厚黑 360

@独立调查员

拆解周鸿祎与奇虎 360 之厚黑本性

第一辑 2013-03-15

目录

写在前面

自 2 月 26 日《每日经济新闻》发表重大专题报道——《360 黑匣子之谜：奇虎 360“癌”性基因大揭秘》以来，360 公司通过各种渠道散布谣言，攻击抹黑媒体、记者与有关专业人士，并竭力诡辩掩饰其软件产品的种种问题，周鸿祎亲自出面忽悠其它媒体记者，还推出“驳斥《每日经济新闻》九大谎言”继续蒙骗用户。

近日 360 的诡辩，依然是典型的 360 式“辟谣”逻辑：利用用户技术知识空白，胡编乱造，忽悠菜鸟，有些知名媒体人也被 360 言论迷惑。为正视听，本人现针对所谓“九大谎言”与 360 负责人周鸿祎公开对质，以帮助人们看清楚：谁在撒谎？谁在造谣？

人们能否全面认清周鸿祎与 360 的厚黑本性，本人并不乐观，但深信真理越辩越明。

这谈不上是一本什么书，只是资料汇编。

事后分批上传用户行为记录，与安全何干？

周鸿祎狡辩

【谣言】 360 安全卫士 7.3.0.2003l 版本记录和上传软件操作行为，会“泄露用户信息”

【真相】 云安全软件判断进程安全性的过程中必然要与云端进行交互

安全软件都有“进程防护”功能，也就是对运行程序的安全性进行判断。国内外包括 360、金山、腾讯、趋势等云安全软件都会联网检测运行程序的文件指纹、文件签名、命令行参数等信息，否则无法拦截和查杀木马病毒。对此，《360 用户隐私保护白皮书》已经有非常详细的说明。

我的批驳

1、在未告知用户并取得同意的情况下，默认加入涉及隐私权的云安全计划，其安装过程就侵权。

2、用户手动取消加入云安全计划后，并未真正取消，仍上传用户所有行为（联网条件下）。

3、所谓安全防护，必须在程序运行前分析判断，发现安全威胁时阻止运行并报告用户，其时间特征是事前、实时。360 安全卫士则是实时记录用户的所有行为（无论是否涉及安全性，且每一条用户行为记录中都有一个域“m”，其值就是用户机器的唯一标识码。该标识码建立了 360 服务器存储的用户行为记录与用户机器之间的持久关系），周期性地分批次明文提交给 360 服务器 upload.360safe.com，其时间特征是事后、非实时。显然 360 安全卫士的此类动作目的并非安全防护，而是行为记录监视，这是间谍软件、而非安全软件的行为模式。

4、360 安全卫士的用户行为收集策略可从云端操控，随时变更其延迟周期、随时开/关用户行为收集功能。既然是为用户安全防护服务，并声称尊重用户权益，那么暗设云端开/关控制接口的动机何在？一旦其间谍能力被曝光便立即从云端向所有安全卫士客户端下达关闭指令，使得罪证不可重现，而后倒打一耙诬指曝光者造谣。这样的烂戏码，360 玩过多少次了？好在这个相关视频证据已经公证，360 如何抵赖？

以上，与《360 用户隐私保护白皮书》中云安全计划相关内容完全不是一回事，360 以此为据自证清白，实为愚弄媒体人和网民的智商。

证据视频于 2012 年 12 月发布于 56 视频网站，播放 15 万余次，但却于“每日经济新闻”专题报道后被以“审核未通过”为由停播（不知道周鸿祎花了多少钱收买 56.com），视频网页：

http://www.56.com/u16/v_ODExMDM1MzM.html

在此继续提供证据视频高清原版，欢迎下载（周鸿祎，你若能收买百度也把这个删了，就算你狠）：

http://pan.baidu.com/share/link?shareid=155072&uk=858396104

反问周鸿祎

1、事后分批上传用户行为记录，与用户安全何干？

2、给云端预留可关闭此功能的配置接口，动机何在？

360 发新闻稿《360 诉<每日经济新闻>名誉侵权正式立案》

淘宝、网易、新浪、百度、搜狗、优酷、腾讯、……谁是可疑网址？

周鸿祎狡辩

【谣言】 360 服务器上的“用户隐私”数据被谷歌搜索爬虫抓取

【真相】 所谓“隐私数据”是 360 安全卫士对可疑网址的查询记录，主流杀软均采用该机制

这是混淆隐私概念的说法。这些数据只是 360 安全卫士对可疑网址的查询记录。目前各种钓鱼、欺诈网站已经成为中国网民面临的主要安全威胁。360 安全卫士为全国网民每天拦截 3000 万次恶意网址访问。之所以能做到这点，就是得益于基于云的网址安全体系。事实上，这也是目前主流安全软件的通行做法，包括诺顿、趋势等莫不如此。360 可以提供公证材料，证明金山服务器上传用户的 3100 余万条网址被谷歌、百度等搜索引擎抓取，其中存在带有用户名和密码的网址。

