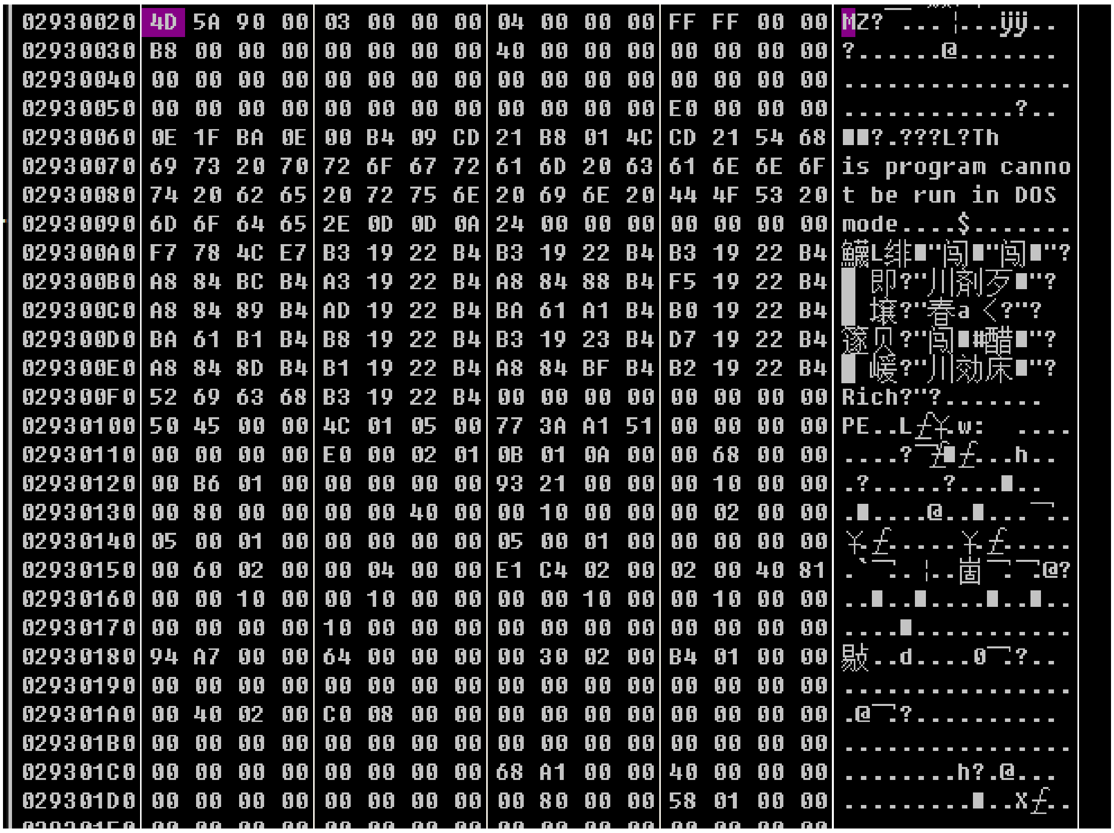
```
00408034=111111.00408034 (ASCII "|kernel32.dll|GetProcAddress|LoadLibraryA|nt

地址      HEX 数据                                            ASCII
00408034  7C 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C 7C 47 65  |kernel32.dll|Ge
00408044  74 50 72 6F 63 41 64 64 72 65 73 73 7C 4C 6F 61  tProcAddress|Loa
00408054  64 4C 69 62 72 61 72 79 41 7C 6E 74 64 6C 6C 2E  dLibraryA|ntdll.
00408064  64 6C 6C 7C 77 69 6E 69 6E 65 74 2E 64 6C 6C 7C  dll|wininet.dll|
00408074  6F 6C 65 33 32 2E 64 6C 6C 7C 73 68 65 6C 6C 33  ole32.dll|shell3
00408084  32 2E 64 6C 6C 7C 47 65 74 4D 6F 64 75 6C 65 48  2.dll|GetModuleH
00408094  61 6E 64 6C 65 41 7C 57 72 69 74 65 50 72 6F 63  andleA|WriteProc
004080A4  65 73 73 4D 65 6D 6F 72 79 7C 43 72 65 61 74 65  essMemory|Create
004080B4  50 72 6F 63 65 73 73 57 7C 53 65 74 54 68 72 65  ProcessW|SetThre
004080C4  61 64 43 6F 6E 74 65 78 74 7C 47 65 74 54 68 72  adContext|GetThr
004080D4  65 61 64 43 6F 6E 74 65 78 74 7C 52 65 73 75 6D  eadContext|Resum
004080E4  65 54 68 72 65 61 64 7C 46 69 6E 64 52 65 73 6F  eThread|FindReso
004080F4  75 72 63 65 41 7C 4C 6F 61 64 52 65 73 6F 75 72  urceA|LoadResour
```

