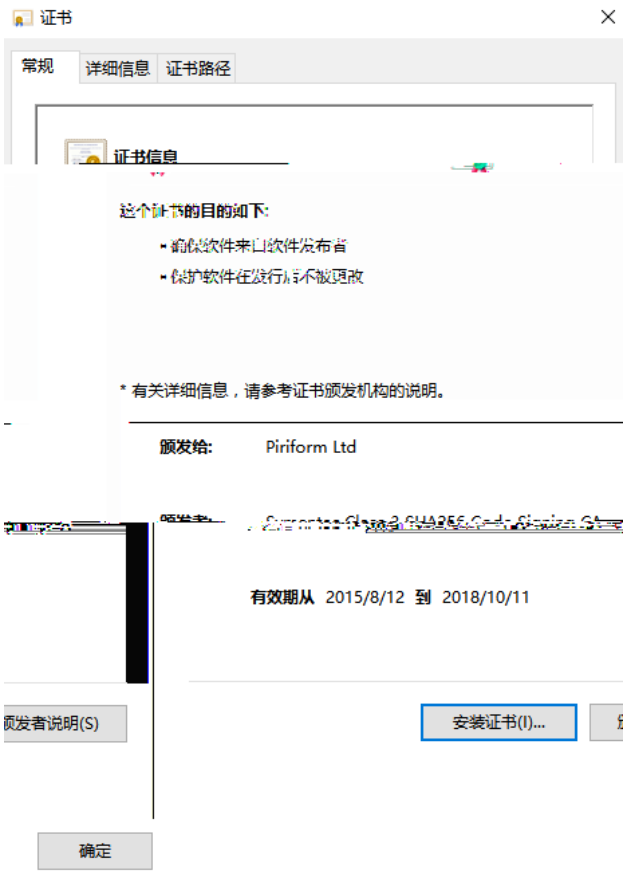
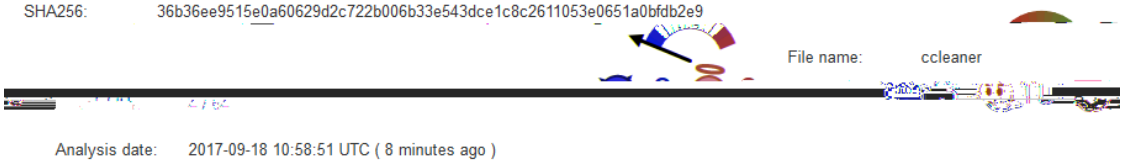
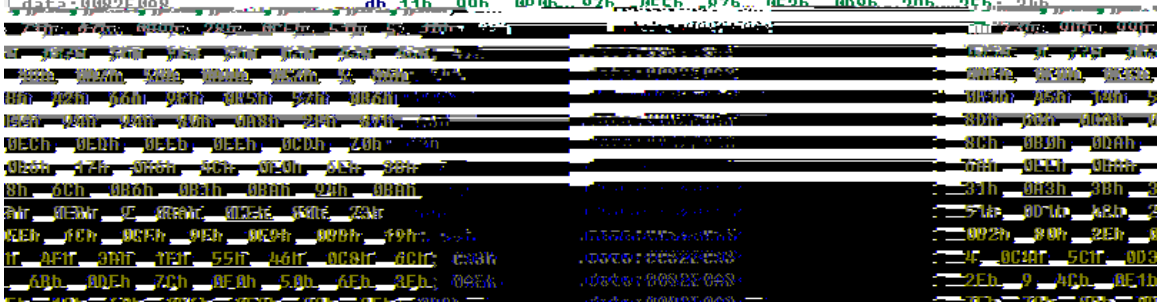
y



