

# Analysis Notes on CrowdStrike's Library Loading and Rapid Upgrade Mechanism

Antiy Attack & Defense Laboratory

Time of first release: 3 August 2024

*The original report is in Chinese, and this version is an AI-translated edition.*

In response to a large Windows host blue screen event caused by CrowdStrike, Antiy Cloud Security Center, Antiy CERT and Antiy Attack and Defense Laboratory released a long analysis report on July 21, "Technical Analysis of CrowdStrike Resulting in Large-scale System Crash: A Meditation on" Falcon Feather "(hereinafter referred to as" Falcon Feather "report). At the same time, it has also promoted the analysis and verification of multiple points, some of which are disclosed in this report.

As for the way to quickly upgrade and delete the problem "channel file," there is a phenomenon that the problematic C- \* 291 \* sys file and the latest C- \* 291 \* 001. sys are allowed to coexist without networking. The problem files are also automatically cleared after the restart. In terms of that mechanism, we have put forward two guesses, the first is that when a category in the upgrade system reappears a file with version number 01 (possibly with a timestamp judgment), the category is considered to be reinitialized. Automatically delete old version number files. Second, the handling definition for deleting the corresponding problem file is put in the new file No. 01.

In the first category, there are two guesses: No file with version number 01 can coexist with other versions of files in other categories, and the classification rule is the rule that C- \* 291 \* should be the main protection type for different scenarios. Document processing should not be carried out directly. The second case is not excluded. the format supports a retention mechanism for self-emergency handling. We're leaning towards the first. However, our analysis may not be made public in the future. based on the traditional principle in the industry, we can disclose the contents of reverse analysis for the products of other banks, and shall not go beyond the boundary of accident analysis.

- - Antiy Attack and Defense Laboratory

# CrowdStrike C-\*.sys Series Channel File (Rule Upgrade File) Loading Mechanism

## 1.1 Review of channel file formats

We have analyzed the format of C-\*.sys files in the Falcon Falling Report. It is pointed out that the file that conforms to the relevant file name is actually a CrowdStrike custom format file instead of a Windows PE format file although it is the suffix. ".sys" of the Windows driver file. In that file head structure of this type of file, as shown in the format analysis result in our previous report, the file head content is strongly related to the file name, the program will check the file name according to the file header information, and the file also contains hash check information, For the second check, the method of hash calculation is to call Windows own library function calculation.

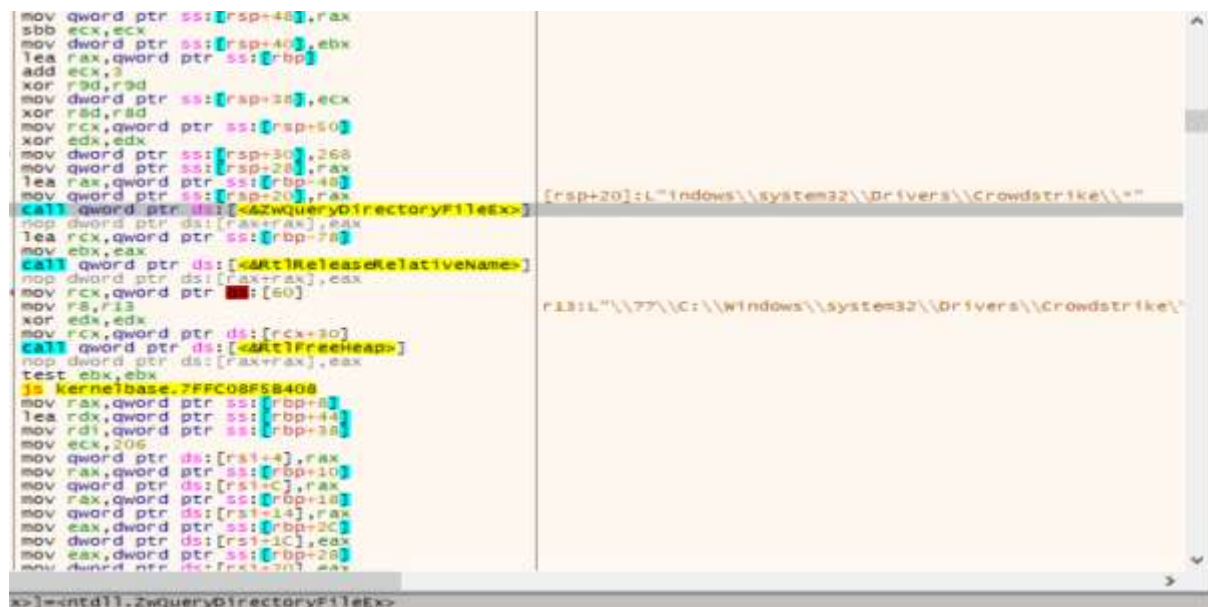
C-00000291-00000000-00000029.sys															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e
00000000h:	AA	AA	AA	AA	01	00	23	01	00	00	05	00	00	00	00
00000010h:	1D	00	00	00	20	A0	00	00	04	A0	00	00	06	00	00
00000020h:	F8	9F	00	00	04	00	00	00	40	00	00	00	07	00	00
00000030h:	C0	9F	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060h:	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00
00000070h:	00	00	00	00	00	00	00	00	00	00	00	40	00	00	00
00000080h:	15	00	00	00	1D	00	00	00	80	9F	00	00	02	00	00
00000090h:	02	00	00	00	C0	00	00	00	08	01	00	00	C0	01	00
000000a0h:	F8	04	00	00	98	06	00	00	48	07	00	00	D8	07	00

Figure 1 C-\*.sys Series File Header Format Review 1

## 1.2 The channel file verifies how it is loaded

The C-\*.sys files are loaded by the CSFalconService.exe process of the CrowdStrike Main Service "CrowdStrike Falcon Sensor Service," which uses Microsoft's antivirus product protection service open to antivirus vendors. Start with SERVICE\_LAUNCH\_PROTECTED\_ANTIMALWARE\_LIGHT protection type to realize service protection, and call a series of kernel functions for directory traversal and file reading after service startup to verify the validity of relevant C-00000xxx-00000000-00000xxx files. Policies are then passed to the driver and engine through IPC (inter-process communication) to execute policies.

