大陆浏览器安全

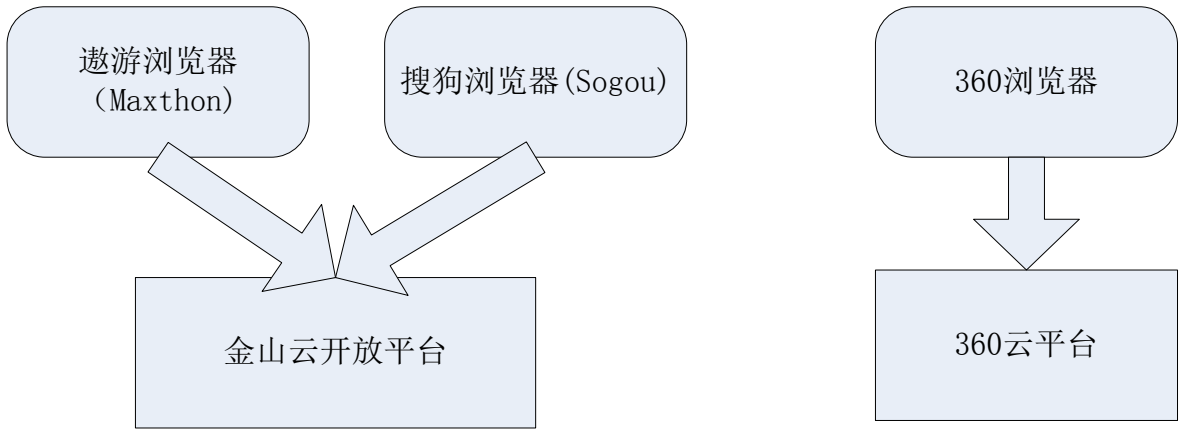
宋雷

大陆浏览器市场特点

- 面临安全问题与国际市场迥异
- 由于金山/腾讯/360，导致漏洞补丁很快，0day几乎不会规模性出现。
- 主要威胁为：小成本钓鱼，下载欺骗，点对点社会工程（网购诈骗）

金山网络在浏览器安全的积累

- 2009年，我们在业界率先推出了首款基于浏览器的专业防护产品 - 金山网盾
- 除360以外的国内主流浏览器产品安全技术几乎全部基于金山云开放平台开发
- 金山毒霸在网购保护方面做出了诸多的创新，如敢陪模式等


遨游浏览器
(Maxthon)
搜狗浏览器(Sogou)
金山云开放平台
360浏览器
360云平台

- 在做安全的路上，我们反复在思考：

  到底什么样的浏览器才是安全的？

- 让我们先来看看我们遇到的威胁，并分类介绍各类威胁的解决方案

威胁一：钓鱼与欺诈

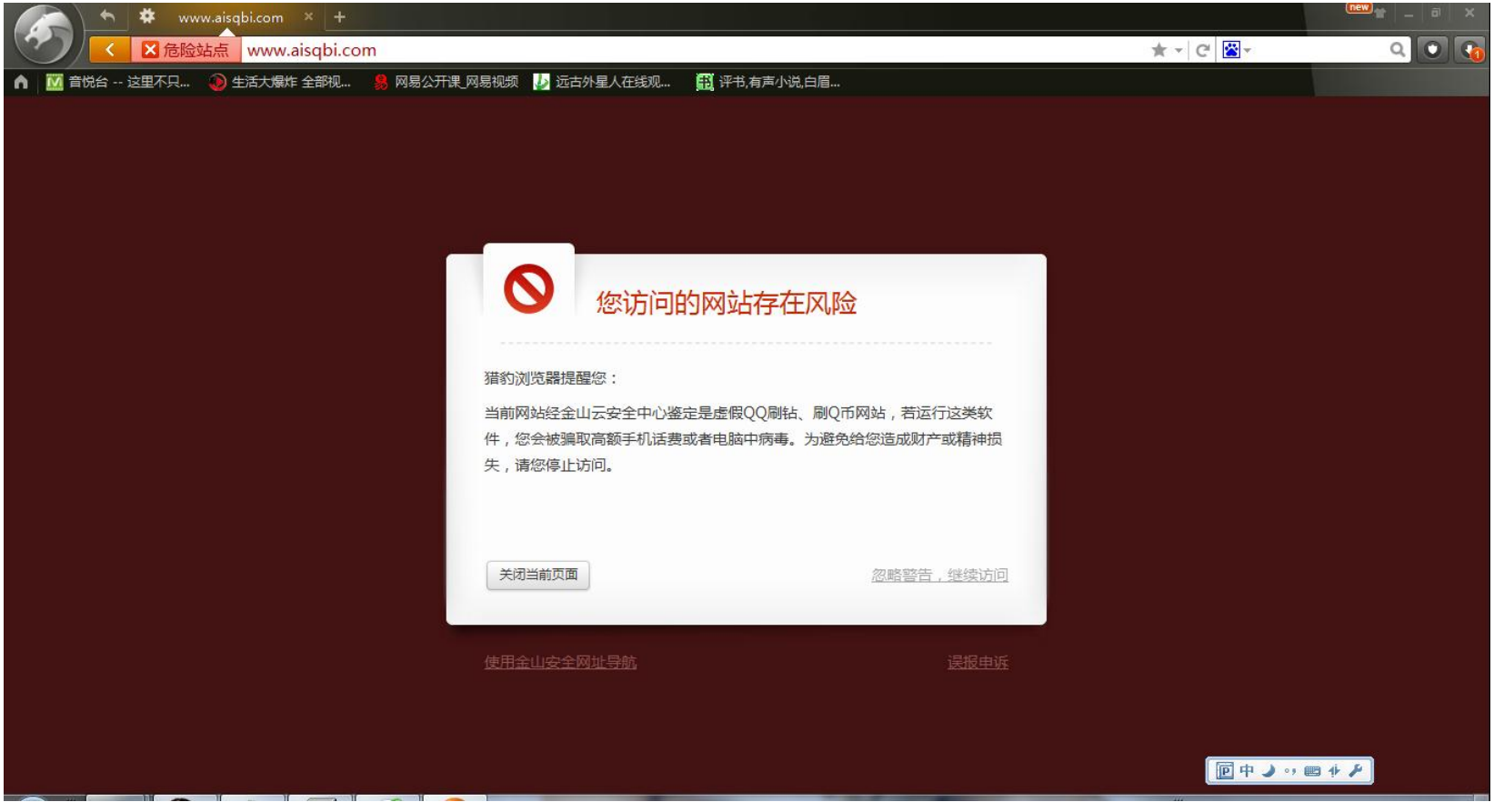
- 在用户浏览网页过程中，浏览器将用户访问的网址hash后提交给服务器，服务器根据恶意网址库获取当前网址安全性。

