Ч Ѧ

v ⷢ



Ꮒ Ð

ˇ Ὗ Ϛ Ќ ϗ Ӈ ѡ ضِ Ⅾρ Â ỉ Ţ ₩ ѡ

ˆ ǐ ˈ ˇ ˇ ~ Ὗ˗ Ⅾρ ڏ ⷢ Â

ŋ ﬡ Ⅾρ ą ǐ ≠

ϗ № ˇ ŋ v ڏ ⷢ Â

Ⅾρ

Ὗ ₩ Ð O Ч Ľ Ⅾρ

ỉ ≠ ˚ Ð ⷢ Â Ð Ч ₩ ѡ ˇ ỉ Ţ ~ ϗ

ˇ W Â ضِ ϒ U ˇ

ا ضِ ϗ ٧ Ţ Â Ч ϗ

Ľ ˇ ą ϗ Â ϼ

ỉ ≠ ϒ ǐ Ὗ U № Â

Ḥ

Ð ِ	
Ð ﻗﻤﻢ	Ð
Ð	

№

/

ч ₩ ₡ ﻓﻤﻢ Â G ƀ ﻓﻤﻢ ˘

Ɗρ ˜ ≠ ˘ └ ƀ ⁚ ν˘ ɾ ǐ ɳ

Â

/

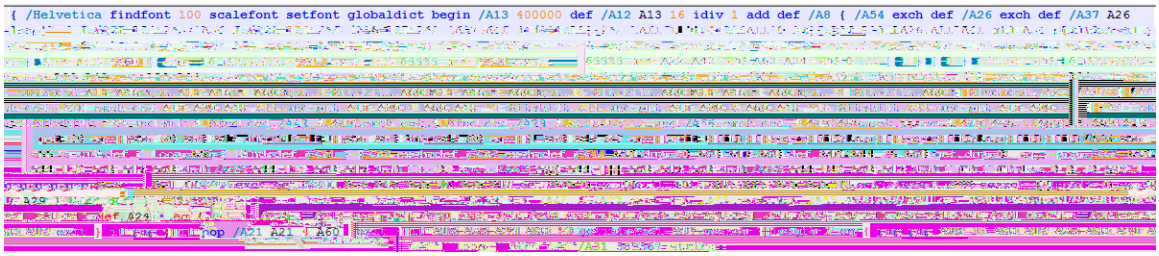
ч ˘ Ţ Ð ϶ ϒ ˘

ﻣﺾ ₡ ė ˆ ~ Â ʜ U Â

ν ɳ Й'



U ɳ Й'



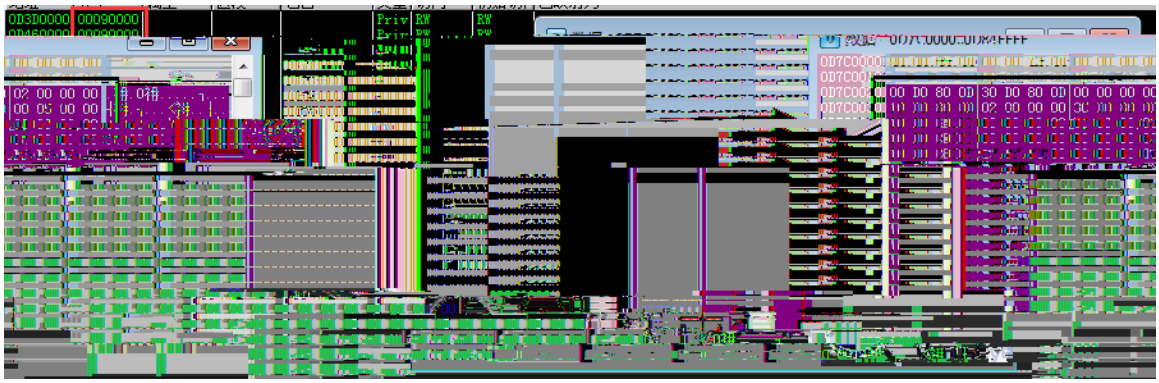
ɨ

№ ρ ˘ ʜ ѽ ɣ └ ⌡ ρ Ţ˘

U ꞌP м˘ ρ Â

```
/A31 589567 string <
A8 def
```

ɔ U˘ ˆ ɣ ⌡ Ţ№ ɔ ṗ ˘ ì Ţ خش ⁘
Â



ß

ƀ D ǎ Â ì ƀ ض ╠˘ ƀ ضU Â ⌡ ƀ
ㅅ ˘ ⌡ ƀ ɾ ∓ ƀ ˘ ˈP ㅅ Â
ᴅ ˘ ↕ ч Â ѽ ɇ №≠ ㅅ ˘ ҥ U ₱
ҥ ɷ ǎ ŭ ∓˘ U ˈP ㅅ ⱬ Â