Use the ZwQueryDirectoryFile function to traverse C:\Windows\System32\drivers\CrowdStrike directory C-00000xxx-00000000-00000000xxx. Sys file is shown in Figure 2 and Figure 3.错误!未找到引用源。错误!未找到引用源。



```

mov qword ptr [rsp+40],rax
sbb ecx,ecx
mov dword ptr [rsp+40],ebx
lea rax,qword ptr [rbp+40]
add ecx,3
xor r9d,r9d
mov dword ptr [rsp+30],ecx
xor r9d,r9d
mov rcx,qword ptr [rsp+50]
xor edx,edx
mov dword ptr [rsp+30],268
mov qword ptr [rsp+20],rax
lea rax,qword ptr [rbp+40]
mov qword ptr [rsp+20],rax
call qword ptr [ZwQueryDirectoryFileEx]
nop dword ptr [rax+rax],eax
lea rcx,qword ptr [rbp+70]
mov ebx,eax
call qword ptr [ZwQueryDirectoryFileEx]
nop dword ptr [rax+rax],eax
mov rcx,qword ptr [rbp+50]
mov rax,12
xor edx,edx
mov rcx,qword ptr [rcx+30]
call qword ptr [ZwQueryDirectoryFileEx]
nop dword ptr [rax+rax],eax
test ebx,ebx
je kernelbase.7FFC08F5B40B
mov rax,qword ptr [rbp+80]
lea rdx,qword ptr [rbp+44]
mov rdi,qword ptr [rbp+38]
mov ecx,206
mov qword ptr [rsi+4],rax
mov rax,qword ptr [rsi+10]
mov qword ptr [rsi+C],rax
mov rax,qword ptr [rsi+18]
mov qword ptr [rsi+14],rax
mov eax,dword ptr [rbp+2C]
mov dword ptr [rsi-1C],eax
mov eax,dword ptr [rbp+28]
mov dword ptr [rsi+70],eax
x>=ntdll.ZwQueryDirectoryFileEx
  
```

Figure 2 Traversal of the C-00000xxx-00000000-00000xxx file using the ZwQueryDirectoryFile function (1) 2



```

call qword ptr [ZwQuerySystemTime]
mov rax,qword ptr [rbp+50]
lea r15,qword ptr [ZwQuerySystemTime]
mov dword ptr [rbp+40],rsi
mov rsi,qword ptr [rbp+50]
mov qword ptr [rbp+20],rax
lea rcx,qword ptr [rbp+60]
call csfalconservice.7FF665832590
xor edx,edx
lea rcx,qword ptr [rbp+50]
call qword ptr [ZwQuerySystemTime]
cmp byte ptr [rsi+25],0
je csfalconservice.7FF6657660E7
mov byte ptr [rsi+25],0
jmp csfalconservice.7FF665766100
mov rcx,qword ptr [rbp+50]
lea rdx,qword ptr [rsi+8]
mov rcx,qword ptr [rsi+8]
call qword ptr [ZwQuerySystemTime]
test eax,eax
je csfalconservice.7FF6657664B2
mov eax,dword ptr [rsi+8]
shr eax,4
test al,1
jne csfalconservice.7FF6657660D5
mov rdx,qword ptr [rbp+50]
lea rcx,qword ptr [rbp+10]
add rdx,34
call qword ptr [ZwQuerySystemTime]
movzx ebx,word ptr [rbp+10]
mov eax,1
test rdx,rdx
cmovbe ebx,eax
call qword ptr [ZwQuerySystemTime]
mov r9d,ebx
xor edx,edx
mov rcx,rax
call qword ptr [ZwQuerySystemTime]
mov qword ptr [rbp+50],rax
lea rcx,qword ptr [rbp+60]
test rax,rax
<kernel32.FindNextFile>
  
```

Figure 3 Traversal of the C-00000xxx-00000000-00000xxx file using the ZwQueryDirectoryFile function (2) 3

Use ZwCreateFile and ZwReadFile to open and read the file content, and parse the file header to verify the file name, as shown in Figure 4 and Figure 5. Figure 4 Use ZwCreateFile and ZwReadFile to open and read the file content, parse the file header to verify the file name (1) 4 错误!未找到引用源。

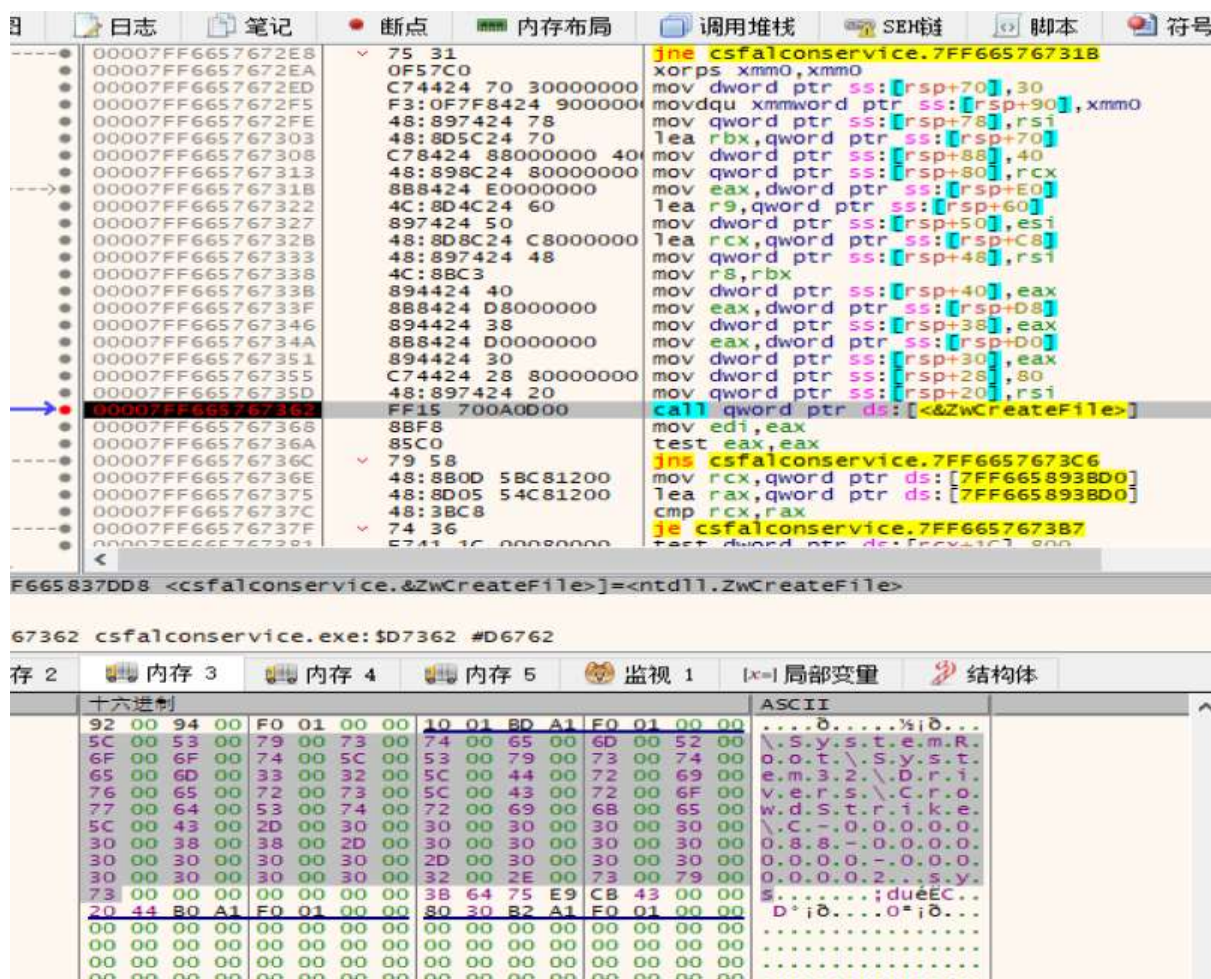


Figure 4 Use ZwCreateFile and ZwReadFile to open and read the file content, parse the file header to verify the file name (1) 4



