《如何分析潜在威胁文件》

作者：MUSYIDA

随着互联网的发展，网站也多了起来，我们可以从各类网站下载软件使用，但是这些软件安全性怎么样？普通人可能察觉不到，但是通过一些简单的技术手段，我们可以进行一些分析。遵循先易后难的原则，本文将从自动向手动过渡。萌新写作，水平有限请 dalao 多多海涵。

0x00 浏览器

一般情况下，浏说器都会对下载的文件进行安全检查支持的浏缆器包括但不限于:EDGE、谷歌、火狐、360 安全、360 极速浏览器。 其中，最为严格的是谷歌浏览器，一但检测到危胁程序将中下断载。如果要下载一些破解版的文件或病毒样本，笔者建议使用 360 极速浏览器。轻快，无广告，下载功能由迅雷提供技术支持，并且下载危胁程序不会被强制删除。

0x01 安全软件（以 360 安全卫士为例）

一般情况下， 安全软件也会对下载的文件进行检查，但笔者用了一款较为流行的 MBR 锁机病毒进行测试(RAR 文件)，被 360 安全卫士（右下角弹窗的文件检测）判为安全或未知，根据我对这个检测机制的大致研究，文件被下载后的安全检测使用的引擎与查杀引擎不同,前者只进行了粗略检测。所以笔者提议未和文件被下载后不要急于打开，而是通过安全软件进行查杀之后再做判断(仅供参考)。如从浏览器上下载文件，360 安全卫士会对下载的文件进行安全检查，如果是木马病毒，下载后会立即删除威胁文件(可在隔离区找回)。不过,要是你想弄清楚 360 因为什么才报毒，不妨先恢复到原来的位置，在右键点击 360 木马云查杀,片刻后,你可以通过报毒名详情以及报毒引擎来看看为什么报毒了。（可能含有误报）

或是在解压的时候就被 360 安全卫士拦截。

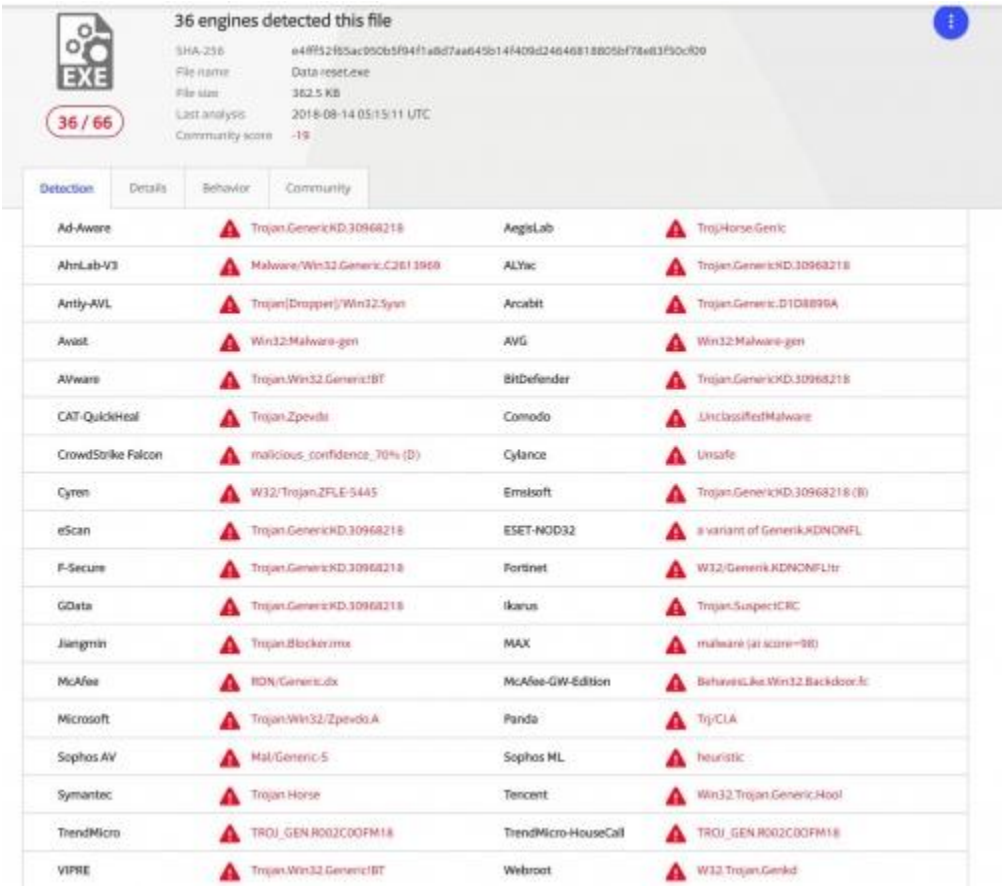
通过看报毒名可以得知是 QVM 引擎报的，但是还是看不出来为什么报，我们换一个样本试试。

