从产业角度试解
手机恶意代码的新趋势

安天实验室

提纲

引子
- 从Android Market说起

现象
- 恶意代码的传统视角和产业视角

应对
- 谁决定移动安全的走向

结论
- 结束语。

演讲者简介

- 肖新光，网名江海客，安天实验室首席技术架构师。
- 中国互联网协协会信息安全专委会委员，国家信息安全研究所应用专家组成员，武汉大学计算机学院兼职教授。29届奥运会应急响应专家组成员。

从ANDROID MARKET说起

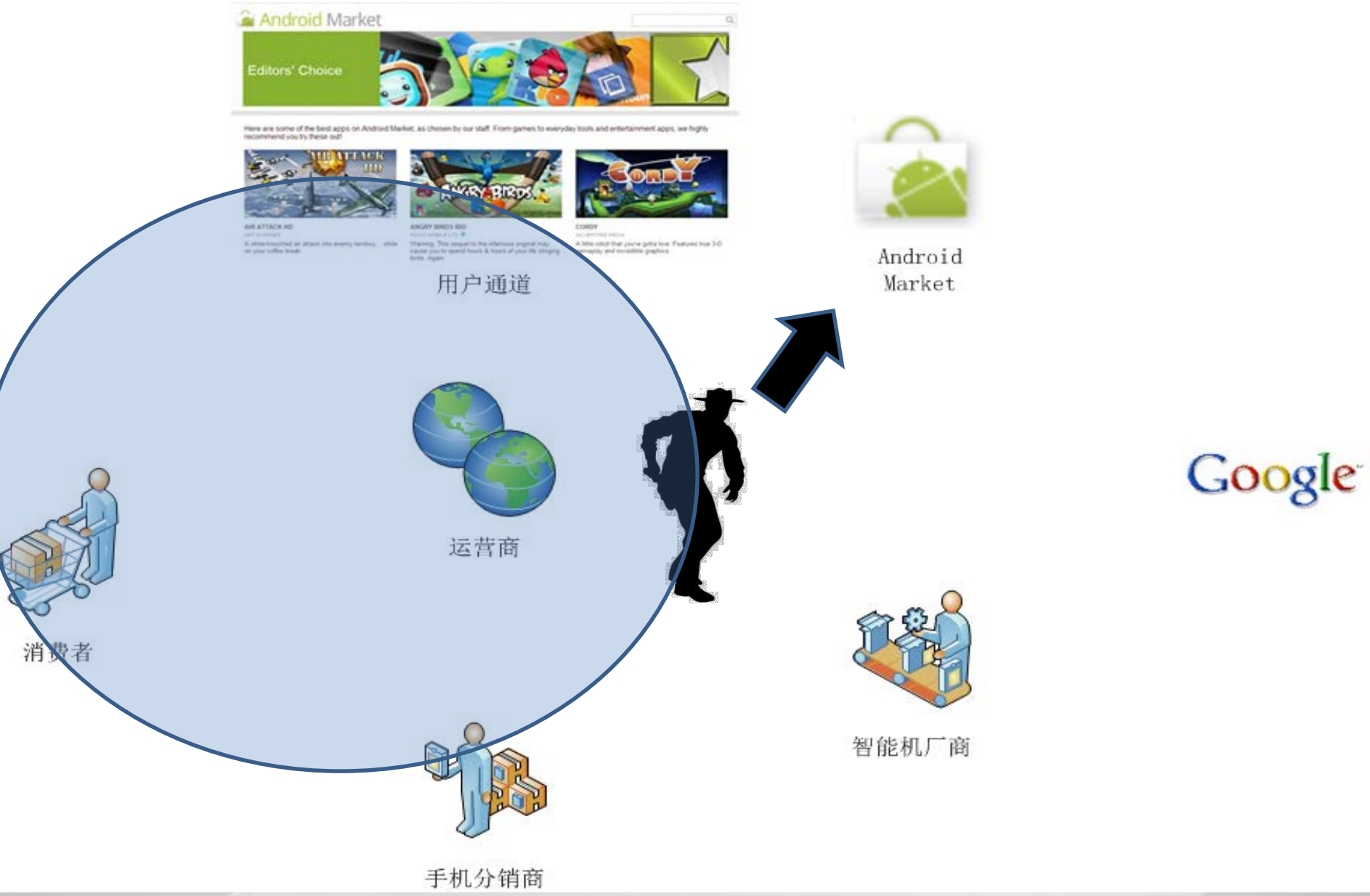
Android Market的事故轨迹

时间	事件
1月1日	Droid09出现在官方市场，冒充网银客户端要求用户输入账号密码。
7月21日	间谍件Tapsnake出现在官方市场，植入游戏，将手机位置发送到远程服务器
10月27日	木马SMSReplicator出现在官方市场。

2010年3起恶意提交事件

时间	事件
2月15日	DroidDream在Android Market 58款软件中开始被夹带。
3月2日	被用户发现。
3月2日	Android Market删除这些软件。
3月4日	Google发布专杀工具并push到客户端。
3月9日	国内论坛出现植入专杀工具的木马BgServ。
5月31日	窃取隐私软件DroidKungFu被发现出现在Android Market 。
6月5日	Plankton被发现出现在Android Market，窃取隐私，采用了全新的免杀技术：dalvik类动态加载。
6月7日	YZHCSMS被发现出现在Android Market，发送恶意扣费短信。
6月13日	色情件SMSreg被发现出现在Android Market，发送扣费短信
7月14日	SndApps被发现出现在Android Market上传用户隐私信息，包括email和联系人。