- 厂商通过自己的蜘蛛与用户反馈来完善自己的恶意网址库

威胁一：钓鱼与欺诈

- DEMO

威胁一：钓鱼与欺诈


www.aisqbi.com
危险站点
www.aisqbi.com
音悦台 -- 这里不只...
生活大爆炸 全部视...
网易公开课_网易视频
远古外星人在线观...
评书,有声小说,白眉...
您访问的网站存在风险
猎豹浏览器提醒您：
当前网站经金山云安全中心鉴定是虚假QQ刷钻、刷Q币网站，若运行这类软件，您会被骗取高额手机话费或者电脑中病毒。为避免给您造成财产或精神损失，请您停止访问。
关闭当前页面
忽略警告，继续访问
使用金山安全网址导航
误报申诉

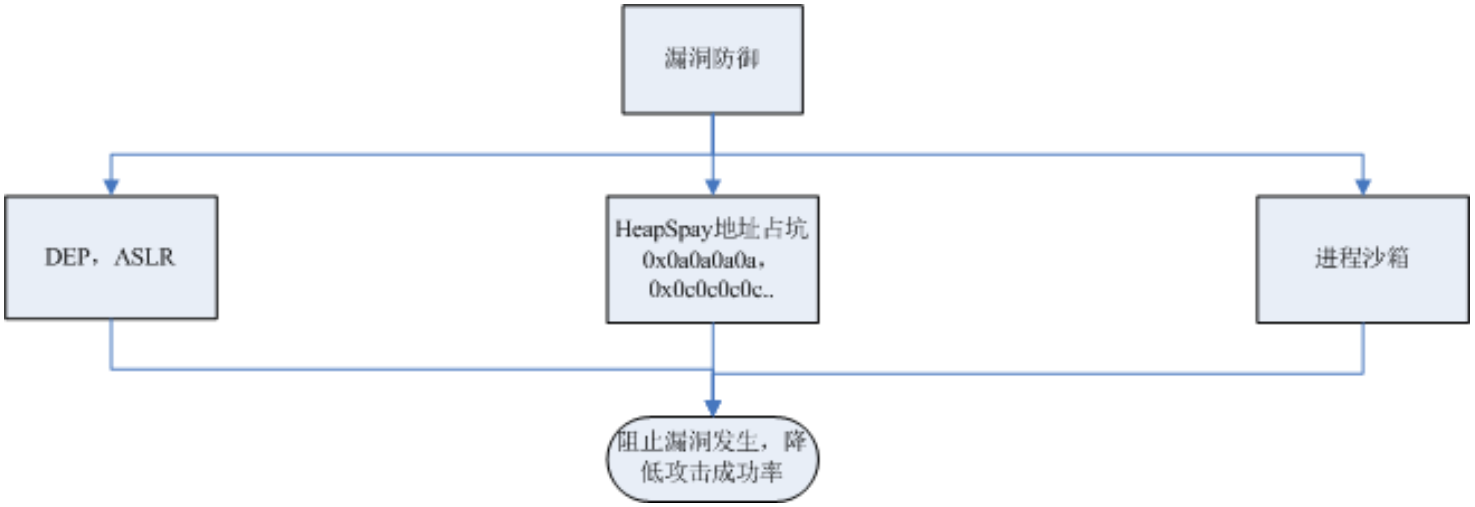
威胁一：钓鱼与欺诈


360安全浏览器 5.0 正式版
文件(F) 查看(V) 收藏(B) 工具(T) 帮助(H)
请登录
http://warn.se.360.cn/warn/?from=se&type=1&url=http%3A%2F%2Fwww%2Eaisqbi%2Ecom%2F&ver=2.6.5.1008&sig
危险
恶意网址
收藏 谷歌 网址大全 游戏中心
扩展中心 翻译 截图 网银 游戏 登录管家
360安全浏览器提醒您：您要访问的是...
360安全浏览器
虚假的购物网站
当前网页存在未经证实的商品、商户、支付等相关信息，虚假交易信息可能会给您造成财产损失，请确认是否为官方网站并谨慎访问。
您访问的网址是：http://www.aisqbi.com/
忽略警告，继续访问
我要安全上网
关闭当前页面
网站申诉
网站安全检测
浏览器医生
IE打开
下载

