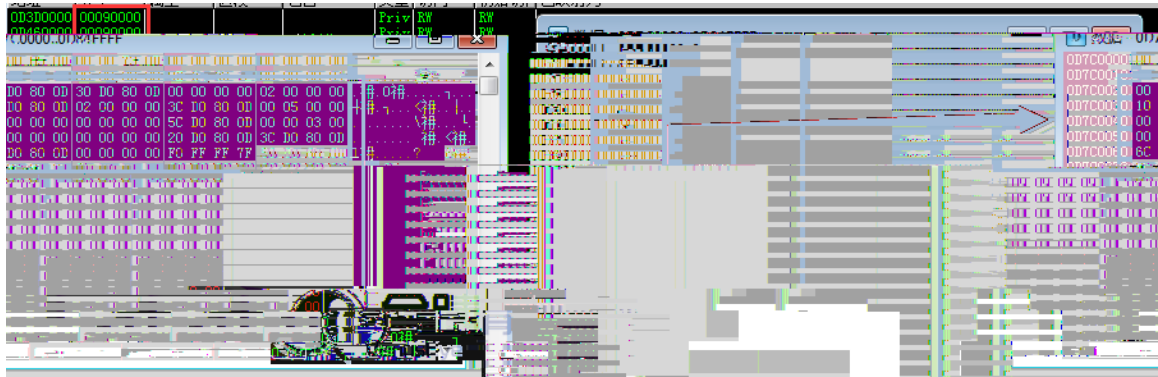




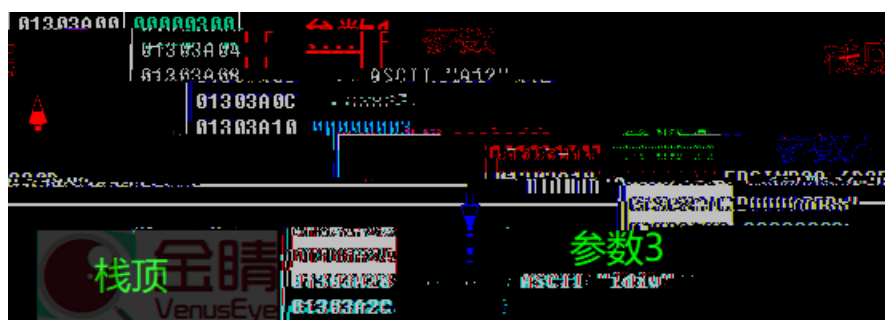
[illegible]

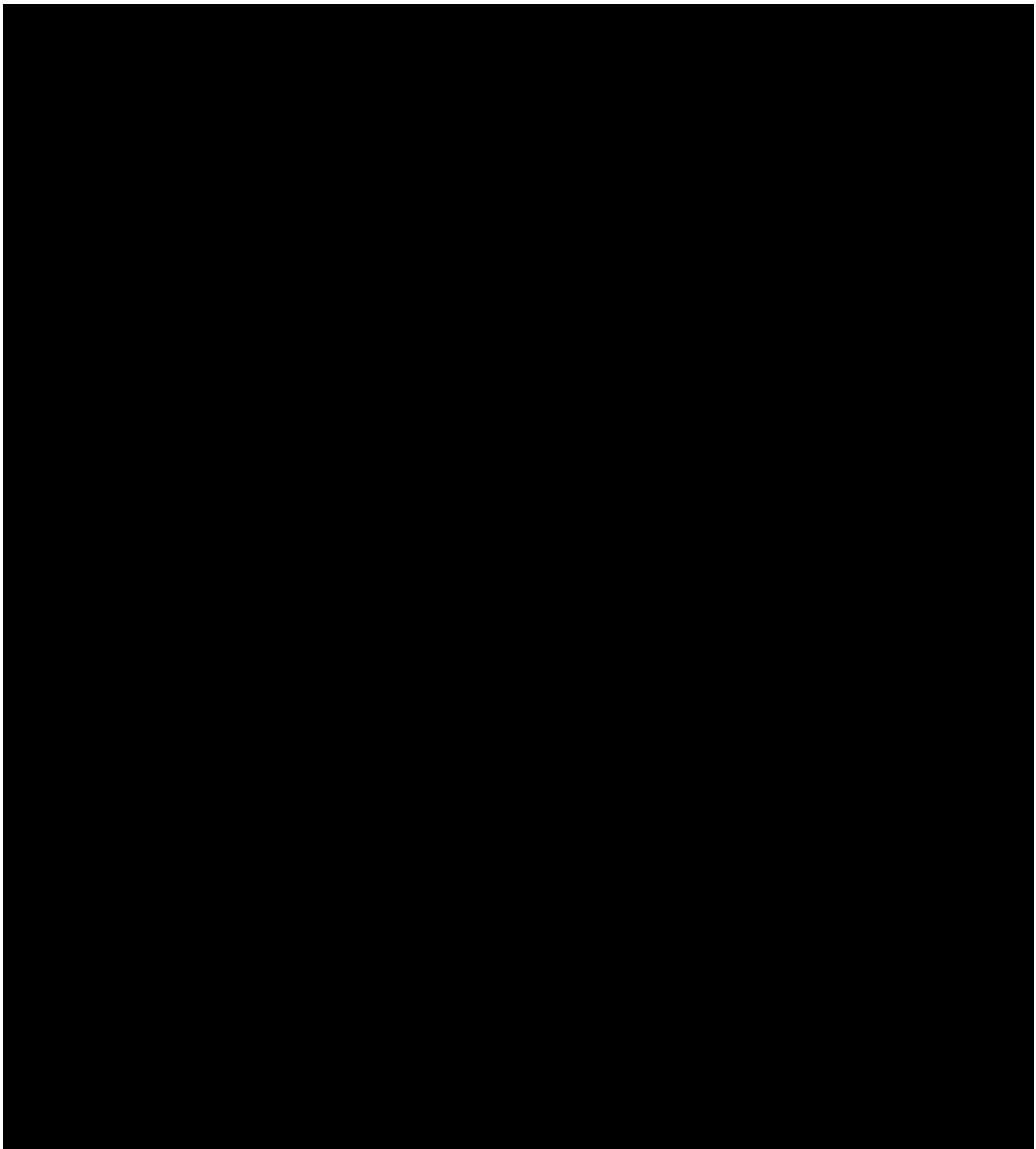
cd0800d000000000f0fff
余晴



● ● ● ● ● ●

地址	数值	注释
00181618	01803000	
0018161C	01803000	
00181620	01803000	
00181624	01803000	
00181628	01803000	
0018162C	01803000	
00181630	01803000	
00181634	01803000	
00181638	01803000	
0018163C	01803000	
00181640	01803000	
00181644	01803000	
00181648	01803000	
0018164C	01803000	
00181650	01803000	
00181654	01803000	
00181658	01803000	
0018165C	01803000	
00181660	01803000	
00181664	01803000	
00181668	01803000	
0018166C	01803000	
00181670	01803000	
00181674	01803000	
00181678	01803000	
0018167C	01803000	
00181680	01803000	
00181684	01803000	
00181688	01803000	
0018168C	01803000	
00181690	01803000	
00181694	01803000	
00181698	01803000	
0018169C	01803000	
001816A0	01803000	
001816A4	01803000	
001816A8	01803000	
001816AC	01803000	
001816B0	01803000	
001816B4	01803000	
001816B8	01803000	
001816BC	01803000	
001816C0	01803000	
001816C4	01803000	
001816C8	01803000	
001816CC	01803000	
001816D0	01803000	
001816D4	01803000	
001816D8	01803000	
001816DC	01803000	
001816E0	01803000	
001816E4	01803000	
001816E8	01803000	
001816EC	01803000	
001816F0	01803000	
001816F4	01803000	
001816F8	01803000	
001816FC	01803000	
00181700	01803000	
00181704	01803000	
00181708	01803000	
0018170C	01803000	
00181710	01803000	
00181714	01803000	
00181718	01803000	
0018171C	01803000	
00181720	01803000	
00181724	01803000	
00181728	01803000	
0018172C	01803000	
00181730	01803000	
00181734	01803000	
00181738	01803000	
0018173C	01803000	
00181740	01803000	
00181744	01803000	
00181748	01803000	
0018174C	01803000	
00181750	01803000	
00181754	01803000	
00181758	01803000	
0018175C	01803000	
00181760	01803000	
00181764	01803000	
00181768	01803000	
0018176C	01803000	
00181770	01803000	
00181774	01803000	
00181778	01803000	
0018177C	01803000	
00181780	01803000	
00181784	01803000	
00181788	01803000	
0018178C	01803000	
00181790	01803000	
00181794	01803000	
00181798	01803000	
0018179C	01803000	
001817A0	01803000	
001817A4	01803000	
001817A8	01803000	
001817AC	01803000	
001817B0	01803000	
001817B4	01803000	
001817B8	01803000	
001817BC	01803000	
001817C0	01803000	
001817C4	01803000	
001817C8	01803000	
001817CC	01803000	
001817D0	01803000	
001817D4	01803000	
001817D8	01803000	