新闻背后的分析


Android Market
Editors' Choice
用户通道
Android
Market
运营商
消费者
手机分销商
智能机厂商
Google

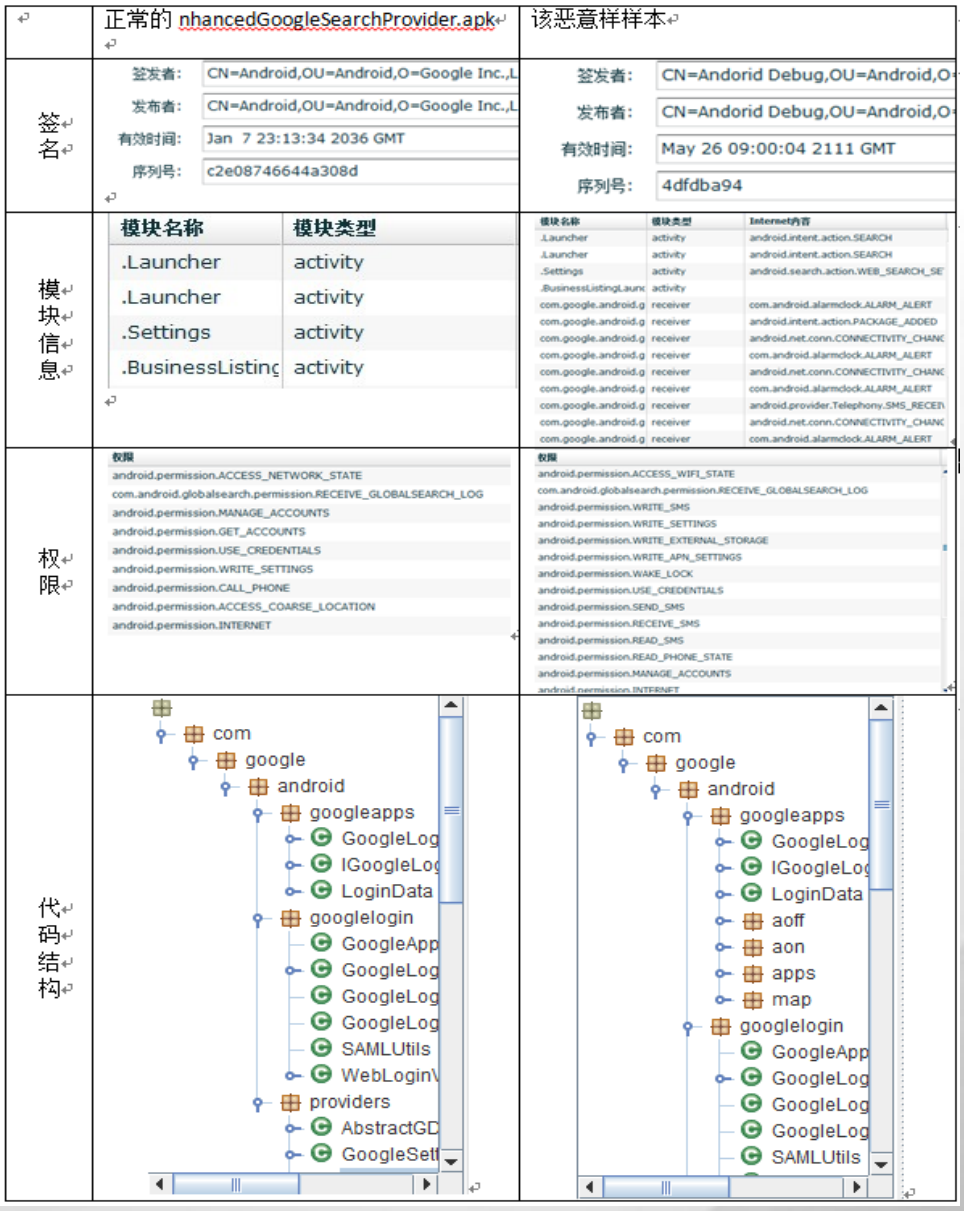
故事因一部水货机被改变

- 扣费
  - 定制收费服务
- 流量
  - 下载其他软件
  - 刷点击量
- 隐私
  - 窃取短信、通讯录等信息

恶意代码分析

场景信息	
名称	com.google.android.providers.enhancedgooglesearch
中文名称	
源文件名	a.apk
来源URL	
采集来源	
系统平台	Android
样本文件格式	apk
样本MD5值	BFBB58D0F8B487869393A0244AE71AFC
样本CRC32值	C1C12A99
样本SHA1值	59EE114166CDBCDDB88B38299934021080053D86
样本大小	

恶意代码信息	
名称	Trojan/Android.droiddg.a[rmt,sys]
CNCERT名称	a.remote.droiddg.a
中文名称	
其它厂商名称	无
原生/捆绑	固件植入！！！（捆绑）
威胁类型	remote system



真正有趣的故事

被刷ROM的水货Android手机

一个香艳的“电子市场”

真正的“电子市场”