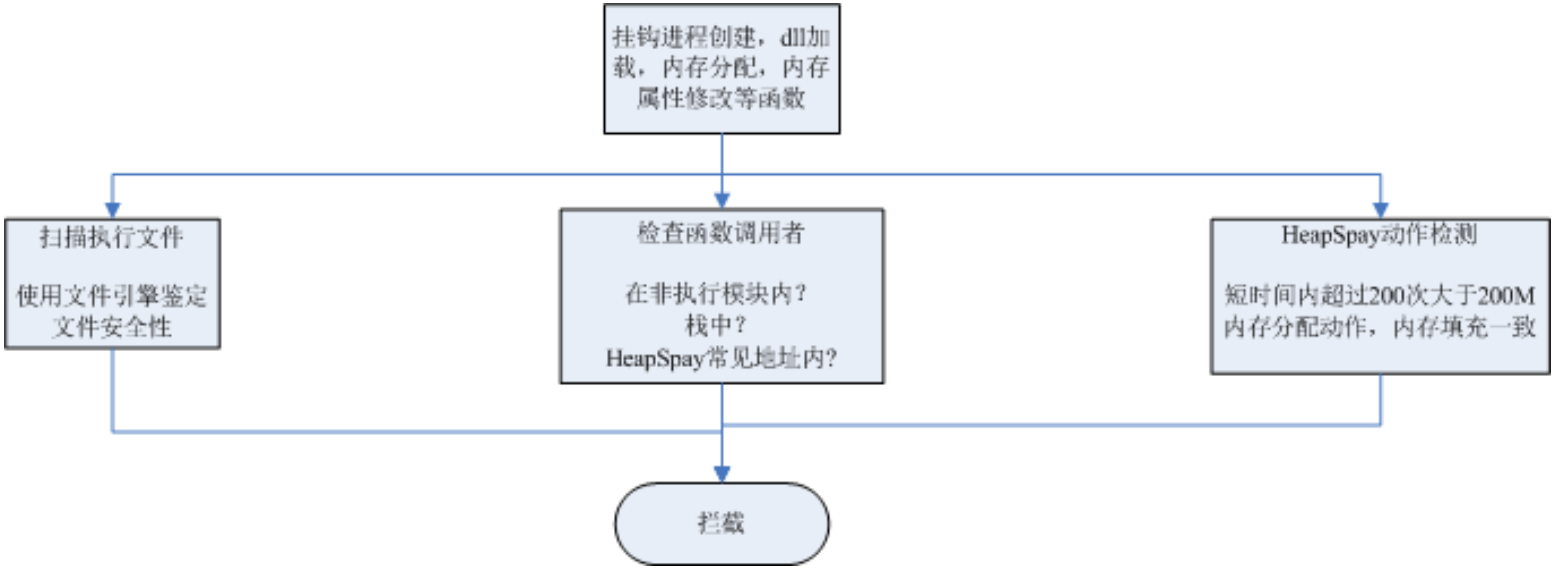
威胁二：漏洞攻击

- 大陆浏览器多基于在IE与chromium开发，比如360安全基于ie，360极速ie+chromium，猎豹基于ie+chromium。
- ie的漏洞，每家都有比较成熟的技术，比如金山的网盾、360的网盾，可以阻止ie核下常见的漏洞攻击，进程启用dep, aslr，拦截可疑文件执行、加载，堆喷射地址占坑，特定函数检测返回地址等等

威胁二：漏洞攻击


漏洞防御
DEP，ASLR
HeapSpay地址占坑
0x0a0a0a0a，
0x0c0c0c0c..
进程沙箱
阻止漏洞发生，降
低攻击成功率

威胁二：漏洞攻击


挂钩进程创建，dll加载，内存分配，内存属性修改等函数
扫描执行文件
使用文件引擎鉴定文件安全性
检查函数调用者
在非执行模块内？
栈中？
HeapSpay常见地址内？
HeapSpay动作检测
短时间内超过200次大于200M内存分配动作，内存填充一致
拦截

威胁二：漏洞攻击

- chromium的漏洞，在一个chromium核的漏洞被公告后，第三方厂商多很被动，多只能等chromium解决后更新。

- 自身引入的漏洞，比如前段时间的360浏览器的external问题，360信任指定域下网站可以使用external导出函数，比如修改首页，历史记录等。如果这个域存在xss问题，将面临很大的安全风险。

