云安全智能反钓鱼
在网络钓鱼犯罪追踪的探索

瑞星攻防实验室主管　封初

当前互联网的威胁是什么？

中国互联网安全趋势

2011年1月至12月
瑞星云安全系统截
获的木马病毒

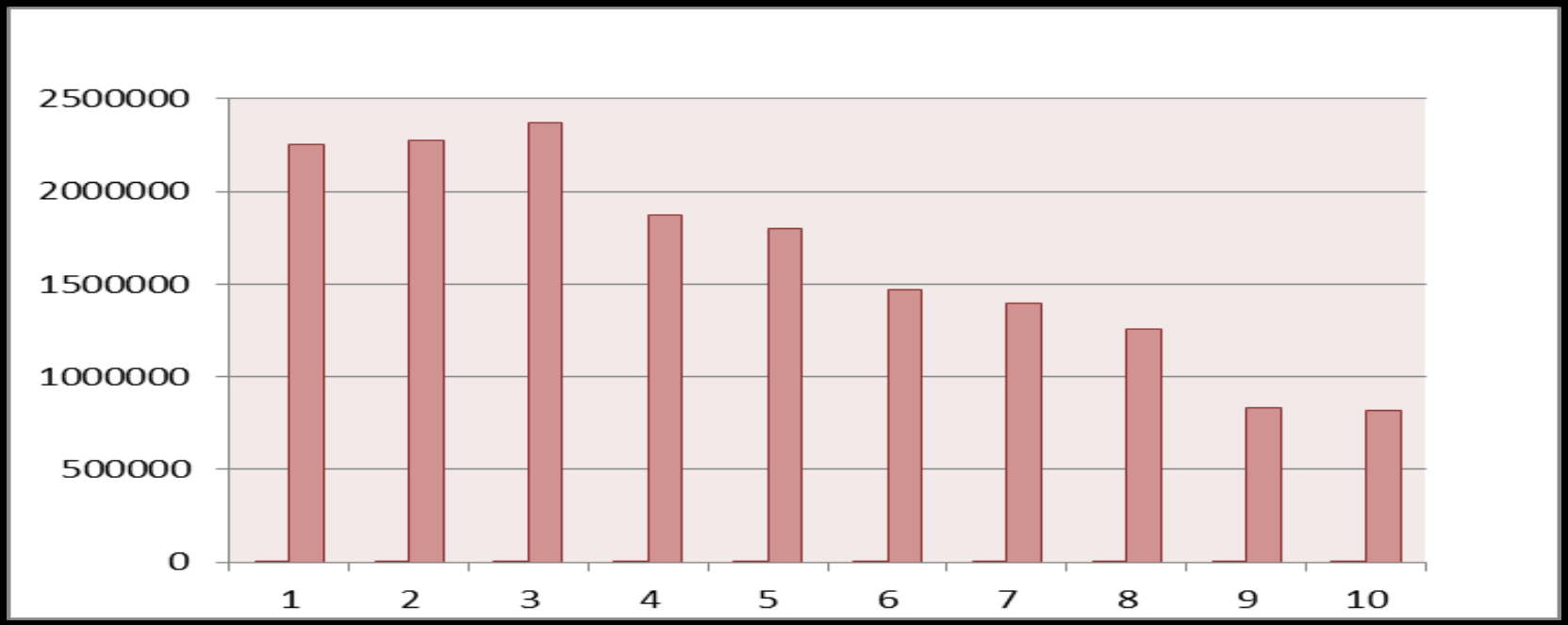
1373万个

2010年1月至12月
瑞星云安全系统截
获的木马病毒

1286万个

中国互联网安全趋势

2011年1月至12月瑞星云安全系统截获的钓鱼网站



共截获钓鱼网站1635万余个

在木马病毒得到有效遏制的情况下，

钓鱼网站异军突起，成为目前中国互联网

成长速度最快、病毒传播**最大的威胁！**

钓鱼网站

骗取用户帐号密码

钓鱼网站

窥视、贩卖用户隐私

钓鱼网站
已越来越成为
黑客们
赖以生存的工具

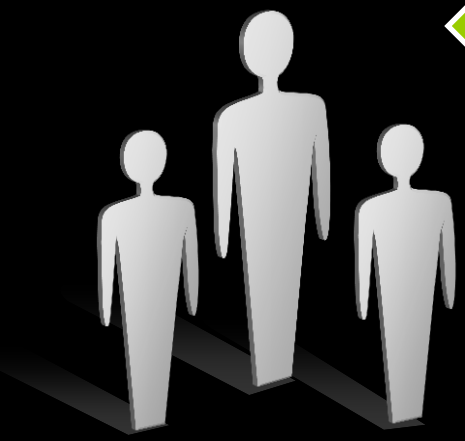
钓鱼网站的背后是经济利益驱使

如何有效打击网络钓鱼犯罪？

1 网络钓鱼犯罪的现状

2 追踪打击网络钓鱼犯罪的困境

3 “云安全”解决困境的作用和探索



网络钓鱼犯罪的现状

1. 两种状态：一种为传统钓鱼犯罪方式，一种为专业钓鱼犯罪方式。
2. 前者是传统诈骗犯罪的延伸，只不过利用了网络的平台。
3. 后者是欺诈针对性较强，结合多种欺诈方式，危害较大。

网络钓鱼犯罪的现状

传统钓鱼犯罪方式

所谓的传统犯罪方式，就是将传统的诈骗犯罪方法，利用网络为载体进行实施的网上诈骗、窃取用户密码等行为的犯罪方式，这类犯罪目前占据整个网络犯罪的 80%。

