

†


```

.text:00401000 sub_401000      proc near                                ; CODE XREF: CC_InfectionBase+16↓p
.text:00401000                                     ; DATA XREF: HEADER:00400164↑o ...
.text:00401000                                     = dword ptr 8
.text:00401000 arg_0      = dword ptr 0Ch
.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, 25h7382h

```

```

; CODE XREF: sub_401000+27↑j
mov     eax, [ebp+arg_0]
imul    ecx, 4786547h
mov     dl, cl
xor     ecx, ecx

```

```

.text:00401012 loc_401012:
.text:00401012
.text:00401015
.text:00401018
.text:0040101B

```

```

; CODE XREF: sub_401000+10↑j

```

```

.text:00401029 loc_401029:
.text:00401029
.text:0040102A
.text:0040102B
.text:0040102B sub_401000

```

```

pop     esi
pop     ebp
retn
endp

```

Address	Disassembly	Comment
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	58 push ebx	
01761E9C	CALL 017621E6	
01761E9D	CALL 017621E6	
01761E9E	CALL 017621E6	
01761E9F	CALL 017621E6	
01761EA0	CALL 017621E6	
01761EA1	CALL 017621E6	
01761EA2	CALL 017621E6	
01761EA3	CALL 017621E6	
01761EA4	CALL 017621E6	
01761EA5	CALL 017621E6	
01761EA6	CALL 017621E6	
01761EA7	CALL 017621E6	
01761EA8	CALL 017621E6	
01761EA9	CALL 017621E6	
01761EAA	CALL 017621E6	
01761EAB	CALL 017621E6	
01761EAC	CALL 017621E6	
01761EAD	CALL 017621E6	
01761EAE	CALL 017621E6	
01761EAF	CALL 017621E6	
01761EB0	CALL 017621E6	
01761EB1	CALL 017621E6	
01761EB2	CALL 017621E6	
01761EB3	CALL 017621E6	
01761EB4	CALL 017621E6	
01761EB5	CALL 017621E6	
01761EB6	CALL 017621E6	
01761EB7	CALL 017621E6	
01761EB8	CALL 017621E6	
01761EB9	CALL 017621E6	
01761EBA	CALL 017621E6	
01761EBB	CALL 017621E6	
01761EBC	CALL 017621E6	
01761EBD	CALL 017621E6	
01761EBE	CALL 017621E6	
01761EBF	CALL 017621E6	
01761EC0	CALL 017621E6	
01761EC1	CALL 017621E6	
01761EC2	CALL 017621E6	
01761EC3	CALL 017621E6	
01761EC4	CALL 017621E6	
01761EC5	CALL 017621E6	
01761EC6	CALL 017621E6	
01761EC7	CALL 017621E6	
01761EC8	CALL 017621E6	
01761EC9	CALL 017621E6	
01761ECA	CALL 017621E6	
01761ECB	CALL 017621E6	
01761ECC	CALL 017621E6	
01761ECD	CALL 017621E6	
01761ECE	CALL 017621E6	
01761ECF	CALL 017621E6	
01761ED0	CALL 017621E6	
01761ED1	CALL 017621E6	
01761ED2	CALL 017621E6	
01761ED3	CALL 017621E6	
01761ED4	CALL 017621E6	
01761ED5	CALL 017621E6	
01761ED6	CALL 017621E6	
01761ED7	CALL 017621E6	
01761ED8	CALL 017621E6	
01761ED9	CALL 017621E6	
01761EDA	CALL 017621E6	
01761EDB	CALL 017621E6	
01761EDC	CALL 017621E6	
01761EDD	CALL 017621E6	
01761EDE	CALL 017621E6	
01761EDF	CALL 017621E6	
01761EE0	CALL 017621E6	
