



恶意代码网络犯罪追踪

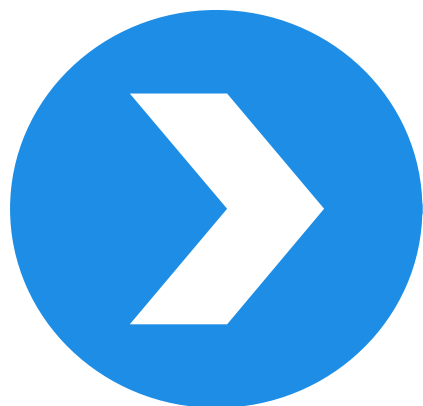
安天反病毒引擎研发中心

www.antiy.com

 安天 | 智者安天下



- 恶意代码犯罪追踪目标
- 恶意代犯罪追踪过程
- 追踪案例
- 挑战



恶意代码犯罪追踪目标



目标

4

- 追踪黑客
 - 黑客信息、角色
- 恶代犯罪类型
 - DDoS、窃取信息（诈骗）、广告流量、敲诈
- 犯罪危害
 - 危害范围、获利资金、危害类型
- 犯罪证据
 - 受害者
 - 网络犯罪工具
 - 犯罪基础设施



- 黑客角色

- 开发、销售、放马、攻击

- 黑客信息

- 邮箱、QQ、电话、姓名、年龄、地域



恶代犯罪类型

6

- DDoS
 - 攻击灰色网站敲诈
 - 攻击商业竞争对手
- 信息窃取
 - 帐号密码（窃取银行、虚拟财产、非法广告）
 - 身份信息
 - 技术资料
- 流量
 - Payforinstall、payforAD
 - SEO
- 敲诈
 - 加密敲诈



- 危害范围

- 受害用户数量

- 危害类型

- 无法提供服务损失
 - 商业机密泄漏

- 资金

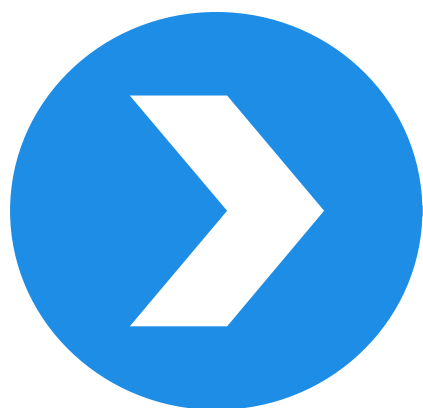
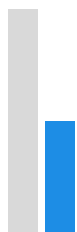
- 广告流量获利
 - 敲诈资金