网络钓鱼犯罪的现状

传统钓鱼犯罪方式

网络游戏一直都是网络钓鱼犯罪的“重灾区”之一。

网络钓鱼犯罪的现状

专业钓鱼犯罪方式

专业网络钓鱼犯罪方式则结合多种欺诈方式，如手机短信、电话语音等欺诈方式，该种犯罪方式针对性较强，危害较大。

网络钓鱼犯罪的现状

网络钓鱼犯罪的特点：低风险高回报

网络钓鱼犯罪的现状

1. 网络钓鱼程序低价兜售，无需复杂技术即可架设钓鱼网站。
2. 互联网没有边界，管辖权不清晰。
3. 网络证据的脆弱性：网络资源方便获取，随意丢弃，容易篡改。
4. 钓鱼攻击一经发生，造成危害大，传统技术手段难以提前预警和事后的证据收集。

网络钓鱼犯罪的现状

云安全智能反钓鱼将是突破口

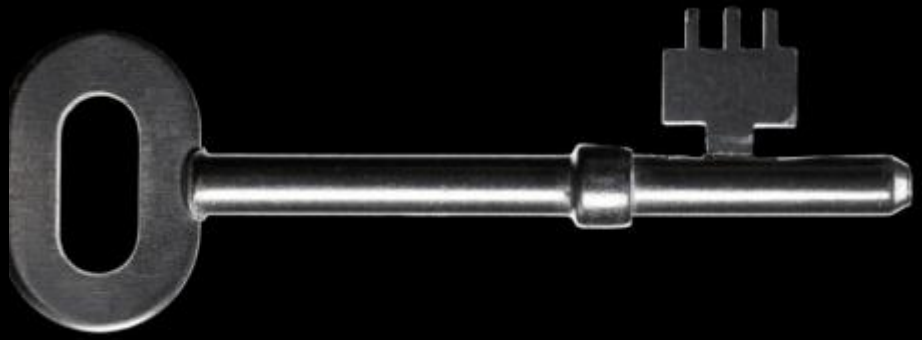
从现在开始，这种情况将得到彻底改变。

“云安全”

“云安全系统”首次把互联网的1.5亿客户端链接起来，并建立统一的安全服务器和智能分析系统。

拥有“云安全”系统之后，我们可以通过服务器与客户端的通讯，了解客户端发生的异常动作。

瑞星首创智能“反钓鱼”技术



智能黑名单系统

智能白名单系统

钓鱼网站特征码智能识别技术

钓鱼网站网页行为智能分析技术

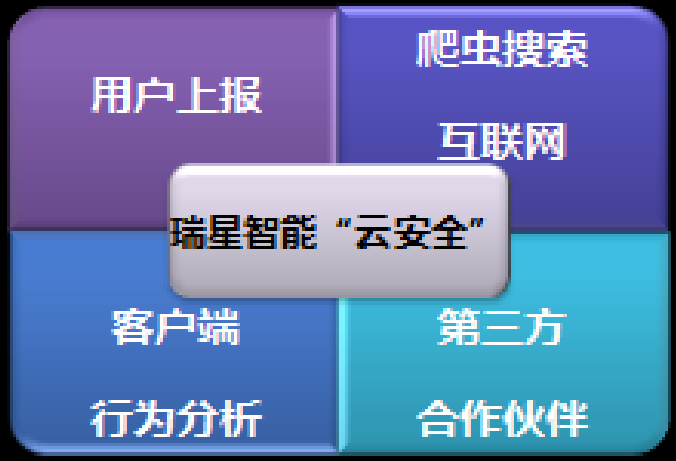
自动虚拟分析技术

辅助智能分析技术

图片分析技术

文本分析技术

瑞星智能反钓鱼流程



1

访问行为模拟

文本特征分析

域名特征分析

图片识别

.....