就像这个一样，360 报的是 Backdoor，从 Backdoor 就可以看出是后门木马了。当然 360 的主动防御在你双击的时候也会拦截。

当然，QVM 是机器学习，可能会存在误报的情况，这就请大家擦亮双眼。

0x02 在线扫描

网上有许多综合各家安全软件的结果来给出文件安全性的网站，但笔者选择最常用的提供给大家。就是: VirusTotal ，为什么会选择它呢?因为它的杀软病毒库是最新的，根据杀毒率判断，就会给出你的文件是安全还是危险(仅作为参考)。据卡饭网友反映，VirusTotal 上的杀软存在互抄报毒结果结果的情况况。有可能被一家误报，另家也跟着报，一般新手到这里就可以结束了。后面的内容需要些编程基础。



原文：原来 ESET 自动机误报为 a variant of Generik.KDNONFL trojan， 后来虚拟机验证确认误报后提交至 ESET，现在报法为：Data reset.exe - Win32/HackTool.Crack.GI potentially unsafe application.

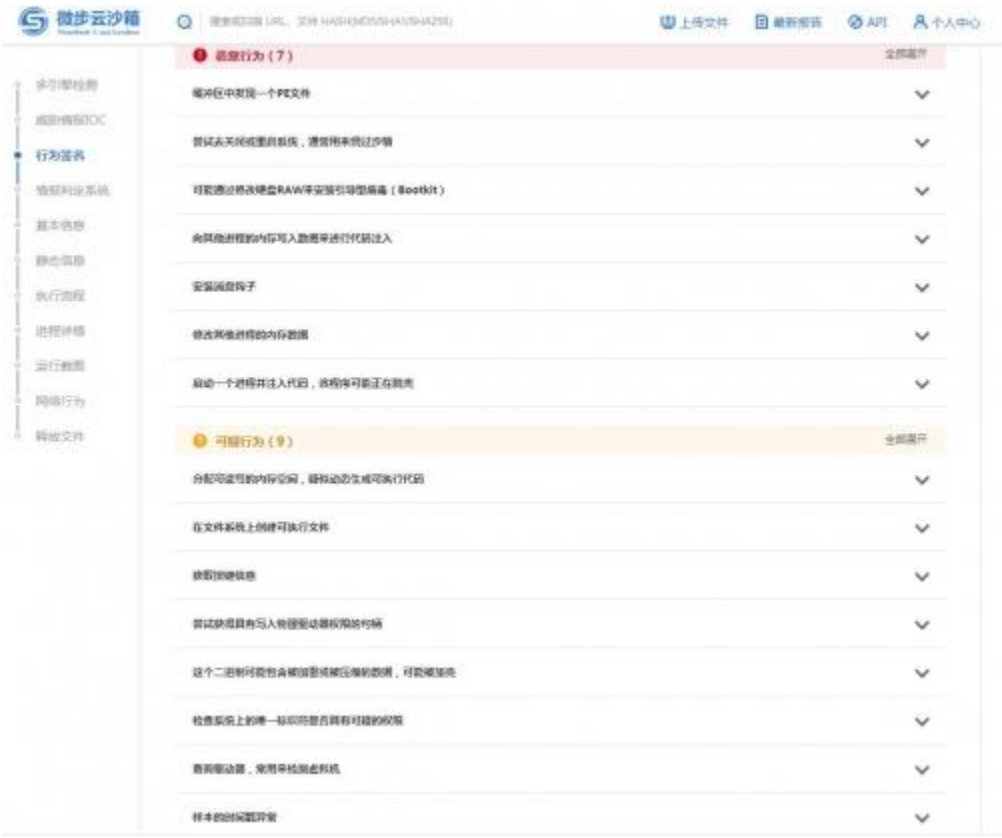
然后看看 VT，认真看有报的中 没有一个报 RiskTool 或者 PUP， Hacktool，反而全部都是 Trojan Generi 的报法，可以说都是抄的我自己都吓到了。（来源卡饭网友 191196846）