威胁二：漏洞攻击

- DEMO

威胁二：漏洞攻击


360网盾提醒您 - 风险
危险行为已被拦截
360网盾帮您拦截了 1 个威胁，您可以继续访问。
威胁详情：
360网盾检测到 IE浏览器 试图执行危险脚本：
脚本名称：暴雷漏洞
为了您的计算机安全，360网盾已拦截这些行为。
2012-06-13 17:45:12
相同情况不再提醒
查看拦截详情
关闭

威胁二：漏洞攻击


金山毒霸
成功拦截网页挂马攻击
您正在访问的网页含有挂马网址，该网页含有恶意攻击代码，会通过浏览器漏洞下载并运行木马。可能会盗取您的财产及隐私信息。
挂马网址：http://[redacted]java.html
恶意代码已被过滤，您可以安全地继续浏览。
确 定

威胁三：下载威胁

- 2011年的病毒木马传播更加依赖互联网通道，依靠下载（包括浏览器下载和聊天工具传送）的病毒达到86.4%，通过网页挂马等形式比以前大大减少

- 比如前段时间的 PuTTY、 WinSCP和SSH Secure工具汉化版被人植入后门，导致大量服务器落入黑客手中

威胁三：下载威胁

- 一个完整的下载安全解决方案应该包括：

  a. 下载前拦截
  下载前预先收集了可疑的下载URL，不用扫描文件即可通过URL进行拦截。用户不用经历下载过程。

  b. 下载后拦截
  通过扫描下载后的文件进行拦截

威胁三：下载威胁

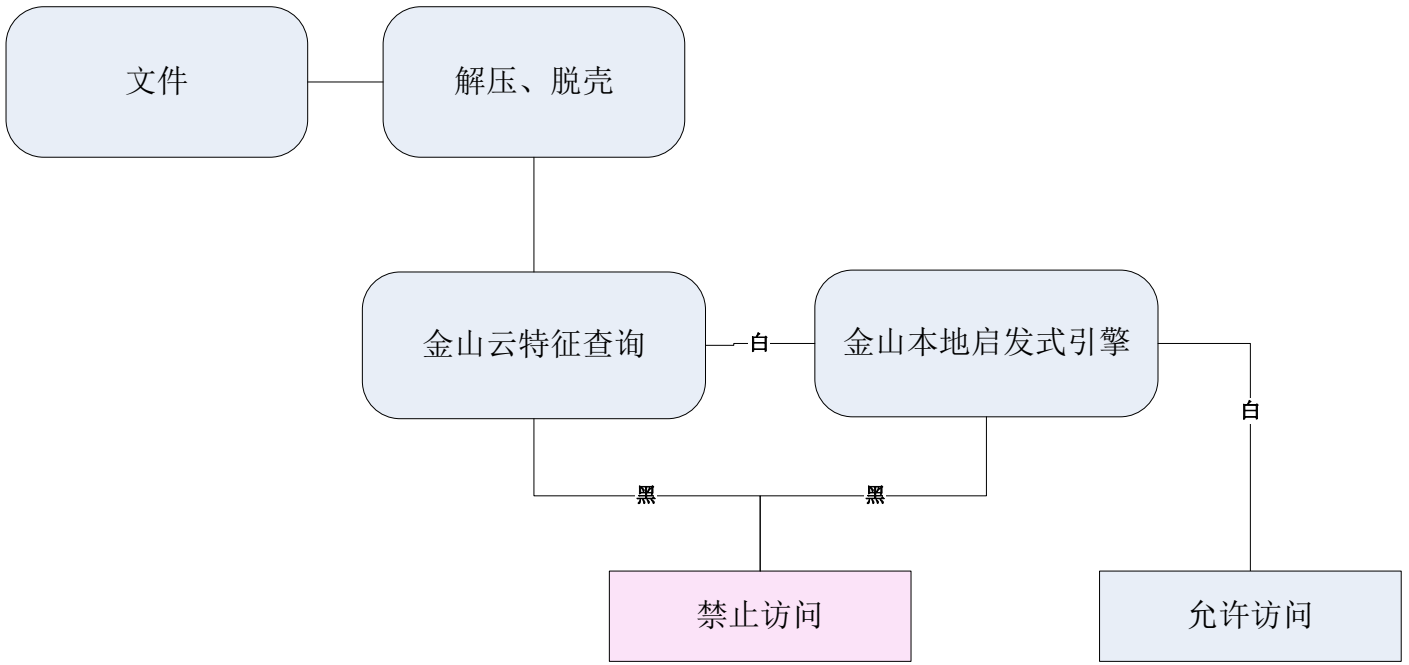
- 为什么要下载后拦截

  a. 基于云的URL收集未必是最及时的
  b. 一次一变的下载链接

  我们要让每个用户都不是那个“最倒霉“的用户

威胁三：下载威胁

- 下载后拦截技术



威胁三：下载威胁

- DEMO

威胁三：下载威胁


360网盾
假冒WinSCP的网站
当前页面不是“WinSCP”的官方网站，在假冒网站下载软件可能带有木马，为避免对您的电脑安全造成威胁，请您在官方网站进行软件下载。
您访问的网址是：http://www.winscp.cc/
WinSCP的官方网址是：http://www.winscp.net/
忽略警告，继续访问
我要安全上网
访问真正的官网
网站申诉
网站监测中心