原厂的ROM

被改道的产业链条

用户通道

Android Market

运营商

消费者

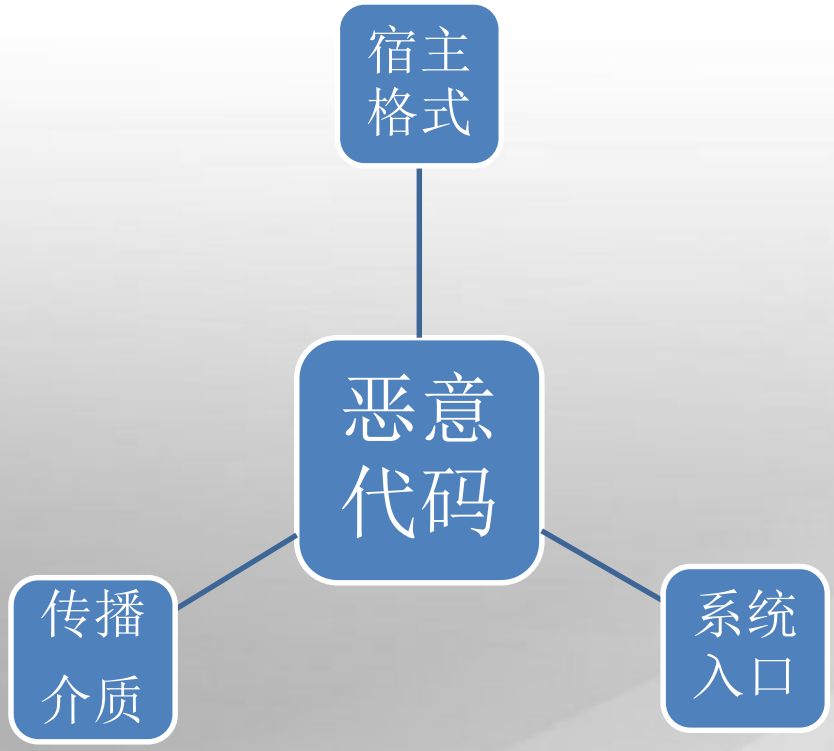
手机分销商

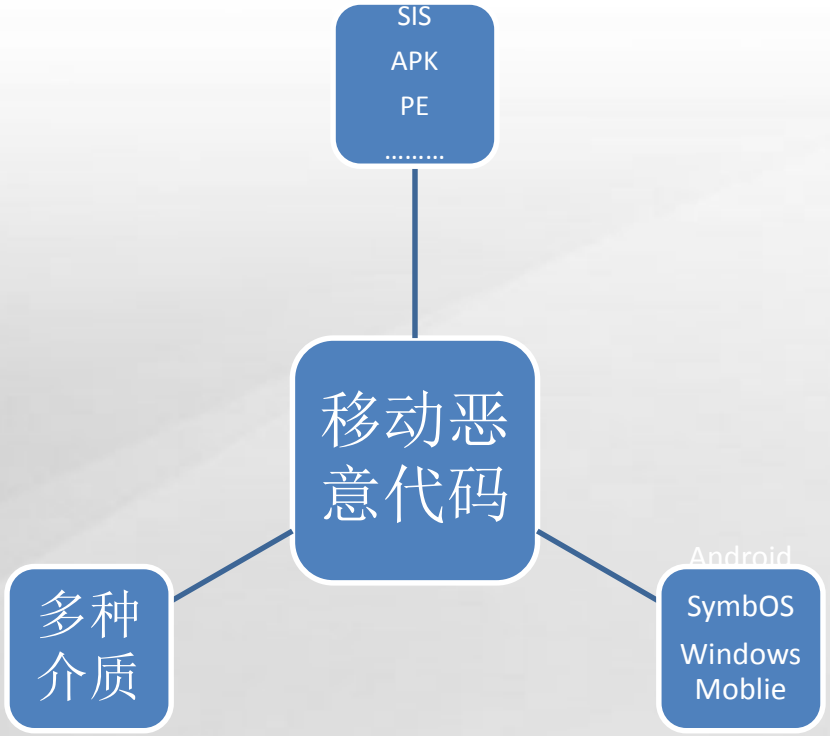
智能机厂商

Google