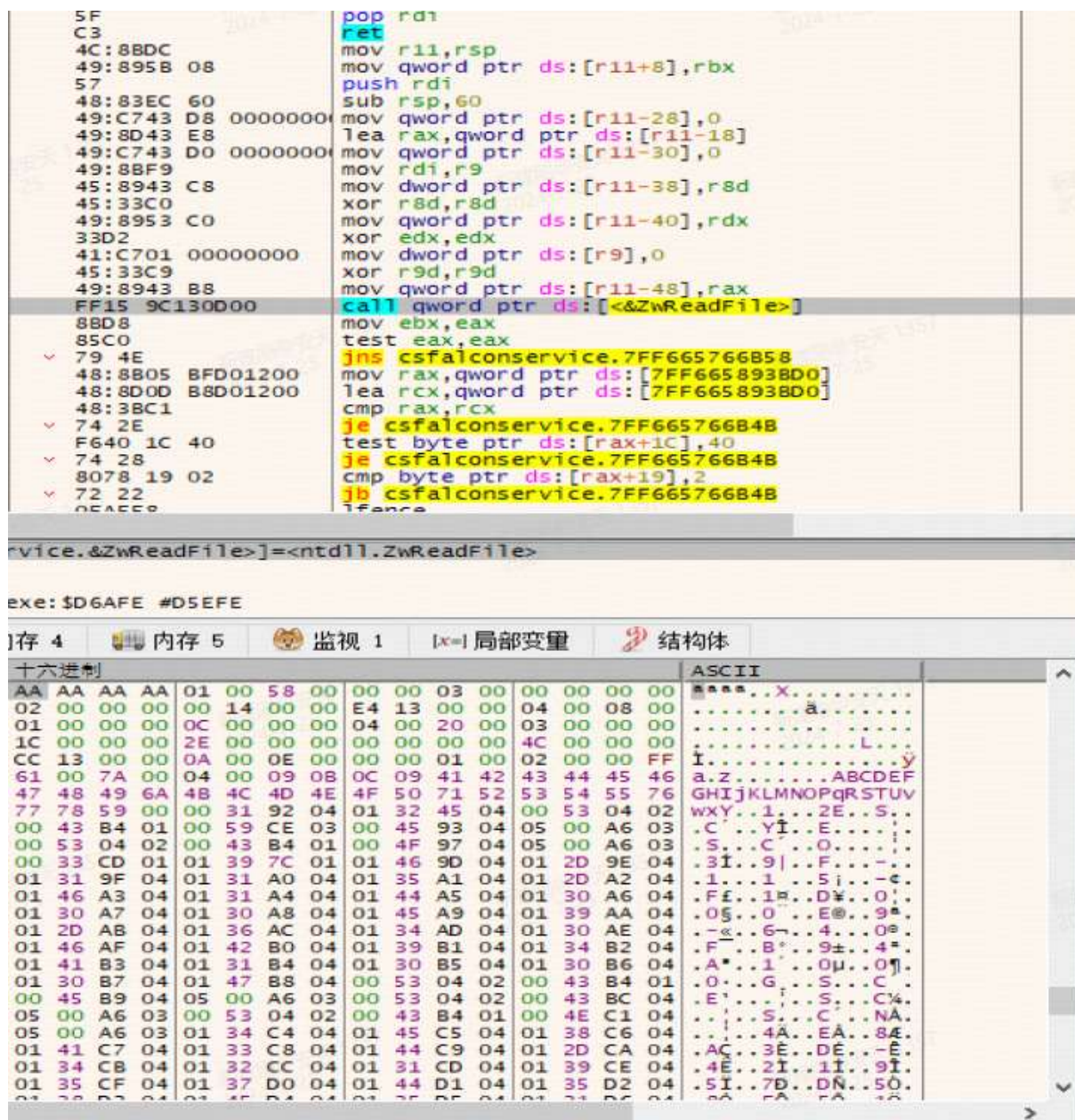


Figure 5 Use ZwCreateFile and ZwReadFile to open and read the file content, parse the file header to verify the file name (2) 5

Call the BCryptFinish Hash function in the Windows encryption primitive library bcrypt.dll to perform hash verification on the file content, which is defined in bcrypt.h, and perform further parsing operations after the verification is passed, as shown in Figure 6.错误!未找到引用源。

```

00007FF661 CC int3
00007FF661 CC int3
00007FF661 CC int3
00007FF661 CC int3
00007FF661 CC int3
00007FF661 40:53 push rbx
00007FF661 48:83EC 20 sub rsp,20
00007FF661 44:8B02 mov r8d,dword ptr ds:[rdx]
00007FF661 45:33C9 xor r9d,r9d
00007FF661 48:8B52 08 mov rdx,qword ptr ds:[rdx+8]
00007FF661 48:8B49 10 mov rcx,qword ptr ds:[rcx+10]
00007FF661 FF15 0E5F0900 call qword ptr ds:[<&BCryptHashData>]
00007FF661 8BD8 mov ebx,eax
00007FF661 85C0 test eax,eax
00007FF661 79 46 jns csfalconservice.7FF6657A1D46
00007FF661 48:8B05 C91E0F00 mov rax,qword ptr ds:[7FF6658938D0]
00007FF661 48:8D0D C21E0F00 lea rcx,qword ptr ds:[7FF6658938D0]
00007FF661 48:3BC1 cmp rax,rcx
00007FF661 74 31 je csfalconservice.7FF6657A1D44
00007FF661 F740 1C 00200000 test dword ptr ds:[rax+1C],2000
00007FF661 74 28 je csfalconservice.7FF6657A1D44
00007FF661 8078 19 02 cmp byte ptr ds:[rax+19],2
00007FF661 72 22 jb csfalconservice.7FF6657A1D44
00007FF661 0FAEE8 lfence
00007FF661 48:8B0D A41E0F00 mov rcx,qword ptr ds:[7FF6658938D0]
00007FF661 4C:8D05 AD8D0800 lea r8,qword ptr ds:[7FF66585DAE0]
00007FF661 BA 0E000000 mov edx,E
00007FF661 44:8BCB mov r9d,ebx
00007FF661 48:8B49 10 mov rcx,qword ptr ds:[rcx+10]
00007FF661 E8 2C12EFFF call csfalconservice.7FF665692F70
00007FF661 8BC3 mov eax,ebx
00007FF661 48:83C4 20 add rsp,20
00007FF661 5B pop rbx
00007FF661 C3 ret
00007FF661 CC int3
00007FF661 CC int3
00007FF661 CC int3
00007FF661 CC int3
00007FF661 48:895C24 08 mov qword ptr ss:[rsp+8],rbx
00007FF661 48:897474 10 mov qword ptr ss:[rsp+10],rsi

```

FF665837C08 <csfalconservice.&BCryptHashData>]=<bcrypt.BCryptHashData>

Figure 6 Calling the BCryptFinish Hash function to hash verify the contents of the file 6