威胁三：下载威胁


www.liebao.cn/lab-2.html
音悦台 -- 这里不只...
生活大爆炸 全部视...
网易公开课_网易视频
远古外星人在线观...
Test.eicar.aa
设置
全部开始
下载管理
(发现病毒)EICAR.zip
大小:220B
Win32.Troj.Generic.(kcloud)

威胁三：下载威胁

- 浏览器带一个扫描引擎，将下载的文件抽取特征，提交给云服务器查询安全性

威胁四：网购威胁

- 在网购过程中，除了网页钓鱼威胁外，越来越多的是在客户端环境不安全情况下，网页遭篡改，键盘被监听的问题。

威胁四：网购威胁

- 解决方案：

  支付前网购环境扫描

  网购过程中阻止未知程序执行

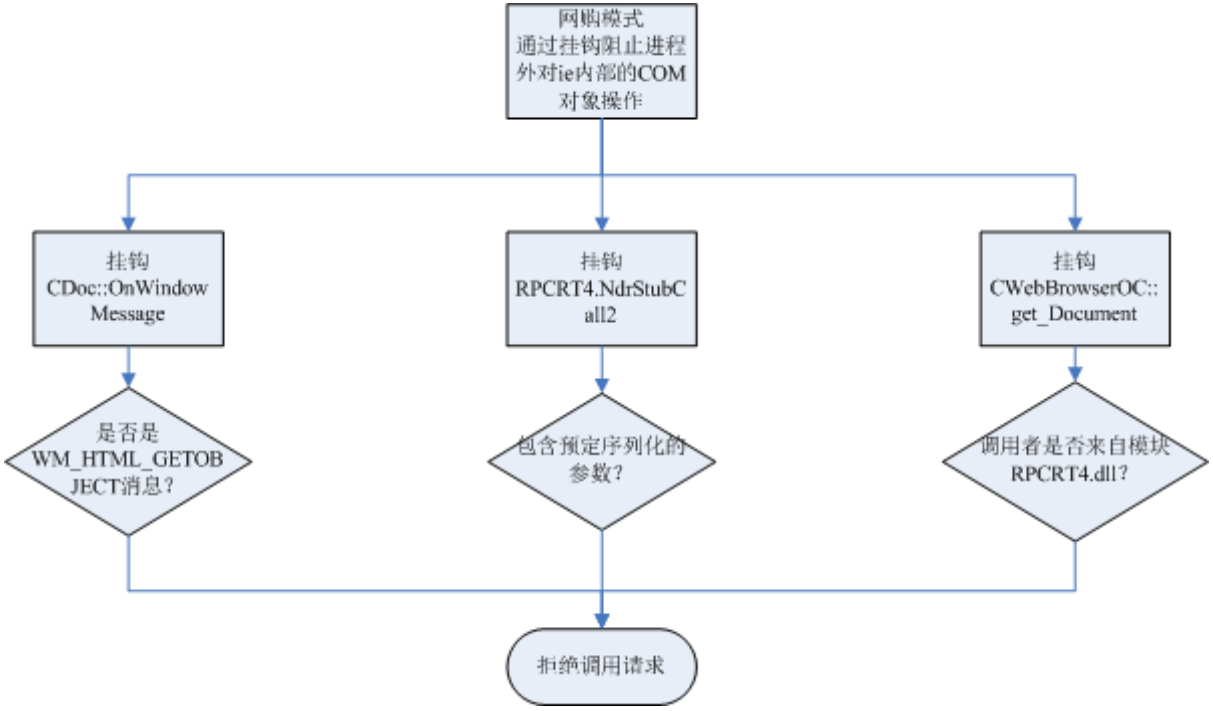
  网购过程中阻止未知驱动加载

  网购过程中阻止注入浏览器

  网购过程中阻止篡改浏览器页面

  网购过程中阻止网页键盘记录

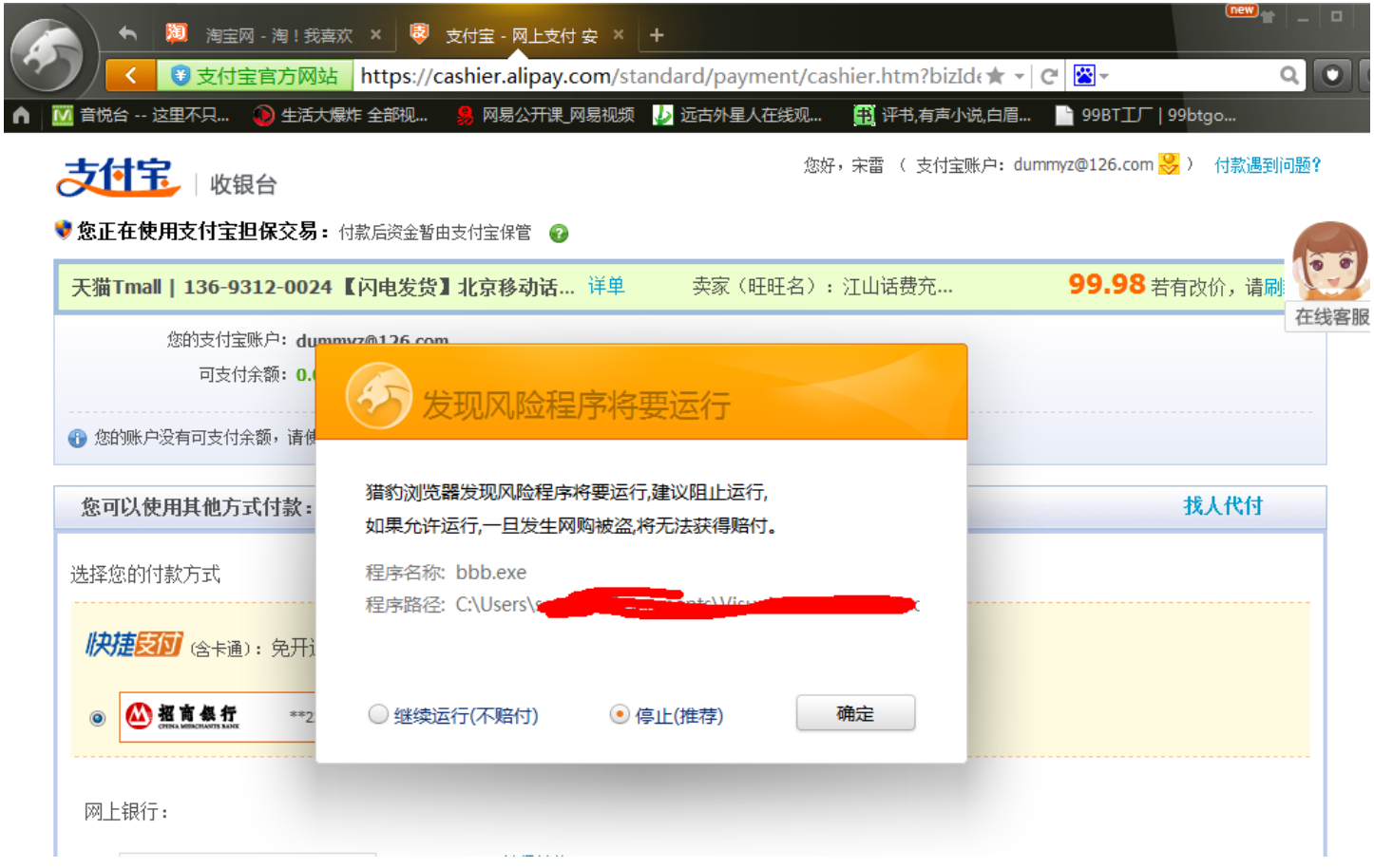
威胁四：网购威胁


网购模式
通过挂钩阻止进程外对ie内部的COM对象操作
挂钩
CDoc::OnWindowMessage
挂钩
RPCRT4.NdrStubCall2
挂钩
CWebBrowserOC::get_Document
是否是WM_HTML_GETOBJECT消息?
包含预定序列化的参数?
调用者是否来自模块RPCRT4.dll?
拒绝调用请求

