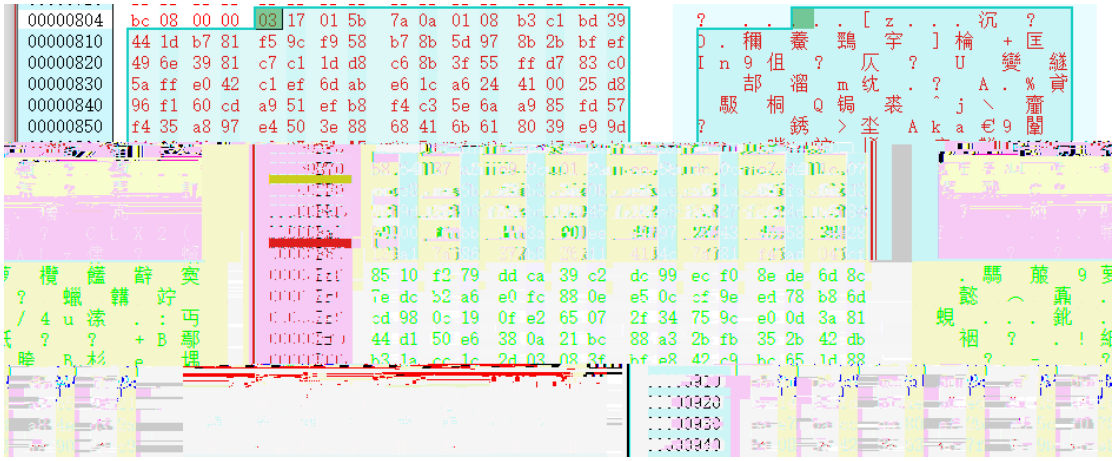

RTF
File name new order. SMA MNT00901236.doc
File size 9.16 KB
Last analysis 2018-03-18 12:29:09 UTC
5 / 59
Win32:ShellCode [Expl]
Win32.Outbreak
Clean
Clean
Clean
Avast
Win32:ShellCode [Expl]
AVG
F-Secure
Exploit:W97M/CVE-2017-0199.B
Ikarus
NANO-Antivirus
Exploit.Rtf.Heuristic-rtf.dinbqn
Ad-Aware
AegisLab
Clean
AhnLab-V3
ALYac
Clean
Antiy-AVL
Avast Mobile Security
AVware
BitDefender
CAT-QuickHeal
Arcabit
Avira
Baidu
BKAV
Clean
Comodo
DrWeb
F-Prot
Gdata
Kaspersky
Clean

Ä

```
v11 = (*(int (__stdcall **)(int, wchar_t *, _DWORD, signed int, _DWORD, int *))(*(_DWORD *)a2 + 16))(
, int *))(*(_DWORD *)a2 + 16))(
        s_EquationNative,
        0,
        16,
        0,
        &v10);
if ( v11 )
{
  v11 = (*(int (__stdcall **)(int, void *, _DWORD, signed int, _DWORD
    a2,
    &s_Ole10Native,
    0,
    16,
    0,
    &v10);
```