网络犯罪证据

8

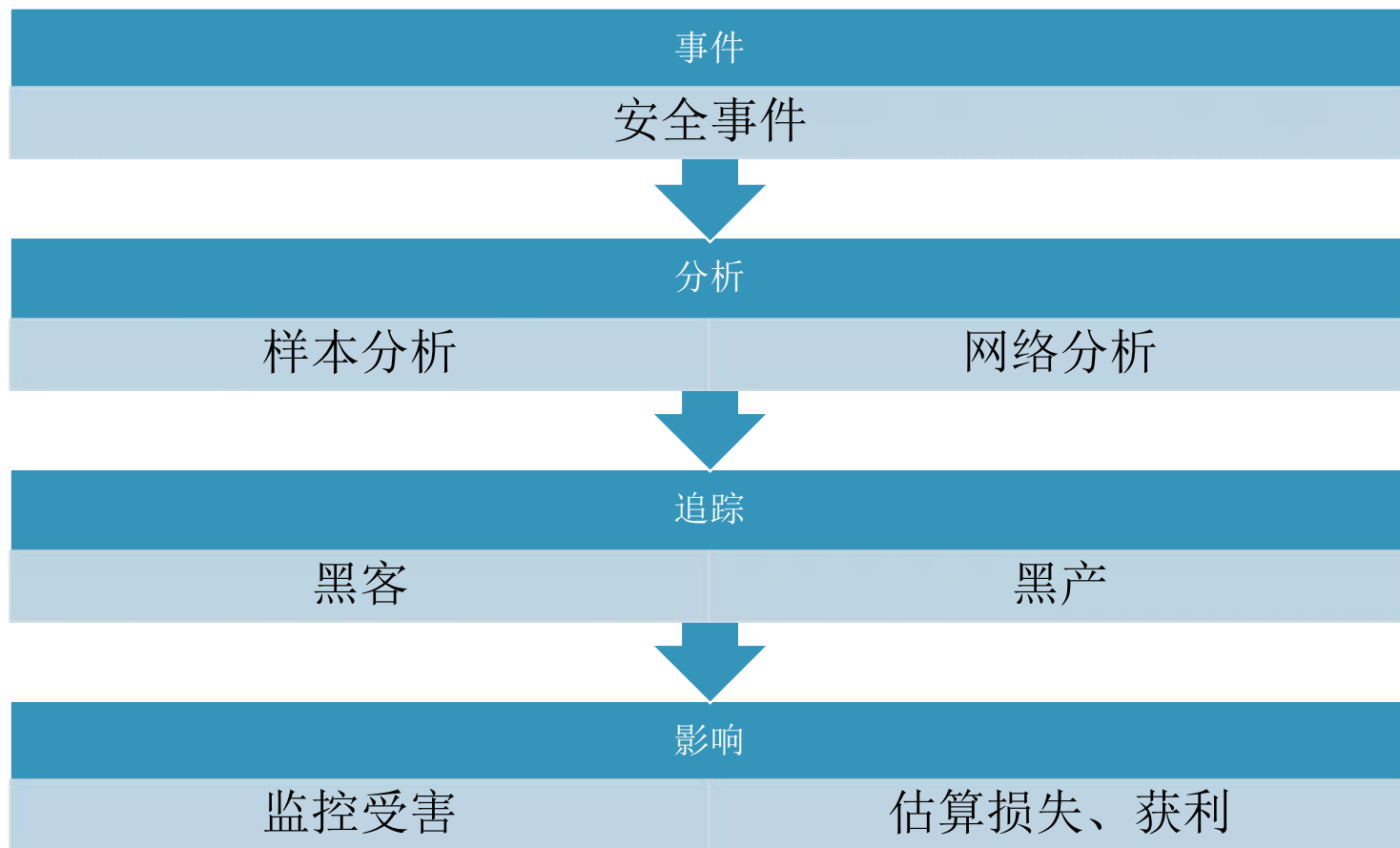
- 受害者机器
- 恶意代码
- 攻击数据包
- 控制服务器数据



恶意代码犯罪追踪过程



1. 安全事件
2. 样本分析
3. 网络架构
4. 危害范围
5. 线索追踪
6. 网络验证





1、安全事件

11

- 事件来源

- 网络流量

- 受害者、攻击者、时间、威胁类型、威胁名称、网络数据

- 终端（PC&手机&server）

- 取证或上报受害者、时间、威胁类型、主机数据

- 云分析

- 样本信息、威胁类型、控制C2、开发时间

- 人工

- 事件描述、事件样本、来源、威胁

- 人工处理

- 最新、规模大、重点受害者

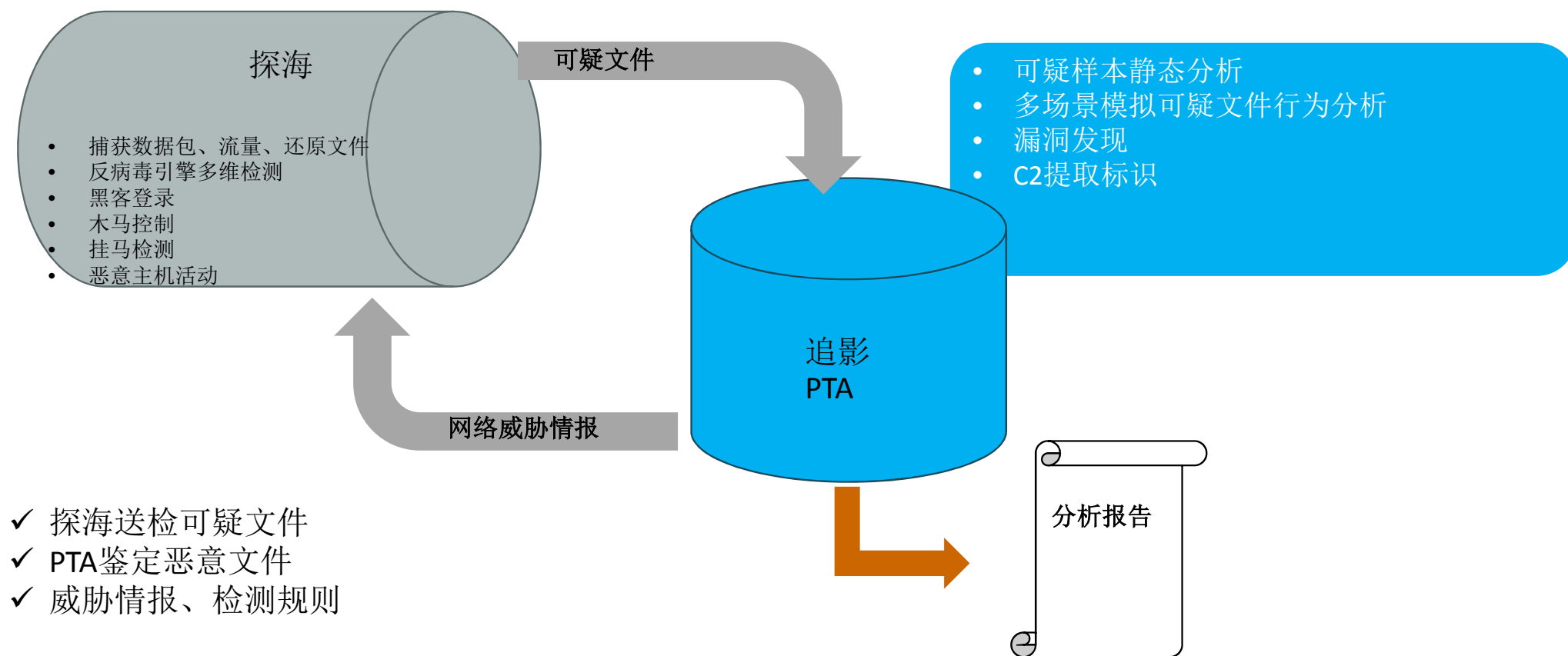
- 事件发现能力

- 知识：漏洞、特征、行为、威胁情报



探海威胁检测安全事件

12





2、样本分析

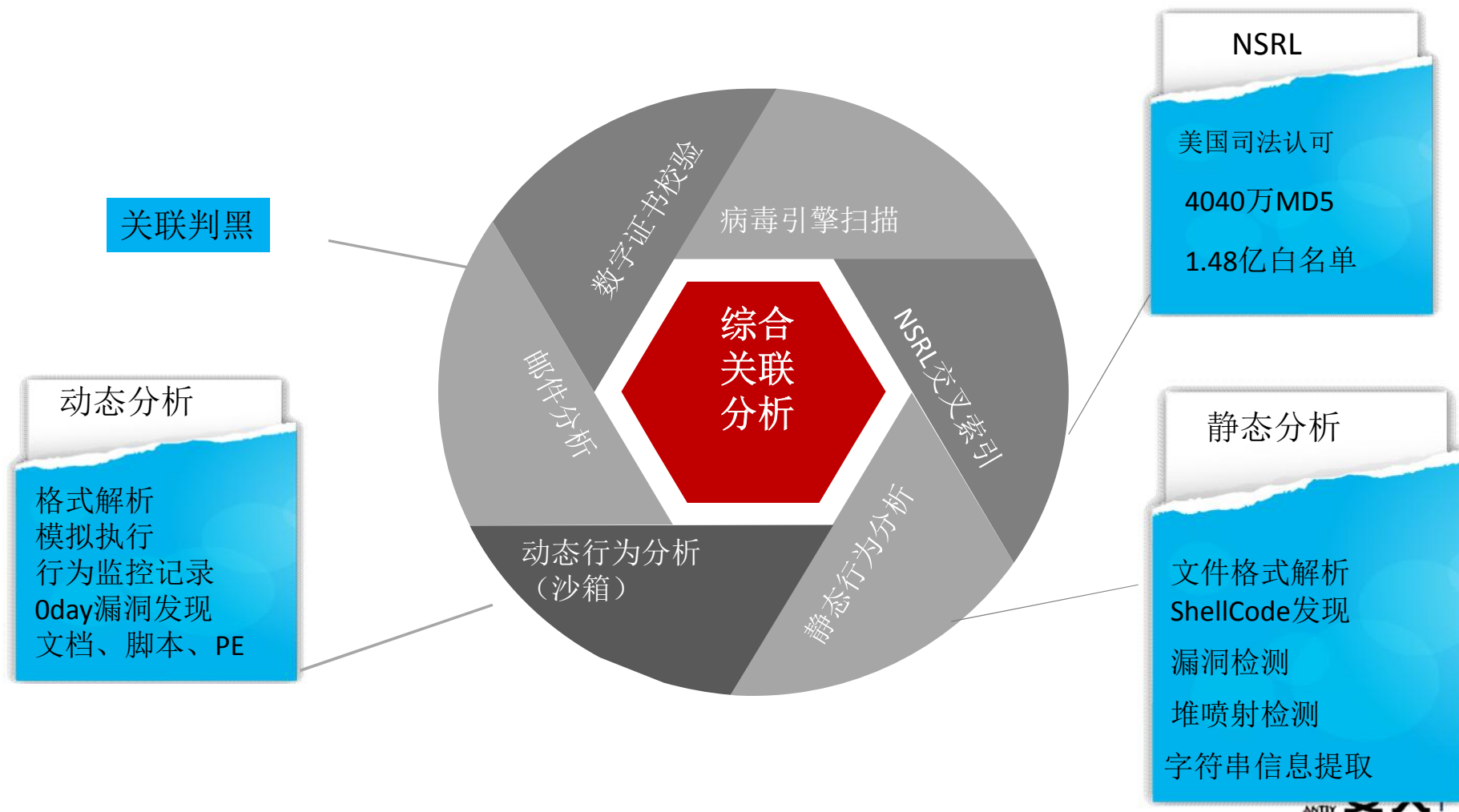
13

- 判定
 - 黑、白
- 分类
 - 核心目的、DDoS、广告、盗号、敲诈
 - 组件（漏洞、下载者、核心、扩散）
 - 格式类型（文档、脚本、PE、ELF）
- 网络信息
 - C2
 - 放马



