后续前言：

4 个月前本人原创的《瑞星 2012 万字评测及建议》受到卡卡论坛和卡饭论坛很多会员的好评！官方工程师对这篇报告也很重视并在新版 V16 UI 的开发中采纳了很多建议。最近看了看其他安全厂商的新版本功能，我选取了一些个人认为不错的功能结合我在使用中的一些体验和想法写了这篇后续建议，希望能继续给瑞星 V16 后续的研发提供一些有价值的用户感受。

目 录

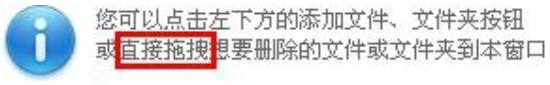
3.14 建议增加扫描结束预计时间 2
3.15 文件粉碎器建议 2
3.16 流量监控条建议 2
3.17 扫描结果页面建议 4
3.18 建议增加病毒“名片卡”功能 5
3.19 人工智能引擎及新主防建议 6
3.20 弹窗 UI 建议 7
3.21 建议增加云鉴定功能 8
3.22 建议增加沙箱功能 9
3.23 建议将开发模式分为正式版和开发版 11

3.14 建议增加扫描结束预计时间

这个功能 2010 版有，后来去掉了。虽说给出的预计时间不一定非常准确但大致能告诉用户需要多少时间，我单位电脑中的文件比较少，要是换别人的二、三十万文件总得扫个半小时左右吧，如果能给出扫描预算时间大家就可以在这段时间忙别的事情了比现在这样干等着强多了。

3.15 文件粉碎器建议

1.希望增加拖拽功能，现在的粉碎器只能手动添加文件和目录，如果文件“藏”的太深的话记不住，所以需要拖拽功能和鼠标右键集成该功能的加入。其他日志功能啥的现在都支持拖拽了，所以这个从开发上应该不难。



2.希望在用户删除文件失败时自动弹出粉碎器，由于许多人不知道这个功能所以自动弹出粉碎器功能显得很人性化，也可以当广告宣传了。

3.16 流量监控条建议

瑞星的流量监控一打开就是一个大界面！界面大妨碍其他界面的显示！

建议加入精简的监控条

360 卫士的：

联网程序、网速、CPU 占用等一目了然，还有天气预报等实用功能显示

金山卫士的：

金山直接在右边加入了系统占用统计，个人感觉金山在颜色使用和设计上比 360 做的更好，希望瑞星能参考做出有自己特色的流量监控条。

3.17 扫描结果页面建议

新版 V16 的扫描结果页面过于空旷，看着人心里发慌：

可以参考一下 360 和金山毒霸的扫描结果页面：扫描文件数、威胁数、扫描时间、对于结果的满意度、详情等等非常详细！

这样做一方面充分利用了页面空间，另一方面可以让用户对本次扫描的概况有一个大致了解，直接提示一个没有发现威胁给人敷衍了事的感觉。

3.18 建议增加病毒“名片卡”功能

很多朋友对杀软扫描出的病毒和木马都很好奇，这个程序究竟对系统和文件有什么危害？所以增加这个名片卡功能可以帮助用户更好的了解所发现威胁的危害另外能激起一部分用户学习反病毒知识的兴趣。

3.19 人工智能引擎及新主防建议

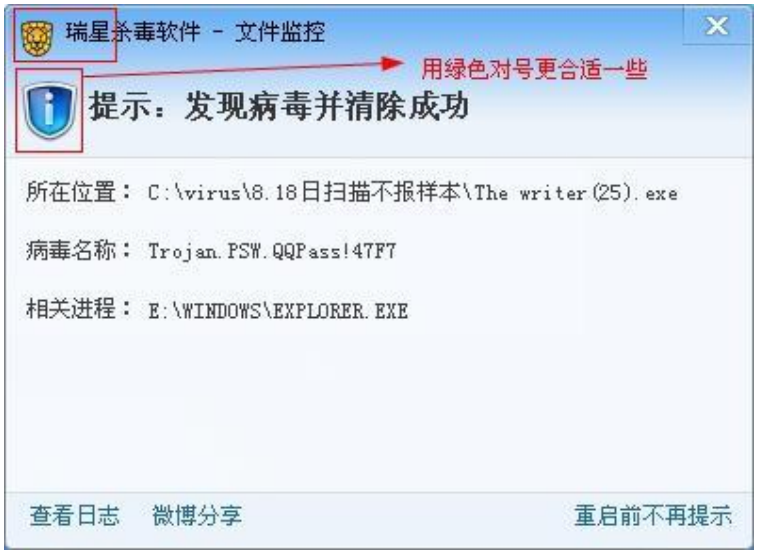
首先“智能”两字来源已久但一直基于启发算法上如最早的静态启发到后期的动态启发+虚拟机最后到现在的人工智能。现在分析一下将人工智能付诸于安全领域实际产品的两家厂商：首先是 360 的 QVM（QihooSupport Vector Machine）人工智能引擎，此项目在 2008 年立项经过 3 年研发于 2011 年正式应用于 360 杀毒 2.0 上后期与云端结合的云 QVM 效果卓著在对未知病毒检测能力上大幅提升！QVM 的原理虽然 360 官方始终保密但有兴趣的朋友还是猜出了一些“端倪” 首先其先扫描海量黑样本并进行数学概率统计建模，对毒木马样本的动作充分掌握并计算概率，一旦一个未知文件的动作超过了这个概率便判定为黑；但与其他启发式引擎一样初始时 QVM 误报比较高所以后期让其再“学习”海量白文件再进行概率统计建模这样误报便降低了。所以 QVM 的主要判定是从文件本身发起的。另外一种人工智能是金山的 KSC（Kingsoft System Intelligent Cloud）其原理是以系统维度出发分析木马文件的启动点（不是启动项），打个比方就是一个不应该出现在 QQ 文件夹下的病毒文件出现了那么 KSC 就根据云端启动点规则进行判定。由于只扫描“活体”病毒所以这种技术在文件静态查杀检出率上不会有

