



SHA256: 36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0bfd2e9

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+10f0
.data:0082E0A8 ; CC_InfectionBase:loc_40107Bfâ
.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, 00h, 90h, 71h, 67h, 0A0h, 28h, 0CEh, 51h, 5, 1Dh; 3Eh
.data:0082E0A8 db 0E7h, 0E8h, 0E9h, 48h, 0D2h, 58h, 0D0h, 0C7h, 5, 0Eh; 3Fh
.data:0082E0A8 db 0E7A: 45h, 14h, 58h, 42h, 66h, 9Eh, 0E5h, 57h, 0B6h; 40h
.data:0082E0A8 db 8Dh, 60h, 00Ah, 0E9h, 94h, 94h, 00h, 0A8h, 2Fh, 87h; 41h
.data:0082E0A8 db 0Ch, 0B0h, 0DAh, 0ECh, 0EDh, 0FFh, 0EEh, 0CDh, 70h; 42h
.data:0082E0A8 db 6Ah, 0EEh, 0BAh, 0D6h, 17h, 0A6h, 4Ch, 0F0h, 6Eh, 3Bh; 43h
.data:0082E0A8 db 31h, 0A3h, 3Bh, 38h, 6Ch, 0B6h, 0B1h, 0BAh, 94h, 0BAh; 44h
.data:0082E0A8 db 51h, 0D1h, 4Ch, 2Ah, 0E8h, 9, 0AAh, 0CEh, 80h, 23h; 45h
.data:0082E0A8 db 0B2h, 80h, 2Eh, 0FEh, 1Ch, 0CFh, 9Fh, 0F9h, 0BBh, 19h; 46h
.data:0082E0A8 db 4, 0C4h, 5Ch, 0D3h, 4Fh, 3Ah, 1Fh, 55h, 46h, 0C8h, 6Ch; 47h
.data:0082E0A8 db 2Fh, 9, 4Ch, 0E1h, 6Bh, 0DEh, 7Ch, 0F0h, 50h, 6Eh, 3Eh; 48h
.data:0082E0A8 db 7Eh, 70h, 00h, 0Eh, 40h, 30h, 0E5h, 0E6h, 0Ch, 0Eh; 49h

```