建立新的线程



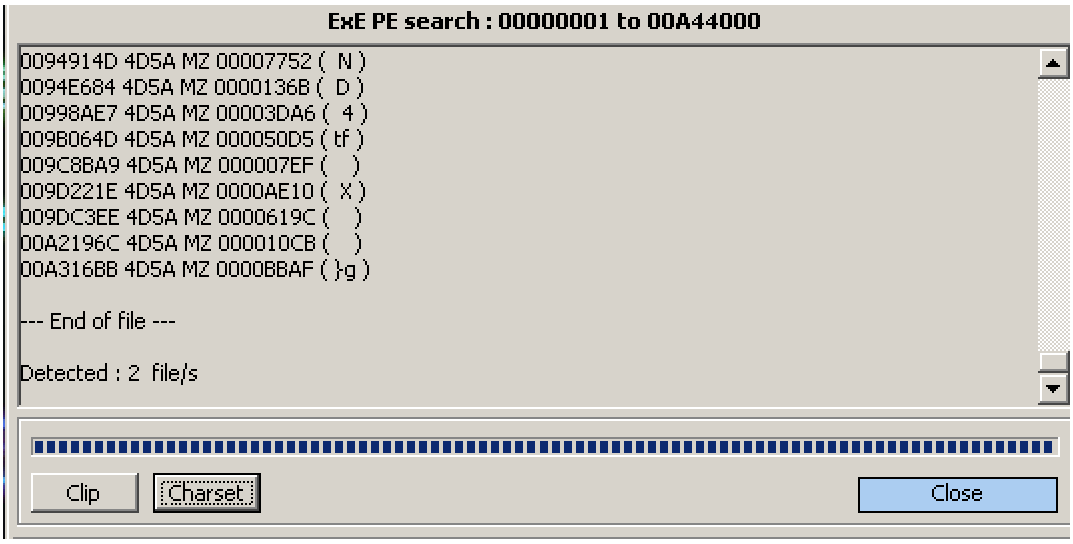
```
004026CB   FF15 B4AF4000    call dword ptr ds:[0x40AFB4]          kernel32.CreateThread
004026D1   A3 C0AF4000      mov dword ptr ds:[0x40AFC0],eax
004026D6   A1 DCB14000      mov eax,dword ptr ds:[0x40B1DC]
004026DB   99               cdq
004026DC   B9 5F000000      mov ecx,0x5F
004026E1   F7F9             idiv ecx
004026E3   A1 3CAF4000      mov eax,dword ptr ds:[0x40AF3C]
004026E8   0FAFC2           imul eax,edx                          111111.0040AFCC
004026EB   A3 DCB14000      mov dword ptr ds:[0x40B1DC],eax
004026F0   6A FF            push -0x1
004026F2   8B0D C0AF4000    mov ecx,dword ptr ds:[0x40AFC0]
004026F8   51               push ecx
004026F9   FF15 F8B14000    call dword ptr ds:[0x40B1F8]          kernel32.WaitForSingleObject
004026FF   C745 F8 1300000  mov dword ptr ss:[ebp-0x8],0x13
00402706   33C0             xor eax,eax
00402708   8BE5             mov esp,ebp
0040270A   5D               pop ebp
0040270B   C2 1000          retn 0x10
0040270E   55               push ebp
0040270F   8BEC             mov ebp,esp
00402711   83EC 20          sub esp,0x20
ds:[0040AFB4]=76651EA8 (kernel32.CreateThread)

地址      HEX 数据                                          ASCII
0018FD40  47 00 00 00 58 02 00 00 46 0E 00 00 20 00 00 00  G...X..F■.. ...
0018FD50  03 00 00 00 3F 00 00 00 43 00 00 00 83 00 00 00  ...?...C...?..
0018FD60  8C 01 00 00 03 00 00 00 01 00 00 00 1B 00 00 00  ?.. ...£..■...
0018FD70  11 00 00 00 09 00 00 00 5D 00 00 00 04 00 00 00  ■.......]...¦...
0018FD80  4C 00 00 00 03 00 00 00 0C 00 00 00 B2 16 00 00  L... .......?..

0018FED8   00000000   pSecurity = NULL
0018FEDC   00000000   StackSize = 0x0
0018FEE0   00402580   ThreadFunction = 111111.00402580
0018FEE4   00000000   pThreadParm = NULL
0018FEE8   00000000   CreationFlags = 0
0018FEEC   0040B1F4   └pThreadId = 111111.0040B1F4
```