2

专家输入智能判定规则到“云安全”智能反钓鱼系统中

3

钓鱼网站黑名单

可信地址库

互联网钓鱼网站现状全貌

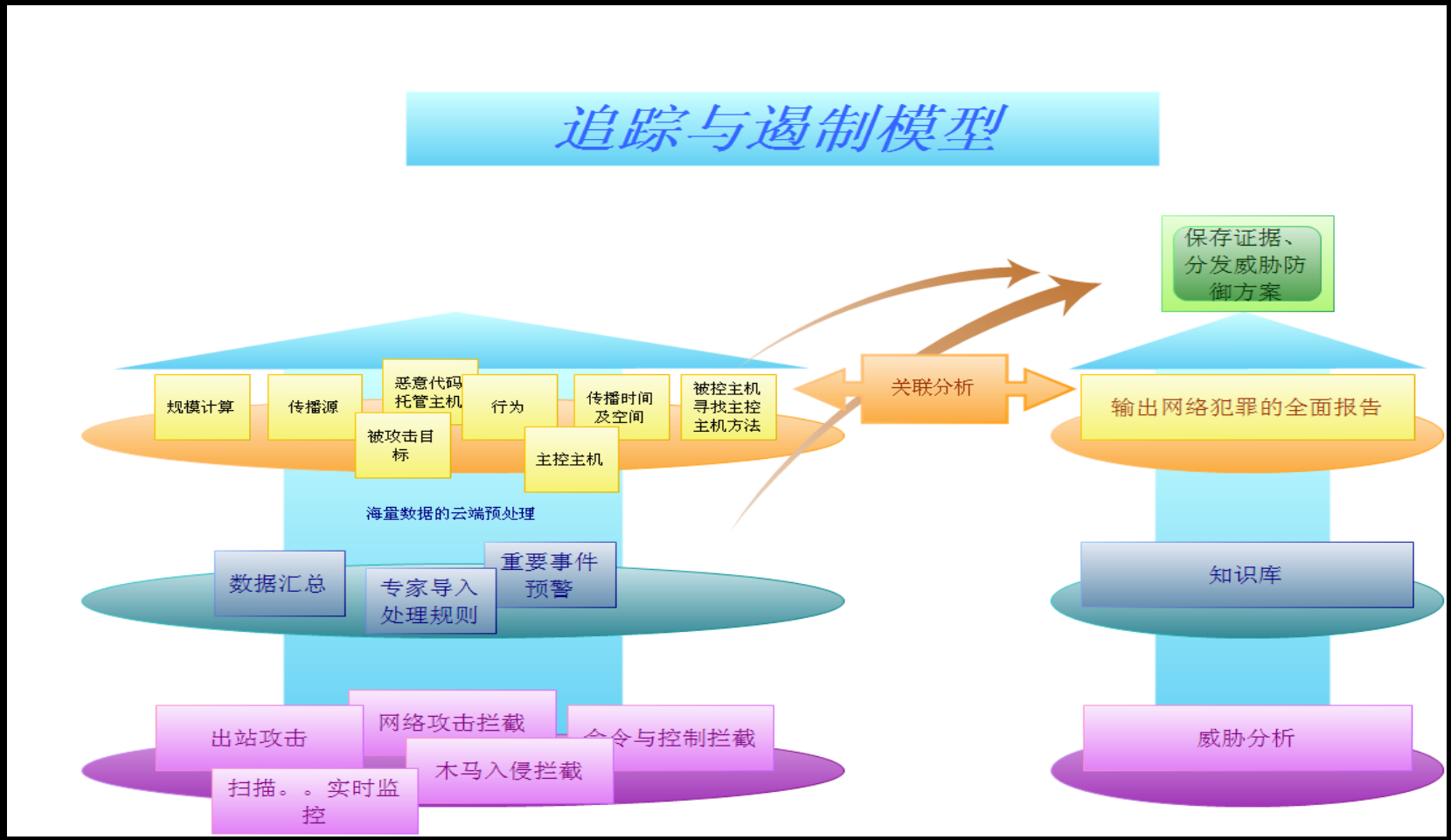
云安全在追踪网络钓鱼犯罪的探索

云安全在追踪网络钓鱼犯罪上的作用

1. 通过云安全的电子证据收集功能，针对网络钓鱼犯罪集团的动作，可以形成完整的证据链。

2. 针对钓鱼网站的形成、传播和发起攻击前的所有过程进行监控和遏制。

云安全追踪数据模型


追踪与遏制模型
保存证据、分发威胁防御方案
规模计算
传播源
恶意代码托管主机
行为
传播时间及空间
被控主机寻找主控主机方法
被攻击目标
主控主机
关联分析
输出网络犯罪的全面报告
海量数据的云端预处理
数据汇总
专家导入处理规则
重要事件预警
知识库
出站攻击
网络攻击拦截
命令与控制拦截
木马入侵拦截
扫描。。实时监控
威胁分析