追影威胁分析系统 (PTA)

14



ANTIV

智者安天下



深度分析和关联分析效果

15



沙箱的差别直接影响分析的质量

模拟环境真实度



移动介质



运行环境



网络模拟



行为触发



诱饵文件

office
QQ
PDF reader

DNS解析
HTTP响应

沙箱功能成熟度



自我保护



自我学习



智能消重



3、网络架构

16

- 黑客组织所使用的网络基础设施
 - IP、域名
 - 操作系统
 - Web结构
 - 地理位置
 - 活动时间
- 作用
 - C2、放马、跳转
 - 公共、独立



4、影响

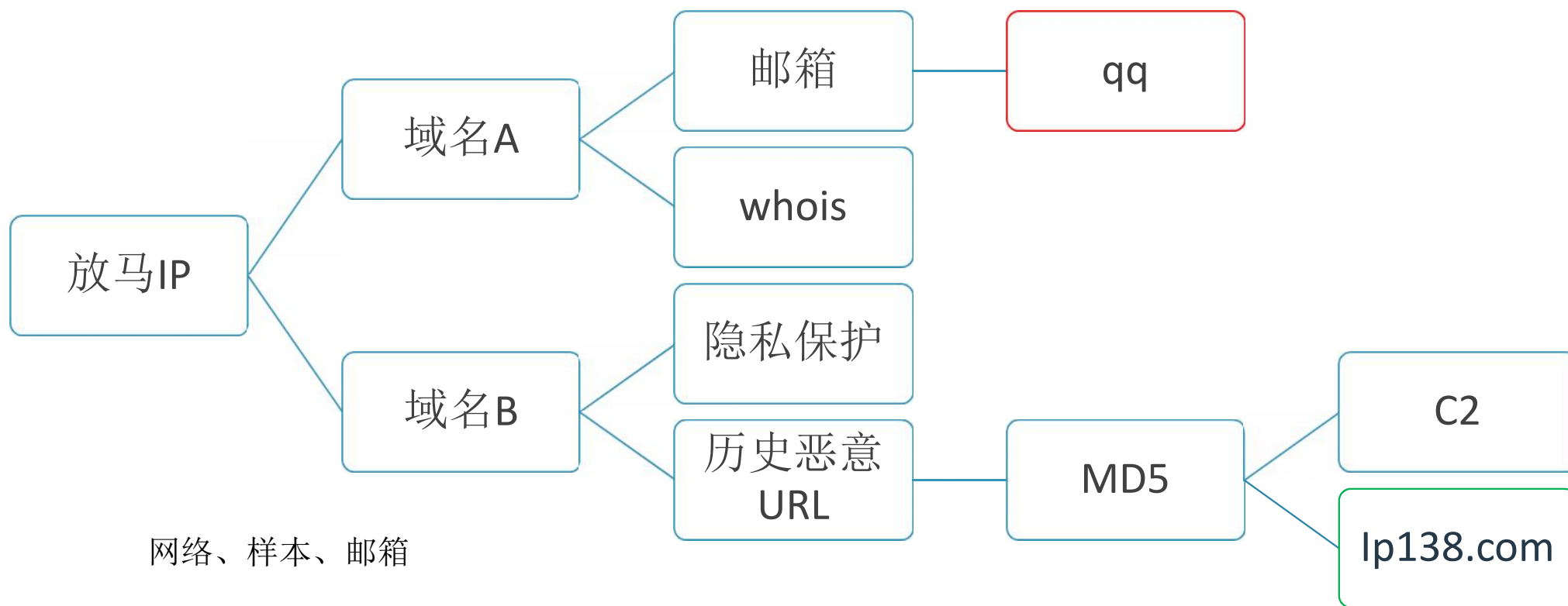
17

- 威胁范围
- 威胁时间
- 资金获利
- 威胁类型
- 威胁目标
- 方法
 - 再监控
 - 统计历史



5、线索追踪—攻击者

18



网络、样本、邮箱

增加、排除、标记



5、线索追踪—开发者

19

- 寻找控制端

- 精确特征
- 时间戳
- 默认配置
- 资源图标
- PDB

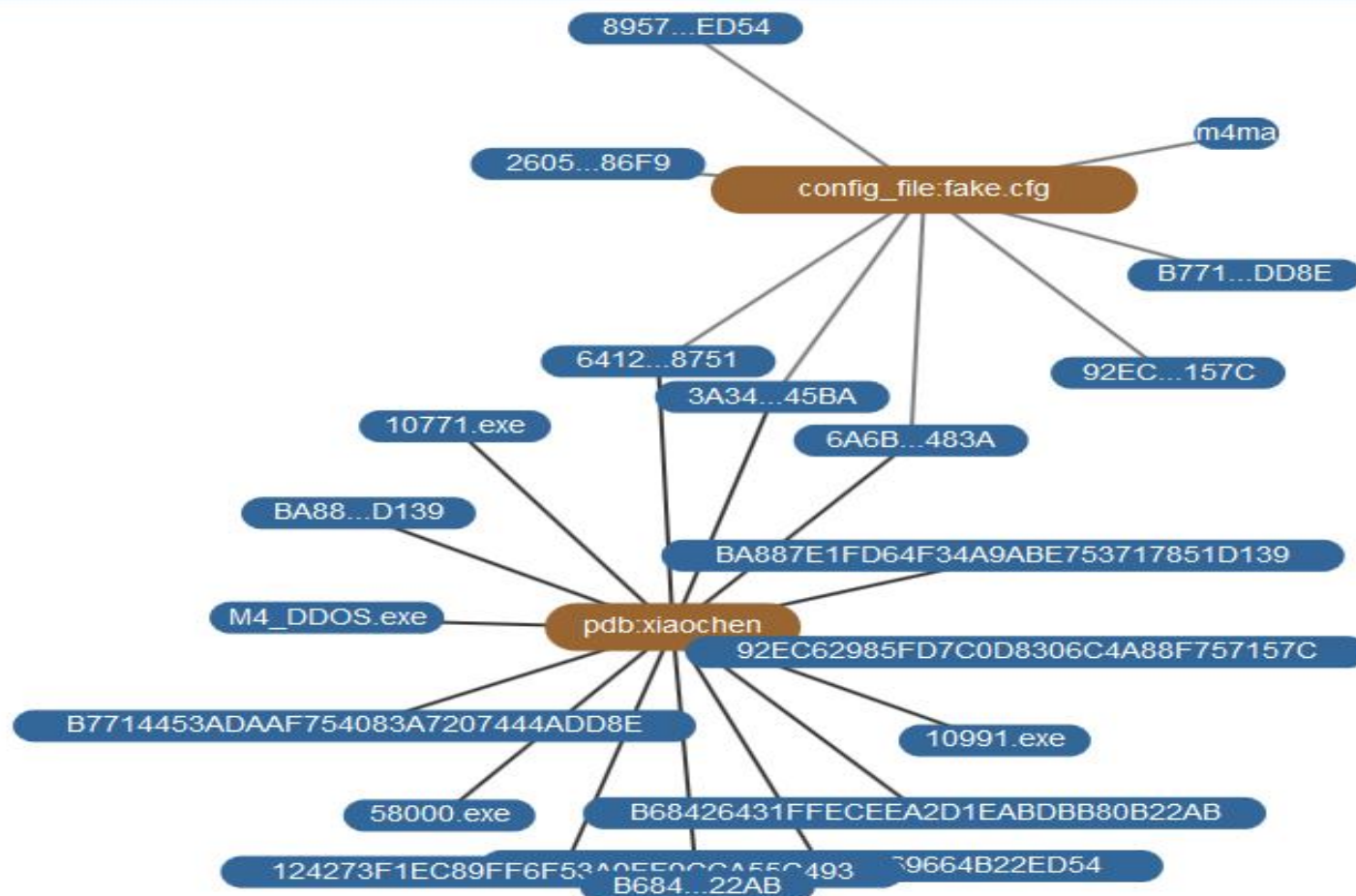
MD5	64120efd52597f3a66b87bfccf1b8751
PDB路径	E:\SVN\trunk\2014\小陈\反向\被控\反向2008 \Chicken\x64\Release\svchost.pdb