至于为何会在网址中出现用户名和密码，是由于极少数网站缺乏安全意识，把用户口令编写在网址中。打个比方，就好像银行给用户邮寄信用卡的邮件，把卡号和密码写在了信封上。对于这类存在安全缺陷的网站，360 也采用了措施，过滤可能带有用户数据的网址。

我的批驳

1、 那些记录不是“查询记录”，而是“存储（在 360 服务器上的用户上网）记录”，且每条记录都有用户机器识别码（混装）。

2、 收集可疑网址是正常的、也是必要的，前提是所收集网址确属可疑网址。在被抓取的数据文件中发现新浪、网易大量用户帐号和密码，以及淘宝、网易、新浪、百度、搜狗、优酷、腾讯等知名大网站的链接，甚至还有不少企业内部网络地址。难道这些网站的网址在 360 眼里也都是“可疑网址”、甚至是“钓鱼、欺诈网站” ？

3、 事实上，几乎所有主流网站网址都在列——360 眼里，世界人民都“可疑” ？显然这是假命题。

4、 综上三点，结论：360 假安全之名，行取隐私之实，且事前不告知、事后不认账，侵犯群体隐私权事实成立。

5、 360 不对其窃取的用户隐私数据加密，在服务器被攻破后，海量用户上网行为的明文记录被泄漏。罪加一等有木有？

证据视频，请欣赏：

http://v.youku.com/v_show/id_XNDYyNzM2NTcy.html

反问周鸿祎

1、淘宝、网易、新浪、百度、搜狗、优酷、腾讯、……谁是可疑网址？

2、究竟谁在一再混淆隐私概念？难道 360 享有独家“隐私”定义权？

3、用户隐私遭大规模泄漏，360 何时认错/道歉？

周鸿祎，你语文是体育老师教的？

周鸿祎狡辩

【谣言】 全新安装 Win7 在开启自动更新、尚未安装任何第三方软件前，360 体检 0 分

【真相】 这是赤裸裸的谎言

赤裸裸的谎言，任何用户都可以自行验证。试问，一个“全新安全的 Windows7”为何会有百度工具栏，为何会在收藏夹中有百度、腾讯的收藏项？这个所谓的全新 Windows 从何而来？

我的批驳

1、先看每经专题报道相关原文：

比如全新安装的 Windows7，在开启自动更新、尚未安装任何第三方软件前，360 安全卫士对其安全评估结果竟是 0 分 （满分 100 分）。这个 0 分意味着什么？Windows 真的很不安全？实际测试发现，根据其安全警示清单一项一项“优化或修复”后，评分逐步增加，但始终处于低位、不到 60 分，直到“优化浏览器”并“锁定首页”后，安全性评分迅速接近满分！事实上，所谓“优化浏览器”就是“安装 360 浏览器并设定为默认浏览器”，“锁定首页”就是“修改首页为 360 导航”。

需要修复的项目还有（不限于）：卸载“差评插件”百度浏览器工具栏、优化 IE（实为篡改 IE 的首页、标签页、默认搜索引擎为 360 的有关服务）、删除收藏夹中对手的项目（百度、腾讯、谷歌等）等等。

360 安全卫士甚至曾伪装成微软 Windows 补丁安装程序 KB360018，以“IE6 内核升级”的名义欺骗用户安装 360 浏览器。国外权威技术网站 SystemExplorer 已将 360 的这个假冒微软系统补丁文件定为“100%安全威胁”，从而使后者遭遇微软调查。