将解密后的 PE 文件释放，在内存中执行



```
02930020  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ? ... ¦...ÿÿ..
02930030  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ?.......@.......
02930040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02930050  00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00  ............?..
02930060  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ■■?.???L?Th
02930070  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
02930080  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
02930090  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
029300A0  F7 78 4C E7 B3 19 22 B4 B3 19 22 B4 B3 19 22 B4  鱫L绯■"闯■"闯■"?
029300B0  A8 84 BC B4 A3 19 22 B4 A8 84 88 B4 F5 19 22 B4  ▌即?"川剳歹■"?
029300C0  A8 84 89 B4 AD 19 22 B4 BA 61 A1 B4 B0 19 22 B4  ▌壤?"春a く?"?
029300D0  BA 61 B1 B4 B8 19 22 B4 B3 19 23 B4 D7 19 22 B4  篴贝?"闯■#醋■"?
029300E0  A8 84 8D B4 B1 19 22 B4 A8 84 BF B4 B2 19 22 B4  ▌嶐?"川効床■"?
029300F0  52 69 63 68 B3 19 22 B4 00 00 00 00 00 00 00 00  Rich?"?........
02930100  50 45 00 00 4C 01 05 00 77 3A A1 51 00 00 00 00  PE..L£¥w:  ....
02930110  00 00 00 00 E0 00 02 01 0B 01 0A 00 00 68 00 00  ....? ■£...h..
02930120  00 B6 01 00 00 00 00 00 93 21 00 00 00 10 00 00  .?.....?...■..
02930130  00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00  .■....@..■......
02930140  05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00  ¥£.....¥£.....
02930150  00 60 02 00 00 04 00 00 E1 C4 02 00 02 00 40 81  .`..¦..崮...@?
02930160  00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ..■..■.....■..■..
02930170  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ....■...........
02930180  94 A7 00 00 64 00 00 00 00 30 02 00 B4 01 00 00  敡..d.....0.?..
02930190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
029301A0  00 40 02 00 C0 08 00 00 00 00 00 00 00 00 00 00  .@.?..........
029301B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
029301C0  00 00 00 00 00 00 00 00 68 A1 00 00 40 00 00 00  ........h?.@...
029301D0  00 00 00 00 00 00 00 00 00 80 00 00 58 01 00 00  .........■..X£..
```

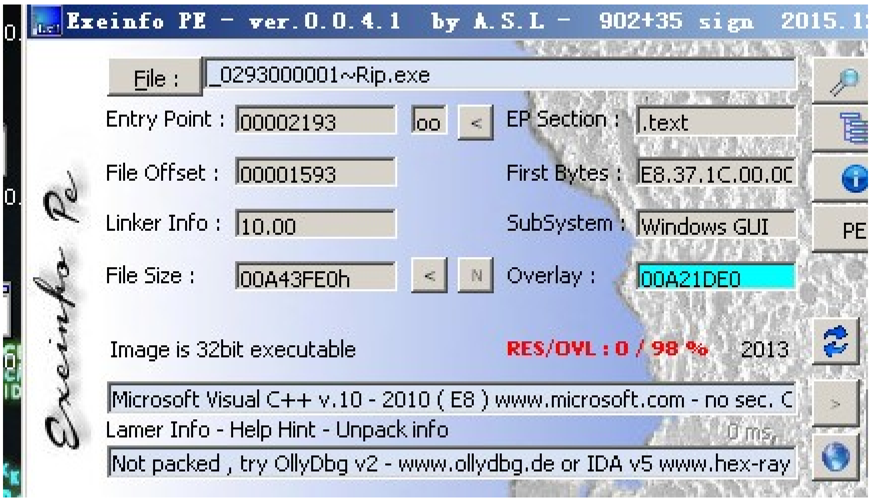
将内容提取保存



ExE PE search : 00000001 to 00A44000

```
0094914D 4D5A MZ 00007752 (  N )
0094E684 4D5A MZ 0000136B (  D )
00998AE7 4D5A MZ 00003DA6 (  4 )
009B064D 4D5A MZ 000050D5 ( tf )
009C8BA9 4D5A MZ 000007EF (    )
009D221E 4D5A MZ 0000AE10 (  X )
009DC3EE 4D5A MZ 0000619C (    )
00A2196C 4D5A MZ 000010CB (    )
00A316BB 4D5A MZ 0000BBAF ( }g )

--- End of file ---

Detected : 2  file/s
```