001817DC	01803000	
001817E0	01803000	
001817E4	01803000	
001817E8	01803000	
001817EC	01803000	
001817F0	01803000	
001817F4	01803000	
001817F8	01803000	
001817FC	01803000	
00181800	01803000	
00181804	01803000	
00181808	01803000	
0018180C	01803000	
00181810	01803000	
00181814	01803000	
00181818	01803000	
0018181C	01803000	
00181820	01803000	
00181824	01803000	
00181828	01803000	
0018182C	01803000	
00181830	01803000	
00181834	01803000	
00181838	01803000	
0018183C	01803000	
00181840	01803000	
00181844	01803000	
00181848	01803000	
0018184C	01803000	
00181850	01803000	
00181854	01803000	
00181858	01803000	
0018185C	01803000	
00181860	01803000	
00181864	01803000	
00181868	01803000	
0018186C	01803000	
00181870	01803000	
00181874	01803000	
00181878	01803000	
0018187C	01803000	
00181880	01803000	
00181884	01803000	
00181888	01803000	
0018188C	01803000	
00181890	01803000	
00181894	01803000	
00181898	01803000	
0018189C	01803000	
001818A0	01803000	
001818A4	01803000	
001818A8	01803000	
001818AC	01803000	
001818B0	01803000	
001818B4	01803000	
001818B8	01803000	
001818BC	01803000	
001818C0	01803000	
001818C4	01803000	
001818C8	01803000	
001818CC	01803000	
001818D0	01803000	
001818D4	01803000	
001818D8	01803000	
001818DC	01803000	
001818E0	01803000	
001818E4	01803000	
001818E8	01803000	
001818EC	01803000	
001818F0	01803000	
001818F4	01803000	
001818F8	01803000	
001818FC	01803000	
00181900	01803000	
00181904	01803000	
00181908	01803000	
0018190C	01803000	
00181910	01803000	
00181914	01803000	
00181918	01803000	
0018191C	01803000	
00181920	01803000	
00181924	01803000	
00181928	01803000	
0018192C	01803000	
00181930	01803000	
00181934	01803000	
00181938	01803000	
0018193C	01803000	
00181940	01803000	
00181944	01803000	
00181948	01803000	
0018194C	01803000	
00181950	01803000	
00181954	01803000	
00181958	01803000	
0018195C	01803000	
00181960	01803000	
00181964	01803000	
00181968	01803000	
0018196C	01803000	
00181970	01803000	
00181974	01803000	
00181978	01803000	
0018197C	01803000	
00181980	01803000	
00181984	01803000	
00181988	01803000	
0018198C	01803000	
00181990	01803000	
00181994	01803000	
00181998	01803000	
0018199C	01803000	
001819A0	01803000	
001819A4	01803000	
001819A8	01803000	
001819AC	01803000	
001819B0	01803000	
001819B4	01803000	
001819B8	01803000	
001819BC	01803000	
001819C0	01803000	