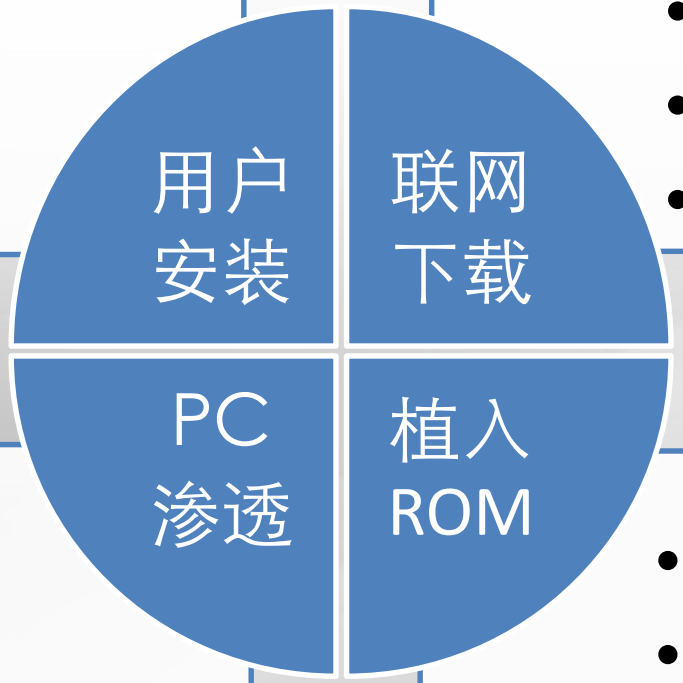
移动恶意代码的传统视角与产业视角

传统视角——技术解析


宿主格式
恶意代码
传播介质
系统入口


SIS
APK
PE
.....
移动恶意代码
多种介质
Android
SymbOS
Windows Moblie

主要传播途径



- 官方市场/网站
- 第三方市场等
- 短信/彩信