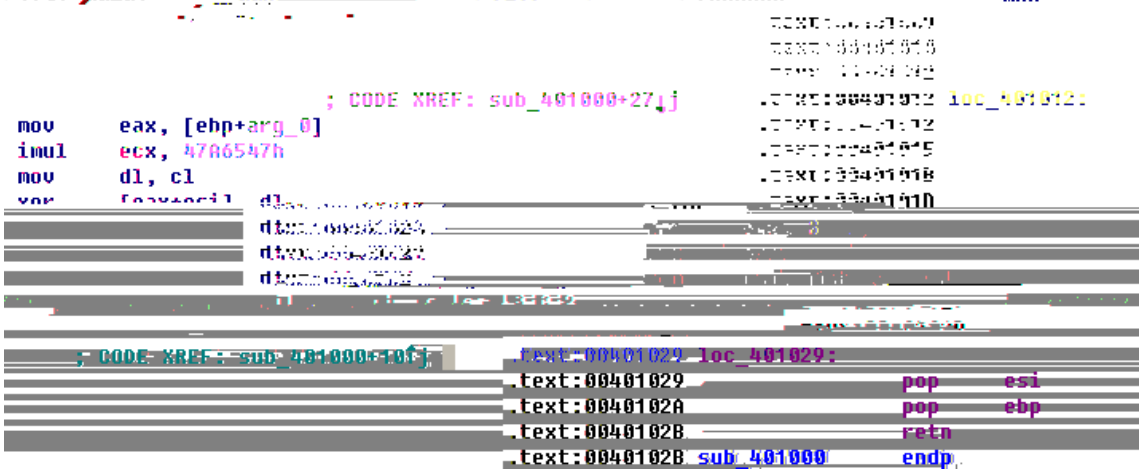


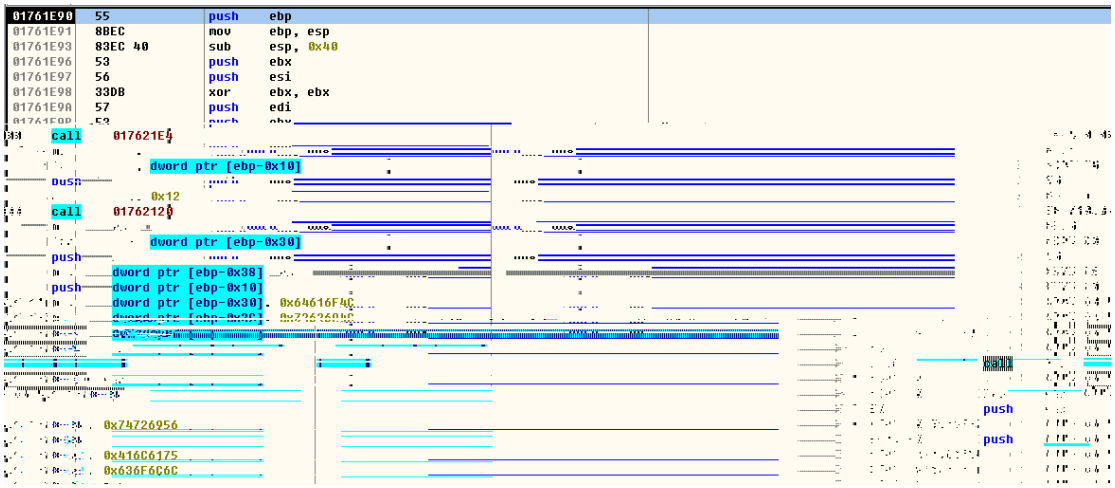
Analysis date: 2017-09-18 10:58:51 UTC (8 minutes ago)