2、以上原文概要：

a）360 安全卫士给新装 Windows7 系统评分为 0，且给 360 浏览器权重超高属不正当竞争（360 日前已因此遭工商局行政告诫）；

b）列举 360 安全卫士假“修复”为名作恶的若干典型例子（注意“不限于”），并不受前一段实例“全新安装的 Windows7”限定词的限制（缺省主语应是“一般用户电脑上安装的 360 安全卫士”）；

c）特别列举 360 安全卫士“太岁头上动土”，以给 Windows 打安全补丁为名静默安装 360 安全浏览器，极其粗暴恶劣地欺骗用户、践踏国际领袖企业微软公司的声誉。

3、显然，原文三段内容关系是递进的，而非并列的，且内容非常丰富，360 的无厘头反问“这个所谓的全新 Windows 从何而来？”实为装疯卖傻、回避全部实质问题、糊弄媒体和用户，令人不齿。

4、事实上，本人早于 2012/11/22 在新浪微博发文披露“360 安全卫士给新装 Windows7 系统评分为 0”（本人亲测）：

360 的口号是“没有问题就制造问题”。我一个新装的 Windows7+SP1，360 安全卫士首次运行“体检”评分为 0 分，折腾半天、要我装这个装那个，到了 40 多分，最后“听话”安装 360 安全浏览器后，评分陡升到 97 分。360 安全卫士的恐吓、欺骗、诱导手段都不是盖的。流氓充警察，

不知“耻”为何物。

来源：http://weibo.com/2902756801/z6lW9lGlO

5、请从新浪微博或百度、谷歌等搜索引擎搜索“windows7 360 安全卫士 体检 0 分”，去看看有多少人证、书证。下面是用 Google 搜到的几个（BTW，感受一下这个 0 分带给小白用户多大的不安吧，不安又不懂的情况下自然会乖乖就范、安装 360 的这个那个……话说 360 会不会说以下网页都是我“穿越时空”伪造的呢）：

a）新装 的 WIN7 旗舰 64 位原版，360 安全卫士 体检 0 分？

来源：http://bbs.ithome.com/thread-448437-1-1.html

时间：2012-4-30

b）360 安全卫士体检提示电脑得分为 0 分！有 78 个高危漏洞！要一键修复吗？卖电脑的人说不用去修复？求高人

来源：http://wenwen.soso.com/z/q333692295.htm

时间：2011-11-21

c）今天刚买的电脑，正版的 WINDOWS7 家庭普通版，回家装了个 360 体检显示 0 分，卖电脑的说有什么漏洞都不能修复

来源：http://zhidao.baidu.com/question/510477851.html

时间：2012-12-25

d）急急急！刚做的 win7 系统用 360 安全卫士体检检测出 70 多个高危漏洞。需要修复吗？

来源：http://zhidao.baidu.com/question/314182058.html

时间：2011-08-31

6、360 软件的重要策略几乎全部受其云端控制，可随时更改（能够快速响应工商局行政告诫，停止不正当竞争行为、不再给 360 浏览器超高权重，即是一例），目前暂时不可重现，因为时空已变。我在确认已暂时更改后第一时间就发了帖子（发帖时间为 2013 年 2 月 12 日）：

前几天收到工商局“利用安全卫士在浏览器领域不正当竞争”的指控后，360 已经暂时收敛。

来源：http://weibo.com/2902756801/ziPNU6yWy

7、所谓“赤裸裸的谎言”，实为“悄悄更改后再抵赖”又一例，这顶“谎言”帽子必须奉还给周鸿祎自己戴上。

反问周鸿祎

1、 用户新系统被评分为 0，究竟有没有？

2、 给 360 安全浏览器超高安全分权重，是何时以何种方式更改的？更改原因是否与受工商行政告诫有关？

3、 冒充 Windows 补丁欺骗用户静默安装 360 浏览器，究竟有没有？

4、 篡改 IE 的首页、标签页及默认搜索引擎，算哪门子“IE 优化”？

5、凭什么认定用户收藏夹中百度、腾讯、谷歌等项目是广告项目？（可笑的是，当把收藏夹项目名称保持不变、但更改目标网址为 360 官网时，仍然被视为广告项目予以删除，可见 360 安全卫士是根据收藏夹项目名称是否“百度”、“腾讯”或“谷歌”来判定是否广告项目，毫无疑问是不正当竞争行为，与用户安全没有半毛钱的关系。）

