

Office

Office (CVE-2017-11882)

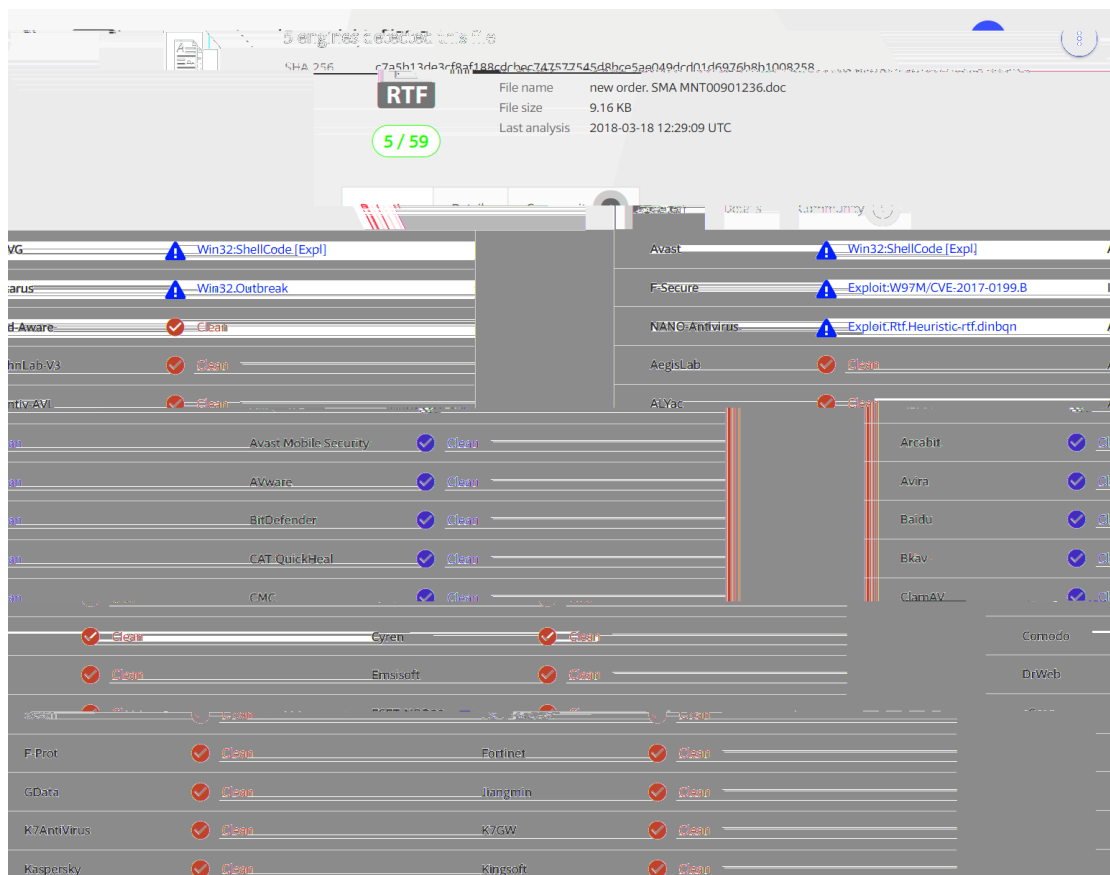
CVE-2018-0798 CVE-2018-0802) Office

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



Binary Format) CFBF(Compound File
"\x010le10Native"

URL

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

CLSID Microsoft Equation 3.0 3.0

```

26 | v11 = (*(int (__stdcall **)(int, wchar_t *, _DWORD, signed int, _DWORD, int *)))(*(__DWORD *)a2 + 16))(
27 |
28 | s_EquationNative,
29 | 0,
30 | 16,
31 | 0,
32 | &v10);
33 | if (v11)
34 | {
35 |     v11 = (*(int (__stdcall **)(int, void *, _DWORD, signed int, _DWORD, int *)))(
36 |         a2,
37 |         &s_Ole10Native,
38 |         0,
39 |         16,
40 |         0,
41 |         &v10);

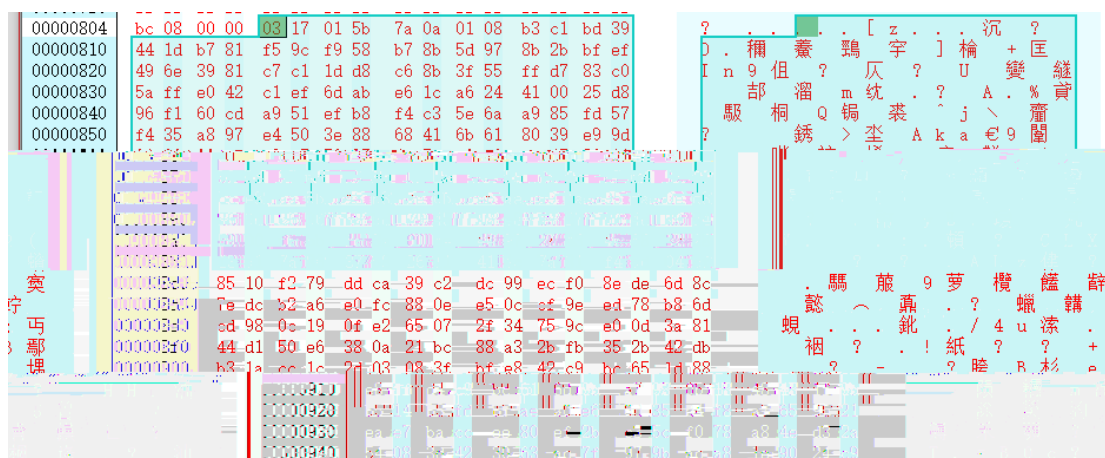
```