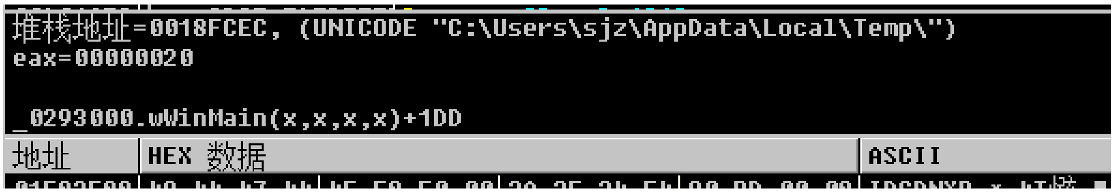
对保存下的文件用侦壳软件检查，发现无壳



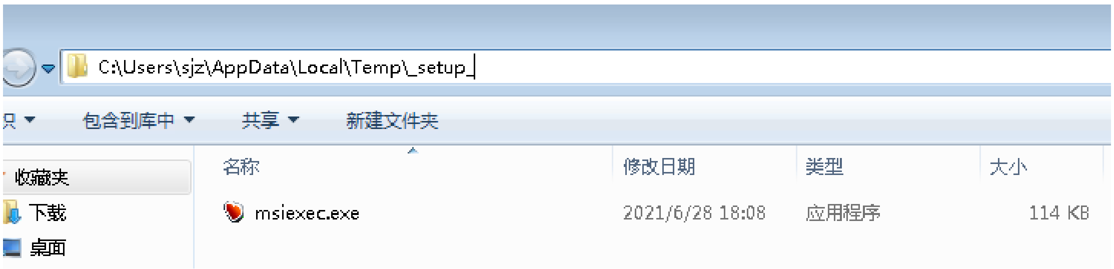
Exeinfo PE - ver.0.0.4.1 by A.S.L - 902+35 sign 2015.1

File : _0293000001~Rip.exe
Entry Point : 00002193
EP Section : .text
File Offset : 00001593
First Bytes : E8.37.1C.00.00
Linker Info : 10.00
SubSystem : Windows GUI
File Size : 00A43FE0h
Overlay : 00A21DE0
Image is 32bit executable
RES/OVL : 0 / 98 %
2013
Microsoft Visual C++ v.10 - 2010 (E8) www.microsoft.com - no sec. C
Lamer Info - Help Hint - Unpack info
0 ms.
Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

动态加载函数后，将自身复制到临时目录下，并改名为 msiexec.exe



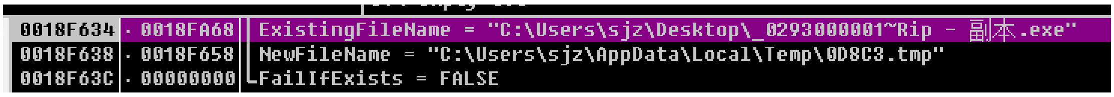
```
堆栈地址=0018FCEC, (UNICODE "C:\Users\sjz\AppData\Local\Temp\")
eax=00000020

_0293000.wWinMain(x,x,x,x)+1DD
```



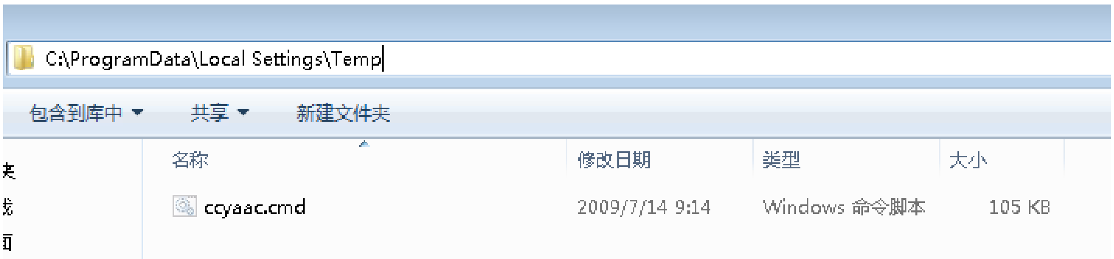
C:\Users\sjz\AppData\Local\Temp_setup_

名称	修改日期	类型	大小
msiexec.exe	2021/6/28 18:08	应用程序	114 KB

再次将自身复制到临时目录下，在注册表添加自启动

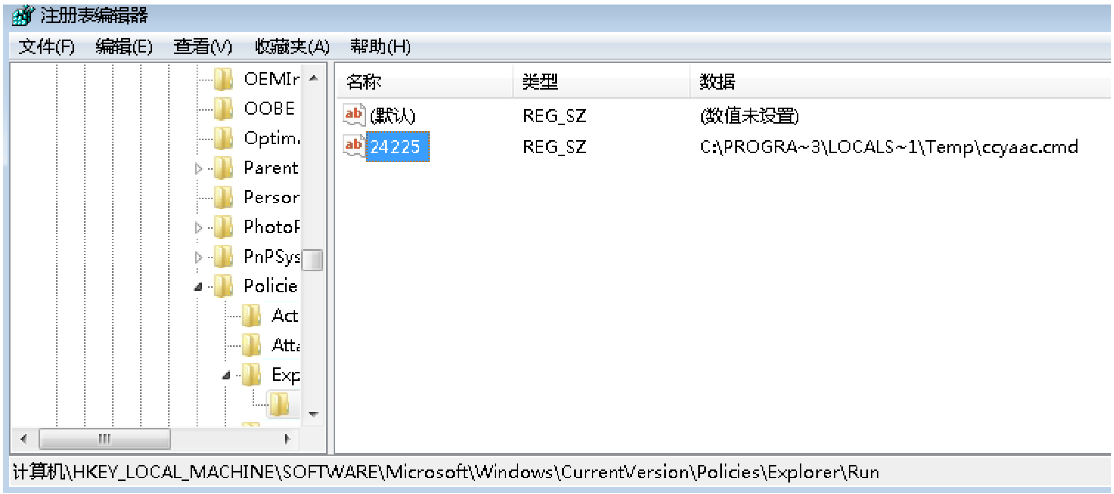


```
0018F634 . 0018FA68 ║ ExistingFileName = "C:\Users\sjz\Desktop\_0293000001~Rip - 副本.exe"
0018F638 . 0018F658 ║ NewFileName = "C:\Users\sjz\AppData\Local\Temp\0D8C3.tmp"
0018F63C . 00000000 └FailIfExists = FALSE
```