所谓“配置文件”，却反汇编出近万行汇编程序——周鸿祎敢不敢押上 360 的生死否认此事？

周鸿祎狡辩

【谣言】 360 浏览器有“后门”，从服务器定期下载 dll 可执行程序

【真相】 该 dll 文件只是配置文件，并不具有“遥控”作用

这是恶意歪曲的说法。报道中提到的 dll 文件，实际上只是配置文件，并不具有“遥控”作用。配置文件做成 dll 形式并添加数字签名校验是安全软件常规做法，可以保证程序在加载配置文件时，能够确认文件没有被木马篡改过。这种做法还可避免下载文件时被中间人攻击。比如黑客通过 ARP 攻击劫持下载过程，返回由黑客构造的恶意配置文件

我的批驳

1、360 安全浏览器暗设后门的视频证据：

- 在线播放 http://my.tv.sohu.com/u/vw/33484498
- 高清下载 http://pan.baidu.com/share/link?shareid=115587&uk=858396104

2、《论证 360 安全浏览器后门机制》

http://i.sohu.com/p/=v2=bcdsBXalk3VpmZc3ZXZlLmNvbQ==/blog/view/246730306.htm

3、《杀鸡请牛刀》（与多位专家公开论证 360 安全浏览器后门）

http://i.sohu.com/p/=v2=bcdsBXalk3VpmZc3ZXZlLmNvbQ==/blog/view/246958843.htm

4、《公开举报奇虎 360 公司——致工信部、公安部公开信》

http://i.sohu.com/p/=v2=bcdsBXalk3VpmZc3ZXZlLmNvbQ==/blog/view/243590884.htm

5、《就当吃一回狗屎吧——回 360 陶伟华》

http://i.sohu.com/p/=v2=bcdsBXalk3VpmZc3ZXZlLmNvbQ==/blog/view/244191687.htm

6、看周鸿祎如何偷换概念愚弄记者：

提问：我是独立媒体人，我们集中在《每日经济新闻》有什么疑虑，稿件里面说 360 的安全浏览器在后台频繁与服务器进行通信，在用户没有交易情况下，安全浏览器有没有用户不操作，也会有交互的行为，如果交互的话信息是什么？

周鸿祎：在整个互联网当中，钓鱼和欺诈、挂马网站是主要安全威胁。这些恶意网址的生存周期是以小时来计算的。做一个网站骗几个人，马上把域名一换。报道所谓的 360 安全浏览器“后台交互”，其实就是查询最新出现的恶意网址，诺顿宣传是秒级更新，和很多软件与服务器之间保持一个心跳概念是一样的。其中并没有传递用户的任何信息，就是一个安全更新服务。《360 用户隐私保护白皮书》里也写得很清楚，浏览器拦截恶意网址最主要的基础是，360 服务器建立一个恶意网址库，每天不断加入最新发现的钓鱼网站，现在已经有上亿条网址。如果把恶意网址库放在用户电脑里，会占据大量系统资源。而当用户访问一个网址时，浏览器会计算网址的指纹去服务器做查询，看它是不是恶意网址，这种情况会和服务器有交互。

显然，记者问的是“后门机制”，周鸿祎答的是“云网址安全”。

很遗憾，可能由于专业知识有限，这位记者没有表现出临场快速反击能力，如果当时我在现场，周鸿祎会不会四处找地洞？

事实上，“云网址安全”也仅当用户提交访问网页请求时才触发，而在用户无操作时浏览器不应与云网址安全服务器（恶意网址数据库）发生任何关系。

然而，记者问的正是“在用户无操作时”，周鸿祎完全答非所问。

但是，我敢打赌，现场记者大多会认为周鸿祎“有道理”——都被赤裸裸地愚弄了。

事实上，“后门机制”首先是下载（DLL：Windows 系统的动态加载程序库）、而非上传，其对用户的恶意行为决定于下载的 DLL，并非定数——服务器随时换个不同功能的 DLL，会在几分钟内自动（浏览器主动循环请求）进入全国所有 360 浏览器用户电脑悄悄加载执行——这不是后门是什么？360 不是把全国所有 360 浏览器用户电脑当“肉鸡”吗？

反问周鸿祎

1、 所谓“配置文件”既然是“正常”的，为什么现在从 http://se.360.cn/cloud/cset.ini 到 http://se.360.cn/cloud/cset17.ini 这 17 个历史文件的内容全部清空或删除了？既然你在极力掩饰这个自认为不是秘密的秘密，又凭什么要求公众信任你？