明显提升但是却对整个计算机系统有全局的把握。

分析完两种现行的人工智能引擎再说说瑞星。由于瑞星的主防是本地行为分析所以选择类似 QVM 的人工智能引擎不太适合。鉴于瑞星的系统修复能力一般所以建议开发类似金山 KSC 的从系统维度鉴定的人工智能引擎。待成熟后将其融入系统加固可以使判定更准确、误报更少！这样的智能系统加固+本地行为分析的主防架构可以使拦截能力大幅提升而误报将至最低，而且到时对感染病毒的系统修复能力也将提高！

3.20 弹窗 UI 建议

新版 V16 虽然改进了所有程序界面，但弹窗 UI 仍然不好。首先左上角瑞星 LOGO 和右边的文字不再同一水平线上。



这个是一个网友给江民设计的，瑞星可以参考一下，这种设计简洁大方，安全、风险、高危通过弹窗颜色的变换一目了然。

3.21 建议增加云鉴定功能

既然新版瑞星重点主打“云”，所以本地云鉴定功能就有必要研发了。况且现在主流的杀软如 360、金山、江民等都已开发了该功能，所以瑞星不能落后。关于云鉴定给出几点个人建议：

首先了解一下 360 和金山两款软件的云鉴定

金山的云鉴定分为自动和主动两项，主动当然就是指用户上传程序进行鉴定，鉴定速度还可以但有时候会转人工，智能性不高，最“坑爹”的是很多病毒都被判定安全，注意这里说的是很多不是个例，相信用过的朋友都知道。

360 的云鉴定器相对来说比较好，不光给出了是否安全还对文件的发布时间和流行度进行了统计，在 QVM 的辅助下鉴定准确度也不错。

简单分析了一下 360 和金山的云鉴定的特点，那么瑞星应该如何做呢？

（1）在云端部署其他杀软的杀毒引擎，这个在万字评测上篇的云查杀建议中提过了即对上传的未知程序先调用其他引擎扫描如果超过一定比率都报毒那么可以判黑返回结果并自动入瑞星云库；

（2）如果其他引擎没有给出明确结果那么瑞星管研发的人工智能引擎或云端动态鉴定器进行动态分析；

（3）如果上述两条都无法判定可以转人工但一定要提示用户此文件是未知建议在沙箱中运行！病毒文件判定安全这个比较坑人，拿不准的话不如说是未知“瞎”判定对用户是极其不负责的表现！

（4）最后云鉴定功能无需捆绑只做成模块放在实用工具中即可。

3.22 建议增加沙箱功能

沙箱这个功能在杀软上已经基本过时了，做沙箱首先要保证沙箱安全性即不能“漏沙”！而能做到的厂商不多 comodo、卡巴、avast、金山等在沙箱方面均存在漏洞，沙箱一旦漏沙还不如没有。但瑞星在云鉴定加入的情况下沙箱还是有必要开发的，毕竟如果判定的文件是未知用户还想运行的话在沙箱中跑肯定比在真实系统中安全，这里给出几条建议：

（1）首先重中之重的就是上面提到的安全性问题，沙箱尽量做到不要漏沙，这比软件的兼容性更重要！

（2）在保障安全性的前提下提高对程序的兼容性，极少数不能运行的或反沙箱的程序不必“纠缠”保证对绝大多数程序的兼容性即可；

（3）增加保存功能：即在沙箱运行的程序可以保存，这个功能很实用；

（4）日志记录要全面：详尽的日志记录可以帮助用户对未知程序的动作做到“明察秋毫”，如果怕显示过多的话可以添加只记录危险或可疑动作选项。

云鉴定和沙箱是两个连带功能，这两项功能的加入可以帮助主防分担一部分压力！

3.23 建议将开发模式分为正式版和开发版

瑞星 2012 版从 2011 年 12 月 26 日公测到现在已经测试了 8 个月!产品性能基本稳定,但新增功能却不多在 03.37 版本增加了卡卡助手中的七项实用工具后便没有更进一步的更新，虽然 V16 推出了新 UI 但软件的实质功能提升却不大。这里建议将目前的版本尽快正式让用户先体验已经成熟的变频杀毒、云查杀技术和新 UI 等，并另放出开发版本或 beta 版集成新功能如支持 X64 的主防、系统加固、木马防御调节等等。这样既可以让着急使用新版但又怕公测版软件不稳定的用户尽快使用新版的亮点功能,又可以让喜欢测试尝鲜的朋友对开发版进行测试并提出改进建议。这种版本分类很多厂商都采用了比如 360 卫士的正式版和 beta 版，beta 版基本每日更新一个字母加入新功能并修复一些 bug,待稳定后下放部分新功能推出正式版，360 杀毒也分为正式版和尝鲜版；金山毒霸采用每周四发布的迭代更新 SP+数字命名规则；QQ 管家也是正式版和 beta 版共存。这样可以让用户感觉到软件真正在更新而不是出一个年度版就完事大吉了。最后 360 和金山还分别有督导和体验联盟,这都是后话了希望瑞星尽快正式 V16 并推出开发版增加功能。