C:\ProgramData\Local Settings\Temp

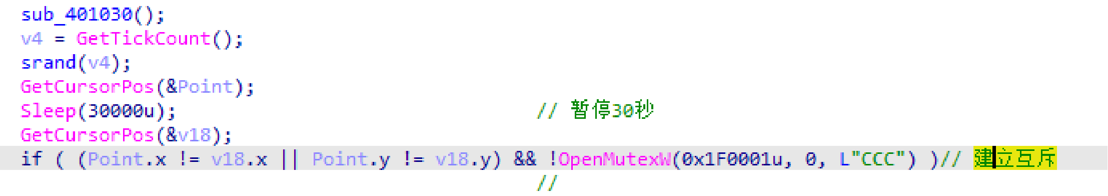
名称	修改日期	类型	大小
ccyaac.cmd	2009/7/14 9:14	Windows 命令脚本	105 KB



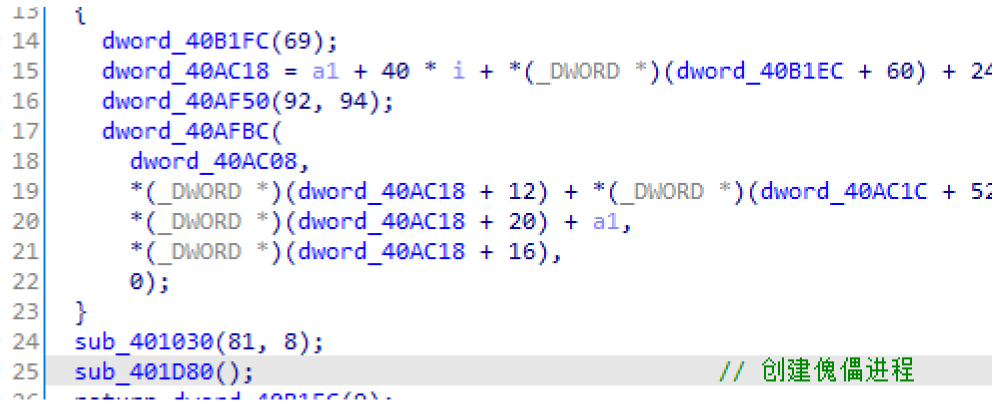
名称	类型	数据
(默认)	REG_SZ	(数值未设置)
24225	REG_SZ	C:\PROGRA~3\LOCALS~1\Temp\ccyaac.cmd