01761EE1	CALL 017621E6	
01761EE2	CALL 017621E6	
01761EE3	CALL 017621E6	
01761EE4	CALL 017621E6	
01761EE5	CALL 017621E6	
01761EE6	CALL 017621E6	
01761EE7	CALL 017621E6	
01761EE8	CALL 017621E6	
01761EE9	CALL 017621E6	
01761EEA	CALL 017621E6	
01761EEB	CALL 017621E6	
01761EEC	CALL 017621E6	
01761EED	CALL 017621E6	
01761EEF	CALL 017621E6	
01761EF0	CALL 017621E6	
01761EF1	CALL 017621E6	
01761EF2	CALL 017621E6	
01761EF3	CALL 017621E6	
01761EF4	CALL 017621E6	
01761EF5	CALL 017621E6	
01761EF6	CALL 017621E6	
01761EF7	CALL 017621E6	
01761EF8	CALL 017621E6	
01761EF9	CALL 017621E6	
01761EFA	CALL 017621E6	
01761EFB	CALL 017621E6	
01761EFC	CALL 017621E6	
01761EFD	CALL 017621E6	
01761EFE	CALL 017621E6	
01761EFF	CALL 017621E6	
01761F00	CALL 017621E6	
01761F01	CALL 017621E6	
01761F02	CALL 017621E6	
01761F03	CALL 017621E6	
01761F04	CALL 017621E6	
01761F05	CALL 017621E6	
01761F06	CALL 017621E6	
01761F07	CALL 017621E6	
01761F08	CALL 017621E6	
01761F09	CALL 017621E6	
01761F0A	CALL 017621E6	
01761F0B	CALL 017621E6	
01761F0C	CALL 017621E6	
01761F0D	CALL 017621E6	
01761F0E	CALL 017621E6	
01761F0F	CALL 017621E6	
01761F10	CALL 017621E6	
01761F11	CALL 017621E6	
01761F12	CALL 017621E6	
01761F13	CALL 017621E6	
01761F14	CALL 017621E6	
01761F15	CALL 017621E6	
01761F16	CALL 017621E6	
01761F17	CALL 017621E6	
01761F18	CALL 017621E6	
01761F19	CALL 017621E6	
01761F1A	CALL 017621E6	
01761F1B	CALL 017621E6	
01761F1C	CALL 017621E6	
01761F1D	CALL 017621E6	
01761F1E	CALL 017621E6	
01761F1F	CALL 017621E6	
01761F20	CALL 017621E6	
01761F21	CALL 017621E6	
01761F22	CALL 017621E6	
01761F23	CALL 017621E6	
01761F24	CALL 017621E6	
01761F25	CALL 017621E6	
01761F26	CALL 017621E6	
01761F27	CALL 017621E6	
01761F28	CALL 017621E6	
01761F29	CALL 017621E6	
01761F2A	CALL 017621E6	
01761F2B	CALL 017621E6	
01761F2C	CALL 017621E6	
01761F2D	CALL 017621E6	
01761F2E	CALL 017621E6	
01761F2F	CALL 017621E6	
01761F30	CALL 017621E6	
01761F31	CALL 017621E6	
01761F32	CALL 017621E6	
01761F33	CALL 017621E6	
01761F34	CALL 017621E6	
01761F35	CALL 017621E6	
01761F36	CALL 017621E6	
01761F37	CALL 017621E6	
01761F38	CALL 017621E6	
01761F39	CALL 017621E6	
01761F3A	CALL 017621E6	
01761F3B	CALL 017621E6	
01761F3C	CALL 017621E6	
01761F3D	CALL 017621E6	
01761F3E	CALL 017621E6	
01761F3F	CALL 017621E6	
01761F40	CALL 017621E6	
01761F41	CALL 017621E6	
01761F42	CALL 017621E6	
01761F43	CALL 017621E6	
01761F44	CALL 017621E6	
01761F45	CALL 017621E6	
01761F46	CALL 017621E6	
01761F47	CALL 017621E6	
01761F48	CALL 017621E6	
01761F49	CALL 017621E6	
01761F4A	CALL 017621E6	