ƀ Йˈ

خض

Ţ ǎ ɷ

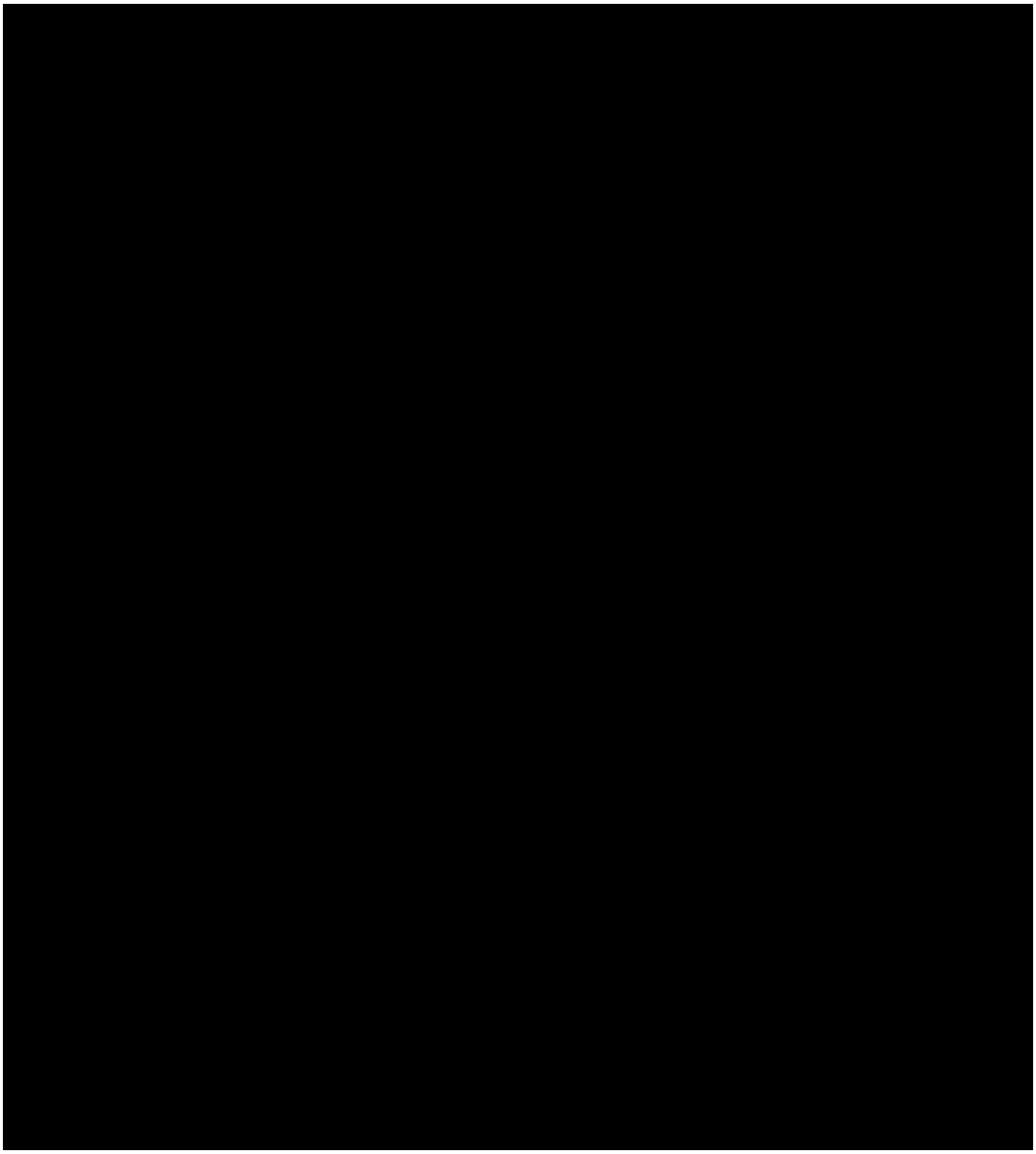


⁘ ɷ ǎ ₩ ɷ ˘ ɷ ˘ ì Йˈ

فمم



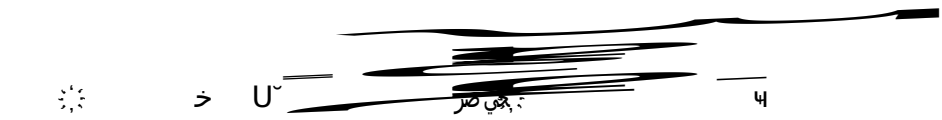
ضي ₱ Ǔ˘ ıı ê Ì ⌡ ˜ ɢ Â
ˆ ɣ ⌡ ₱ ƀ ₩ ɷ ă̋ Ţ ₩ ɷ U ₱ ˆ ʜ
ɷ ă̋ ~ Â ﻉ ɢ ʜ ɷ ă̋ فمم ∞ Ъ Ҥ Â



