争奇斗艳 360与金山的云查杀技术

■ 文/小二黑

金山毒霸2012正式推出时，有一个非常轰动的宣传字眼：30核，即通过30种不同的病毒查杀引擎保护系统的安全。单从数字上看，貌似30核的交叉查杀远比360的4引擎更为稳妥和先进，但实际上到底是怎么一回事呢？今天我们就要来揭开隐藏在云端下两种不同查杀技术的真相。

其实在金山毒霸和360杀毒中，云查杀已经占据了越来越重要的地位，而前文所说的30核其实也是云查杀的一部分，但金山毒霸和360杀毒两者在云查杀上使用的技术却完全不同。

360杀毒的QVM

如果留意的话，会发现360杀毒并没有以往杀毒软件必须的病毒特征库，这是由于360杀毒抛弃了传统杀毒软件“引擎+特征库”的架构，直接与服务端的360云安全数据中心组成云安全体系。在本地进行文件扫描时，360杀毒的四引擎之一360QVM人工智能引擎将发挥作用。QVM即Qihoo Support Vector Machine的缩写，是360完全自主研发的第三代引擎，2010年11月12日推出，集合在360杀毒2.0正式版中。

本地加云端双重查杀构成了完整的QVM

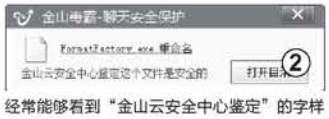
从本质上讲，QVM是一种启发式引擎，也可以说是启发式鉴定器。从运作方式上来看，QVM要从文件中提取某些特征，诸如文件的大小、需要调用哪些API、是否自解压等等，然后再根据这些特征比对海量的黑白样本来判断此文件是否安全。就好比警察抓小偷，警察抓了很多的小偷和很多好人，发现小偷一般都贼眉鼠目，好人都是大方坦荡。而且，通过不断的扫描样本，QVM引擎不断地扩大自己对已知黑白文件特征的特性数据库，进而判断未知文件的黑白属性，逐步提高对病毒的检测率和降低对白文件的误报率，使得“抓小偷”的结果更为精准和可信。

QVM引擎不像以往被动的行为防御，小偷伸手了才确认去抓住它，也不像病毒特征码，等确认后才去抓。它不在乎文件的具体细节，而是通过一个数学统计的方式宏观地判断一个文件的黑白。

如果遇到拿不准的文件，本地QVM引擎提取文件特征后会上传，上传的特征数据量很小，所以很快就能完成，最后通过云端的三款QVM鉴定器检查。因云端的QVM每天扫描的是海量样本，总结了更多的经验，所以比本地查杀更加准确，瞬间得出结果后就会反馈到本地。

金山毒霸的云鉴定

金山毒霸2012采用了边界防御的方式，对每一个进入电脑的文件都会验证它的黑白，而对于未知的文件就上传到云端进行鉴定。



经常能够看到“金山云安全中心鉴定”的字样

金山毒霸的云鉴定体系采用了与360的云QVM完全不同的方式。毒霸的云采用的是微特征的方式，在云端通过病毒特征库中的微特征与文件对应的方式来判定一个文件的黑白。毒霸的云鉴定可以用“微观”来表示。

毒霸云端目前有30多款鉴定器，有启发式的，也有行为判定的，还有其它的专门针对某些病毒的鉴定器。这些鉴定器是在每天更新甚至更换，但是绝对不是想象中简单的多引擎扫描。金山的云端鉴定器用各种不同的方式鉴定一个样本的安全性，然后通过加权或者其它的算法给出一个总评，最终判断文件的安全性。

一般一个未知文件进入用户的电脑，如果用户没有手动鉴定，那么这个文件将会被自动上传并返回结果。如果用户主动上传，99秒内就返回结果。金山毒霸的查杀率体现在云端，就是所有上传过来的文件，必须要趋近于100%的鉴定准确率，如果鉴定器鉴定不出来的，就会转人工，由金山工程师判断。

各自的优缺点

这里的比对并不意味着我们推荐使用某一款杀毒产品，因为两种云都各有特色，360杀毒的本地和云端QVM对于变种或新型病毒有较好的防御能力（90%以上），金山毒霸追求的是精确且占用资源更少，但完全不能离开网络环境。