```

.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, 25A7382h

```

```

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

```

```

1000+10↑j | .text:00401029 loc_401029:                ; CODE XREF: sub_40
.text:00401029                                     pop     esi
.text:0040102A                                     pop     ebp
.text:0040102B                                     retn
.text:0040102B sub_401000      endp

```

The screenshot shows a debugger's instruction list window. The left pane displays assembly instructions with their addresses and hex values. The right pane shows the corresponding mnemonics and operands. The instructions are as follows:

Address	Hex	Mnemonic	Operands
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	5B	push	ebx
017621E5	Call	call	017621E5
017621E6	Call	call	017621E6
017621E7	Call	call	017621E7
017621E8	Call	call	017621E8
017621E9	Call	call	017621E9
017621EA	Call	call	017621EA
017621EB	Call	call	017621EB
017621EC	Call	call	017621EC
017621ED	Call	call	017621ED
017621EE	Call	call	017621EE
017621EF	Call	call	017621EF
017621F0	Call	call	017621F0
017621F1	Call	call	017621F1
017621F2	Call	call	017621F2
017621F3	Call	call	017621F3
017621F4	Call	call	017621F4
017621F5	Call	call	017621F5
017621F6	Call	call	017621F6
017621F7	Call	call	017621F7
017621F8	Call	call	017621F8
017621F9	Call	call	017621F9
017621FA	Call	call	017621FA
017621FB	Call	call	017621FB
017621FC	Call	call	017621FC
017621FD	Call	call	017621FD
017621FE	Call	call	017621FE
017621FF	Call	call	017621FF
01762200	Call	call	01762200
01762201	Call	call	01762201
01762202	Call	call	01762202
01762203	Call	call	01762203
01762204	Call	call	01762204
01762205	Call	call	01762205
01762206	Call	call	01762206
01762207	Call	call	01762207
01762208	Call	call	01762208
01762209	Call	call	01762209
0176220A	Call	call	0176220A
0176220B	Call	call	0176220B
0176220C	Call	call	0176220C
0176220D	Call	call	0176220D
0176220E	Call	call	0176220E
0176220F	Call	call	0176220F
01762210	Call	call	01762210
01762211	Call	call	01762211
01762212	Call	call	01762212
01762213	Call	call	01762213
01762214	Call	call	01762214
01762215	Call	call	01762215
01762216	Call	call	01762216
01762217	Call	call	01762217
01762218	Call	call	01762218
01762219	Call	call	01762219
0176221A	Call	call	0176221A
0176221B	Call	call	0176221B
0176221C	Call	call	0176221C
0176221D	Call	call	0176221D
0176221E	Call	call	0176221E
0176221F	Call	call	0176221F
01762220	Call	call	01762220
01762221	Call	call	01762221
01762222	Call	call	01762222
01762223	Call	call	01762223
01762224	Call	call	01762224
01762225	Call	call	01762225
01762226	Call	call	01762226
01762227	Call	call	01762227
01762228	Call	call	01762228
01762229	Call	call	01762229
0176222A	Call	call	0176222A
0176222B	Call	call	0176222B
0176222C	Call	call	0176222C
0176222D	Call	call	0176222D
0176222E	Call	call	0176222E
0176222F	Call	call	0176222F
01762230	Call	call	01762230
01762231	Call	call	01762231
01762232	Call	call	01762232
01762233	Call	call	01762233
01762234	Call	call	01762234
01762235	Call	call	01762235
01762236	Call	call	01762236
01762237	Call	call	01762237
01762238	Call	call	01762238
01762239	Call	call	01762239
0176223A	Call	call	0176223A
0176223B	Call	call	0176223B
0176223C	Call	call	0176223C
0176223D	Call	call	0176223D
0176223E	Call	call	0176223E
0176223F	Call	call	0176223F
01762240	Call	call	01762240
01762241	Call	call	01762241
01762242	Call	call	01762242
01762243	Call	call	01762243
01762244	Call	call	01762244
01762245	Call	call	01762245
01762246	Call	call	01762246
01762247	Call	call	01762247
01762248	Call	call	01762248
01762249	Call	call	01762249
0176224A	Call	call	0176224A
0176224B	Call	call	0176224B
0176224C	Call	call	0176224C
0176224D	Call	call	0176224D
0176224E	Call	call	0176224E
0176224F	Call	call	0176224F
01762250	Call	call	01762250
01762251	Call	call	01762251
01762252	Call	call	01762252
01762253	Call	call	01762253
01762254	Call	call	01762254
01762255	Call	call	01762255
01762256	Call	call	01762256
01762257	Call	call	01762257
01762258	Call	call	01762258
01762259	Call	call	01762259
0176225A	Call	call	0176225A
0176225B	Call	call	0176225B
0176225C	Call	call	0176225C
0176225D	Call	call	0176225D
0176225E	Call	call	0176225E
0176225F	Call	call	0176225F
01762260	Call	call	01762260
01762261	Call	call	01762261
01762262	Call	call	01762262
01762263	Call	call	01762263
01762264	Call	call	01762264
01762265	Call	call	01762265
01762266	Call	call	01762266
01762267	Call	call	01762267
01762268	Call	call	01762268
01762269	Call	call	01762269
0176226A	Call	call	0176226A
0176226B	Call	call	0176226B
0176226C	Call	call	0176226C
0176226D	Call	call	0176226D
0176226E	Call	call	0176226E
0176226F	Call	call	0176226F
01762270	Call	call	01762270
01762271	Call	call	01762271
01762272	Call	call	01762272
01762273	Call	call	01762273
01762274	Call	call	01762274
01762275	Call	call	01762275
01762276	Call	call	01762276
01762277	Call	call	01762277
01762278	Call	call	01762278
01762279	Call	call	01762279
0176227A	Call	call	0176227A
0176227B	Call	call	0176227B
0176227C	Call	call	0176227C
0176227D	Call	call	0176227D
0176227E	Call	call	0176227E
0176227F	Call	call	0176227F
01762280	Call	call	01762280
01762281	Call	call	01762281
01762282	Call	call	01762282
01762283	Call	call	01762283
01762284	Call	call	01762284
01762285	Call	call	01762285
01762286	Call	call	01762286
01762287	Call	call	01762287
01762288	Call	call	01762288
01762289	Call	call	01762289
0176228A	Call	call	0176228A
0176228B	Call	call	0176228B
0176228C	Call	call	0176228C
0176228D	Call	call	0176228D
0176228E	Call	call	0176228E
0176228F	Call	call	0176228F
01762290	Call	call	01762290
01762291	Call	call	01762291
01762292	Call	call	01762292
01762293	Call	call	01762293
01762294	Call	call	01762294
01762295	Call	call	01762295
01762296	Call	call	01762296
01762297	Call	call	01762297
01762298	Call	call	01762298
01762299	Call	call	01762299
0176229A	Call	call	0176229A
0176229B	Call	call	0176229B
0176229C	Call	call	0176229C
0176229D	Call	call	0176229D
0176229E	Call	call	0176229E
0176229F	Call	call	0176229F
017622A0	Call	call	017622A0
017622A1	Call	call	017622A1
017622A2	Call	call	017622A2
017622A3	Call	call	017622A3
017622A4	Call	call	017622A4
017622A5	Call	call	017622A5
017622A6	Call	call	017622A6
017622A7	Call	call	017622A7
017622A8	Call	call	017622A8
017622A9	Call	call	017622A9
017622AA	Call	call	017622AA
017622AB	Call	call	017622AB
017622AC	Call	call	017622AC
017622AD	Call	call	017622AD
017622AE	Call	call	017622AE
017622AF	Call	call	017622AF
017622B0	Call	call	017622B0
017622B1	Call	call	017622B1
017622B2	Call	call	017622B2
017622B3	Call	call	017622B3
017622B4	Call	call	017622B4
017622B5	Call	call	017622B5
017622B6	Call	call	017622B6
017622B7	Call	call	017622B7
017622B8	Call	call	017622B8
017622B9	Call	call	017622B9
017622BA	Call	call	017622BA
017622BB	Call	call	017622BB
017622BC	Call	call	017622BC
017622BD	Call	call	017622BD
017622BE	Call	call	017622BE
017622BF	Call	call	017622BF
017622C0	Call	call	017622C0
017622C1	Call	call	017622C1
017622C2	Call	call	017622C2
017622C3	Call	call	017622C3
017622C4	Call	call	017622C4
017622C5	Call	call	017622C5
017622C6	Call	call	017622C6
017622C7	Call	call	017622C7
017622C8	Call	call	017622C8
017622C9	Call	call	017622C9
017622CA	Call	call	017622CA
017622CB	Call	call	017622CB
017622CC	Call	call	017622CC
017622CD	Call	call	017622CD

