५ ऋ

४ ऐ

ᴨ ᴅ

ˇ ὖ Ç ḱ ২ ᵸ ɑ ض Ð ρ Â ì Ţ ŵ ɑ

ˆ ἷ ˈ ˇ ˇ ˜

№

۸

ԿՈ ۵ ﻫﻫﻫ Â G Ъ ﻫﻫﻫ ˘

Ď℘ ˜ ≠ ˘ L Ъ ⁘ V˘ ɾ Ĭ ๅ

Â

۸

Կ ˘ Ţ Ð ২ ۱ ˘

ضم ۵ ġ ˆ ˜ Â Ԥ U Â

۶ ๅ Ŭ'

U ๅ Ŭ'

۶

№ ṗ ˘ Ԥ ṗ ۲ L ⌡ ṗ Ţ˘

U 'P м˘ ṗ Â

خ U˘ ˝ γ ⌠ Ţ № ৩ ṗ ˘ ỉ Ţ شخ ⁘
Â

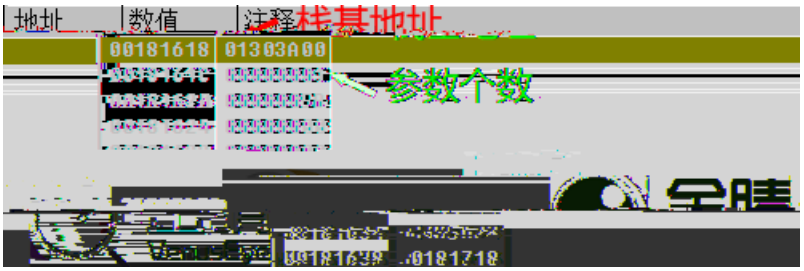
ȣ

ƀ D ǎ Â ỉ ƀ ضي ╟˘ ƀ ضي U Â ⌠ ƀ
ɿ ˘ ⌠ ƀ ɾ ₹ ƀ ˘ 'P ɿ Â
D ˘ ↕ ч Â ѿ ع №≠ ɿ ˘ ɦ U ₱
ɦ ɷ ǎ ŭ ₹˘ U 'P ɿ ع Â

ƀ Ŭ'

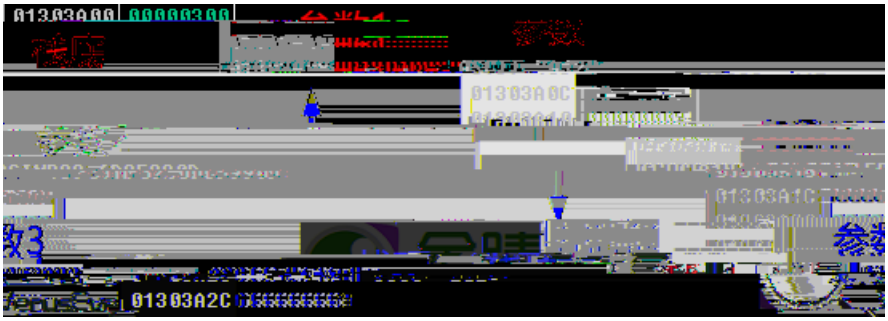
خي ضر

Ţ ǎ ɷ



⁘ ɷ ǎ ɯ ɷ ˘ ỉ Ŭ'