- Hacking back



关联

20

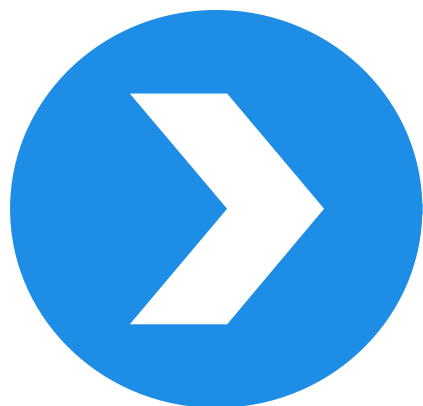




6、网络印证

21

- 位置
 - 空间、贴吧、微博、论坛
- 非法广告信息
 - D单、打死付款、包收流量
 - 备案域名销售
- 更多攻击者信息
 - 电话、地址、昵称
- 其他分析报告

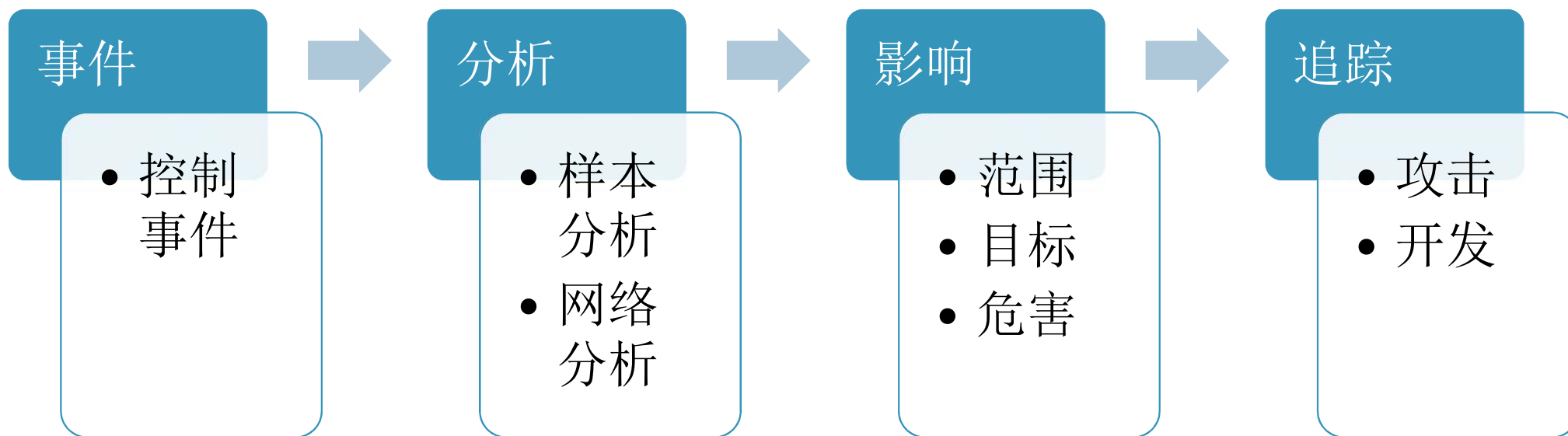


追踪案例



案例一 DDoS追踪

23





案例一 DDoS 控制事件

24

- 捕获时间@2015-11-18 14:43:35
恶意代码名称: Trojan/Win32.STORMDDOS2
源IP: 111.113.14.90
源端口: 49436
目的IP: 222.186.56.8
目的端口: 8080
网络协议: TCP
通信方向: C2S



案例一 关联样本查询

网络监控

IP

IP地址	端口
222.186.56.8	8080
65.19.157.232	8880
113.10.190.251	888

域名解析

域名	IP
az	192.168.122.97
2c3tn3a.ssdqp.xyz	65.19.157.232
www.hacker22.com	113.10.190.251

进程监控

PID : 1756	创建 : hufzuk.exe	
	命令行 : C:\WINDOWS\hufzuk.exe	
PID : 1188	创建 : C:\WINDOWS\system32\cmd.exe	
	命令行 : "C:\WINDOWS\system32\cmd.exe" /c del C:\target.exe > nul	
PID : 1344	创建 : C:\WINDOWS\system32\cmd.exe	
	命令行 : "C:\WINDOWS\system32\cmd.exe" /c del C:\target.exe > nul	
PID : 212	创建 : hrl3.tmp	
	命令行 : C:\WINDOWS\TEMP\hrl3.tmp	
	ExistingFileName	C:\WINDOWS\system32\cmd.exe
	NewFileName	C:\Documents and Settings\Administrator\Application D
	newFileName	\\192.168.122.1\F3\gitd.exe
危险等级 : ★★★		