001819C4	01803000	
001819C8	01803000	
001819CC	01803000	
001819D0	01803000	
001819D4	01803000	
001819D8	01803000	
001819DC	01803000	
001819E0	01803000	
001819E4	01803000	
001819E8	01803000	
001819EC	01803000	
001819F0	01803000	
001819F4	01803000	
001819F8	01803000	
001819FC	01803000	
00181A00	01803000	
00181A04	01803000	
00181A08	01803000	
00181A0C	01803000	
00181A10	01803000	
00181A14	01803000	
00181A18	01803000	
00181A1C	01803000	
00181A20	01803000	
00181A24	01803000	
00181A28	01803000	
00181A2C	01803000	
00181A30	01803000	
00181A34	01803000	
00181A38	01803000	
00181A3C	01803000	
00181A40	01803000	
00181A44	01803000	
00181A48	01803000	
00181A4C	01803000	
00181A50	01803000	
00181A54	01803000	
00181A58	01803000	
00181A5C	01803000	
00181A60	01803000	
00181A64	01803000	
00181A68	01803000	
00181A6C	01803000	
00181A70	01803000	
00181A74	01803000	
00181A78	01803000	
00181A7C	01803000	
00181A80	01803000	
00181A84	01803000	
00181A88	01803000	
00181A8C	01803000	
00181A90	01803000	
00181A94	01803000	
00181A98	01803000	
00181A9C	01803000	
00181AA0	01803000	
00181AA4	01803000	
00181AA8	01803000	
00181AAC	01803000	
00181AB0	01803000	
00181AB4	01803000	
00181AB8	01803000	
00181ABC	01803000	
00181ABD	01803000	
00181ABE	01803000	
00181ABF	01803000	
00181AC0	01803000	
00181AC4	01803000	
00181AC8	01803000	
00181ACC	01803000	
00181ACD	01803000	
00181ACE	01803000	
00181ACF	01803000	
00181AD0	01803000	
00181AD4	01803000	
00181AD8	01803000	
00181ADC	01803000	
00181ADD	01803000	
00181ADE	01803000	
00181ADF	01803000	
00181AE0	01803000	
00181AE4	01803000	
00181AE8	01803000	
00181AEC	01803000	
00181AED	01803000	
00181AEE	01803000	
00181AEF	01803000	
00181AF0	01803000	
00181AF4	01803000	
00181AF8	01803000	
00181AFC	01803000	
00181B00	01803000	
00181B04	01803000	
00181B08	01803000	
00181B0C	01803000	
00181B10	01803000	
00181B14	01803000	
00181B18	01803000	
00181B1C	01803000	
00181B20	01803000	
00181B24	01803000	
00181B28	01803000	
00181B2C	01803000	
00181B30	01803000	
00181B34	01803000	
00181B38	01803000	
00181B3C	01803000	
00181B40	01803000	
00181B44	01803000	
00181B48</		





```
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 46B0DFF	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]	EPSIMP32.6B5E9E2E
6B5D122E	3BC7	cmp eax,edi	
6B5D1230	7F 03	jg XEPSIMP32.6B5D1235	
6B5D1232	83C8 FF	or eax,0xFFFFFFFF	