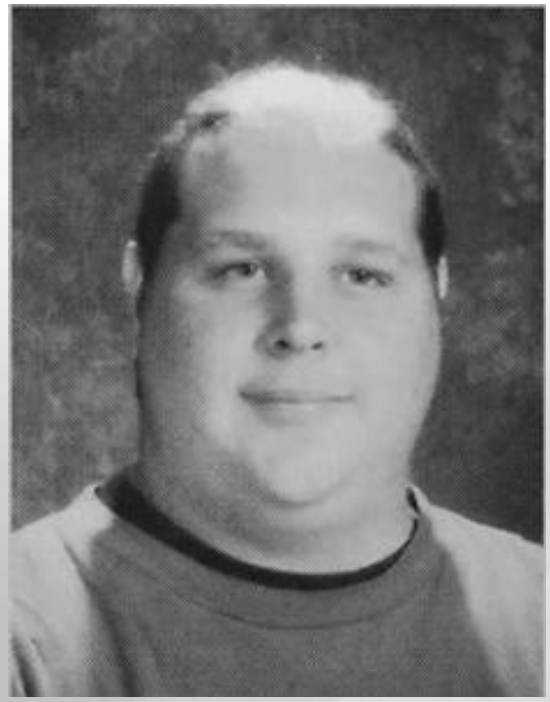
- GPRS/3G
- Wi-Fi
- PC共享网络

- 闪存共享
- USB通信

- 用户刷机
- 销售商预装

关于传统：被遗忘的那些灰色面孔？

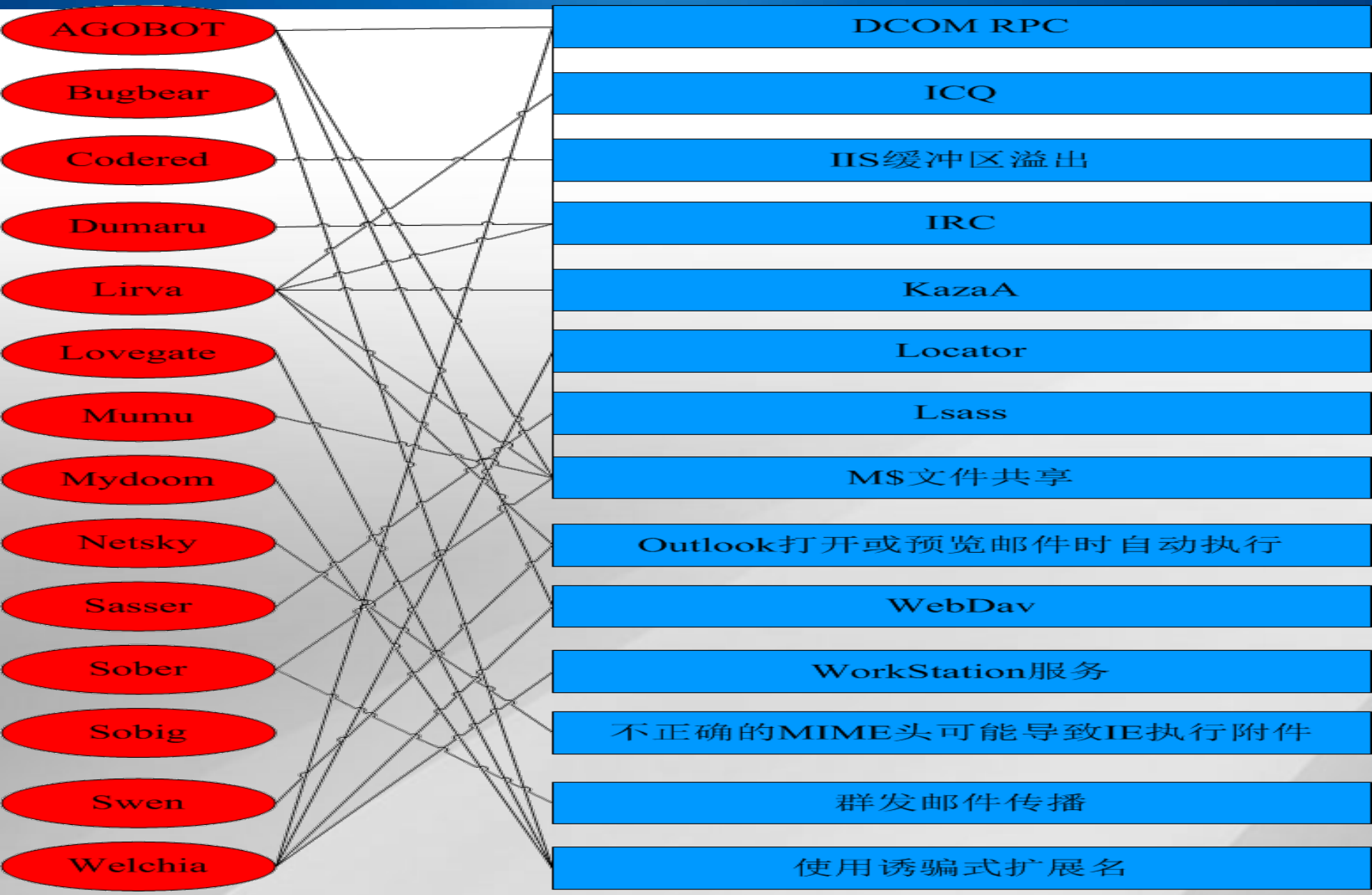
CIH
1998