2、 所谓“配置文件”，实为 dll 文件（可动态执行程序），为什么伪装成 ini 文件（纯文本）？

3、 所谓“配置文件”，你们在不同时间、不同人给出了完全不一致的“解释”，为什么？

4、所谓“配置文件”却反汇编后出了近万行汇编程序——你敢不敢押上 360 的生死来否认此事？

5、 客户机无条件的固定小周期轮询服务器的行为模式，实际上实现了客户机和服务器的角色互换——客户机变成了服务器，服务器变成了客户机，客户机完全听命于服务器——表面是 360 为用户服务，实际上暗设一个让用户为 360 服务的机制——这不是“遥控”是什么？目的何在？

我说你木有小鸡鸡，你说你有 6 根手指？

周鸿祎狡辩

【谣言】 360 安全浏览器“浸润”网银安全，屏蔽权威认证机构 VeriSign，换为自己的认证

【真相】 360 浏览器并未屏蔽 VeriSign 认证

360 安全浏览器访问被 DNS 劫持的招商银行，用户看到的是一个页面（点这里查看>>），在这样强烈的提示下，任何用户都不会进行下一步了。所以根本不存在 360 安全浏览器屏蔽 Versign 认证，如果屏蔽，这个拦截网页根本不会出现。用户可以自行下载 360 安全浏览器来验证，将系统时间改成 2010-1-1 就能重现

我的批驳

1、《360 绿色网站的安全谎言：“偷梁换柱”浸润电商网银安全体系》的中心思想是解构奇虎 360 宣扬的安全谎言：“解决网站难辨真伪问题：辨别钓鱼假冒网站，保护企业网站权益，让用户放心访问。”（来源：网站认证介绍 http://trust.360.cn/introduction.php），以揭露其安全承诺的欺骗性。

2、证书识别是浏览器内核功能，而非浏览器软件额外功能。众所周知，360 浏览器软件的内核是 IE 和 Chrome 的内核，内核的功能特性并非 360 浏览器软件独有，而我们关注的是 360 浏览器软件独有的安全特性——网址栏的“认证铭牌”及其“网购保镖”的可信度问题。

3、确认以下事实：1）所有网银均支持的浏览器内核是 IE，用户访问网银时 360 浏览器软件亦自动切换为 IE 内核，在网银被 DNS 劫持的情况下其“认证铭牌”并无证书风险提示（360 回应中声称的“认证铭牌”证书风险提示仅限使用 Chrome 内核时），仍然显示正常认证信息；2）在网银被 DNS 劫持时（强调 :修改 hosts 只是劫持 DNS 的低级手段 ,且可识别 ,其它手段则无法识别），其“网购保镖”仍然报告“可以放心网购”；3）网址栏看不到网银的 SSL 证书信息，只有“认证铭牌”，是谓“屏蔽”。

4、360 对网银的“浸润”还包括所谓“网银无忧”（自动安装网银安全控件）等，“网银无忧”干扰或拦截网银自身的自动下载和安装，且据了解并未取得各商业银行的授权。另外，该功能的可用性非常低，网上有大量的安装失败报告记录，我们在测试时也多次发现安装失败，而网银自身的下载和安装并无此问题。

5、360 浏览器软件以安全的名义在网银领域所伸的手太长了，但并未给用户带来实质性安全增加值，相反其虚假安全提示及错误操作反而可能误导用户信任钓鱼网站。我们认为 360 并非网银安全价值的建设者而是破坏者，我们对其浏览器软件深度涉入网银的动机高度存疑。

反问周鸿祎

1、 你的“认证名牌”取代了 SSL 证书信息位置、使用户失去了一个可信依据，是否事实？

2、 你是否承认，你的浏览器无法有效识别 DNS 劫持（修改 hosts 的低级手段除外）、因此仅根据域名认证网站不具可信度？如果不可信，你凭什么吆喝“（360 绿色认证）让用户放心访问”？

3、 安全警告信息和状态信息都是必要的。我说你屏蔽了状态信息，你回答说内核警告选项还在，糊弄谁啊？谁要跟你说内核？你不是鼓吹比内核原生浏览器更“安全”吗？牛皮吹不下去了？

