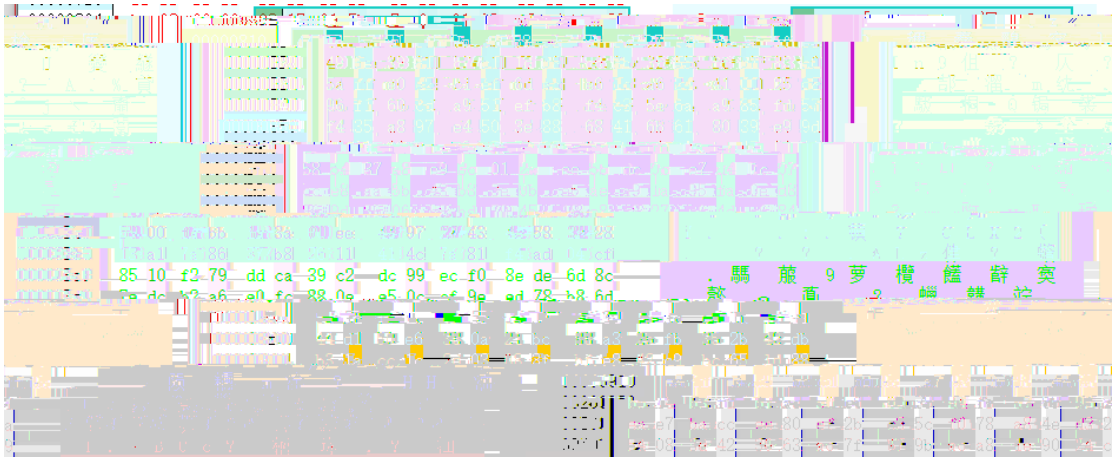
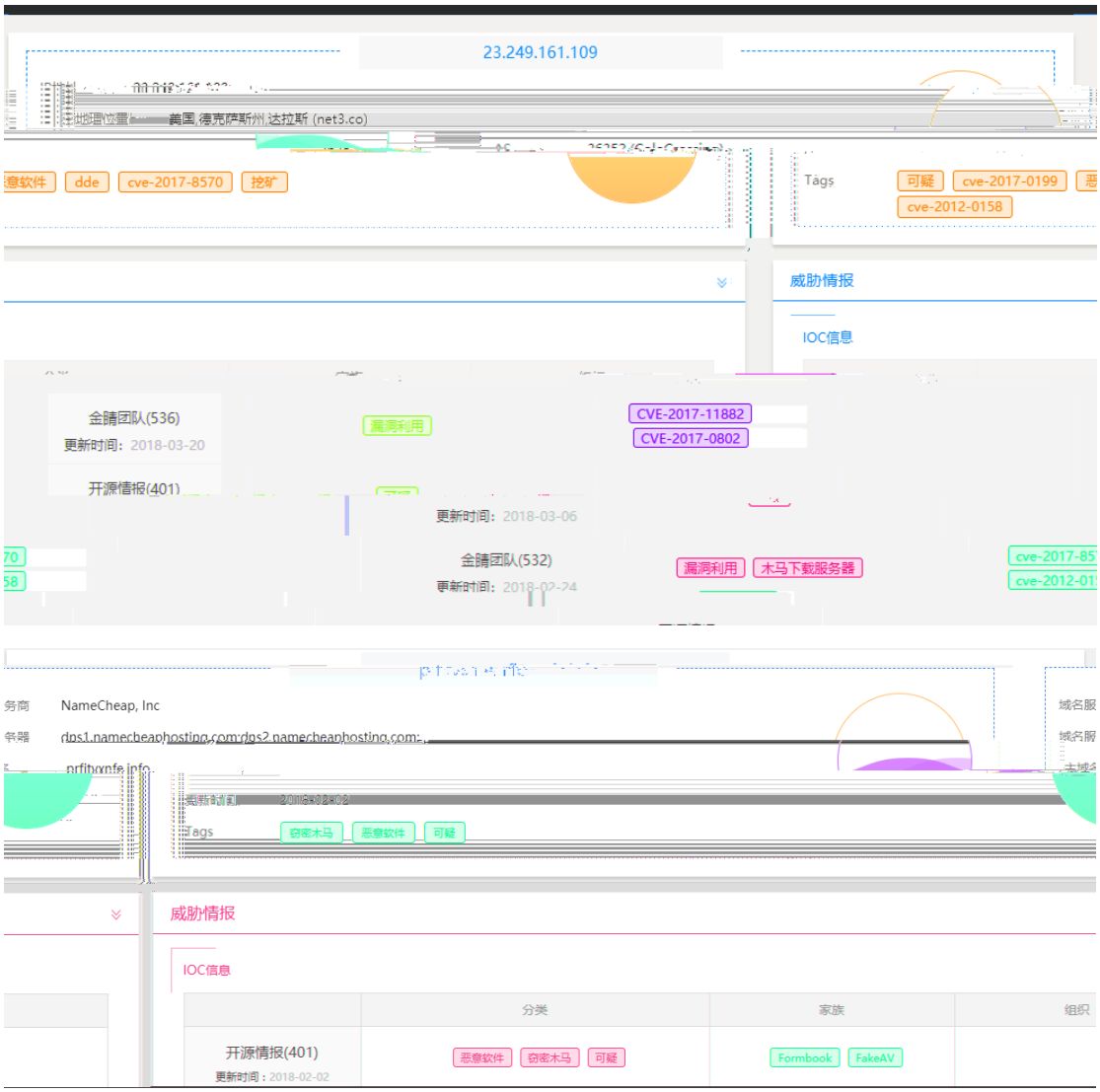
,



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


23.249.161.109
美国 德克萨斯州 达拉斯 (net3.co)
意软件
dde
cve-2017-8570
挖矿
Tags
可疑
cve-2017-0199
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
金睛团队(532)
更新时间：2018-02-24
漏洞利用
木马下载服务器
NameCheap, Inc
dns1.namecheaphosting.com;dns2.namecheaphosting.com;
Tags
窃密木马
恶意软件
可疑
威胁情报
IOC信息
分类
家族
组织
开源情报(401)
更新时间：2018-02-02
恶意软件
窃密木马
可疑
Formbook
FakeAV



