Office

Office (CVE-2017-11882 CVE-2018-0798 CVE-2018-0802) Office CVE-2018-0798 http://venustech.com.cn/NewsInfo/4/49366.Html CVE-2017-11882 http://venustech.com.cn/NewsInfo/4/48671.Html CVE-2017-11882+CVE-2018-0802 RTF CVE-2018-0802

CFBF(Compound File Binary Format) "\x01Ole10Native"

URL

CVE-2017-11882 CVE-2018-0802 CFBF Root Entry CLSID {0002CE02-0000-0000-C000-000000000046}

CLSID Microsoft Equation 3.0 3.0

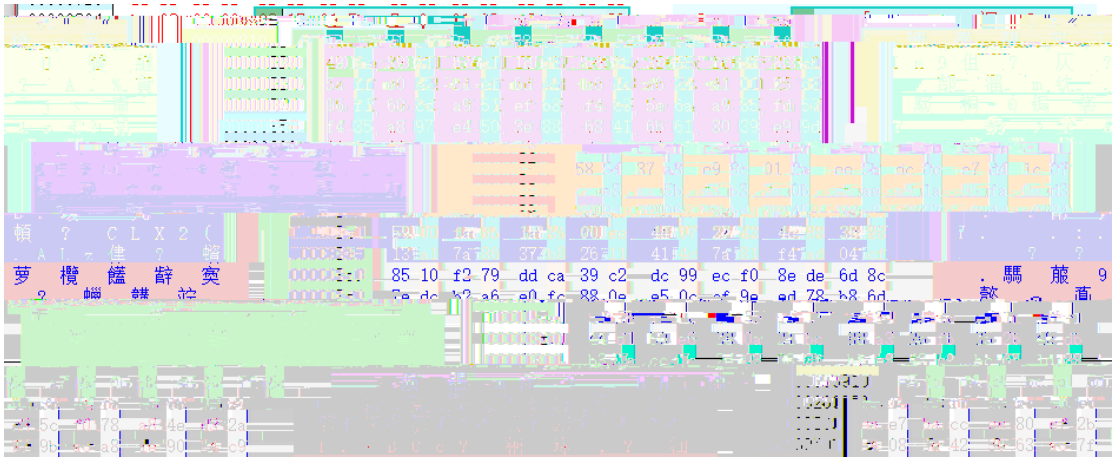
28 s_EquationNative v10
out IStream a2 IStorage

26~29 CFBF "Equation Native"
(v11 0) "\x01Ole10Native"
35
"Equation Native" 0x1C
"\x01Ole10Native" 4 CVE-2017-11882
OLE
38 "\x01Ole10Native"
"Equation Native" OLE
0x001C( ) 0x00020000( )
40~43
"\x01Ole10Native" 4 ([v9+0])
"Equation Native" 8 DWORD
v14([esp+0x3C]) v13([esp+0x34]) 8
50~53

66

"Equation Native"

0x1C "\x01Ole10Native" 4



5

MTEF header (version 2 and later):

The version 2 header consists of a 5-byte header:

byte	description	value
0	MTEF version	3
1	generating platform	0 for Macintosh, 1 for Windows
2	[illegible]	[illegible]
3	product version	3
t subversion	0	4 produc