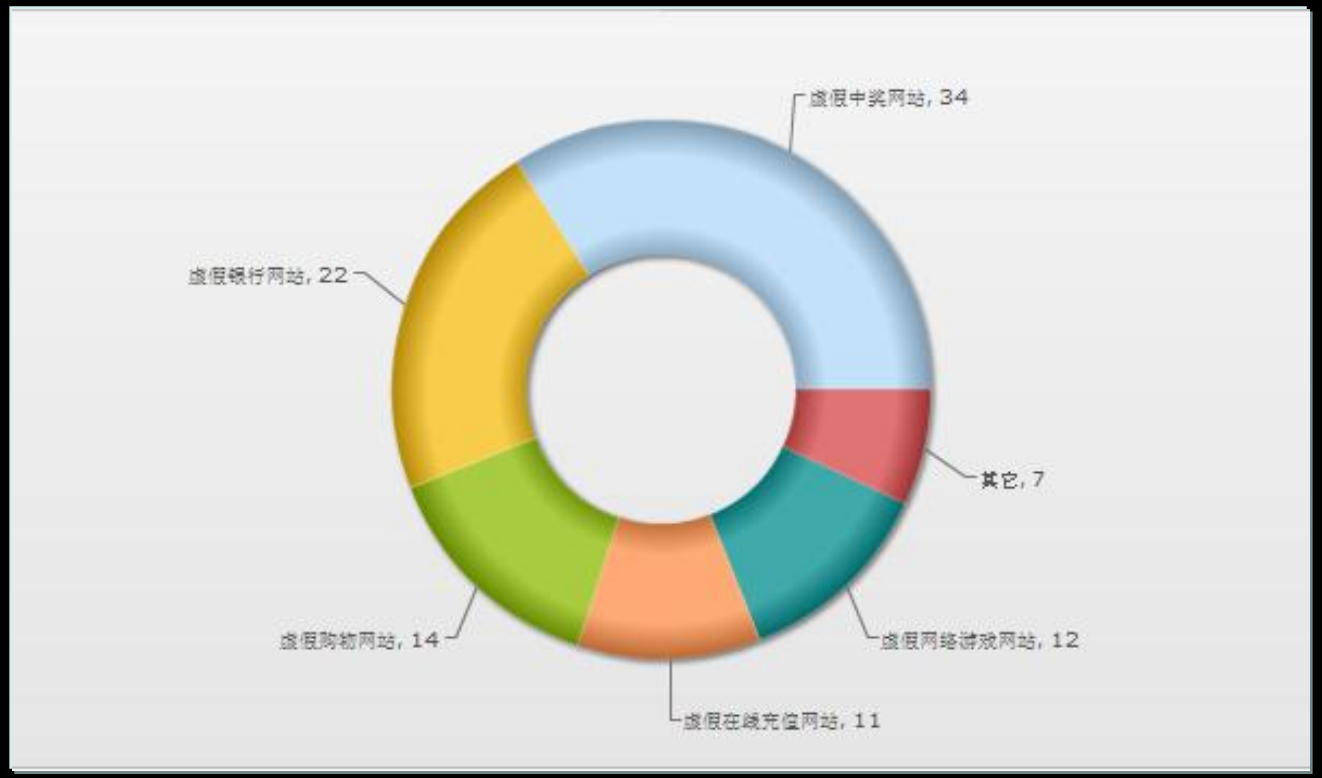
云安全重组“传播证据链”模型

云安全监测钓鱼网站的数量

2011年1月到12月瑞星云安全系统截获的钓鱼网站

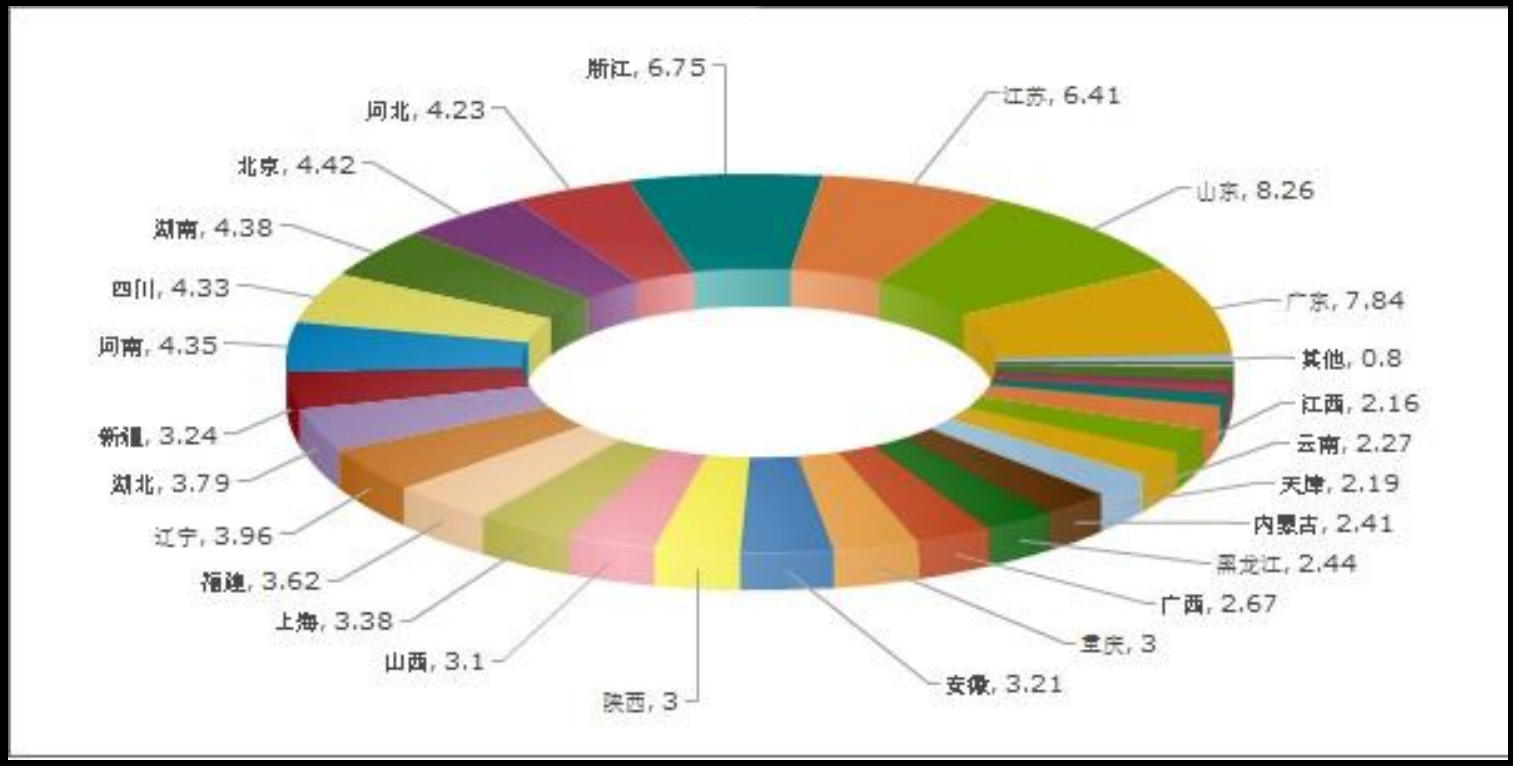
云安全监测钓鱼网站的类型

2011年1月到12月瑞星云安全系统截获的钓鱼网站类型统计及所占比例



云安全按地区监测钓鱼网站

2011年1月到12月瑞星云安全系统截获的钓鱼网站各地区域上报数量及所占比例



总结

取证难题

- 难以定位、易于修改
- 保存困难、销毁迅速

云安全的探索

- 全程监控：完整的网络钓鱼犯罪证据链
- 全面遏制：从犯罪准备、形成、进行的所有环节进行遏制

不只是瑞星的责任
需要合作伙伴的参与


谢谢！