01761F4B	CALL 017621E6	
01761F4C	CALL 017621E6	
01761F4D	CALL 017621E6	
01761F4E	CALL 017621E6	
01761F4F	CALL 017621E6	
01761F50	CALL 017621E6	
01761F51	CALL 017621E6	
01761F52	CALL 017621E6	
01761F53	CALL 017621E6	
01761F54	CALL 017621E6	
01761F55	CALL 017621E6	
01761F56	CALL 017621E6	
01761F57	CALL 017621E6	
01761F58	CALL 017621E6	
01761F59	CALL 017621E6	
01761F5A	CALL 017621E6	
01761F5B	CALL 017621E6	
01761F5C	CALL 017621E6	
01761F5D	CALL 017621E6	
01761F5E	CALL 017621E6	
01761F5F	CALL 017621E6	
01761F60	CALL 017621E6	
01761F61	CALL 017621E6	
01761F62	CALL 017621E6	
01761F63	CALL 017621E6	
01761F64	CALL 017621E6	
01761F65	CALL 017621E6	
01761F66	CALL 017621E6	
01761F67	CALL 017621E6	
01761F68	CALL 017621E6	
01761F69	CALL 017621E6	
01761F6A	CALL 017621E6	
01761F6B	CALL 017621E6	
01761F6C	CALL 017621E6	
01761F6D	CALL 017621E6	
01761F6E	CALL 017621E6	
01761F6F	CALL 017621E6	
01761F70	CALL 017621E6	
01761F71	CALL 017621E6	
01761F72	CALL 017621E6	
01761F73	CALL 017621E6	
01761F74	CALL 017621E6	
01761F75	CALL 017621E6	
01761F76	CALL 017621E6	
01761F77	CALL 017621E6	
01761F78	CALL 017621E6	
01761F79	CALL 017621E6	
01761F7A	CALL 017621E6	
01761F7B	CALL 017621E6	
01761F7C	CALL 017621E6	
01761F7D	CALL 017621E6	
01761F7E	CALL 017621E6	
01761F7F	CALL 017621E6	
01761F80	CALL 017621E6	
01761F81	CALL 017621E6	
01761F82	CALL 017621E6	
01761F83	CALL 017621E6	
01761F84	CALL 017621E6	
01761F85	CALL 017621E6	
01761F86	CALL 017621E6	
01761F87	CALL 017621E6	
01761F88	CALL 017621E6	
01761F89	CALL 017621E6	
01761F8A	CALL 017621E6	
01761F8B	CALL 017621E6	
01761F8C	CALL 017621E6	
01761F8D	CALL 017621E6	
01761F8E	CALL 017621E6	
01761F8F	CALL 017621E6	
01761F90	CALL 017621E6	
01761F91	CALL 017621E6	
01761F92	CALL 017621E6	
01761F93	CALL 017621E6	
01761F94	CALL 017621E6	
01761F95	CALL 017621E6	
01761F96	CALL 017621E6	
01761F97	CALL 017621E6	
01761F98	CALL 017621E6	
01761F99	CALL 017621E6	
01761F9A	CALL 017621E6	
01761F9B	CALL 017621E6	
01761F9C	CALL 017621E6	
01761F9D	CALL 017621E6	
01761F9E	CALL 017621E6	
01761F9F	CALL 017621E6	
01761FA0	CALL 017621E6	
01761FA1	CALL 017621E6	
01761FA2	CALL 017621E6	
01761FA3	CALL 017621E6	
01761FA4	CALL 017621E6	
01761FA5	CALL 017621E6	
01761FA6	CALL 017621E6	
01761FA7	CALL 017621E6	
01761FA8	CALL 017621E6	
01761FA9	CALL 017621E6	
01761FAA	CALL 017621E6	
01761FAB	CALL 017621E6	
01761FAC	CALL 017621E6	
01761FAD	CALL 017621E6	

[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]	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 "\00000001"
017A258D	6A 0A	push	0x0A	

[illegible]