### 1.3 The reason for the blue screen

On the specific analysis of blue screen, Microsoft has given a more detailed analysis. We verify that it is correct.

```

IMAGE_NAME: csagent.sys
MODULE_NAME: csagent
FAULTING_MODULE: fffff80671430000 csagent
PROCESS_NAME: System

TRAP_FRAME: fffff94058305ec20 -- (.trap 0xffff94058305ec20)
.trap 0xffff94058305ec20
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=ffff94058305f200 rbx=0000000000000000 rcx=0000000000000000
rdx=ffff94058305f1d0 rsi=0000000000000000 rdi=0000000000000000
rip=fffff806715114ed rsp=ffff94058305edb0 rbp=ffff94058305ee
r8=ffff840500000074 r9=0000000000000000 r10=0000000000000000
r11=0000000000000014 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na po nc
csagent+0xe14ed:
fffff806`715114ed 458b08          mov     r9d,dword ptr [r8]
.trap
Resetting default scope

STACK_TEXT:
ffff9405`8305e9f8 fffff806`5388c1e4 : 00000000`00000050
ffff9405`8305ea00 fffff806`53662d8c : 00000000`00000000
ffff9405`8305eb00 fffff806`53827529 : ffffffff`00000030
ffff9405`8305ec20 fffff806`715114ed : 00000000`00000000
ffff9405`8305edb0 fffff806`714e709e : 00000000`00000000
ffff9405`8305ef50 fffff806`714e8335 : 00000000`00000000
ffff9405`8305f080 fffff806`717220c7 : 00000000`00000000
ffff9405`8305f1b0 fffff806`7171ec44 : fffff9405`8305f668

```

Figure 7 Reasons for Blue Screen 7



Microsoft pointed out in the analysis report [FootnoteRef: 1] that since WER (Windows Error Reporting) data only provides a compressed version of the current state, a wider range of disassembly instructions cannot be viewed. By searching for the command feature "45 8B 08," it is not difficult to locate the key command position of FIG. 8, for further analysis. [1: <https://www.microsoft.com/en-us/security/blog/2024/07/27/windows-security-best-practices-for-integrating-and-managing-security-tools/>]<sup>1</sup>错误!未找到引用源。

<pre> 00000001400E14C9 00000001400E14C9 49 8B 55 00 00000001400E14CD 45 8B CA 00000001400E14D0 E3 3A 04 00000001400E14D3 48 8B 42 08 00000001400E14D7 4E 8B 04 D8 00000001400E14D8 75 08 00000001400E14DD 4D 85 C0 00000001400E14E0 74 12 00000001400E14E2 45 0F B7 08 00000001400E14E6 EB 08 00000001400E14E8 00000001400E14E8 00000001400E14E8 00000001400E14E8 4D 85 C0 00000001400E14E8 74 07 00000001400E14ED 45 8B 08 00000001400E14F0 00000001400E14F0 00000001400E14F0 4D 8B 50 08 00000001400E14F4 00000001400E14F4 00000001400E14F4 4D 8B C2 00000001400E14F7 48 8D 40 08 00000001400E14FB 48 8B D6 00000001400E14FE E8 21 2C 00 00 00000001400E1503 45 33 D2 00000001400E1506 8B D8 00000001400E1508 85 C0 00000001400E150A 79 7C </pre>	<pre> loc_1400E14C9: mov     rdx, [r13+0]           ; CODE XREF: sub_1400E11D0+1B9fj mov     r9d, r10d cmp     dword ptr [rdx], 4 mov     rax, [rdx+8] mov     r8, [rax+r11*8] jnz     short loc_1400E14E8 test    r8, r8 jz      short loc_1400E14F4 movzx   r9d, word ptr [r8] jmp     short loc_1400E14F0  loc_1400E14E8: test    r8, r8           ; CODE XREF: sub_1400E11D0+308fj jz      short loc_1400E14F4 mov     r9d, [r8]  loc_1400E14F0: mov     r10, [r8+8]       ; CODE XREF: sub_1400E11D0+315fj  loc_1400E14F4: mov     r8, r10           ; CODE XREF: sub_1400E11D0+318fj lea     rcx, [rbp+98h+var_100] mov     rdx, rsi call    sub_1400E4124 xor     r10d, r10d mov     ebx, eax test    eax, eax jns     short loc_1400E1588 </pre>
---	--

Figure 8 Search Instruction Feature "45 8B 08" locates critical instruction locations 8

As can be seen from FIG. 8, although the program determines whether the r8 register is 0 at the 01400E14E8 offset (avoiding access to the null pointer), it does not further verify the validity of the address pointed to by the r8 register. Then the program accesses the illegal address pointed to by the r8 register at 01400E14ED offset, and finally causes the blue screen to occur.错误!未找到引用源。

## 1.4 New channel file to remedy blue screen events

In response to the blue screen event, CrowdStrike generated the policy file C-00000291-00000000-00000001 in an emergency manner, and directly deleted the existing C-00000291-\*. Sys in the entire upgrade policy to carry out startup processing. There is no C-00000291-00000000-00000001 in the file name of the existing C-00000291-\* sys series. the last section of the file name is the library version (number of updates) according to our guess. Judging from the preliminary rules, when the last section of server file returns to reference number 1, it may mean that the rule file of the corresponding category is cleaned based on the deletion policy.