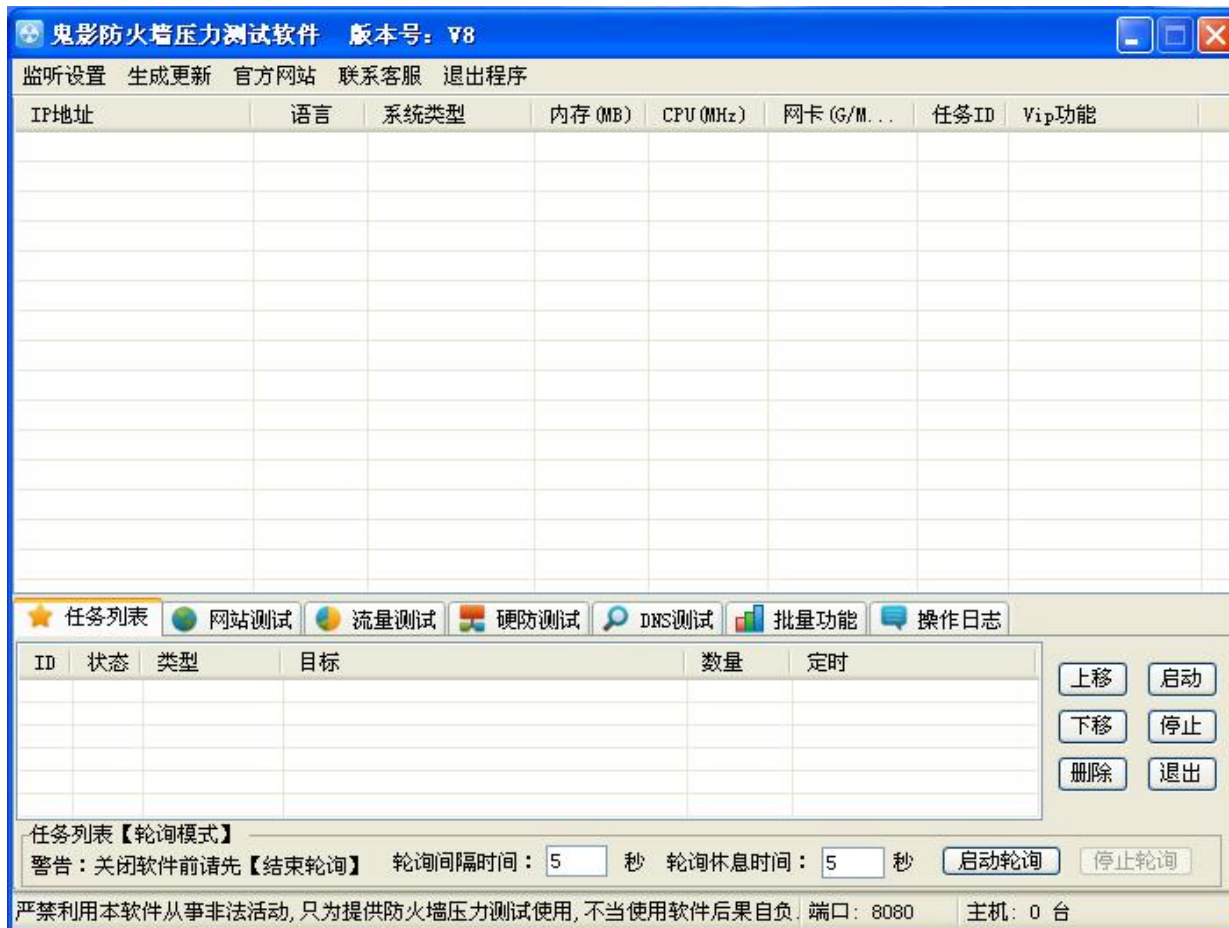




案例一 开发销售者

27

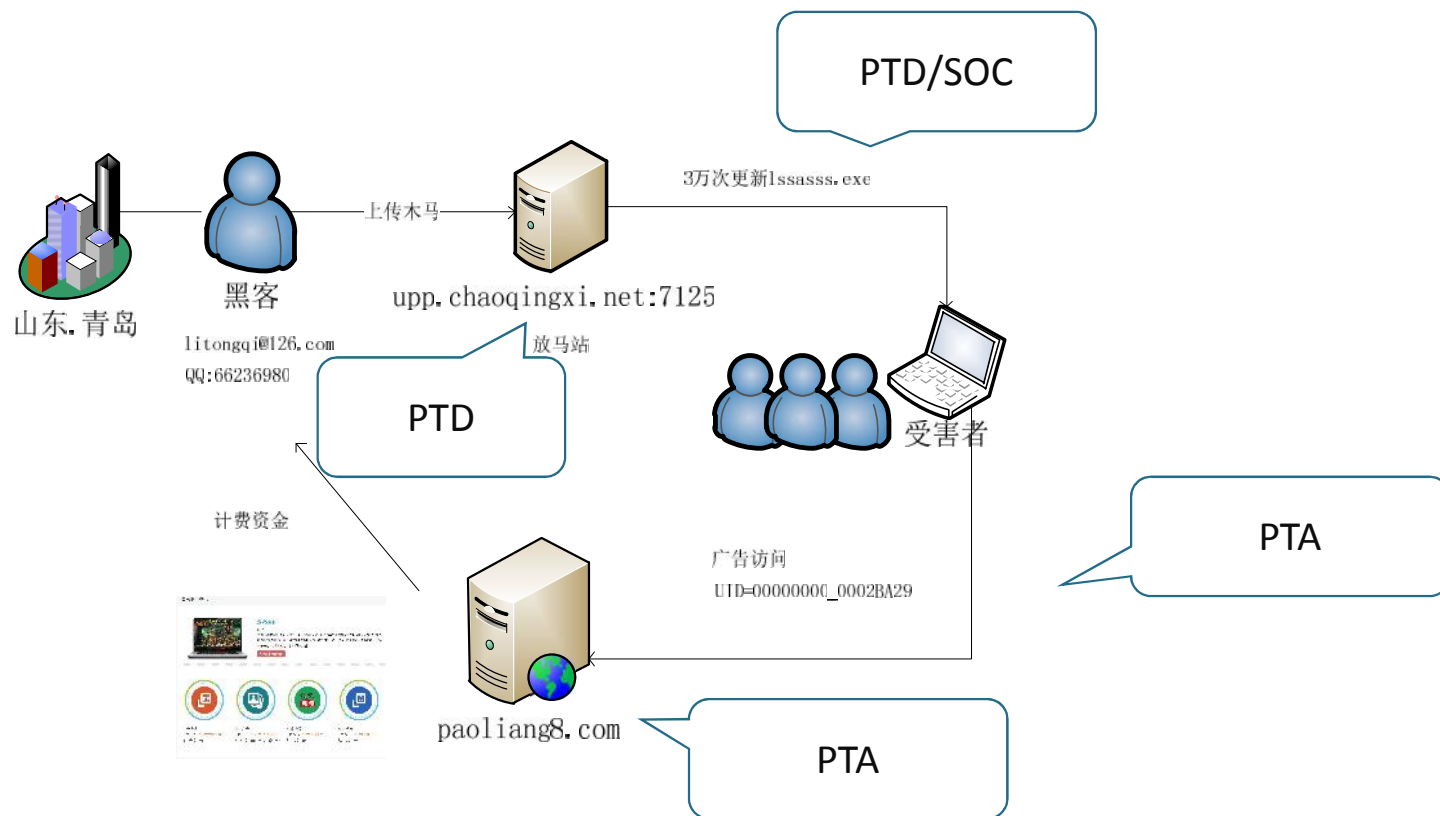
• 图标关联





案例二 流量黑产

28





案例二 传输事件

29

🏠 放马打击指数

所选来源：

下载+经T验证

域名：

uup.chaoqingxi.net

捕获事件段 开始： 结束：

查询

显示

10

记录

域名	累计传输次数	含样本数	最早捕获事件	活跃时间	生存天数	含URL数	含IP数	含恶意代码数	最新出现日期	放马认定指数	放马波及指数	放马打击指数
uup.chaoqingxi.net	125601	2	2014-09-14 13:49:31	2015-11-18 23:21:33	138	2	5	1	2015-11-18	0.089295	1.08433	0.288301