把“请求网址”中的数据偷换成“数据实体”骗人，很有趣吗？

周鸿祎狡辩

【谣言】 用 360 手机卫士及 360 手机通讯录进行云备份或云恢复时，用户数据是明文传输的

【真相】 所谓明文传输是谣言，这些数据采用高强度的工业级加密算法进行保护

这是不负责任的说法。360 手机卫士和 360 通讯录，只有在用户主动使用 360 云备份功能时，才会将用户所选择的通讯录、短信、通话记录等数据进行加密后上传。这些数据在网络传输和服务器存储的全过程中，都采用了高强度的工业级加密算法进行保护。即便用户手机连接到黑客的钓鱼 WiFi，这些数据也难以被解密泄露。

我的批驳

1、专题报道相关部分原文如下：

只要登录 360 手机卫士及 360 手机通讯录，或者进行云备份或云恢复，用户名（手机号）、手机 IMEI 码和密码等高度敏感信息就会通过请求网址明文传输，有了这些身份鉴别信息，可以使用任何浏览器从 360 通讯录服务器 tongxunlu.360.cn 的非安全通道直接下载用户云备份的通讯录等隐私。

对此，独立调查员进行了相应复检，发现含高度敏感信息的请求网址的参数部分，仅以 BASE64 编码（可简单解码，与明文无异），而用户密码虽然经过 MD5 加密、但是可直接用于登录，且对客户端合法性没有任何校验。独立调查员向《每日经济新闻》记者说，请求网址极易被非法拦截，在网址中明文夹带传输高度敏感信息，以及使用非安全通道下载用户隐私数据，等于把手机用户隐私暴露在阳光下。

2、对比原文与 360 的回应，可知 360 的回应纯属偷换概念，我们说的是网址包含用户隐私信息。

网址实例：

http://tongxunlu.360.cn/service/MultiServiceRestore?**para**=QWN0aW9uPU11bHRpU2VydmljZVJlc3RvcmUmSW1laT0wMDAwMDAwMDAwMDAwMDAmVWlWZXI9MTAwJk15VmVyPTEuMy41JlVzZXI9MTUxMDEwNzYwNjAmUGFzc3dvcmQ9ZTEwYWRjMzk0OWJhNTlhY

mJlNTZlMDU3ZjIwZjg4M2UmQXBwVHlwZT0xLDIsNSZSZWNvcmRJZD0tMQ==

其中参数“para”的串值是 BASE64 编码，看似密文、实为明文，可直接解码，解码后的文本如下：

Action=MultiServiceRestore&**Imei**=000000000000000&UiVer=100&MyVer=1.3.5&**User**=15101076060&**Password**=e10adc3949ba59abbe56e057f20f883e&AppType=1,2,5&RecordId=-1

这还好意思叫“360 手机卫士”吗？应更名为“360 手机尾失”——让用户随时露出尾巴给别人踩。

反问周鸿祎

1、 你是否承认用户名（手机号）、密码、IMEI 码是应予保护的用户隐私？

2、 你是否承认网址很容易被非法拦截从而导致用户隐私外泄？

3、 你是否承认网址中携带用户隐私信息是低级错误？

4、 你是否承认“360 手机卫士”不仅未能有效保护用户隐私安全，反而严重增加了泄露风险？

5、 你是否愿意立即向所有“360 手机卫士”用户发出安全警告并道歉、以彰显 360 的社会责任？否则你还有什么资格继续混江湖？

为什么苹果禁令几个月后仍未解禁？

周鸿祎狡辩

【谣言】 360 旗下 iOS 平台多款应用遭苹果应用商店下架是因为“窃取隐私”

【真相】下架是由于 360 手机卫士企业版测试时违反了苹果开发者规则，与用户隐私无关

360 公司就 APP 下架一事已发表声明：通过与苹果公司沟通，下架一事是由于 360 手机卫士企业版测试时违反了苹果开发者规则，与用户隐私没有关系。360 手机卫士企业版尝试为中国境内企业用户提供“骚扰电话拦截”、“来电归属地显示”功能。之前，金山公司诽谤“360 窃取用户隐私”，北京海淀法院已判决金山公司刊登道歉声明，并赔偿 30 万元