计算机\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

运行后暂停 30 秒，建立互斥，申请虚拟内存，建立傀儡进程

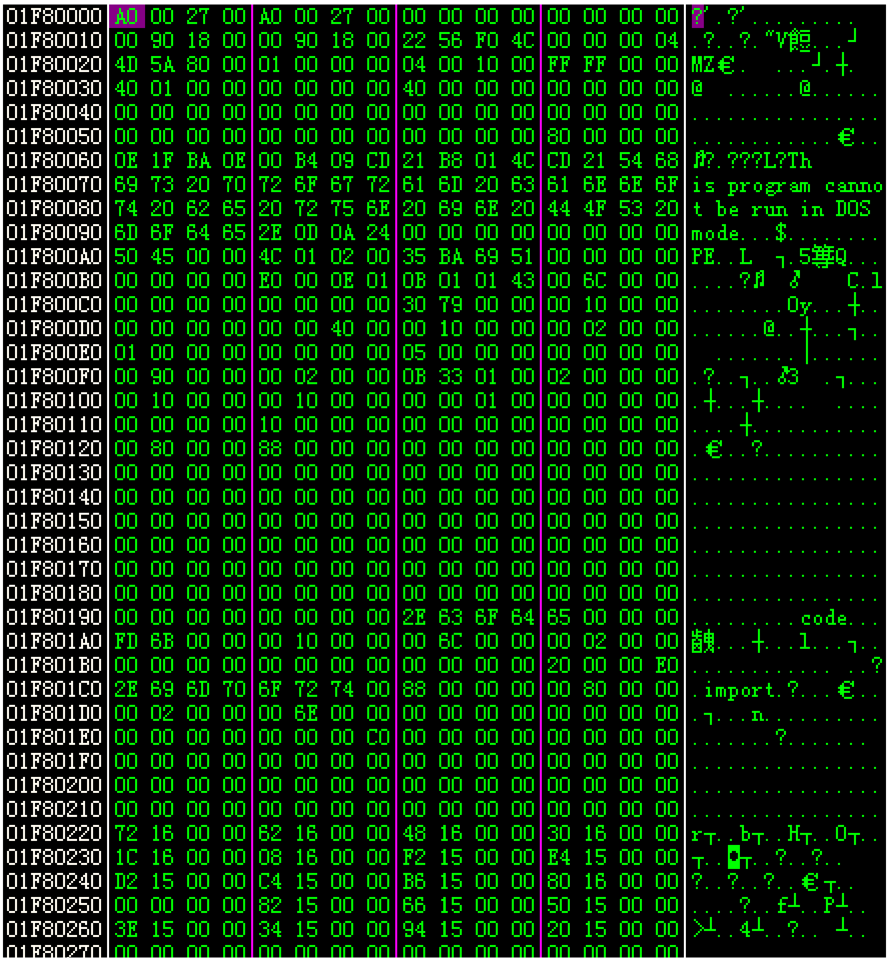


```
sub_401030();
v4 = GetTickCount();
srand(v4);
GetCursorPos(&Point);
Sleep(30000u);                                         // 暂停30秒
GetCursorPos(&v18);
if ( (Point.x != v18.x || Point.y != v18.y) && !OpenMutexW(0x1F0001u, 0, L"CCC") )// 建立互斥
                                                       //
```



```
  {
    dword_40B1FC(69);
    dword_40AC18 = a1 + 40 * i + *(_DWORD *)(dword_40B1EC + 60) + 24
    dword_40AF50(92, 94);
    dword_40AFBC(
      dword_40AC08,
      *(_DWORD *)(dword_40AC18 + 12) + *(_DWORD *)(dword_40AC1C + 52
      *(_DWORD *)(dword_40AC18 + 20) + a1,
      *(_DWORD *)(dword_40AC18 + 16),
      0);
  }
  sub_401030(81, 8);
  sub_401D80();                                // 创建傀儡进程
  return dword_40B1FC(0);
```