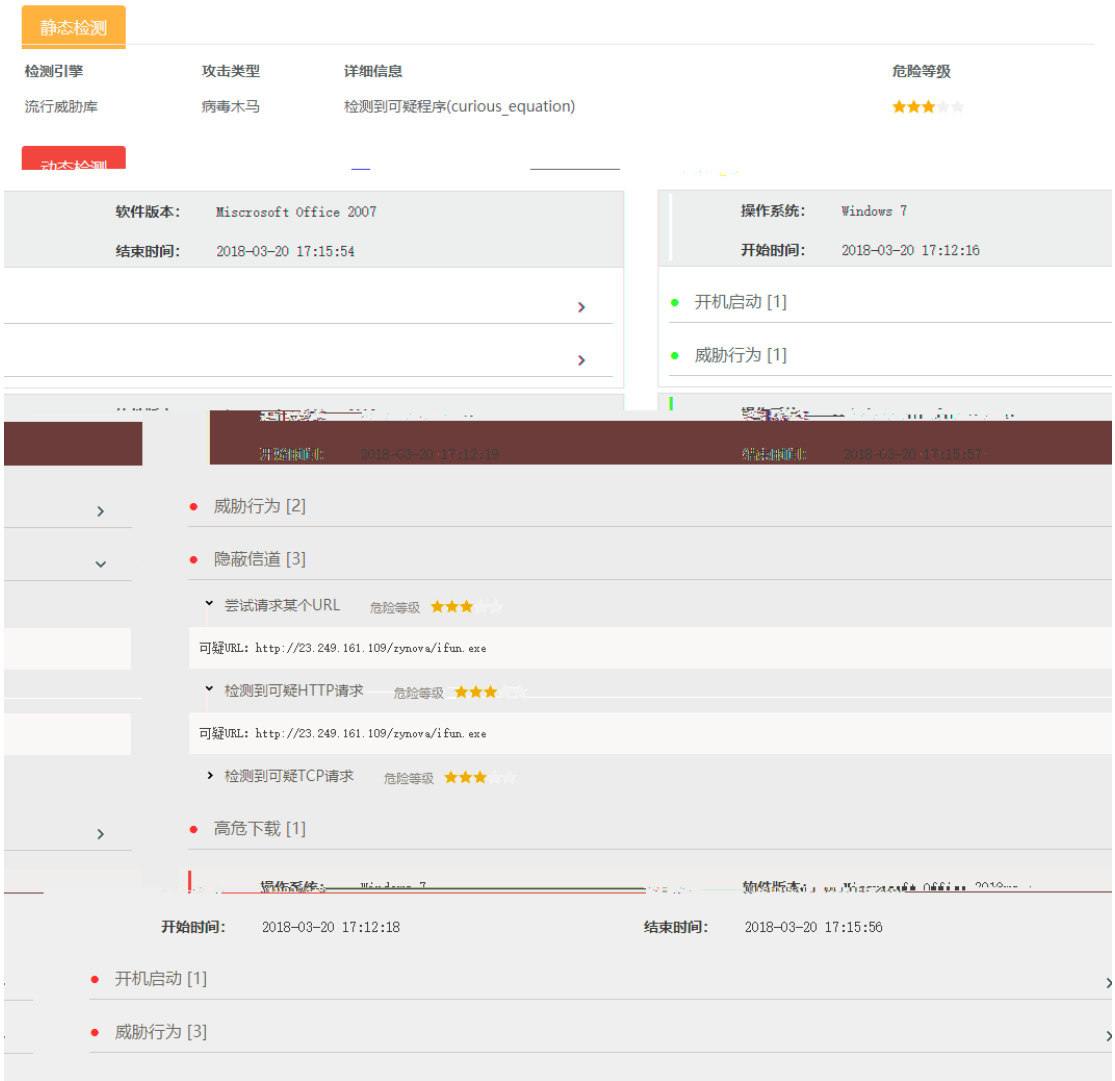
```
v11 = root->lpVtbl->OpenStream(root, s_EquationNative, 0, STGM_SHARE_EXCLUSIVE, 0, &v10);
if ( v11 )
{
// flag -> "\x01Ole10Native" stream
if (!v11)
2) <= 0x20000 )
+ 0x8]
  if ( flag || (unsigned __int16)v13 == size && *(unsigned int *)((char *)&v13 +
  {
    if ( flag )
      v2 = GlobalAlloc(2u, v9);
    else
      v2 = GlobalAlloc(2u, v14);
    hMem = v2;
    if ( v2 )
    {
      v7 = GlobalLock(hMem);
      if ( v7 )
      {
        if ( flag )
          v3 = v10->lpVtbl->Read(v10, v7, v9, (ULONG *)&size);
        else
          v3 = v10->lpVtbl->Read(v10, v7, v14, (ULONG *)&size);//
                                                // v13 -> [esp + 0x34]
                                                // v14 -> [esp + 0x3C] = [esp + 0x34
        v11 = v3;
        if ( v3 )
        {
          v11 = E_FAIL;
        }
        else
        {
          GlobalUnlock(hMem);
          v7 = 0;
          sub_403A20(v8);
          sub_42F8FF((char *)hMem);         // data processed here
          sub_4032D1(v8, 0);
```

