



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+10f0
.data:0082E0A8 ; CC_InfectionBase:loc_40107Bf ...
.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, 3Bh, 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
.data:0082E0A8 db 7Fh, 70h, 0Bh, 0FEh, 40h, 40h, 0B6h, 0FEh, 0Bh, 0FEh; 0B0h
```

```

.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 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 var_4 = dword ptr -4
.text:0040101F var_8 = dword ptr -8
.text:00401021 var_0 = dword ptr 0
.text:00401023 var_4 = dword ptr -4
.text:00401025 var_8 = dword ptr -8
.text:00401027 var_0 = dword ptr 0
.text:00401029 loc_401029: ; CODE XREF: sub_401000+10↑j
.text:00401029 pop esi
.text:0040102A pop ebp
.text:0040102B retn
sub_401000 endp

```

[illegible]

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]	shell132.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 "====\"
017A258D	60 00	push	0x10000	

Address	Disassembly	Comment
017A215E	0FB645 F8 movzx eax, byte ptr [ebp-0x8]	
017A2161	push eax	
017A2162	lea eax, dword ptr [ebp-0x28]	
017A2165	push eax	
017A2166	push dword ptr [ebp+0xC]	
017A2169	call dword ptr [0x17A106C]	memset.sprintf
017A216C	add esp, 0x18	
017A216F	lea eax, dword ptr [ebp-0x28]	
017A2172	push 0x20	
017A2175	pop ecx	
017A2178	pop edi	
017A217B	mov byte ptr [eax], 0x0	
017A217E	inc eax	
017A2181	dec ecx	
017A2184	jnz short 017A217A	
017A2187	mov eax, dword ptr [ebp+0xC]	
017A218A	ret 0	

