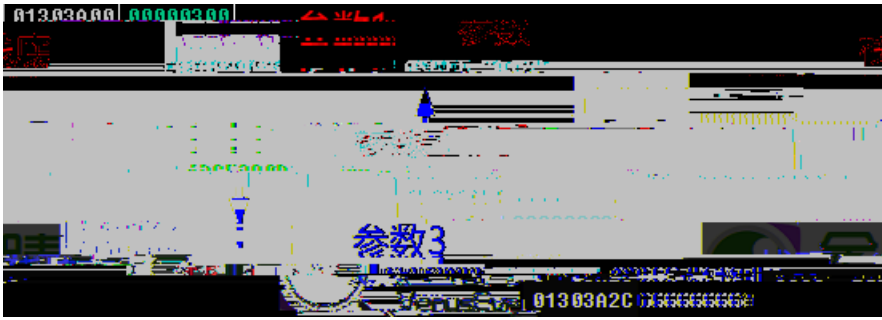
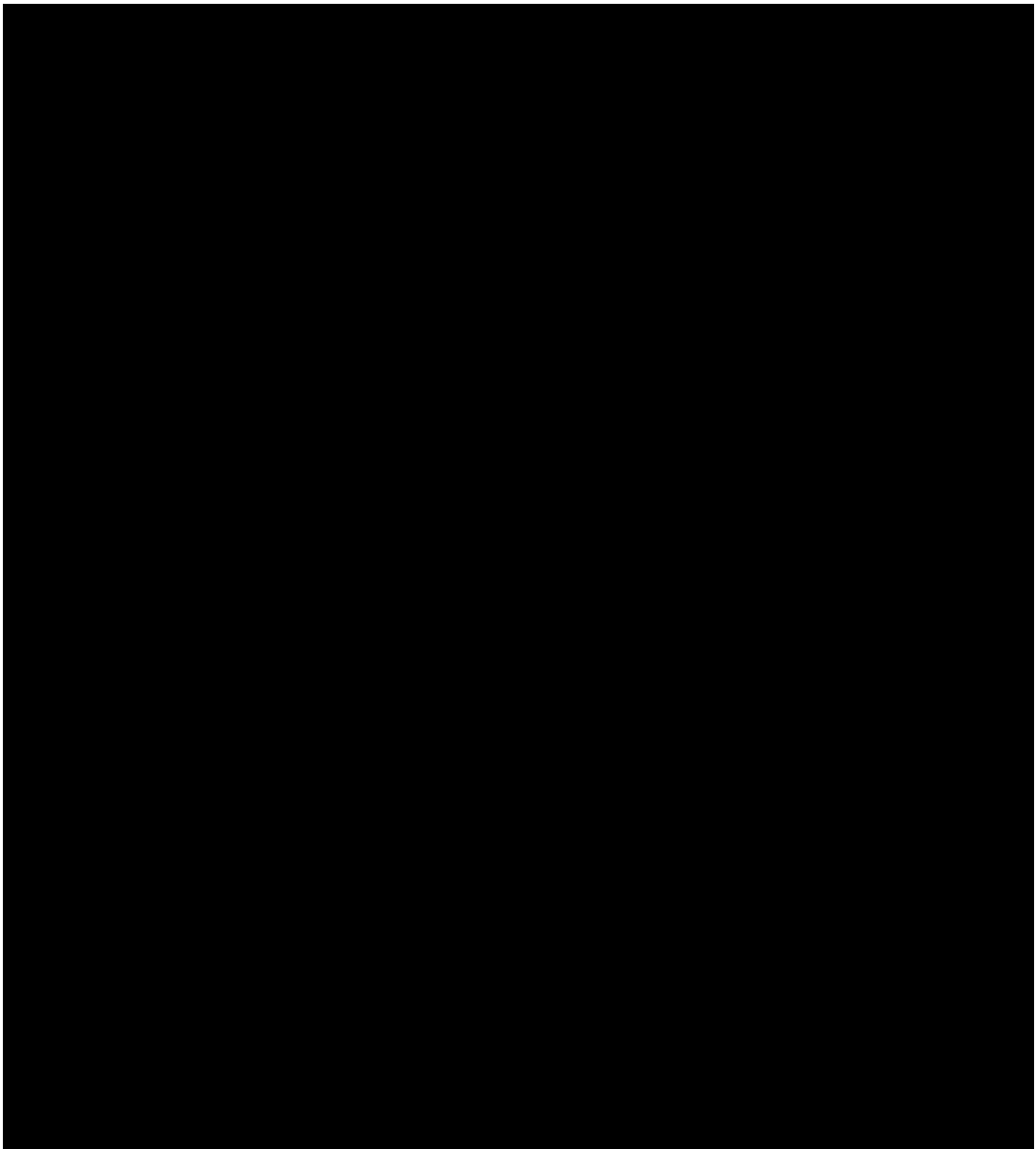