6B5D1235	8B45 F0	mov dword ptr esi,dword ptr ds:[0x000000F0]	
ds:[026A5F54]=6B5E9E2F (EPSIMP32.6B5E9E2F)			
地址 数值 注释			
026A5F40	026A5F44		
026A5F44	6B5AB522	EPSIMP32.6B5AB522	
026A5F48	6B5E9E30	EPSIMP32.6B5E9E30	
026A5F50	00000000		
026A5F54	6B5E9E2F	EPSIMP32.6B5E9E2F	
026A5F58	76ED5F18	ntdll.ZwProtectVirtualMemory	
026A5F5C	026A6140		
026A5F60	FFFFFFFF		
026A5F64	026A6040		
026A5F68	026A6044		
026A5F6C	00000000		

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	
026B683E	75 40	jnz short 026B6851	
026B683E	8B43 0C	mov eax,dword ptr [ebp+0x4]	
026B6841	3D 00100000	cmp eax,0x1000	
026B6846	73 09	jnb short 026B6851	
026B6848	813C18 50450000	scasd	
026B684F	74 03	short 026B6854	
026B6851	43	inc ebx	
026B6852	EB E0	jmp short 026B6834	
026B6854	83CF FF	dec edi,-0x1	
026B6857	8BC2	cmp ebx,edx	

edi=5A4D
ds:[026B6D17]=5A4D

地址	HEX 数据	ASCII	地址
026B6D17	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ?jij..	02
026B6D27	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	?.....@.....	02
026B6D37	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		02
026B6D47	00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00	f..	02
026B6D57	0E 1F BA 0E 00 04 09 CD 21 B8 01 4C CD 21 54 68	■■?.???L?Th	02
026B6D67	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno	02

026B6C01	8B43 00	mov ebx,dword ptr ds:[ebx]	
026B6C04	33D2	xor edx,edx	
026B6C06	6A 00	push 0x0	
026B6C08	FFD2	call edx	
026B6C0A	8B45 FC	mov eax,dword ptr ss:[ebp-0x4]	
026B6C0D	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	

00412D88	74 1D	jle short 00412DD7	
00412D8A	6A 00	push 0x0	
00412D8C	6A 01	push 0x1	
00412D8E	57	push edi	
00412D8F	FFD0	call eax	
00412DC1	E8 D0EDFFFF	call 00411BA3	
00412DC6	83F8 03	cmp eax,0x3	
00412DCB	74 05	jle short 00412DD7	
00412DCE	E8 11F6FFFF	call 004123E1	

A screenshot of a Windows Explorer window. The left sidebar shows a tree view with the following structure: 'Office test' (folder), 'Special' (folder), and 'Perf' (folder, highlighted with a blue selection bar). The main pane displays a table with three columns: 'Name', 'Type', and 'Data'. The table contains one entry: 'ab (Default)' (Name), 'REG_SZ' (Type), and 'C:\User\ [redacted] \AppData\Local\Temp\apisecconnect.dll' (Data). The 'ab' part of the name is highlighted in red. In the bottom right corner, there is a watermark for 'VenusEye'.