28 s_EquationNative v10

out IStream a2 IStorage

26~29	CFBF	"Equation Native"
(v11 0)	"\x010le10Native"	
35		
"Equation Native"	0x1C	
"\x010le10Native"	4	CVE-2017-11882
	OLE	
38		"\x010le10Native"
	"Equation Native"	OLE
0x001C()	0x00020000()	
40~43		
"\x010le10Native"	4 ([v9+0])	
"Equation Native"	8	DWORD
v14([esp+0x3C])	v13([esp+0x34])	8
50~53		

4



5

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	generating product	0 for MathType, 1 for Equation Editor
3	product version	3
4	product subversion	0

1 3 4

EQNEDT32.EXE

```
Reg add
HKLM\SOFTWARE\Microsoft\Office\Common\COM Compatibility\{0002CE02-
0000-0000-C000-000000000046} /v Compatibility Flags /t REG_DWORD /d
0x400
```

2

```
reg add HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\Common\COM Compa
tibility\{0002CE02-0000-0000-C000-
000000000046} /v Compatibility Flags /t REG_DWORD /d 0x400
```

64

32

Office

3

静态检测			
检测引擎	攻击类型	详细信息	危险等级
流行威胁库	病毒木马	检测到可疑程序(curious_equation)	★★★★☆
动态检测			
Microsoft Office 2007		操作系统: Windows 7	软件版本: MS
2018-03-20 17:15:54		开始时间: 2018-03-20 17:12:16	结束时间: 2018-03-20 17:15:57
>		● 开机启动 [1]	
>		● 威胁行为 [1]	
2018-03-20 17:12:19		结束时间: 2018-03-20 17:15:57	开始时间: 2018-03-20 17:12:19
>		● 威胁行为 [2]	
>		● 隐藏对管道 [8]	
ynova/ifun.exe		可疑URL: http://23.249.161.109/z	
>		可疑URL: http://23.249.161.109/z	
ynova/ifun.exe		可疑URL: http://23.249.161.109/z	
>		可疑URL: http://23.249.161.109/z	
>		● 高速下载 [1]	
2018-03-20 17:12:18		结束时间: 2018-03-20 17:15:56	开始时间: 2018-03-20 17:12:18
>		● 开机启动 [1]	
>		● 威胁行为 [3]	

4 VenusEye

23.249.161.109

IP地址

23.249.161.109

地理位置

美国,德克萨斯州,达拉斯 (net3.co)

AS

36352 (ColoCrossing)

Tags

可疑

cve-2017-0199

恶意软件

dde

cve-2017-8570

挖矿

cve-2012-0158

威胁情报

IOC信息

金睛团队(536) 更新时间: 2018-03-20	漏洞利用	CVE-2017-11882 CVE-2017-0802
开源情报(401) 更新时间: 2018-03-06	可疑	
金睛团队(532) 更新时间: 2018-02-24	漏洞利用 木马下载服务器	cve-2017-8570 cve-2012-0158

prfitvxnfe.info

域名服务商

NameCheap, Inc

域名服务器

dns1.namecheaposting.com;dns2.namecheaposting.com;

主域名

prfitvxnfe.info

更新时间

2018-02-02

Tags

窃密木马

恶意软件

可疑

威胁情报

IOC信息

家族	组织	分类
book	FakeAV	开源情报(401) 更新时间: 2018-02-02 恶意软件 窃密木马 可疑 Form

IOC

www[.]pensandwoodworking[.]com
 www[.]euroasianbridge[.]com
 www[.]dlpestscontrol[.]com
 www[.]salihatasarim[.]com
 www[.]datascienceactuaries[.]net
 www[.]wisataanambas[.]com
 www[.]5nesglaz[.]online
 www[.]tewyt[.]info
 www[.]rahafim[.]com
 www[.]gardenshades[.]com
 www[.]beb-sef-sufficient[.]com
 www[.]femmefeline[.]com
 www[.]edosensei[.]com
 www[.]outdoormerk[.]com
 www[.]prfitvxnfe[.]info

www[.]bloggingsays[.]com

www[.]rahafim[.]com



VenusEye

VenusEye

www.venuseye.vip