0x03 安全沙箱

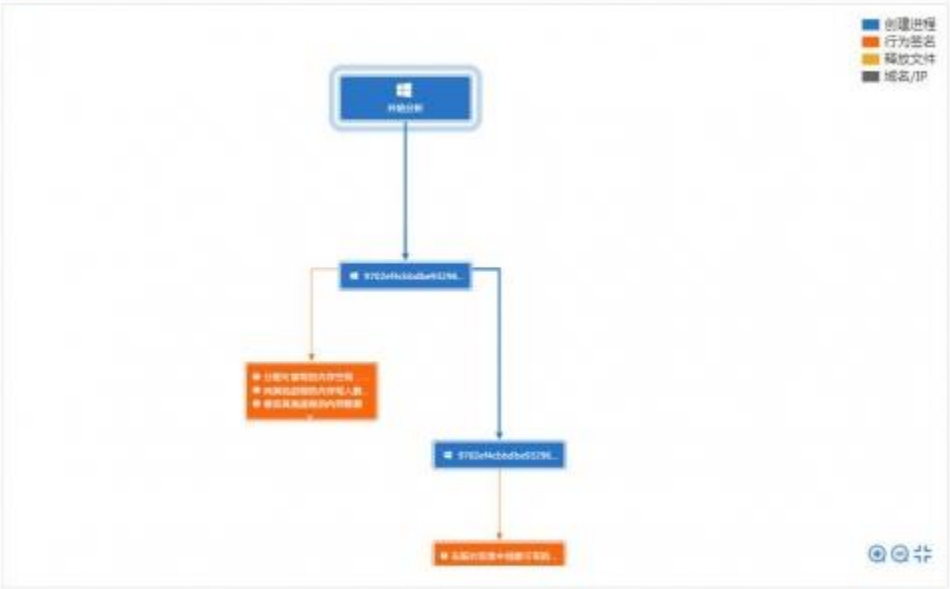
目前国内能使用的网上的沙箱就只有腾讯哈勃和微步云沙箱，金山火眼已在几年前下线。你只需要把文件上传上去，稍等片刻就能得到结果，但是它们后都有

文件大小和格式限制。通过沙箱，你可以弄清文件的大概行为。

微步云沙箱界面如下。



执行流程



进程详情

腾讯哈勃界面如下。

0x04 程序逆向

我对这方面研究不太深，但是还是有点干货给你们的。我在这里谢谢Crazyman_Army 表哥。

传送门：

标题 :从零开始的程序逆向之路基础篇 第一章——认识 OD(Ollydbg)以及常用汇编扫盲 地址：https://bbs.ichunqiu.com/thread-43041-1-1.html

标题 :从零开始的程序逆向之路基础篇 第二章——用 OllyDbg(OD)分析一个简单的程序 地址：https://bbs.ichunqiu.com/thread-43469-1-1.html

0x05 总结

如果技术不够好，一定要装杀软。不要和我说什么勤打补丁，用 WIN10 自带，那东西，小学生易语言都能免杀。

完