Melisa
1999

Sasser
2004

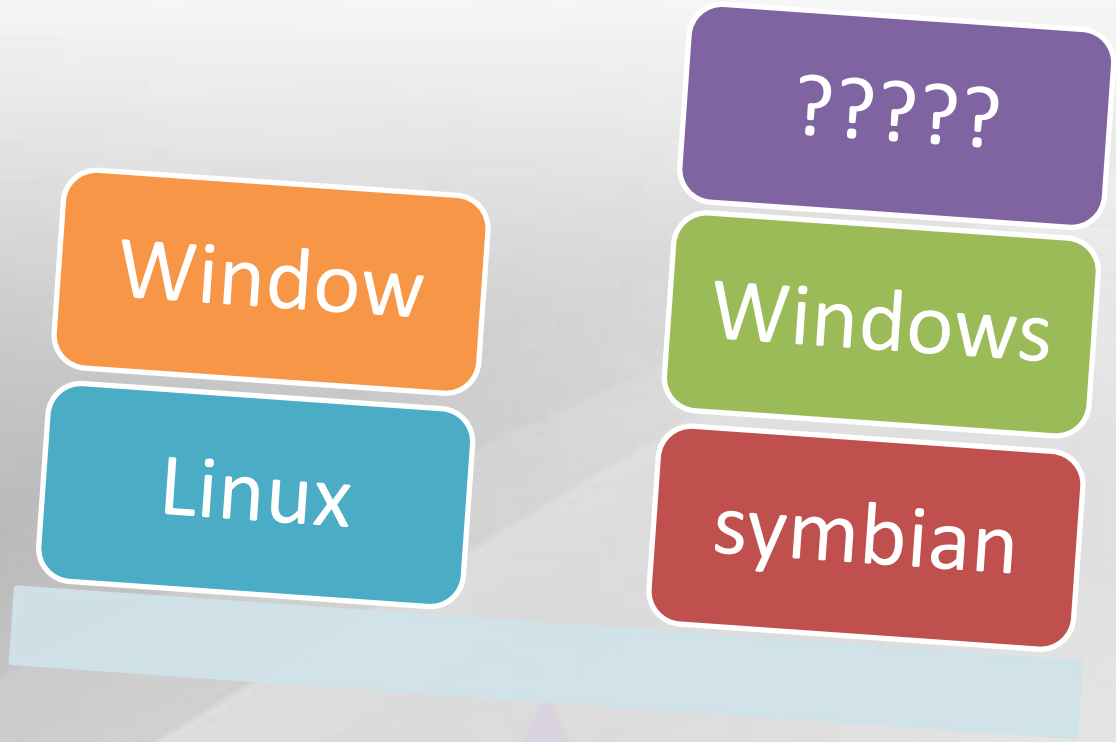
关于传统：被遗忘的那些红色警报？



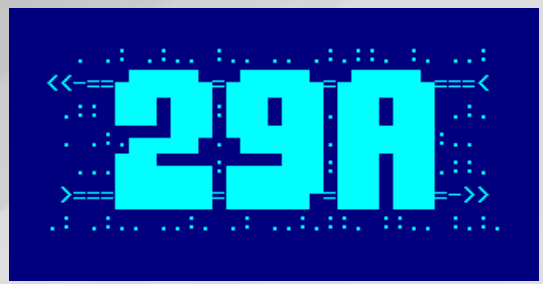
一个跨平台的对比

2001

2010



Winux (2001)