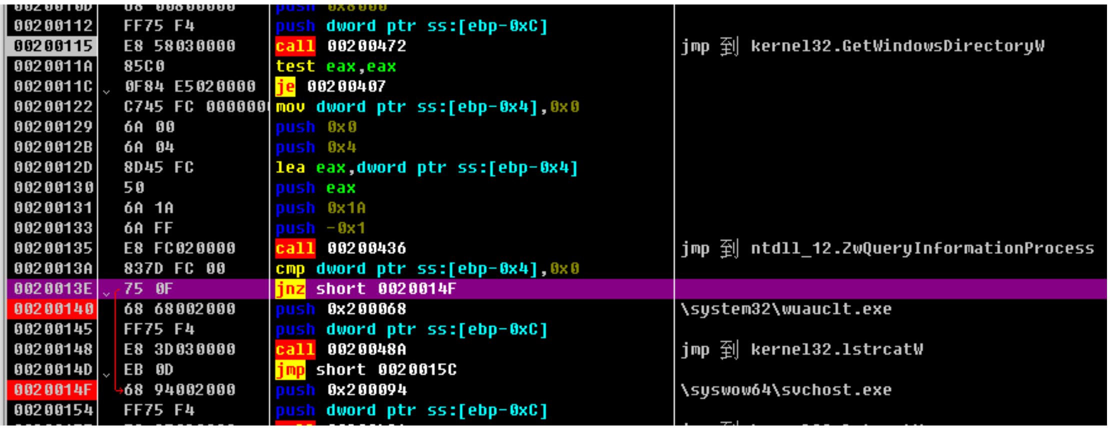
将傀儡进程注入的PE文件提取，运行后，将资源解密成明文，加载运行



```
01F80000 A0 00 27 00 A0 00 27 00 00 00 00 00 00 00 00 00 ?'.?'.........
01F80010 00 90 18 00 00 90 18 00 22 56 F0 4C 00 00 00 04 .?..?."V饐...┘
01F80020 4D 5A 80 00 01 00 00 00 04 00 10 00 FF FF 00 00 MZ€.   ...┘.┼.
01F80030 40 01 00 00 00 00 00 00 40 00 00 00 00 00 00 00 @  ......@......
01F80040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80050 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 ............€..
01F80060 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ?.???L?Th
01F80070 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
01F80080 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
01F80090 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 mode...$........
01F800A0 50 45 00 00 4C 01 02 00 35 BA 69 51 00 00 00 00 PE..L ┐.5簺Q...
01F800B0 00 00 00 00 E0 00 0E 01 0B 01 01 43 00 6C 00 00 ....?   C.l
01F800C0 00 00 00 00 00 00 00 00 30 79 00 00 00 10 00 00 ........0y...┼..
01F800D0 00 00 00 00 00 00 40 00 00 10 00 00 00 02 00 00 ......@..┼...┐..
01F800E0 01 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00  .......│......
01F800F0 00 90 00 00 00 02 00 00 0B 33 01 00 02 00 00 00 .?..┐..3  .┐...
01F80100 00 10 00 00 00 10 00 00 00 00 01 00 00 00 00 00 .┼...┼....  ....
01F80110 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ....┼...........
01F80120 00 80 00 00 88 00 00 00 00 00 00 00 00 00 00 00 .€..?...........
01F80130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80190 00 00 00 00 00 00 00 00 2E 63 6F 64 65 00 00 00 ........code...
01F801A0 FD 6B 00 00 00 10 00 00 00 6C 00 00 00 02 00 00 齥...┼...l...┐..
01F801B0 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 E0 ...............?
01F801C0 2E 69 6D 70 6F 72 74 00 88 00 00 00 00 80 00 00 .import.?...€..
01F801D0 00 02 00 00 00 6E 00 00 00 00 00 00 00 00 00 00 .┐...n..........
01F801E0 00 00 00 00 00 00 00 C0 00 00 00 00 00 00 00 00 .......?.......
01F801F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01F80220 72 16 00 00 62 16 00 00 48 16 00 00 30 16 00 00 r┬..b┬..H┬..0┬..
01F80230 1C 16 00 00 08 16 00 00 F2 15 00 00 E4 15 00 00 ┬..◘┬..?..?..
01F80240 D2 15 00 00 C4 15 00 00 B6 15 00 00 80 16 00 00 ?..?..?..€┬..
01F80250 00 00 00 00 82 15 00 00 66 15 00 00 50 15 00 00 ....?..f┴..P┴..
01F80260 3E 15 00 00 34 15 00 00 94 15 00 00 20 15 00 00 >┴..4┴..?..  ┴..
01F80270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

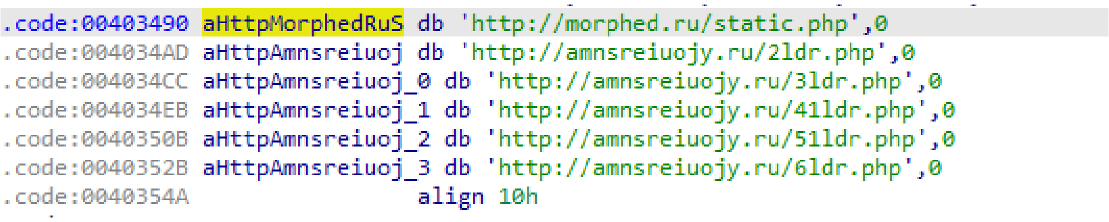
根据系统位数，注入到不同的系统进程，32位注入到wuauclt.exe

64位注入到　svchost.exe



```
00200112    FF75 F4         push dword ptr ss:[ebp-0xC]
00200115    E8 58030000     call 00200472                    jmp 到 kernel32.GetWindowsDirectoryW
0020011A    85C0            test eax,eax
0020011C ⌄  0F84 E5020000   je 00200407
00200122    C745 FC 000000( mov dword ptr ss:[ebp-0x4],0x0
00200129    6A 00           push 0x0
0020012B    6A 04           push 0x4
0020012D    8D45 FC         lea eax,dword ptr ss:[ebp-0x4]
00200130    50              push eax
00200131    6A 1A           push 0x1A
00200133    6A FF           push -0x1
00200135    E8 FC020000     call 00200436                    jmp 到 ntdll_12.ZwQueryInformationProcess
0020013A    837D FC 00      cmp dword ptr ss:[ebp-0x4],0x0
0020013E ⌄  75 0F           jnz short 0020014F
00200140    68 68002000     push 0x200068                    \system32\wuauclt.exe
00200145    FF75 F4         push dword ptr ss:[ebp-0xC]
00200148    E8 3D030000     call 0020048A                    jmp 到 kernel32.lstrcatW
0020014D ⌄  EB 0D           jmp short 0020015C
0020014F    68 94002000     push 0x200094                    \syswow64\svchost.exe
00200154    FF75 F4         push dword ptr ss:[ebp-0xC]
```

程序不断的向黑客服务器发出连接请求，黑客后台地址如下图所示