<sup>1</sup> <https://www.microsoft.com/en-us/security/blog/2024/07/27/windows-security-best-practices-for-integrating-and-managing-security-tools/>

```

fffff807`7ee17194 4881ecc0000000 sub    rsp,0C0h
fffff807`7ee1719b 488b055ee1500 mov    rax,qword ptr [csagent+0x286000 (fffff807`7ef76000)]
fffff807`7ee171a2 483bc4 xor     rax,rsp
fffff807`7ee171a5 48894547 mov    qword ptr [rbp+47h].rax
fffff807`7ee171a9 33d2 xor     edx,edx
fffff807`7ee171ab 488bf9 mov    rdi,rcx
fffff807`7ee171ae 488d4df7 lea     rcx,[rbp-9]
fffff807`7ee171b2 448d4250 lea     r8d,[rdx+50h]
fffff807`7ee171b6 e805b11000 call   csagent+0x2322c0 (fffff807`7ef222c0)
fffff807`7ee171bb 488d4df7 lea     rcx,[rbp-9]
fffff807`7ee171bf e870eaefff call   csagent+0x25c34 (fffff807`7ed15c34)
fffff807`7ee171c4 488b45ff mov    rax,qword ptr [rbp-1]
fffff807`7ee171c8 488d4dc7 lea     rcx,[rbp-39h]
fffff807`7ee171cc 0f57c0 xorps   xmm0,xmm0
fffff807`7ee171cf fe4020 inc     byte ptr [rax+20h]
fffff807`7ee171d2 488b65cf00 and     qword ptr [rbp-31h],0
fffff807`7ee171d7 c745c730000000 mov    dword ptr [rbp-39h].30h
fffff807`7ee171de c745df40020000 mov    dword ptr [rbp-21h].240h
fffff807`7ee171e5 48897dd7 mov    qword ptr [rbp-29h].rdi
fffff807`7ee171e9 f30f7f45e7 movdqu  xmmword ptr [rbp-19h].xmm0
fffff807`7ee171ee 4c8b157b171100 mov    r10,qword ptr [csagent+0x238970 (fffff807`7ef28970)]
fffff807`7ee171f5 e885bf7bfbb call   nt!ZwDeleteFile (fffff807`7a5d31b0)
fffff807`7ee171fa 8bd8 mov    ebx,eax
fffff807`7ee171fc 85c0 test    eax,eax
fffff807`7ee171fe 7949 jns     csagent+0x127249 (fffff807`7ee17249)
fffff807`7ee17200 488b15f1381600 mov    rdx,qword ptr [csagent+0x28aaf8 (fffff807`7ef7aaf8)]
fffff807`7ee17207 488d05ea381600 lea     rax,[csagent+0x28aaf8 (fffff807`7ef7aaf8)]
fffff807`7ee1720e 483bd0 cmp     rdx,rax
fffff807`7ee17211 7438 je      csagent+0x12724b (fffff807`7ee1724b)
fffff807`7ee17213 8b4a2c mov    ecx,dword ptr [rdx+2Ch]
fffff807`7ee17216 f6c140 test    cl,40h
fffff807`7ee17219 7430 je      csagent+0x12724b (fffff807`7ee1724b)
fffff807`7ee1721b 807a2902 cmp     byte ptr [rdx+29h],2
fffff807`7ee1721f 722a jb      csagent+0x12724b (fffff807`7ee1724b)
fffff807`7ee17221 0f8ee0 ifence
fffff807`7ee17224 488b0dc381600 mov    rcx,qword ptr [csagent+0x28aaf8 (fffff807`7ef7aaf8)]
fffff807`7ee1722b 4c8d05d6541400 lea     r8,[csagent+0x26c708 (fffff807`7ef5c708)]
fffff807`7ee17232 ba13000000 mov     edx,13h
fffff807`7ee17237 895c2420 mov     dword ptr [rsp+20h].ebx
fffff807`7ee1723b 4c8bcbf mov     r9,rdi
fffff807`7ee1723e 488b4918 mov     rcx,qword ptr [rcx+18h]
fffff807`7ee17242 e85d0deeff call   csagent+0x7fa4 (fffff807`7efc7fa4)

```

MyDriverTry.c Disassembly

Memory

Virtual	ffff50ea8e58330	Display format	Byte	Previous	Next
ffff50ea8e58330	92 00 94 00 63 00 72 00 40 83 e5 a8 0e e5 ff ff 5c 00 53 00 79		c.r.#		
ffff50ea8e58334	00 73 00 74 00 65 00 6d 00 52 00 6f 00 6f 00 74 00 5c 00 53 00		.s.t.e.a.R.o.o.t.\S.		
ffff50ea8e5833a	79 00 73 00 74 00 65 00 6d 00 33 00 32 00 5c 00 44 00 72 00 63		y.s.t.e.a.3.2.\D.r.i		
ffff50ea8e5836f	00 76 00 65 00 72 00 73 00 5c 00 43 00 72 00 6f 00 77 00 64 00		v.e.r.s.\C.r.o.w.d		
ffff50ea8e58384	53 00 74 00 72 00 69 00 6b 00 65 00 5c 00 43 00 2d 00 30 00 30		S.t.r.i.k.e.\C.-0.0		
ffff50ea8e58399	00 30 00 30 00 30 00 32 00 39 00 31 00 2d 00 30 00 30 00 30 00		.0.0.0.2.9.1.-0.0.0		
ffff50ea8e583ae	30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30		0.0.0.0.0.-0.0.0.0.0		
ffff50ea8e583c3	00 30 00 33 00 32 00 2e 00 73 00 79 00 73 00 00 00 65 00 77 00		.0.3.2..s.y.s..e.v		
ffff50ea8e583d8	79 00 00 00 00 00 00 00 00 00 00 00 0b 57 6e 66 20 8a 3f 9b 62 47		y.....Unf..?..bG		
ffff50ea8e583ed	1d e7 bd 03 09 a8 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 78		.....x		
ffff50ea8e58402	e5 a8 0e e5 ff ff 40 92 e5 a8 0e e5 ff ff 80 9d e5 a8 0e e5 ff		.....@.....		
ffff50ea8e58417	ff 31 50 1a 00 00 00 00 00 00 20 3a ef 9f 0e e5 ff ff 00 10 00 00		.....1P.....		
ffff50ea8e5842c	00 00 00 00 00 00 00 00 00 00 00 00 00 a0 ab f3 9f 0e e5 ff ff 00		.....		
ffff50ea8e58441	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		.....		
ffff50ea8e58456	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 c7 cb		.....		
ffff50ea8e5846b	a8 0e e5 ff ff 10 c7 cb a8 0e e5 ff ff 78 7b e5 a8 0e e5 ff ff		.....x(.....		

Registers Calls Scratch Pad dd fffff803`4316cc60 Watch Locals Memory

Figure 9 Delete the channel file related to the blue screen time 9

## 2 CrowdStrike Agent starts network communication and upgrade mechanism

### 2.1 Network communication opportunity

For CrowdStrike Falcon Sensor, you can refer back to the "Falcon Falling Fines" report. After the loading phase of the Windows startup kernel and the early phase of the session manager startup phase, CrowdStrike Falcon Sensor establishes a link with the remote server in the background, updates the policy file and returns data. The specific process is to obtain the IP of the server on the cloud through DNS resolution of ts01-gyr-maverick.cloudsink.net and lfodown01-gyr-maverick.cloudsink.net domain names, and establish SSL encrypted communication for policy distribution and information uploading.