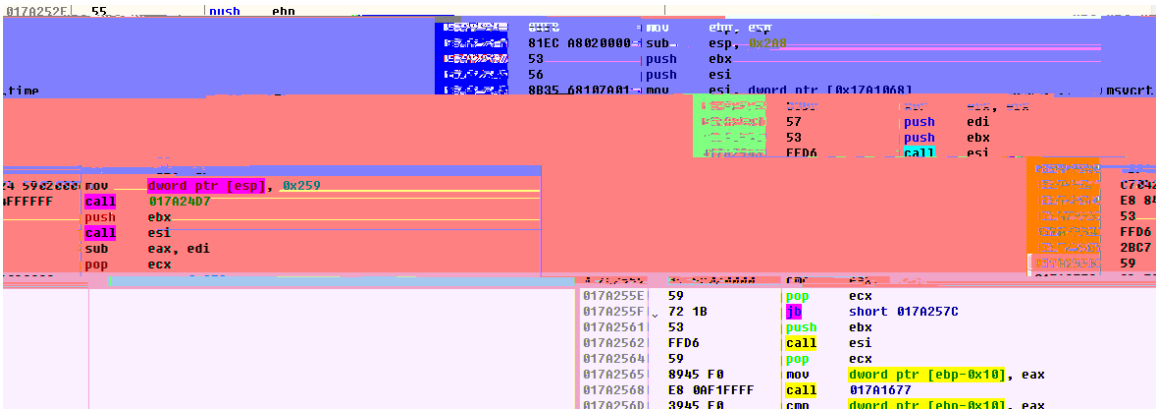
```
.data:0082E0A8 byte_82E0A8      db 0, 83h, 15h, 97h, 0C7h, 2Ch, 0C9h, 95h, 75h, 68h, 0C8h; 0
.data:0082E0A8                                          ; DATA XREF: CC_InfectionBase+10↑o
.data:0082E0A8                                          ; CC_InfectionBase:loc_40107B↑r ...
.data:0082E0A8                  db 0A1h, 3Dh, 76h, 7, 0CCh, 8Eh, 0F7h, 42h, 0B5h, 0BBh; 0Bh
.data:0082E0A8                  db 25h, 0BEh, 43h, 7Eh, 67h, 0ABh, 63h, 3Eh, 0F6h, 8, 37h; 15h
.data:0082E0A8                  db 0D0h, 0C6h, 8Ah, 0F8h, 0B9h, 0FFh, 27h, 5Bh, 3Ch, 6Eh; 20h
.data:0082E0A8                  db 45h, 9Ah, 3Fh, 0D3h, 5Dh, 25h, 2Eh, 1Dh, 0C2h, 6Bh; 2Ah
.data:0082E0A8                  db 11h, 00h, 0F0h, 97h, 0E5h, 87h, 0E2h, 0D9h, 20h, 25h; 2Bh
```