```
.code:00403490 aHttpMorphedRuS db 'http://morphed.ru/static.php',0
.code:004034AD aHttpAmnsreiuoj db 'http://amnsreiuojy.ru/2ldr.php',0
.code:004034CC aHttpAmnsreiuoj_0 db 'http://amnsreiuojy.ru/3ldr.php',0
.code:004034EB aHttpAmnsreiuoj_1 db 'http://amnsreiuojy.ru/41ldr.php',0
.code:0040350B aHttpAmnsreiuoj_2 db 'http://amnsreiuojy.ru/51ldr.php',0
.code:0040352B aHttpAmnsreiuoj_3 db 'http://amnsreiuojy.ru/6ldr.php',0
.code:0040354A                 align 10h
```

附件信息

hash: cb4328d846d668534fb031ba0f1e47dcd8e7e2e3

yara规则

```
rule Andromeda_virus
{
meta:
   description= "Andromeda virus"
strings:
   $url1 = { 68 74 74 70 3A 2F 2F 6D 6F 72 70 68 65 64 2E 72
75 2F 73 74 61 74 69 63 2E 70 68 70 }
    $url2 = { 00 68 74 74 70 3A 2F 2F 61 6D 6E 73 72 65 69 75 6F 6A 79
2E 72 75 2F 32 6C 64 72 2E 70 68 70 00 }
    $url3 = { 68 74 74 70 3A 2F 2F 61 6D 6E 73 72 65 69 75 6F 6A 79 2E
72 75 2F 33 6C 64 72 2E 70 68 70 00 68 74 74 70 3A 2F 2F 61 6D 6E 73 72
65 69 75 6F 6A 79 2E 72 75 2F 34 31 6C 64 72 2E 70 68 70 00 68 74 74 70
3A 2F 2F 61 6D 6E 73 72 65 69 75 6F 6A 79 2E 72 75 2F 35 31 6C 64 72 2E
70 68 70 00 68 74 74 70 3A 2F 2F 61 6D 6E 73 72 65 69 75 6F 6A 79 2E 72
75 2F 36 6C 64 72 2E 70 68 70 00 00 00 }
    $auto_run = { 73 6F 66 74 77 61 72 65 5C 6D 69 63 72 6F 73 6F 66 74
5C 77 69 6E 64 6F 77 73 5C 63 75 72 72 65 6E 74 76 65 72 73 69 6F 6E 5C
50 6F 6C 69 63 69 65 73 5C 45 78 70 6C 6F 72 65 72 5C 52 75 6E 00 }
condition:
   uint16(0)==0x5A4D and filesize < 2MB and all of them
}
```

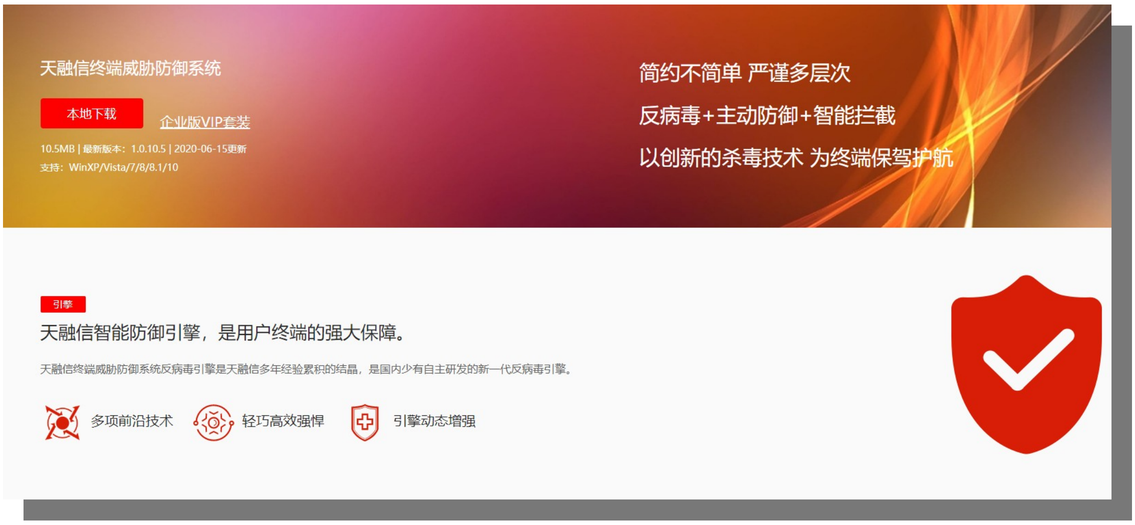
防护建议

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



天融信终端威胁防御系统

10.5MB | 最新版本：1.0.10.5 | 2020-06-15更新

支持：WinXP/Vista/7/8/8.1/10

简约不简单 严谨多层次

反病毒+主动防御+智能拦截

以创新的杀毒技术 为终端保驾护航

天融信智能防御引擎，是用户终端的强大保障。

天融信终端威胁防御系统反病毒引擎是天融信多年经验累积的结晶，是国内少有自主研发的新一代反病毒引擎。