当前显示 1 到 1 条，共 1 条

← 上页

1

下页 →



案例二 样本分析

30

lssasss (1).exe分析报告

(追影高级威胁鉴定系统)

基本信息/概述

名称 lssasss (1).exe
大小 443.50 KB
文件格式 exe
MD5 fda5cf3a25896f5eb08c622e5fec3150
PDB路径 None
壳/编译器 None
恶意判定 yes
病毒类型 RAT
病毒名 None

文件是远程控制木马,主要目的是控制用户计算机,窃取用户私密信息,损害计算机系统,文件类型是BinExecute/Microsoft.EXE[:X86],长度为454144字节,运行它将向其他进程内存写入数据;远程注入其他进程;内联钩子;释放资源到系统目录;壳行为填充导入表;连接网络;隐藏文件;设置调试器权限;释放PE文件;获取主机内存信息;获取系统版本;访问文件尾部;在其他进程中申请内存;获取计算机名;获取指定套接字的一个本地ip地址;枚举进程;DNS请求;创建服务;创建窗口;获取磁盘类型;独占模式打开,防止复制读取,防止杀毒软件扫描上报;打开自身;获得计算机用户名;启动指定服务;查找指定内核模块;查找窗口;获取驱动加载权限;

汇总发现

发现危险	危险等级
向其他进程内存写入数据	★★★
远程注入其他进程	★★★★
内联钩子	★★★★
释放资源到系统目录	★★★



案例二 网络危害活动影响

31

事项：服务器IP数量以及受控IP数量以及对应地点

文件：dip_noreplication_chaoqingxi_data.txt sip_noreplication_chaoqingxi_data.txt

服务器IP数量：4 服务器IP来源地：山东青岛市联通

受控IP数量：78 受控IP来源地：宁夏 特点：电信用户居多，四个城市为主，固原市，吴忠市，中卫市，银川市

事项：服务器IP以及对应受控IP数量

文件：dsip_chaoqingxi_data.txt

服务器IP：221.215.123.238 受控IP数量：72

服务器IP：124.129.3.154 受控IP数量：68

服务器IP：119.167.78.26 受控IP数量：42

服务器IP：119.167.78.18 受控IP数量：53

结论：三个服务器IP均来自于山东青岛市

事项：服务器活跃时间

文件：server_live_list.txt

本次更新时间：2015-10-08

服务器IP：221.215.123.238 活跃记录数：12281 时间开始：2015-08-01 15:34:41 时间结束：2015-10-08 12:12:37

服务器IP：124.129.3.154 活跃记录数：11938 时间开始：2015-08-01 15:28:21 时间结束：2015-10-08 12:12:15

服务器IP：119.167.78.26 活跃记录数：5973 时间开始：2015-08-30 10:16:50 时间结束：2015-10-08 11:57:26

服务器IP：119.167.78.18 活跃记录数：6183 时间开始：2015-08-01 15:35:10 时间结束：2015-08-30 08:31:11

分析：

1.221.215.123.238，124.129.3.154持续活跃，现在仍为活跃

2.119.167.78.26可能为代替119.167.78.18的服务器IP



案例二追踪一-网络信息

32





追踪二-广告资金链

- 领跑吧注册信息
- 领跑吧UID

URL

http://lpvoidray.lingpao8.com/VoidRay_1122.php?UID=00000000_0002BA29

<http://p1.lingpao8.com/Phoenix/20150915.zip>

http://lpvoidray.lingpao8.com/Phoenix_20150202.php?UID=00000000_0002BA29&

客服: 400-6111-926 0175 登录 注册 忘记密码

The Lead Partner Union
领跑吧联盟
LingPao8.com

多样化服务 服务团队专业 产品智能稳定 付款及时安全

您的当前位置: 首页 > 用户注册

基本信息

* 用户名: pao88 ✓
* 登录密码: ***** ✓
* 确认密码: ***** ✓
* 提示问题: pao88 ✓
* 问题答案: pao88 ✓

联系方式

* 联系人: 领跑吧 ✓
* 省市区域: 广东 深圳 ✓
* 联系电话: 13700000000 ✓
* 联系QQ: 888888 ✓
* E-mail: 888888@qq.com ✓

财务信息

以下信息不可随意更改, 需要更改请联系客服!

* 收款人: 领跑吧 ✓
* 身份证: 340811198502083078 ✓
* 开户银行: 农业银行 ✓
* 开户地址: 广东 深圳 ✓
* 手机号码: 13700000000 ✓
* 银行卡号: 6210555555555555 ✓
* 开户网点: 中国农业银行 ✓