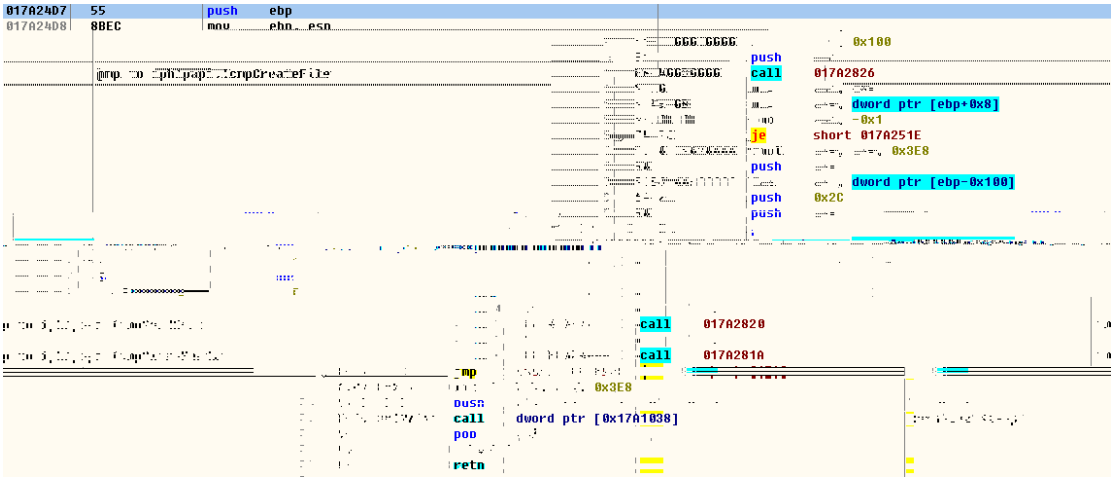


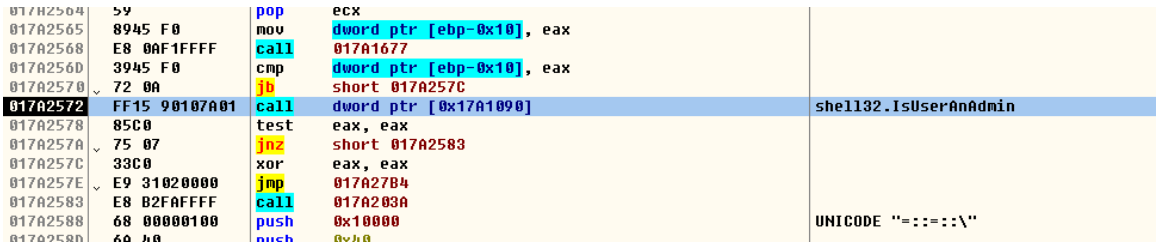
```
.text:00401000 sub_401000      proc near               ; CODE XREF: CC_InfectionBase+16↓p
.text:00401000                                         ; DATA XREF: HEADER:00400164↑o ...
.text:00401000
.text:00401000
.text:00401000 arg_0           = dword ptr  8
.text:00401000 arg_4           = dword ptr  0Ch
.text:00401000
.text:00401000                 mov     edi, edi
.text:00401002                 push    ebp
.text:00401003                 mov     ebp, esp
.text:00401005                 push    esi
.text:00401006                 xor     esi, esi
.text:00401008                 mov     ecx, 25A7383h
```

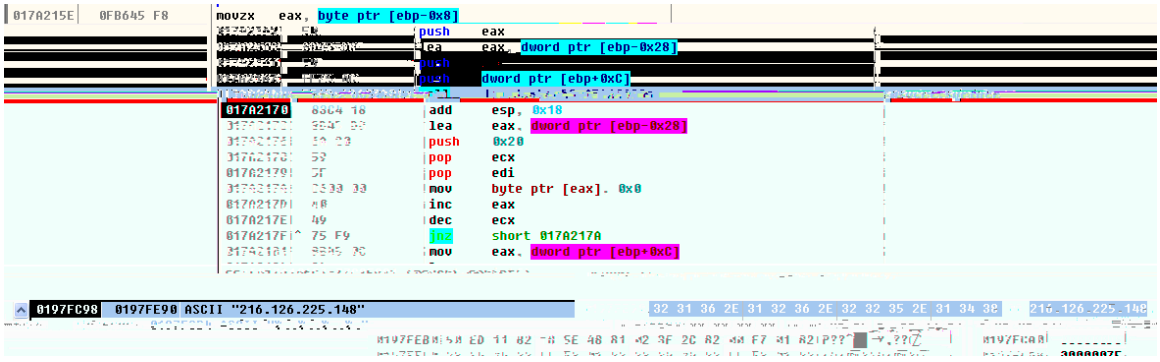









017A2564 59 pop ecx
017A2565 8945 F0 mov dword ptr [ebp-0x10], eax
017A2568 E8 0AF1FFFF call 017A1677
017A256D 3945 F0 cmp dword ptr [ebp-0x10], eax
017A2570 72 0A jb short 017A257C
017A2572 FF15 90107A01 call dword ptr [0x17A1090] shell32.IsUserAnAdmin
017A2578 85C0 test eax, eax
017A257A 75 07 jnz short 017A2583
017A257C 33C0 xor eax, eax
017A257E E9 31020000 jmp 017A27B4
017A2583 E8 B2FAFFFF call 017A203A
017A2588 68 00000100 push 0x10000 UNICODE "=::=::\"


017A215E 0FB645 F8 movzx eax, byte ptr [ebp-0x8]
017A2170 83C4 18 add esp, 0x18
lea eax, dword ptr [ebp-0x28]
push 0x20
pop ecx
pop edi
mov byte ptr [eax], 0x0
inc eax
dec ecx
017A217F 75 F9 jnz short 017A217A
mov eax, dword ptr [ebp+0xC]
0197FC98 0197FE90 ASCII "216.126.225.148"
32 31 36 2E 31 32 36 2E 32 32 35 2E 31 34 38 216.126.225.148