| | |
|--|--|
| | |
| | |
| | |





| | | |
|----------|----------|------------------------------|
| 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 874D7B 93000000 jmp dword ptr ds:[ebx+0x4],0x4558
 026B684A 72 00 jnb short 026B6851
 026B684C 72 00 jnb short 026B6851
 026B684E 72 00 jnb short 026B6851
 026B6850 72 00 jnb short 026B6851
 026B6857 5B cd dx,-0x1
 026B6859 5B cd dx,-0x1
 026B685B 5B cd dx,-0x1
 026B685D 5B cd dx,-0x1
 026B685F 5B cd dx,-0x1
 026B6861 5B cd dx,-0x1
 026B6863 5B cd dx,-0x1
 026B6865 5B cd dx,-0x1
 026B6867 5B cd dx,-0x1
 026B6869 5B cd dx,-0x1
 026B686B 5B cd dx,-0x1
 026B686D 5B cd dx,-0x1
 026B686F 5B cd dx,-0x1
 026B6871 5B cd dx,-0x1
 026B6873 5B cd dx,-0x1
 026B6875 5B cd dx,-0x1
 026B6877 5B cd dx,-0x1
 026B6879 5B cd dx,-0x1
 026B687B 5B cd dx,-0x1
 026B687D 5B cd dx,-0x1
 026B687F 5B cd dx,-0x1
 026B6881 5B cd dx,-0x1
 026B6883 5B cd dx,-0x1
 026B6885 5B cd dx,-0x1
 026B6887 5B cd dx,-0x1
 026B6889 5B cd dx,-0x1
 026B688B 5B cd dx,-0x1
 026B688D 5B cd dx,-0x1
 026B688F 5B cd dx,-0x1
 026B6891 5B cd dx,-0x1
 026B6893 5B cd dx,-0x1
 026B6895 5B cd dx,-0x1
 026B6897 5B cd dx,-0x1
 026B6899 5B cd dx,-0x1
 026B689B 5B cd dx,-0x1
 026B689D 5B cd dx,-0x1
 026B689F 5B cd dx,-0x1
 026B68A1 5B cd dx,-0x1
 026B68A3 5B cd dx,-0x1
 026B68A5 5B cd dx,-0x1
 026B68A7 5B cd dx,-0x1
 026B68A9 5B cd dx,-0x1
 026B68AB 5B cd dx,-0x1
 026B68AD 5B cd dx,-0x1
 026B68AF 5B cd dx,-0x1
 026B68B1 5B cd dx,-0x1
 026B68B3 5B cd dx,-0x1
 026B68B5 5B cd dx,-0x1
 026B68B7 5B cd dx,-0x1
 026B68B9 5B cd dx,-0x1
 026B68BB 5B cd dx,-0x1
 026B68BD 5B cd dx,-0x1
 026B68BF 5B cd dx,-0x1
 026B68C1 5B cd dx,-0x1
 026B68C3 5B cd dx,-0x1
 026B68C5 5B cd dx,-0x1
 026B68C7 5B cd dx,-0x1
 026B68C9 5B cd dx,-0x1
 026B68CB 5B cd dx,-0x1
 026B68CD 5B cd dx,-0x1
 026B68CF 5B cd dx,-0x1
 026B68D1 5B cd dx,-0x1
 026B68D3 5B cd dx,-0x1
 026B68D5 5B cd dx,-0x1
 026B68D7 5B cd dx,-0x1
 026B68D9 5B cd dx,-0x1
 026B68DB 5B cd dx,-0x1
 026B68DD 5B cd dx,-0x1
 026B68DF 5B cd dx,-0x1
 026B68E1 5B cd dx,-0x1
 026B68E3 5B cd dx,-0x1
 026B68E5 5B cd dx,-0x1
 026B68E7 5B cd dx,-0x1
 026B68E9 5B cd dx,-0x1
 026B68EB 5B cd dx,-0x1
 026B68ED 5B cd dx,-0x1
 026B68EF 5B cd dx,-0x1
 026B68F1 5B cd dx,-0x1
 026B68F3 5B cd dx,-0x1
 026B68F5 5B cd dx,-0x1
 026B68F7 5B cd dx,-0x1
 026B68F9 5B cd dx,-0x1
 026B68FB 5B cd dx,-0x1
 026B68FD 5B cd dx,-0x1
 026B68FF 5B cd dx,-0x1