☒ 我已经阅读并同意《领跑吧联盟会员协议》

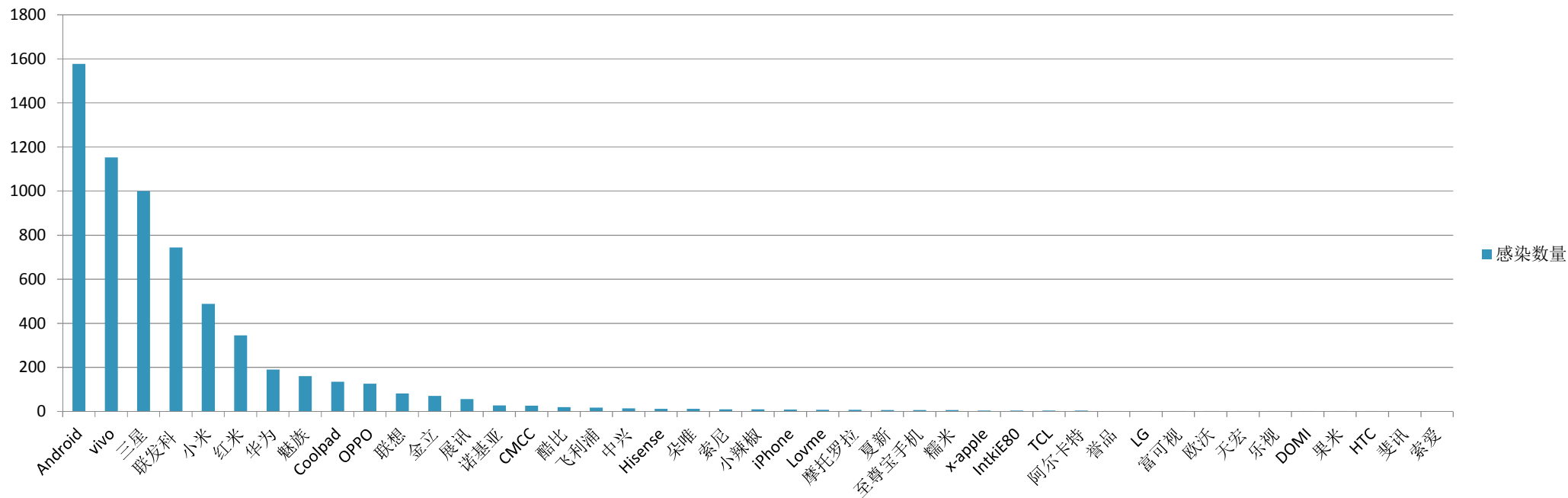
提交

Copyright©2007 - 2013 | All Rights Reserved | 西安领跑吧软件科技有限公司 | Lingpao8.com
陕ICP备12004442号-9 | 站长统计