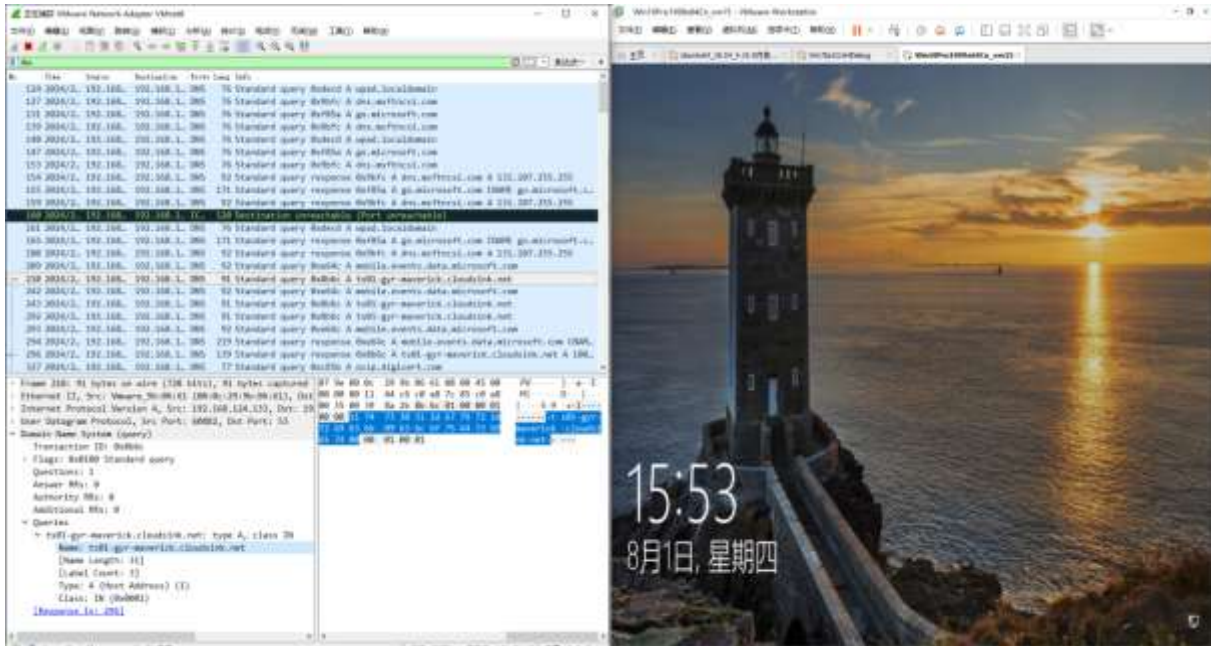


Figure 10 CrowdStrike agent starts network communication 10

Network communication behavior starts after the Windows kernel loading phase is completed, before the Session Manager startup phase and before the user logs on.

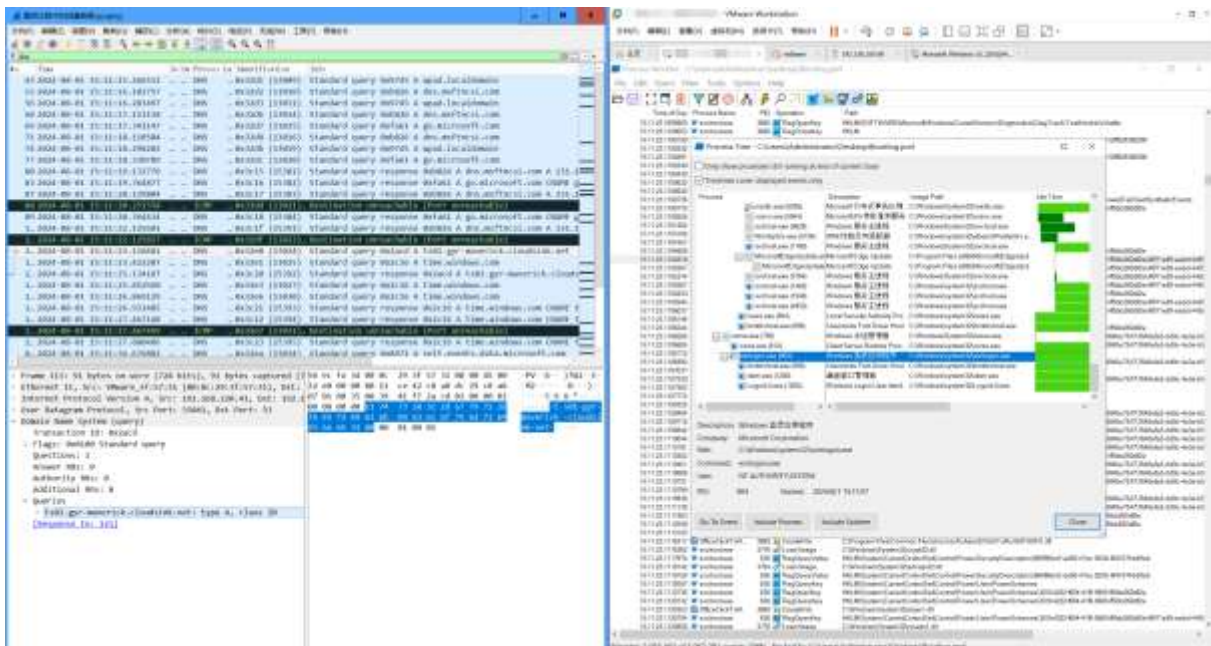


Figure 11 Network communication timing 11

## 2.2 CrowdStrike Falcon Sensor Return Address

Except that the above two cloudnsk. net subdomains are CrowdStrike Falcon Sensor callback addresses, the callback addresses in different regions are different. the known callback addresses are as follows:

**Us-1 environment:**

- [Http: // ts01-b.cloudsink.net](http://ts01-b.cloudsink.net)
- [Http: // lfodown01-b.cloudsink.net](http://lfodown01-b.cloudsink.net)
- [Http: // lfoup01-b.cloudsink.net](http://lfoup01-b.cloudsink.net)
- [Https: // falcon.CrowdStrike .com](https://falcon.CrowdStrike.com)
- [Https: // assets.falcon.CrowdStrike .com](https://assets.falcon.CrowdStrike.com)
- [Https: // assets-public.falcon.CrowdStrike .com](https://assets-public.falcon.CrowdStrike.com)
- [Https: // api.CrowdStrike .com](https://api.CrowdStrike.com)
- [Https: // firehose.CrowdStrike .com](https://firehose.CrowdStrike.com)

**Us-2 environments:**

- [Http: // ts01-gyr-maverick.cloudsink.net](http://ts01-gyr-maverick.cloudsink.net)
- [Http: // lfodown01-gyr-maverick.cloudsink.net](http://lfodown01-gyr-maverick.cloudsink.net)
- [Http: // lfoup01-gyr-maverick.cloudsink.net](http://lfoup01-gyr-maverick.cloudsink.net)
- [Https: // falcon.us-2.CrowdStrike .com](https://falcon.us-2.CrowdStrike.com)
- [Https: // assets.falcon.us-2.CrowdStrike .com](https://assets.falcon.us-2.CrowdStrike.com)
- [Https: // assets-public.us-2.falcon.CrowdStrike .com](https://assets-public.us-2.falcon.CrowdStrike.com)
- [Http: // api.us-2.CrowdStrike .com](http://api.us-2.CrowdStrike.com)
- [Https: // firehose.us-2.CrowdStrike .com](https://firehose.us-2.CrowdStrike.com)