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

| 地址 | HEX 数据 | ASCII |
|----------|-----------------|-------|
| 026B682C | 8D08 | |
| 026B682E | 8D9B 00000000 | |
| 026B6834 | BA 4D5A0000 | |
| 026B6839 | 66 4D4A | |
| 026B683E | 8843 3C | |
| 026B6841 | 3D 00100000 | |
| 026B6845 | 72 00 | |
| 026B6848 | 874D7B 93000000 | |
| 026B684A | 72 00 | |
| 026B684C | 72 00 | |
| 026B684E | 72 00 | |
| 026B6850 | 72 00 | |
| 026B6857 | 5B cd | |
| 026B6859 | 5B cd | |
| 026B685B | 5B cd | |
| 026B685D | 5B cd | |
| 026B685F | 5B cd | |
| 026B6861 | 5B cd | |
| 026B6863 | 5B cd | |
| 026B6865 | 5B cd | |
| 026B6867 | 5B cd | |
| 026B6869 | 5B cd | |
| 026B686B | 5B cd | |
| 026B686D | 5B cd | |
| 026B686F | 5B cd | |
| 026B6871 | 5B cd | |
| 026B6873 | 5B cd | |
| 026B6875 | 5B cd | |
| 026B6877 | 5B cd | |
| 026B6879 | 5B cd | |
| 026B687B | 5B cd | |
| 026B687D | 5B cd | |
| 026B687F | 5B cd | |
| 026B6881 | 5B cd | |
| 026B6883 | 5B cd | |
| 026B6885 | 5B cd | |
| 026B6887 | 5B cd | |
| 026B6889 | 5B cd | |
| 026B688B | 5B cd | |
| 026B688D | 5B cd | |
| 026B688F | 5B cd | |
| 026B6891 | 5B cd | |
| 026B6893 | 5B cd | |
| 026B6895 | 5B cd | |
| 026B6897 | 5B cd | |
| 026B6899 | 5B cd | |
| 026B689B | 5B cd | |
| 026B689D | 5B cd | |
| 026B689F | 5B cd | |
| 026B68A1 | 5B cd | |
| 026B68A3 | 5B cd | |
| 026B68A5 | 5B cd | |
| 026B68A7 | 5B cd | |
| 026B68A9 | 5B cd | |
| 026B68AB | 5B cd | |
| 026B68AD | 5B cd | |
| 026B68AF | 5B cd | |
| 026B68B1 | 5B cd | |
| 026B68B3 | 5B cd | |
| 026B68B5 | 5B cd | |
| 026B68B7 | 5B cd | |
| 026B68B9 | 5B cd | |
| 026B68BB | 5B cd | |
| 026B68BD | 5B cd | |
| 026B68BF | 5B cd | |
| 026B68C1 | 5B cd | |
| 026B68C3 | 5B cd | |
| 026B68C5 | 5B cd | |
| 026B68C7 | 5B cd | |
| 026B68C9 | 5B cd | |
| 026B68CB | 5B cd | |
| 026B68CD | 5B cd | |
| 026B68CF | 5B cd | |
| 026B68D1 | 5B cd | |
| 026B68D3 | 5B cd | |
| 026B68D5 | 5B cd | |
| 026B68D7 | 5B cd | |
| 026B68D9 | 5B cd | |
| 026B68DB | 5B cd | |
| 026B68DD | 5B cd | |
| 026B68DF | 5B cd | |
| 026B68E1 | 5B cd | |
| 026B68E3 | 5B cd | |
| 026B68E5 | 5B cd | |
| 026B68E7 | 5B cd | |
| 026B68E9 | 5B cd | |
| 026B68EB | 5B cd | |
| 026B68ED | 5B cd | |
| 026B68EF | 5B cd | |
| 026B68F1 | 5B cd | |
| 026B68F3 | 5B cd | |
| 026B68F5 | 5B cd | |
| 026B68F7 | 5B cd | |
| 026B68F9 | 5B cd | |
| 026B68FB | 5B cd | |
| 026B68FD | 5B cd | |
| 026B68FF | 5B cd | |

```

026B6C71 8B47 00 lea eax,dword ptr ds:[eax]
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 6A 00 push 0x0
026B6C84 5B push eax
026B6C86 FF call edi

```

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 6A 00 push 0x0
 026B6C84 5B push eax
 026B6C86 FF call edi

0x8000
 0x0

```

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 jg short 00412DD7
00412DBA 6A 00 push 0x0
00412DBC 6A 01 push 0x1
00412DBE 57 push edi
00412DBF FFD0 call eax

```

short 00412DD7
 call 004123E1

VenusEye 00412DCB E8 11F6FFFF

| | | | |
|----------|-------------|------------------|-------------|
| 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 14DFFFFF | call 00412B6B | |
| 00412E57 | 85C0 | test eax,eax | |
| 00412E61 | E8 5CFDFFFF | call 00412BC2 | |

```

00412E04 57          push edi
...
00412F94          show eax
...
push esi
push esi
push esi
push esi
mov esi,0x411D69
push esi
push esi

```

```

54 do
55 {
...
int v1, i) // 将dll文件保存到临时目录
...
} && !(unsigned int)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); // "apiseconnect.dll"
...
const sCHAR * ... int v0
...
decrypt: int v0
...
if ( ... )
...

```