• 尝试静默安装手机品牌

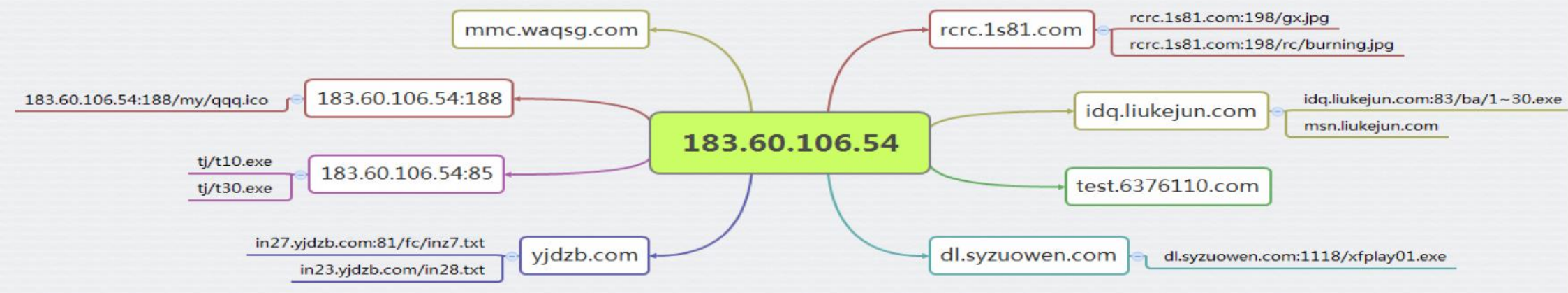
感染数量





案例三 - 盗号放马网络分析系统

35





案例三 放马人追踪

36

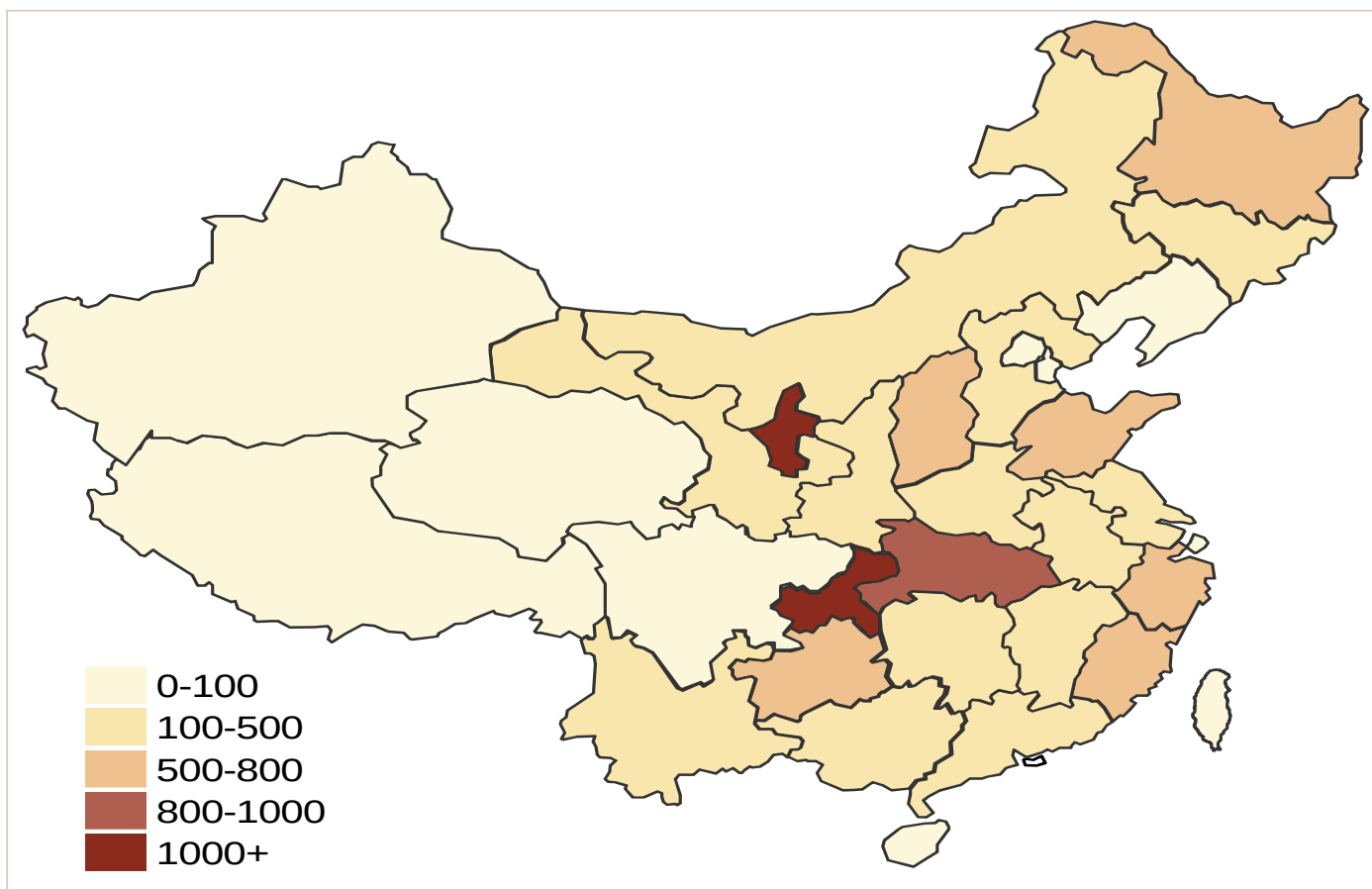
- 域名whois信息
- QQ邮箱





案例三-受害地理分布（监控系统）

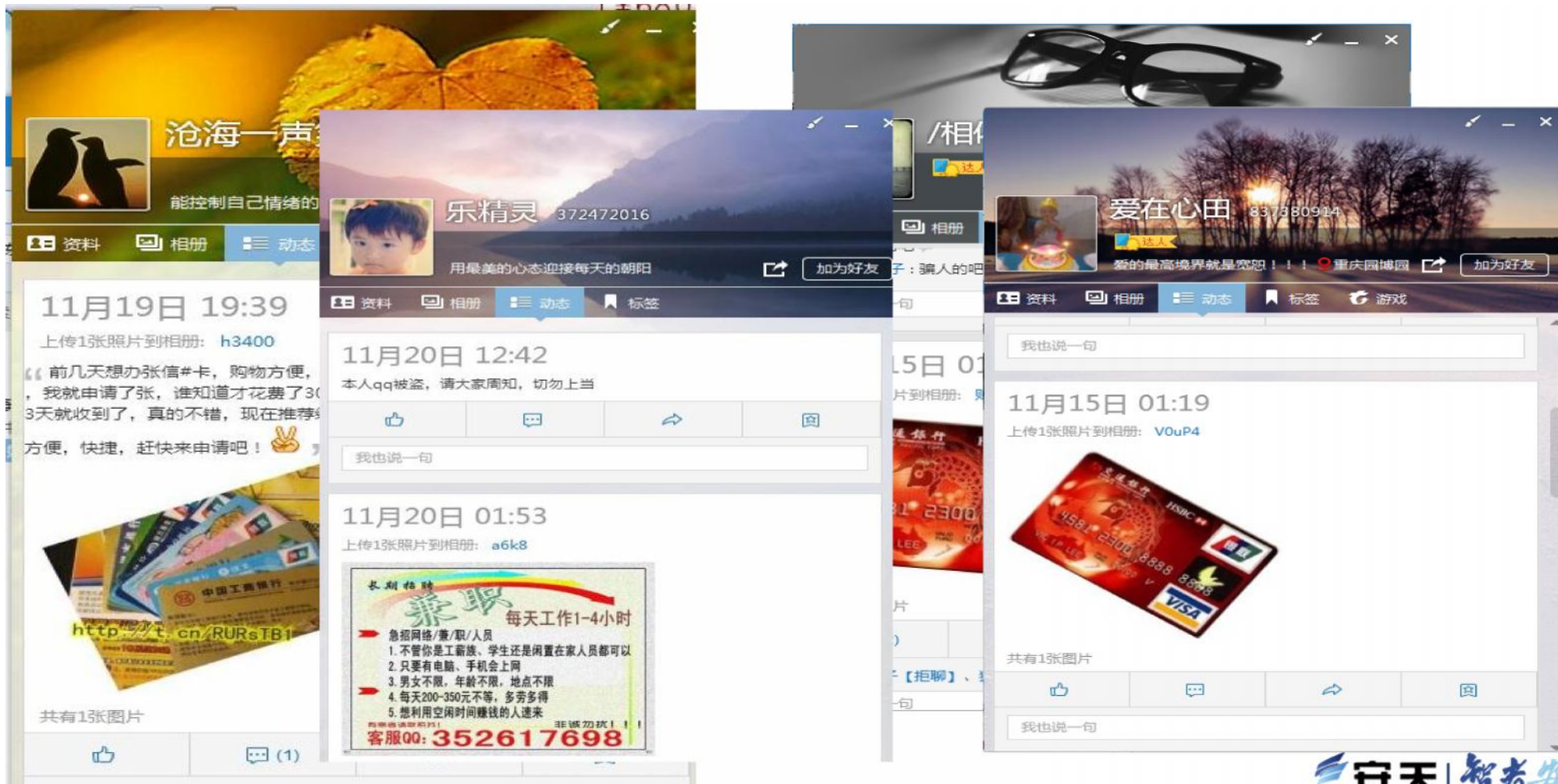
37

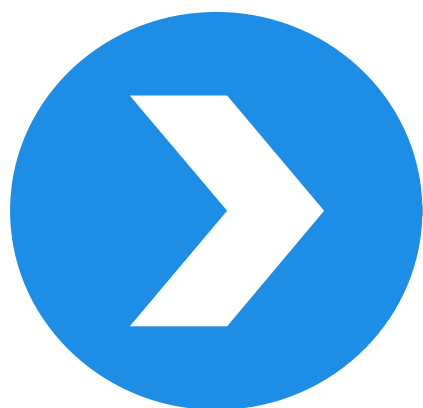




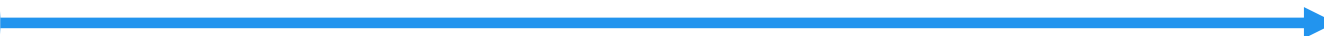
案例三 受害者QQ定位（监控系统）

38





挑战





身份隐藏

40

- 备案域名销售
- 代收短信注册
- 隐私域名保护

搜索

重置

快速查询导航：5数字 | 6数字 | 老域名 | 浏览热门 | 全数字 | 全字母 | 四字母 | 已备案 | 已备案最低价 | 最便宜的

网站推荐：

20171314.com

chengdu.cc

ceyace.com

12366.bj.cn

70435.com

1991.org

搜索结果 (24458) 条记录 [下载本次查询出的列表]

你也有域名想出售？

域名	长度	备案	简介	卖家	注册时间	价格	购买
☐ 214369.com	6	未备案	214	ID:9911	2015-11-4	588元	购买
☐ pp92.cn	4	未备案	精品四字母	ID:89758	2015-11-16	288元	购买
☐ yyth.cc	5	未备案		ID:4293	2015-1-4	18元	购买
☐ 9777n.com	5	未备案	豹子数字加一字母，快速升值中，更多请点击===>	ID:85402	2015-11-13	600元	购买
☐ 787080.com	6	未备案	精品数字，更多点击后面ID！	ID:74945	2015-11-22	8000元	购买
☐ cnyrm.net	5	已备案	已备案360无拦截，更多备案域名点id50836	ID:50836	2015-11-25	60元	购买
☐ 95601888.com	8	未备案		ID:86677	2015-11-14	118元	购买
☐ 688503.com	6	未备案		ID:45456	2015-4-24	1888元	购买
☐ cdLphf.com	6	未备案	点击ID79153 域名多多 快快抢购	ID:79153	2015-5-30	35元	购买
☐ 0539111.com	7	未备案	山东临沂区号	ID:85597	2015-10-10	30000元	购买
☐ manbi.net	5	未备案	2拼：曼比 manbi.net 漫笔	ID:70691	2015-11-6	1588元	购买
☐ njruini.com	7	未备案		ID:67678	2014-12-22	15元	购买
☐ 9522488.com	7	未备案	9522488.com客服95	ID:81845	2015-11-7	98元	购买
☐ jxmsxh.com	6	已备案	精选万网阿里云备案域名 无毒 无拦截	ID:10902	2015-12-16	68元	购买

谢谢大家

THANK YOU FOR YOUR ATTENTION

www.antiy.com

 安天 | 智者安天下