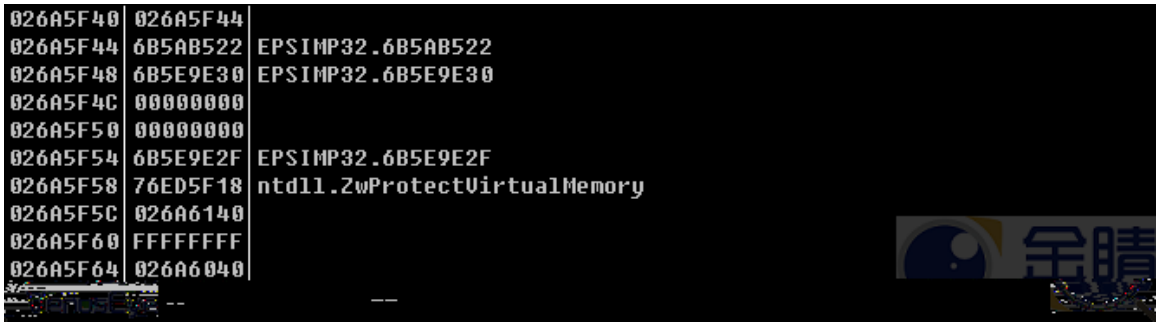
ضي Ţ˘ ₱ ч ₩ ѡ Î ' Â

ضي ₱ ˘ Ţ ' Й˘ ˆ ץ ⌠ ₱ ч

˘ Ì ممم ч Î Â



ˇ U ˇ ˜ ˇ ˇ ∞ ˇ ˇ ˇ

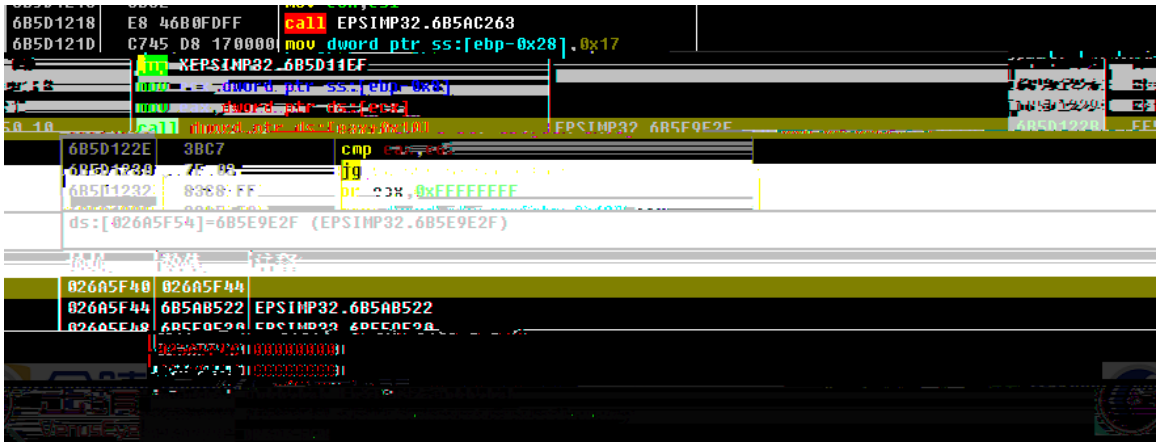


⌠

U Ώ ˜ ṗ Ţ˘ ƀ

ð ˘ ⌠ ˘ ҂ U˘ ₱

ч˜ ˜ Ώ˜ ˘ U ⌠ Â

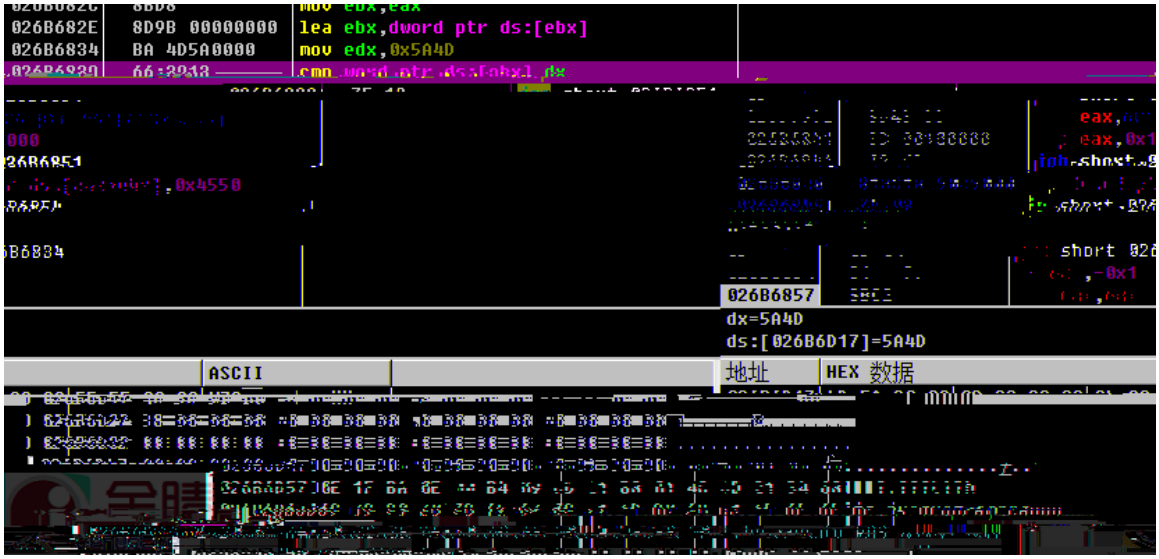


№

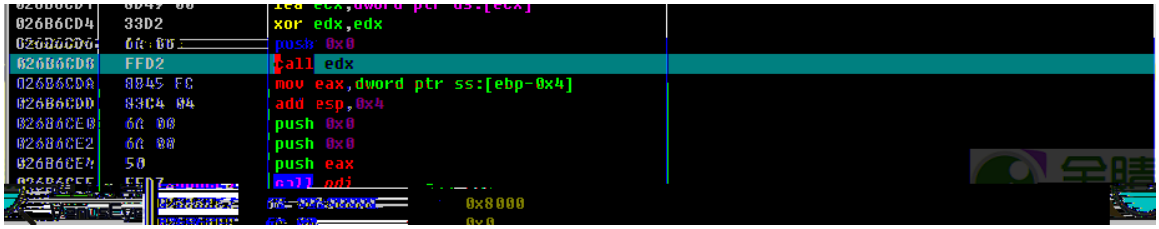
Ꮒ Ӣ'

ץ Й ч ˜ₒ

ѽ Ψ ʌ ˘ ˘ ∫ Ḡ ضي Ţ Ð Â



ң U ض ṗ Ţ ˉ Ð˘ U ₮ ₱ Â



₱ ѽ Ψ ∞ β β ˇ Ь □ Â



□ ˫ ˇ ˇ ң U ∞ Ղ

w˘ w U ƀ˘ Ղ ↕ ₮ Â



w U˘ Ψ ᐟ Ţ ₂ ˇ 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
```

ң U ˆ ㄐ ˜ ˜ ⌠ ˇ ˜ₒ ₱ Â

```
00412ED4   57             push edi
                          call qword ptr ss:[ebp-0x10]
                          short 00412F04
                          eax
                          ecx,ecx
                          push 0x0
                          push 0x0
                          push 0x0
