





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	



6B5D1218	E8 46B0DFF	call EPSIMP32.6B5AC263
6B5D121D	C745 D8 170000	mov dword ptr ss:[ebp-0x28],0x17
		mov dword ptr ss:[ebp-0x28],0x17
		mov dword ptr ds:[026A5F54],0x6B5E9E2F
		call EPSIMP32.6B5E9E2F
		cmp eax,edi
6B5D1230	7F 03	je XEPSIMP32.6B5D1235
6B5D1232	83C8 FF	op_eax,0xFFFFFFFF
		ds:[026A5F54]=6B5E9E2F (EPSIMP32.6B5E9E2F)


```

026B682C 8D08 mov ebx,edx
026B682E 8D9B 00000000 lea ebx,dword ptr ds:[ebx]
026B6834 BA 4D5A0000 mov edx,0x5A4D
026B6839 66 4D4A cmp word ptr ds:[ebx],dx

```

026B683E 8843 3C eax,word ptr [026B683E]
 026B6841 3D 00100000 eax,0x1000
 026B6845 72 00 jnb short 026B6851
 026B6848 87407B 93455800 call dword ptr [eax*4],0x4558
 026B684A 72 00 jnb short 026B6851
 026B6857 5BC3 call short 026B6834
 dx=5A4D
 ds:[026B6D17]=5A4D

地址	HEX 数据	ASCII
026B683E	88 43 3C	
026B6841	3D 00 10 00 00	
026B6845	72 00	
026B6848	87 40 7B 93 45 58 00	
026B684A	72 00	
026B6857	5B C3	

```

026B6C71 8B47 00 lea ecx,dword ptr ds:[ecx]
026B6C74 33D2 xor edx,edx
026B6C76 6A 00 push 0x0
026B6C78 FFD2 call edx
026B6C7A 8B45 FC mov eax,dword ptr ss:[ebp-0x4]
026B6C7C 83C4 04 add esp,0x4
026B6C7E 6A 00 push 0x0
026B6C80 6A 00 push 0x0
026B6C82 50 push eax
026B6C84 50 push eax
026B6C86 50 push eax
026B6C88 50 push eax
026B6C8A 50 push eax
026B6C8C 50 push eax
026B6C8E 50 push eax
026B6C90 50 push eax
026B6C92 50 push eax
026B6C94 50 push eax
026B6C96 50 push eax
026B6C98 50 push eax
026B6C9A 50 push eax
026B6C9C 50 push eax
026B6C9E 50 push eax
026B6CA0 50 push eax
026B6CA2 50 push eax
026B6CA4 50 push eax
026B6CA6 50 push eax
026B6CA8 50 push eax
026B6CAA 50 push eax
026B6CAC 50 push eax
026B6CAE 50 push eax
026B6CB0 50 push eax
026B6CB2 50 push eax
026B6CB4 50 push eax
026B6CB6 50 push eax
026B6CB8 50 push eax
026B6CBA 50 push eax
026B6CBC 50 push eax
026B6CBE 50 push eax
026B6CC0 50 push eax
026B6CC2 50 push eax
026B6CC4 50 push eax
026B6CC6 50 push eax
026B6CC8 50 push eax
026B6CCA 50 push eax
026B6CCB 50 push eax
026B6CCD 50 push eax
026B6CCF 50 push eax
026B6CD1 50 push eax
026B6CD3 50 push eax
026B6CD5 50 push eax
026B6CD7 50 push eax
026B6CD9 50 push eax
026B6CDB 50 push eax
026B6CDD 50 push eax
026B6CDF 50 push eax
026B6CE1 50 push eax
026B6CE3 50 push eax
026B6CE5 50 push eax
026B6CE7 50 push eax
026B6CE9 50 push eax
026B6CEB 50 push eax
026B6CED 50 push eax
026B6CEF 50 push eax
026B6CF1 50 push eax
026B6CF3 50 push eax
026B6CF5 50 push eax
026B6CF7 50 push eax
026B6CF9 50 push eax
026B6CFB 50 push eax
026B6CFD 50 push eax
026B6CFF 50 push eax

```

```

00412D35 56 push esi
00412D36 57 push edi
00412D37 E8 FE010000 call 00412F3A
00412D3C 83F8 01 cmp eax,0x1

```

short 00412D40
 ecx,0x436C68

```

00412DB8 74 1D jz short 00412DD7
00412DBA 6A 00 push 0x0
00412DBC 6A 01 push 0x1
00412DBE 57 push edi
00412DBF FFD0 call eax

```

short 00412DD7
 call 004123E1

00412E41	6A 01	push 0x1	
00412E43	33D2	xor edx,edx	
00412E45	B9 E8974200	mov ecx,0x4297E8	WINWORD.exe
00412E4A	E8 82FFFFFF	call 00412CD1	
00412E4F	59	pop ecx	0041348C
00412E50	8BC8	mov ecx,eax	
00412E52	E8 14FFFFFF	call 00412B6B	
00412E57	85C0	test eax,eax	
00412E61	E8 5CFDFFFF	call 00412BC2	

```

00412E04 57          push edi
...
00412F94    mov     eax, dword ptr [ss:[ebp-0x10]]
...
00412F94    call   ahora ptr ss:[ebp-0x10]
...
00412F94    push  eax
00412F94    push  eax
00412F94    push  eax
00412F94    mov     ecx, 0x411D69
00412F94    push  ecx
00412F94    push  ecx

```

```

54 | do
55 | {
...
int v1, i) // 将dll文件保存到临时目录
...
8) && !(unsigned __int8)sub_1000158B((int)v1, i) // 判断是否通过rundll32执行dll
...

```

```

15 | v0[1] = 00,
16 | lpString2 = (LPCWSTR)decrypt((int)v0); // "apiseconnect.dll"
17 | *v0 = aB0A;
18 | v0[1] = 10;
19 | lpString = (LPCWSTR)decrypt((int)v0); // "TEMP"
...
22 | const sCHAR * s1 = "rundll32";
23 | int u0;
24 | int u1;
25 | int u2 = decrypt((int)v0);
...

```