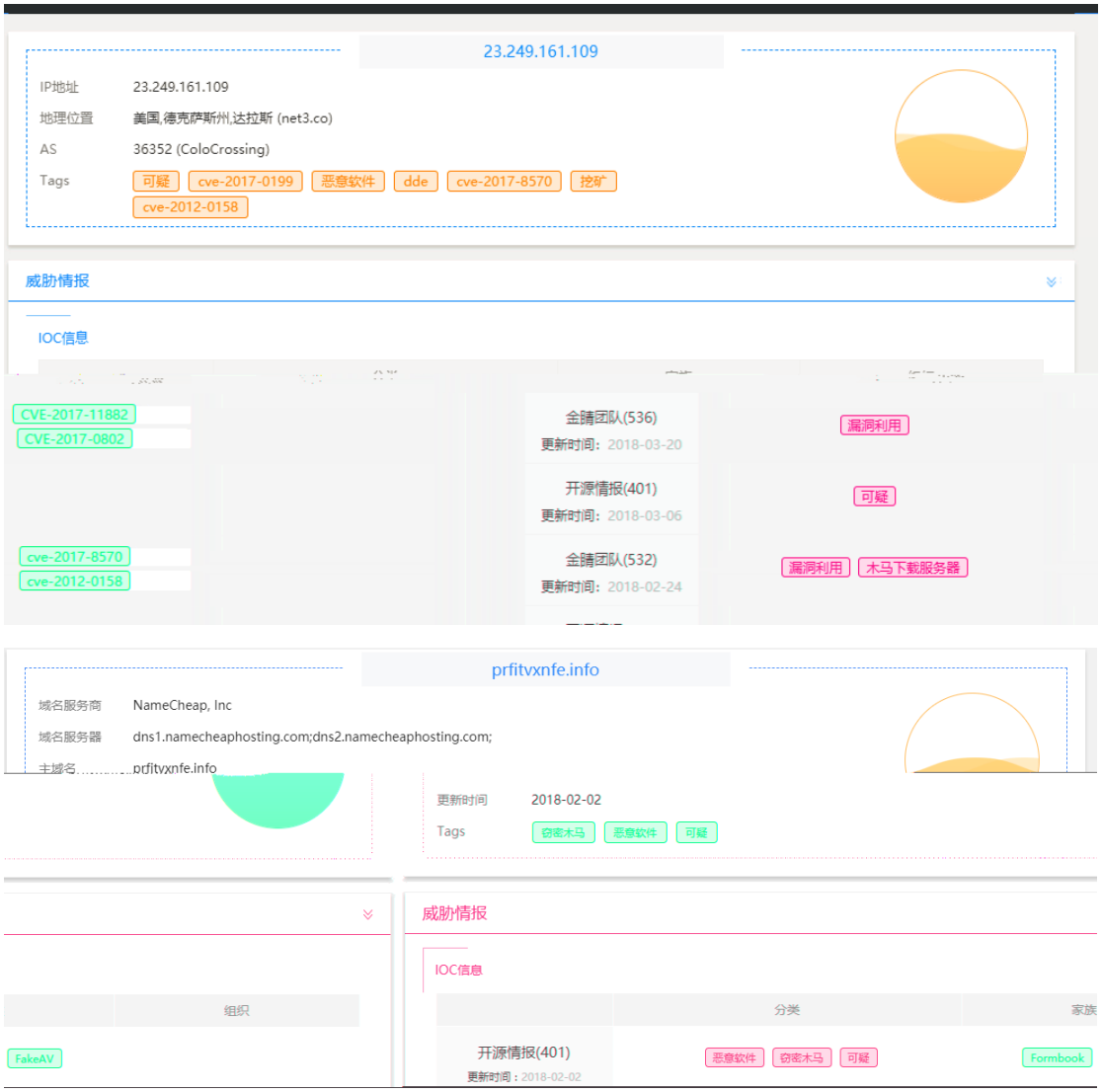


MTEF header (version 2 and later):

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


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)
软件版本: Miscrosoft Office 2007
结束时间: 2018-03-20 17:15:54
操作系统: Windows 7
开始时间: 2018-03-20 17:12:16
开机启动 [1]
威胁行为 [1]
威胁行为 [2]
隐蔽信道 [3]
尝试请求某个URL
危险等级
可疑URL: http://23.249.161.109/zynova/ifun.exe
检测到可疑HTTP请求
危险等级
可疑URL: http://23.249.161.109/zynova/ifun.exe
检测到可疑TCP请求
危险等级
高危下载 [1]
开始时间: 2018-03-20 17:12:18
结束时间: 2018-03-20 17:15:56
开机启动 [1]
威胁行为 [3]


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
CVE-2017-11882
CVE-2017-0802
金睛团队(536)
更新时间：2018-03-20
漏洞利用
开源情报(401)
更新时间：2018-03-06
可疑
cve-2017-8570
cve-2012-0158
金睛团队(532)
更新时间：2018-02-24
漏洞利用 木马下载服务器
prfitvxnfe.info
域名服务商 NameCheap, Inc
域名服务器 dns1.namecheaphosting.com;dns2.namecheaphosting.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
组织
分类
家族
FakeAV
开源情报(401)
更新时间：2018-02-02
恶意软件 窃密木马 可疑
Formbook


VenusEye