```

017A25E1 55      push  ebp
017A25E2 81EC A8020000 sub  esp, 0x208
017A25E3 53      push  ebx
017A25E4 56      push  esi
017A25E5 8B35 681A7A81 mov  esi, dword ptr [0x17A1A81]
017A25E6 57      push  edi
017A25E7 53      push  ebx
017A25E8 FFDA    call  esi
017A25E9 59      pop   ecx
017A25EA 72 1B   jb   short 017A257C
017A25EB 53      push  ebx
017A25EC FFDA    call  esi
017A25ED 59      pop   ecx
017A25EE 8945 F0 mov  dword ptr [ebp-0x10], eax
017A25EF E8 0AF1FFFF call 017A1677
017A25F0 3945 F8 cmp  dword ptr [ebp-0x10], eax

```

```

017A24D7 55      push  ebp
017A24D8 8BEC    mov  ebp, esp
017A2504 59      pop   ecx
017A2505 8945 F0 mov  dword ptr [ebp-0x10], eax
017A2506 E8 0AF1FFFF call 017A1677
017A2507 3945 F0 cmp  dword ptr [ebp-0x10], eax
017A2508 72 0A   jb   short 017A257C
017A2509 FF15 901A7A81 call dword ptr [0x17A1A90]
017A250A 85C0    test  eax, eax
017A250B 75 07   jnz  short 017A2583
017A250C 33C0    xor  eax, eax
017A250D E9 31020000 jmp 017A27B4
017A250E E8 B2FAFFFF call 017A203A
017A250F 68 00000100 push 0x10000
017A2510 6A 0A   push 0x0A

```

```

017A2572 FF15 901A7A81 call dword ptr [0x17A1A90] shell32.IsUserAnAdmin
017A2573 85C0    test  eax, eax
017A2574 75 07   jnz  short 017A2583
017A2575 33C0    xor  eax, eax
017A2576 E9 31020000 jmp 017A27B4
017A2577 E8 B2FAFFFF call 017A203A
017A2578 68 00000100 push 0x10000
017A2579 6A 0A   push 0x0A

```

```

017A215E 0FB645 F8 movzx  eax, byte ptr [ebp-0x8]
017A215F 51      push  eax
017A2160 2307 07 lea  eax, dword ptr [ebp-0x28]
017A2161 59      push  eax
017A2162 FF75 0C push  dword ptr [ebp+0xC]
017A2170 8304 18 add  esp, 0x18
017A2171 2307 07 lea  eax, dword ptr [ebp-0x28]
017A2172 5A 03  push  0x20
017A2173 59      pop   ecx
017A2174 5F      pop   edi
017A2175 2E33 33 mov  byte ptr [eax], 0x0
017A2176 48      inc  eax
017A2177 49      dec  ecx
017A2178 75 F9   jnz  short 017A217A
017A2179 2307 07 lea  eax, dword ptr [ebp+0xC]

```