**Us-GOV-1 environment:**

- [Https: // ts01-laggar-gcw.cloudsink.net](https://ts01-laggar-gcw.cloudsink.net)
- [Http: // sensorproxy-laggar-g-524628337.us-gov-west-1.elb.amazonaws.com](http://sensorproxy-laggar-g-524628337.us-gov-west-1.elb.amazonaws.com)
- [Http: // lfodown01-laggar-gcw.cloudsink.net](http://lfodown01-laggar-gcw.cloudsink.net)
- [Http: // ELB-Laggar-P-LFO-DOWNLOAD-1265997121.us-gov-west-1.elb.amazonaws.com](http://ELB-Laggar-P-LFO-DOWNLOAD-1265997121.us-gov-west-1.elb.amazonaws.com)
- [Https: // falcon.laggar.gcw.CrowdStrike .com](https://falcon.laggar.gcw.CrowdStrike.com)
- [Http: // laggar-falconui01-g-245478519.us-gov-west-1.elb.amazonaws.com](http://laggar-falconui01-g-245478519.us-gov-west-1.elb.amazonaws.com)
- [Http: // api.laggar.gcw.CrowdStrike .com](http://api.laggar.gcw.CrowdStrike.com)
- [Https: // firehose.laggar.gcw.CrowdStrike .com](https://firehose.laggar.gcw.CrowdStrike.com)
- [Http: // falconhose-laggar-01-g-720386815.us-gov-west-1.elb.amazonaws.com](http://falconhose-laggar-01-g-720386815.us-gov-west-1.elb.amazonaws.com)

**Us-GOV-2 environments:**

[Http://ts01-us-gov-2.cloudsink.net](http://ts01-us-gov-2.cloudsink.net)

[Http://lfodown01-us-gov-2.cloudsink.net](http://lfodown01-us-gov-2.cloudsink.net)

[Http://api.us-gov-2.CrowdStrike.com](http://api.us-gov-2.CrowdStrike.com)

[Http://firehose.us-gov-2.CrowdStrike.com](http://firehose.us-gov-2.CrowdStrike.com)

#### **Eu-1 environment:**

[Http://ts01-lanner-lion.cloudsink.net](http://ts01-lanner-lion.cloudsink.net)

[Http://lfodown01-lanner-lion.cloudsink.net](http://lfodown01-lanner-lion.cloudsink.net)

[Http://lfoup01-lanner-lion.cloudsink.net](http://lfoup01-lanner-lion.cloudsink.net)

[Https://assets.falcon.eu-1.CrowdStrike.com](https://assets.falcon.eu-1.CrowdStrike.com)

[Https://assets-public.falcon.eu-1.CrowdStrike.com](https://assets-public.falcon.eu-1.CrowdStrike.com)

[Http://api.eu-1.CrowdStrike.com](http://api.eu-1.CrowdStrike.com)

[Https://firehose.eu-1.CrowdStrike.com](https://firehose.eu-1.CrowdStrike.com)

### **2.3 Network communication channel screening**

CrowdStrike Falcon Sensor has built-in network communication channel screening mechanism. on the premise that a global agent is configured in the Windows system, CrowdStrike Falcon Sensor will analyze the domain name to obtain its server IP, and then perform internal logic verification on the system agent. If the internal logic is not satisfied, the Windows Global Agent shall be bypassed directly, and the server shall be connected directly through the Windows network to obtain the policy and upload the data. (In Figure 12, 192.168.43.73 is Windows Global Agent)Figure 12 Example of bypassing the Windows system agent and connecting directly to its server through the system network to obtain policies and upload data 12



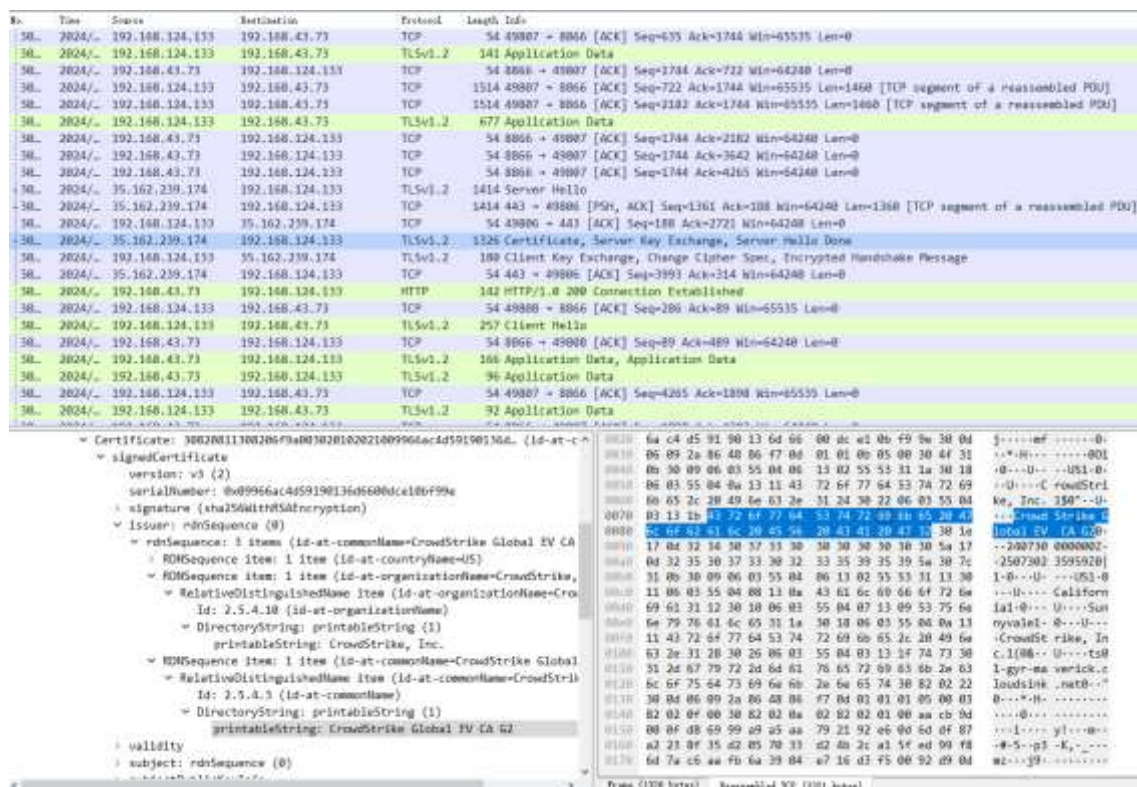


Figure 12 Example of bypassing the Windows system agent and connecting directly to its server through the system network to obtain policies and upload data 12

The relevant data flow is shown in Figure 13Figure 13 Example of bypassing the Windows system agent and directly connecting to its server through the system network to obtain policies and upload data 13