1 3 4

1 3 4

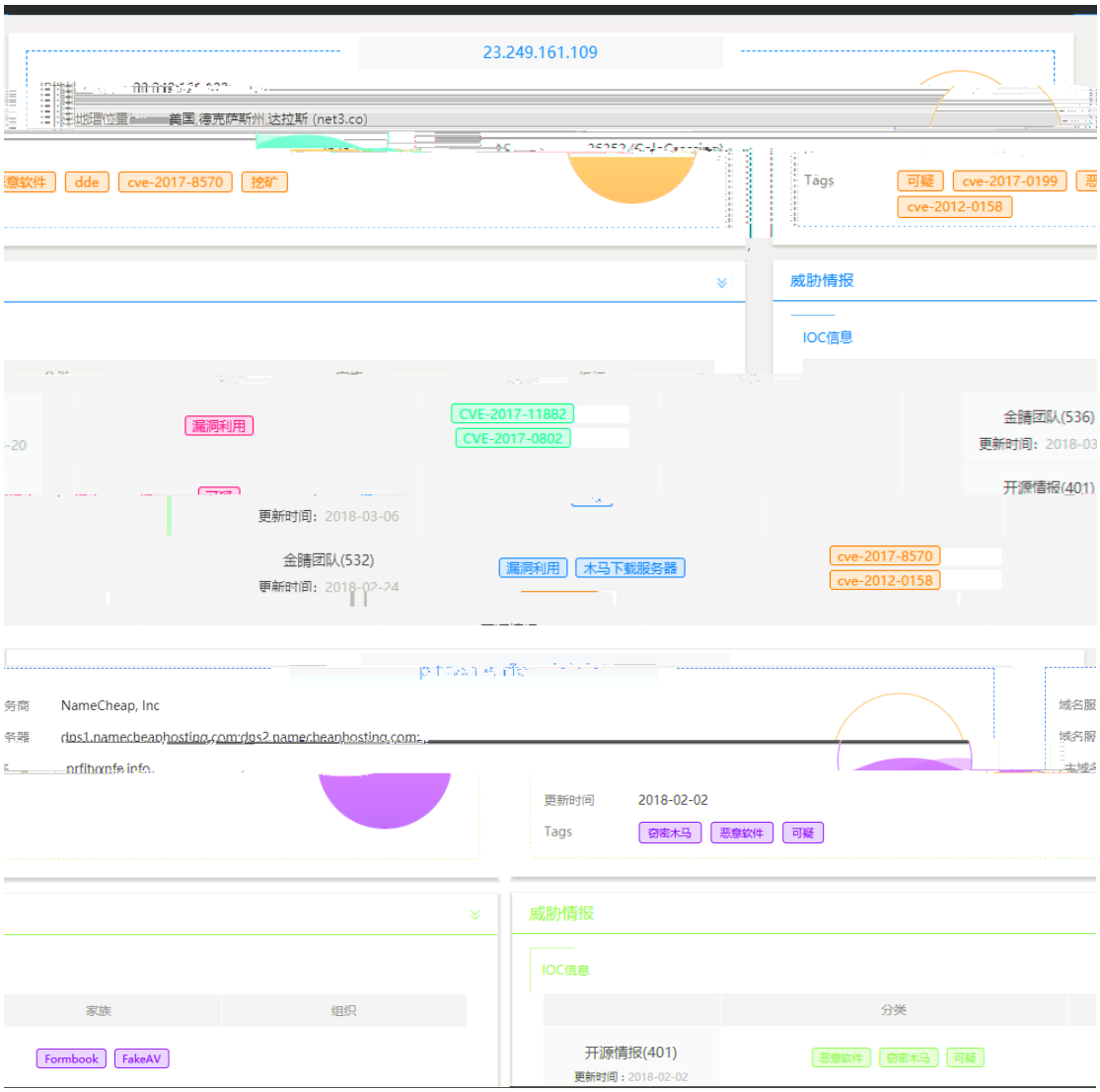
(2) Windows EQNEDT32.EXE

2

64 **32** **Office**

3

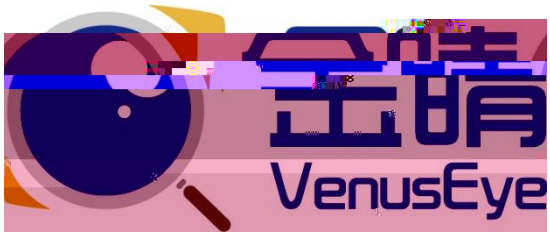
4 VenusEye



IOC

www[.]pensandwoodworking[.]com
www[.]euroasianbridge[.]com
www[.]dlpestscontrol[.]com
www[.]salihatasarim[.]com
www[.]datascienceactuaries[.]net
www[.]wisataa T8mbas[.]com
www[.]5nesglaz[.]onli Tə
www[.]tewyt[.]info
www[.]rahafim[.]com
www[.]gardTənshT8des[.]com
www[.]beb-sef-sufficient[.]com
www[.]femmTəfeline[.]com
www[.]edosTənsei[.]com
www[.]outdoormTərk[.]com
www[.]prfitvxnfe[.]info

www[.]bloggingsays[.]com
www[.]rahafim[.]com



VenusEye

VenusEye www.venuseye.vip