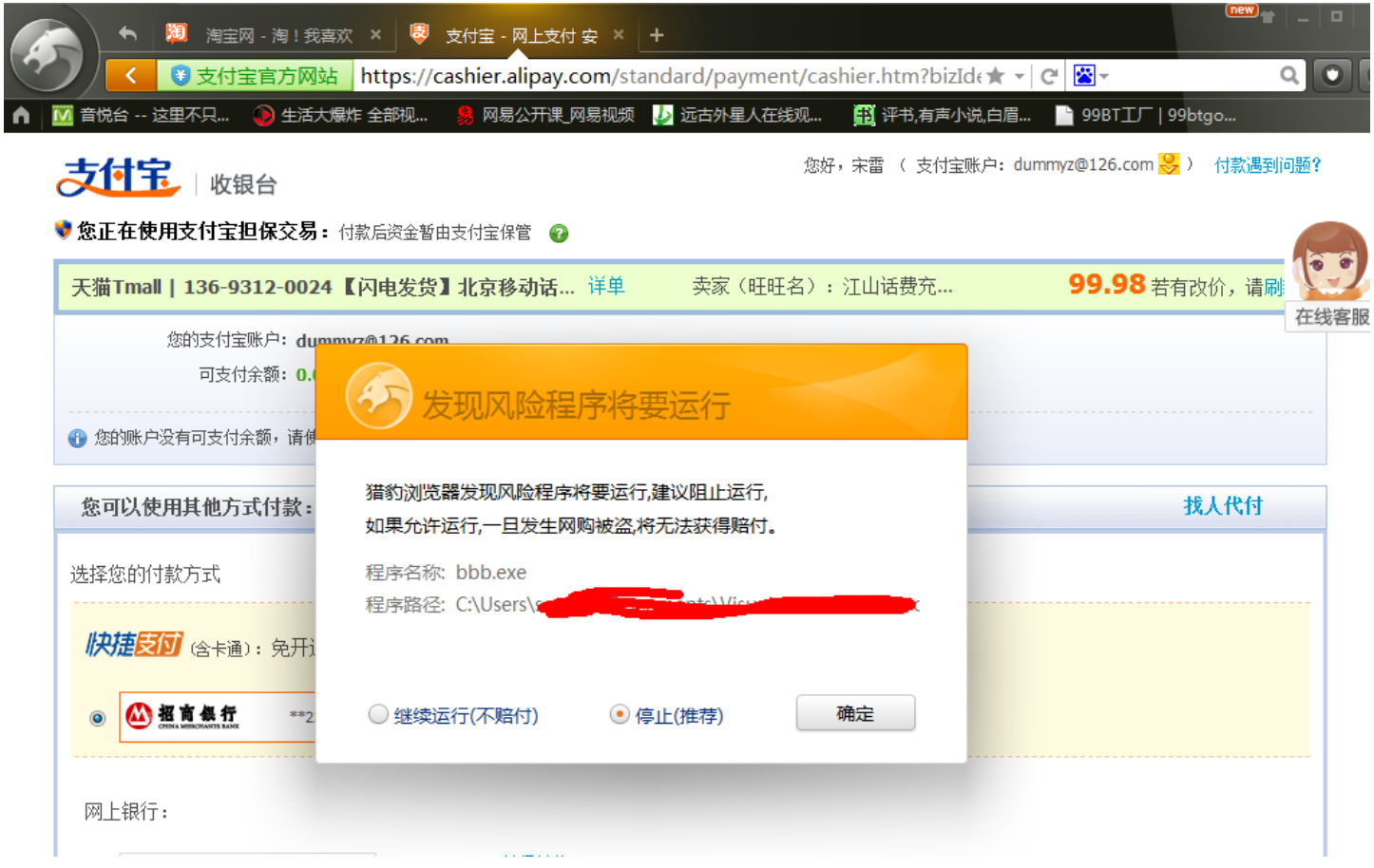
威胁四：网购威胁


淘宝网 - 淘！我喜欢
支付宝 - 网上支付 安
支付宝官方网站
https://cashier.alipay.com/standard/payment/cashier.htm?bizIdentity=trade100018
正在扫描网购环境 15%
音悦台 -- 这里不只...
生活大爆炸 全部视...
网易公开课_网易视频
远古外星人在线观...
评书,有声小说,白眉...
99BT工厂 | 99btgo...
支付宝 | 收银台
您正在使用支付宝担保交易：付款后资金暂由支付宝保管
天猫Tmall | 136-9312-0024【闪电发货】北京移动话... 详单
卖家（旺旺名）：江山话费充...
99.98 若有改价，请刷新

威胁四：网购威胁


淘宝网 - 淘！我喜欢
支付宝 - 网上支付 安
支付宝官方网站
https://cashier.alipay.com/standard/payment/cashier.htm?bizId
音悦台 -- 这里不只...
生活大爆炸 全部视...
网易公开课_网易视频
远古外星人在线观...
评书,有声小说,白眉...
99BT工厂 | 99btgo...
支付宝 | 收银台
您好，宋雷 （ 支付宝账户：dummyz@126.com ） 付款遇到问题？
您正在使用支付宝担保交易：付款后资金暂由支付宝保管
天猫Tmall | 136-9312-0024【闪电发货】北京移动话... 详单
卖家（旺旺名）：江山话费充...
99.98 若有改价，请刷
在线客服
您的支付宝账户：dummyz@126.com
可支付余额：0.
您的账户没有可支付余额，请
发现风险程序将要运行
猎豹浏览器发现风险程序将要运行,建议阻止运行,
如果允许运行,一旦发生网购被盗,将无法获得赔付。
程序名称: bbb.exe
程序路径: C:\Users\
继续运行(不赔付)
停止(推荐)
确定
您可以使用其他方式付款：
找人代付
选择您的付款方式
快捷支付 (含卡通)：免开
招商银行
网上银行：

威胁四：网购威胁


淘宝网 - 淘！我喜欢
支付宝 - 网上支付 安
支付宝官方网站
https://cashier.alipay.com/standard/payment/cashier.htm?bizId
音悦台 -- 这里不只...
生活大爆炸 全部视...
网易公开课_网易视频
远古外星人在线观...
评书,有声小说,白眉...
99BT工厂 | 99btgo...
支付宝 | 收银台
您好，宋雷 （ 支付宝账户：dummyz@126.com ） 付款遇到问题？
您正在使用支付宝担保交易：付款后资金暂由支付宝保管
天猫Tmall | 136-9312-0024【闪电发货】北京移动话... 详单
卖家（旺旺名）：江山话费充...
99.98 若有改价，请刷
在线客服
您的支付宝账户：dummyz@126.com
可支付余额：0.
您的账户没有可支付余额，请
发现风险程序将要运行
猎豹浏览器发现风险程序将要运行,建议阻止运行,
如果允许运行,一旦发生网购被盗,将无法获得赔付。
程序名称: bbb.exe
程序路径: C:\Users\
继续运行(不赔付)
停止(推荐)
确定
您可以使用其他方式付款：
找人代付
选择您的付款方式
快捷支付 (含卡通)：免开
招商银行
网上银行：