غمم



ضي ₱ Ü˘ ı ê Ì ⎧ ˜ G Â

˜ Y ⎧ ₱ ƀ W̄ ɷ ă Ţ W̄ ɷ U ₱ ˆ Н

ɷ ă ˜ Â ɣج / G н ɷ ă غمم ∞ Ъ Н̄ Â

ضي Ţ˘ ₱ ԿԻ ԹԻ ' Â

ضي ₱ ˘ Ţ ' ŬŢ˘ ˆ Ɣ ∫ ₱ Կ
˘ Ì ԿԻ Î Â

[illegible] خ U˘ [illegible] ч Â G

Й

˘ U ˘ˇخي ˇشج ˘ ˜ ˄ ˇشج

ƀ ╬ ∞ ˘ Ţ ˈP ˘ Ů̈

ˆ G ˘ ˊ Ƣ ˘ ˘

```
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 |
```

⌠

U Ώ ˜ ṗ Ţ˘ ъ

Ð ˘ ⌠ ˘ ҥ U˘ ₱

ч˜ ˜ Ώ˜ ˘ U ⌠ Â

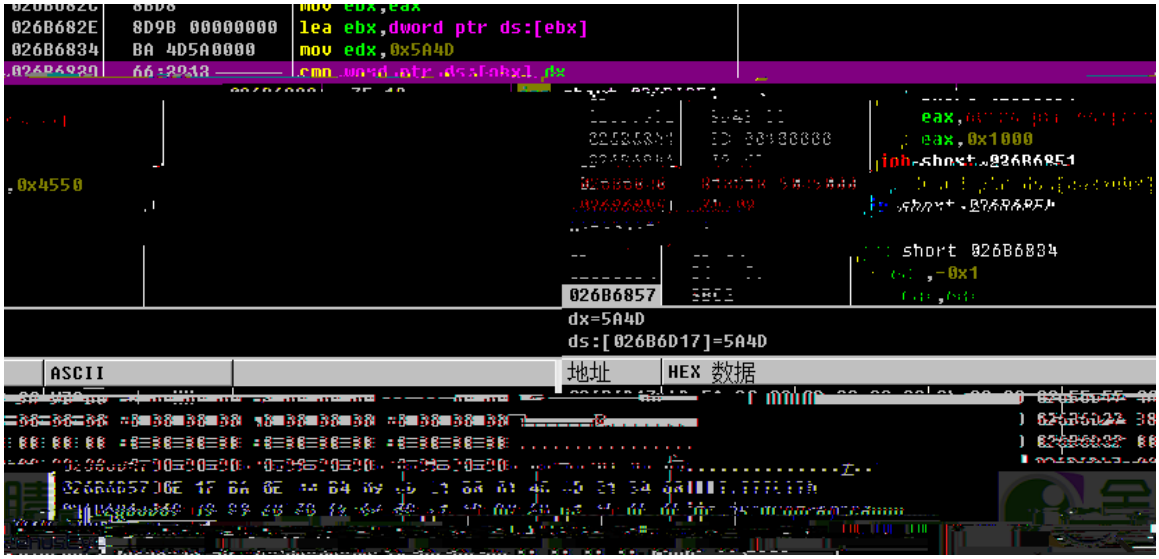
```
6B5D1218   E8 46B0FDFF   call EPSIMP32.6B5AC263
6B5D121D   C745 D8 170000 mov dword ptr ss:[ebp-0x28],0x17
jmp XEPSIMP32.6B5D11EF
6B5D122E   3BC7          cmp
6B5D1230   7F 09         jg XEPSIMP32.6B5D1235
6B5D1232   83C8 FF
ds:[026A5F54]=6B5E9E2F (EPSIMP32.6B5E9E2F)
026A5F40 | 026A5F44 |
026A5F44 | 6B5AB522 | EPSIMP32.6B5AB522
026A5F4C 33333333
026A5F50 33333333
```

№

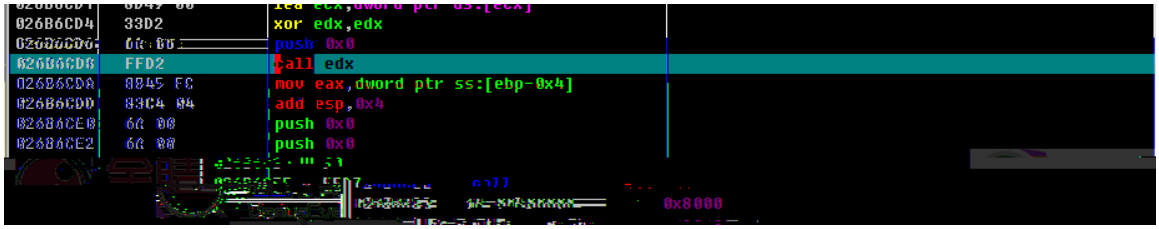
Ꮒ Ѝ'

Ɣ Ѝ ԯ ˜ο

ᾧ Ψ ৲ ˘ ˘ ⌠ Ḡ ضي Ţ Ð Â



ҥ U ض ṗ Ţ ˘ Ð˘ U ₮ ₱ Â



₱ ѿ Ψ ∞ β β ˘ Ъ □ Â

□ ˘ ˘ ˘ ҥ U ∞ ϩ

w˘ w U Ъ˘ ϩ ↕ ₮ Â

w U˘ Ψ ۸ Ţ ₂ ˘ β ⌠ Â

```
00412E41   6A 01          push 0x1
00412E43   33D2           xor edx,edx
00412E45   B9 E8974200    mov ecx,0x4297E8                    WINWORD.exe
00412E4A   E8 82FEFFFF    call 00412CD1
00412E4F   59             pop ecx                             0041348C
00412E50   8BC8           mov ecx,eax
00412E52   E8 14FDFFFF    call 00412B6B
00412E57   85C0           test eax,eax
00412E59   0F84 C8000000  je 00412F27
00412E5F   8BC8           mov ecx,eax
00412E61   E8 5CFDFFFF    call 00412BC2
```

ӊ U ˆ ˂ ˜ ˜ ⎡ ˇ ˜ₒ ₱ Â

```
00412ED4   57             push edi
p-0x10]                   short 00412F04
                          eax
                          ecx,ecx
                          0x411D69
                          call qword ptr ss:[et
```

˜ U ϖ ᾧ Ψ ᾷ ᾳ Ðˆ ˂ Ð˜ ᾗ ᾷ ᾳ Ðˇ U
Ð Ḡ ⎡ ˇ ▯ ⎡ ´Y Ţˇ ӊ U Ψ ∞
ϖ Â

```
54   do
58     return 1;
63     sub_1000153C((int)v1, i)        // 将dll文件保存到临时目录
64
65
66
67   if ( *(_BYTE *)(v13 + 0x18) && *(unsigned __int8)sub_100015BB((int)v1, i)
    // 判断是否通过rundll32执行dll
```

Ḡ ⎡ ´Y
Ŭ Â U Ð ˇ Ψ ⎡ Â

```
16   lpString2 = (LPCWSTR)decrypt((int)v0);        // "apisecconnect.dll"
17   *v0 = aBOA;
18   v0[1] = 10;
22   const WCHAR *
23
24
25   const WCHAR * decrypt, int v1
26   if ( !hEnvironment && (v1 < 0 || v1 >= 20 )
```

Office test
Name
Type
Date
erconnect.dll
Perf
ab