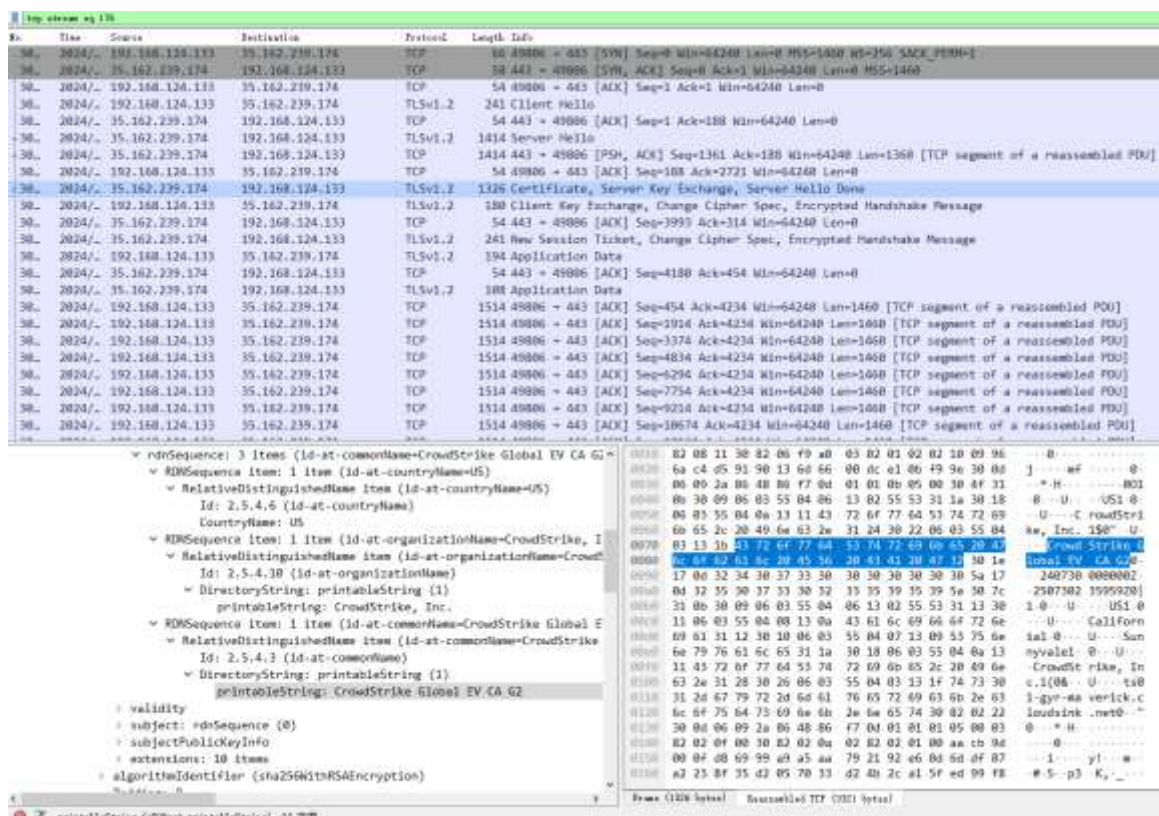


Figure 13 Example of bypassing the Windows system agent and directly connecting to its server through the system network to obtain policies and upload data 13

## 2.4 Internal certificate verification mechanism

CrowdStrike Falcon Sensor has a built-in certificate verification mechanism, which is independent of the Windows certificate management mechanism and does not trust the Windows credit certificate. When communicating with its server, the server certificate is verified using its internal certificate verification mechanism.

```

v26 = v13[1];
if ( v26 )
{
    if ( v26 != 1 || *v15 != 1 )
    {
        v27 = sub_1401E102B(v13, v15);
        v28 = v27;
        if ( v27 < 8 )
        {
            __mm_lfence();
            if ( Process != (PEPROCESS)&Process
                && *((_DWORD *)Process + 11) & 8 != 0
                && *((_BYTE *)Process + 41) >= 2u )
            {
                sub_1400B7EF4((__QWORD *)Process + 3, 125164, &unk_140267CC8, (unsigned int)v27);
            }
            sub_140075204(2164, 4164, "Certificate signature validation failed: %x", (unsigned int)v28);
            v29 = (void (__fastcall *))(__QWORD, __int64, __int64, __QWORD, int, __int64, __QWORD, __QWORD, __QWORD)sub_140075040(12000164);
            if ( v29 )
            {
                __mm_lfence();
                (**v29)(v29, 1006164, 3759276113164, 0164, 3880, v28, 0164, 0164, 0164);
            }
        }
    }
    v5 = 0;
}
else
{
    v3 = -536739819;
    if ( Process != (PEPROCESS)&Process
        && *((_DWORD *)Process + 11) & 8 != 0
        && *((_BYTE *)Process + 41) >= 2u )
    {
        sub_1400B7EF4((__QWORD *)Process + 3, 124164, &unk_140267CC8, 3758227477164);
    }
    sub_140075204(2164, 4164, "ValidateCertificate: CheckCertificate failed: %x", 3758227477164);
}
ExFreePoolWithTag(v13, 0x61435343u);
}

```

Figure 14 Example of data flow for policy acquisition and upload by directly connecting to its server through the system network, bypassing the Windows system agent 14

### 3 Summary

The official website of CrowdStrike gives the following information: "Reboot the host to give it an opportunity to download the diverted channel file. We strongly recommend pushing the host on a wired network (as open to WiFi) Prior to rebooting as the host will acquire internet connectivity reasonably fast via ethernet. Restart the host computer, giving it a chance to download the restored frequency files. We strongly recommend that the host be placed on a wired network (rather than WiFi) before restarting, as the host is much faster to get an internet connection via Ethernet. "From the analysis, CrowdStrike has a mechanism for rapid upgrade, At least after the loading phase of the Windows boot kernel is completed and the session manager is started, there will be an unconditional upgrade mechanism. Crowdstrike may be inclined to think that when the network is fast enough, the mandatory upgrade will be done before the blue screen. However, it is not ruled out that there is a lower level of pre-existing communication mechanism, but we have not been able to reproduce.

// BTW:

During the initial event validation, the Antiy Attack and Defense Lab discovered a strange phenomenon in which an earlier version of CrowdStrike was deployed in a public cloud environment, and the blue screen was triggered



after the deployment of the problem file C-00000291-00000000-00000xxx. But after its restart, the system can start normally. However, the same verification method is adopted in a single machine, and the screen is repeatedly blue.

We noted that in the discussion of the WeChat group, TK teacher suggested that we should pay attention to the CrowdStrike quick upgrade mechanism, and suggested that we resume the restart of the non-blue screen under the public cloud due to its quick growth mechanism.

Therefore, the relevant analysis work of this article was advanced, and thanks to teacher TK. We are continuing to analyze whether CrowdStrike has a lower-level rapid growth mechanism.

## Appendix I: Reference Materials

---

[1]. windows-security-best-practices-for-integrating-and-managing-security-tools/

<https://www.microsoft.com/en-us/security/blog/2024/07/27/>

## Appendix II: Introduction to Antiy Attack and Defense Laboratory

---

Antiy Attack & Defense Lab, affiliated to Antiy Security Service Center, is responsible for red and blue confrontation, vulnerability excavation and emergency analysis, and enhances the safety capability of Antiy products through security research and operation. Focus on the research of attack and defense techniques and tactics, vulnerability excavation and emergency analysis, output security capability plan, and realize the transformation of attack and defense capability. Currently, the department adopts the totem of the woodpecker from the Antiy Service Center. The woodpecker is known as the "doctor of the forest", which is very appropriate for the work of the Security Service Center, as it helps to eliminate network pests for customers.

## Appendix: About Antiy

---

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as “Code Red”, “Dvldr”, “Heartbleed”, “Bash Shellcode” and “WannaCry”. Antiy conducts continuous monitoring and in-depth analysis

against dozens of advanced cyberspace threat actors (APT groups) such as “Equation”, “White Elephant”, “Lotus” and “Greenspot” and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.