国内浏览器的安全现状

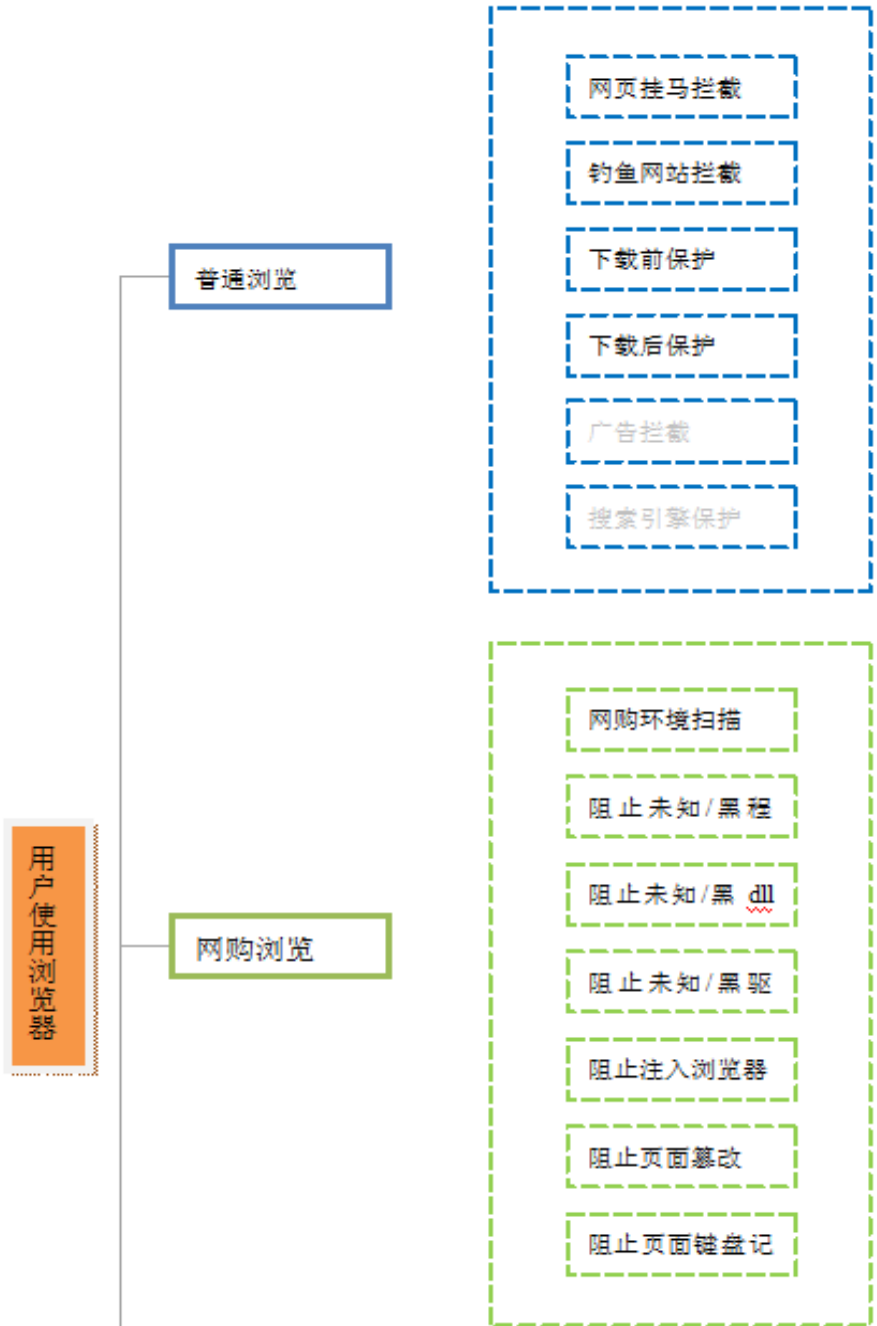
- 普遍不重视安全问题
- 真正冠以安全浏览器名称的只有：

  360安全浏览器
  猎豹浏览器

- 而360安全浏览器真正的安全功能仅只是网址拦截

猎豹浏览器

- 携着对浏览器安全的认识和思考，我们推出了猎豹浏览器
- 猎豹浏览器拥有业界最全面的安全防护体系BIPS: Browser Intrusion Prevention System
- 结合金山多年积累的 云安全 以及 K+ 防御
- 全面解决大陆浏览器的安全威胁问题
- 猎豹浏览器的安全防御组成：


用户使用浏览器
普通浏览
网购浏览
网页挂马拦截
钓鱼网站拦截
下载前保护
下载后保护
广告拦截
搜索引擎保护
网购环境扫描
阻止未知/黑程
阻止未知/黑 dll
阻止未知/黑驱
阻止注入浏览器
阻止页面篡改
阻止页面键盘记

- 猎豹浏览器同时还是全球首个敢赔浏览器

  只要使用猎豹浏览器上网，就可以享受敢赔服务
  并获得￥1000元的敢赔基金，倘若网购时被盗，
  就可以从基金中获取单笔最高￥500元的现金赔付。