我的批驳

1、 此事来源于其它媒体报道，且有苹果公司内部人士证实，姓名不便透露；

2、 此事解释权属于苹果公司，360 没解释权；

3、 据了解，金山“诽谤”案尚未审结，且与苹果下架一事毫无关系，拿来说事纯属转移焦点，居心不正。

反问周鸿祎

1、 你声称这是小事，可为什么苹果禁令几个月后仍未解禁？

2、 为什么扯进未审结且与此事毫无关系的金山案？你是否承认这是你们回应公众质疑的一贯手段？

偷偷安装/卸载，一般用户有感，无需赘言

周鸿祎狡辩

【谣言】 360“利用 V3 升级偷偷卸载竞争对手产品，安装推广软件”

【真相】 360 绝不会偷偷卸载竞争对手产品和安装推广软件

众所周知，互联网软件都带有升级功能。特别为了有效对抗快速变化的木马和 0day 漏洞，要求安全软件必须能够快速升级响应，国内外主流安全软件全都如此，比如 Norton 杀毒软件的升级机制命名为“Live Update”。《每日经济新闻》报道中提到的“V3”就是升级程序的版本号，代表的是第三个主要版本，其作用是把木马防御规则、补丁更新等安全特性快速升级，根本不会偷偷卸载竞争对手产品和安装推广软件。同时，用户也可以在 360 安全卫士的设置界面中，选择是否开启自动升级。

我的批驳

1、所谓“V3 升级”当然包括升级功能，但远非如此，事实上网上能找到的 360 偷偷安装软件、卸载竞争性产品的例子还少吗？

2、关于这部分，我们目前已知的比报道出来的更多，其中部分信息来自 360 内部人士（周鸿祎先

生，有人帮你数钱数累了，要开始卖你了）。

后门或漏洞，边界不容模糊

周鸿祎狡辩

【谣言】瑞星发现 360 有“后门”、首次揭露“不安全”

【真相】瑞星谣言侵犯 360 商誉 已被法院判处罚款 20 万道歉 10 天

360 推出免费杀毒，触动收费杀毒厂商的利益，从而遭到瑞星公司毫无根据的诽谤抹黑。经过中国信息安全测评中心检测，360 安全软件并不存在“后门”程序。根据北京市西城区法院判决，瑞星公司从事了侵犯奇虎 360 商业信誉、商品声誉的不正当竞争行为，其行为构成不正当竞争，应当承担相应的侵权责任。法院判定，瑞星公司立即停止针对奇虎 360 的不正当竞争行为，在《北京青年报》上连续十天发表道歉声明，并赔偿奇虎 360 公司 20 万元

我的批驳

1、法庭的判决书在承认瑞星有向用户和社会发布安全风险警告权利的同时，又表示“瑞星文章的内容对原告的商业信誉、商品声誉造成了影响，文中有大量诋毁原告商誉的内容”。而瑞星发布的技术文档的真实性，判决书并无定论。

2、如果 360 的软件没问题，那瑞星就涉嫌技术文档虚假，那他该承担的责任就该不是“损害商誉”，而是恶意诽谤——但从瑞星公布的文档细节和公证视频来看，瑞星并未弄虚作假，从判决书来看，奇虎公司也未对公证文档和视频的真实性提出异议。

3、360 应该以技术语言回应产品问题，而不应该以法律语言捣浆糊。公众关心的是瑞星指控的 360 软件后门是否存在，而不是 360 和瑞星的口水官司谁输谁赢。

4、事实上，当时瑞星公布了 360 后门程序反编译代码，大量专业人员予以验证后门存在，360 慌忙声明指公布反汇编代码违法，威胁起诉，同时却紧急给后门打补丁——故意的后门被掩饰成无意的“漏洞”。

5、关于中国信息安全测评中心“权威性”，请参考 初评“权威机构”对 360 安全浏览器的“安全评估”和 “权威机构”无独立性须回避。

反问周鸿祎

1、 请以技术语言确认，当时瑞星指出的后门是否存在？

2、 “瑞星败诉”与“360 软件没后门”能否划等号？

360 厚黑之不完全档案

就当吃一回狗屎吧——回 360 陶伟华

【视频证据】360 安全浏览器暗设后门

见识一下 360 的两项专利

关于工信部 360 安全浏览器测评报告的公开声明

谁在用“跟踪 Cookie”恐吓公众？

初评“权威机构”对 360 安全浏览器的“安全评估”

论证 360 安全浏览器后门机制

“权威机构”无独立性须回避

杀鸡请牛刀

拉黑 360

安全策略：拉黑 360

360 浏览器：拒绝访问

软件产品和互联网服务推荐目录