                          0x411D69
                          push eax
                          push ecx
```

˜ U ㄱ ѽ Ψ ₩ ɷ Ðˆ ㄐ Ð˜ ¿ ₩ ɷ Ðˇ U
Ð Ḡ ⌠ ˇ □ ₹ ⌠ Ύ Ţˇ ң U Ψ ∞
ᑐ ɷ Â

```
54  do
58
59  if ( i == v4 - 1 )
60  {
61    sub_100025C0(...
63    else if ( !sub_100
64
65
66
67    if ( *(_BYTE *)(v1
```

```
0153C((int)v1, i)       // 将dll文件保存到临时目录
3 + 0x18) && !(unsigned __int8)sub_100015BB((int)v1, i) /// 判断是否通过rundll32执行dll
```

Ḡ ⌠ Ύ
Й Â U Ð ˇ Ψ ₹ Â

```
15  v0[1] = 30;
16  lpString2 = (LPCWSTR)decrypt((int)v0);        // "apisecconnect.dll"
17  *v0 = aBOA;
18  v0[1] = 10;
22  const WCHAR * decrypt(int a1)
23  {
24    int v1;
25    const WCHAR *decrypt; int i0;
26    if ( !hKey || !RegQueryValueExW(hKey, lpValueName, 0, 0, 0, &cbData) )
27      return 0;
28    v1 = operator new[](cbData);
```


Office test
Name
Type
Data
ercopnect dll
Perf
ab