跨平台-手机+PC双态（2010）

SymbianUpdateSrv.exe

912812352001_3rd.sisx

启动和更新模块

0xe61caca0.dat
（实际为jar）

symbianDL.exe

dlinstall.dat
（实际为sisx）

功能伪装模块

多个class文件

下载模块

install.dat20
（实际为sisx）

symbianSrv.exe

symbianStarter.exe

服务监控模块

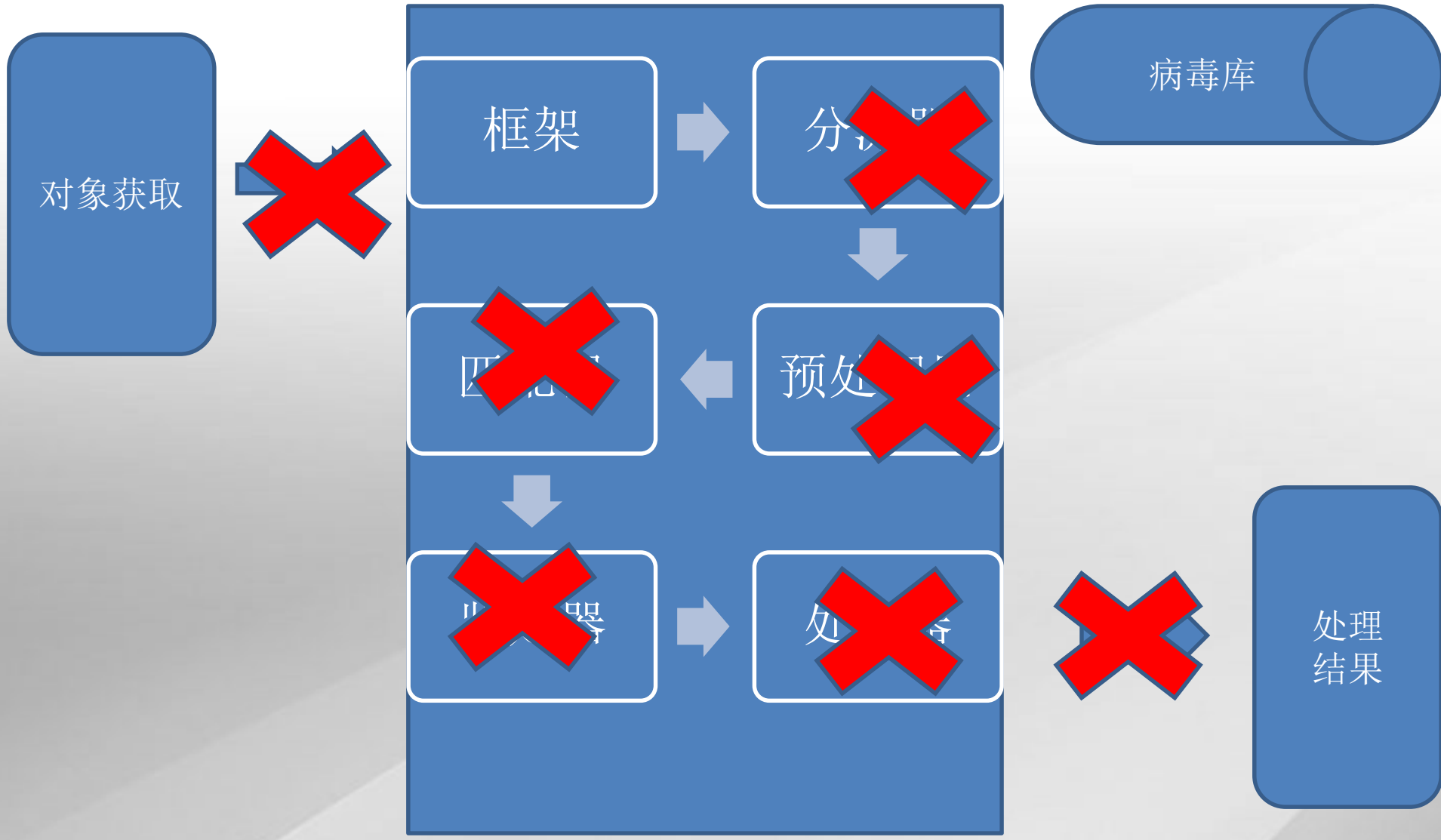
环境清理模块

symbianChkServer.exe

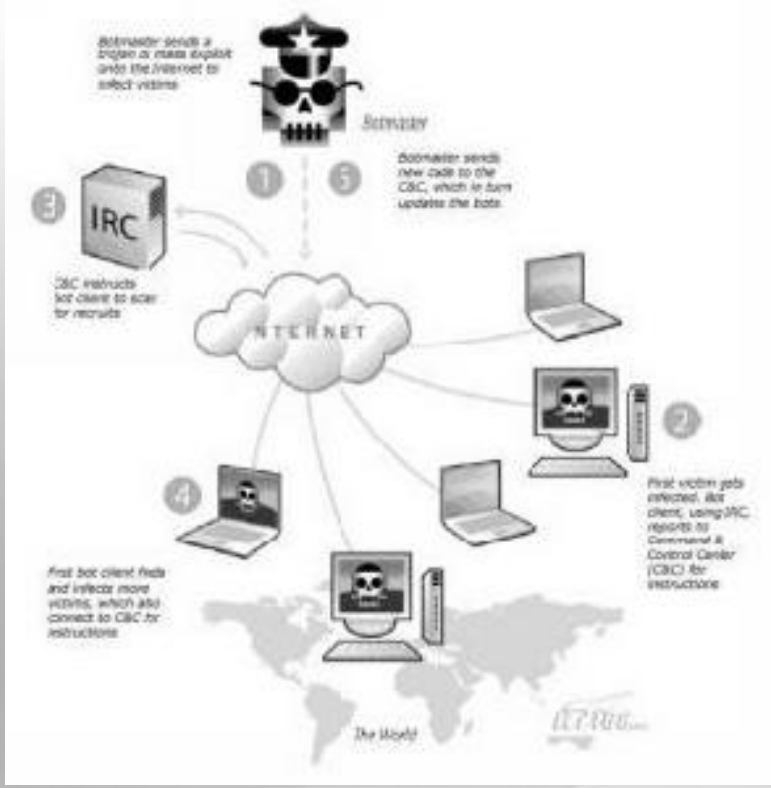
心跳远控模块

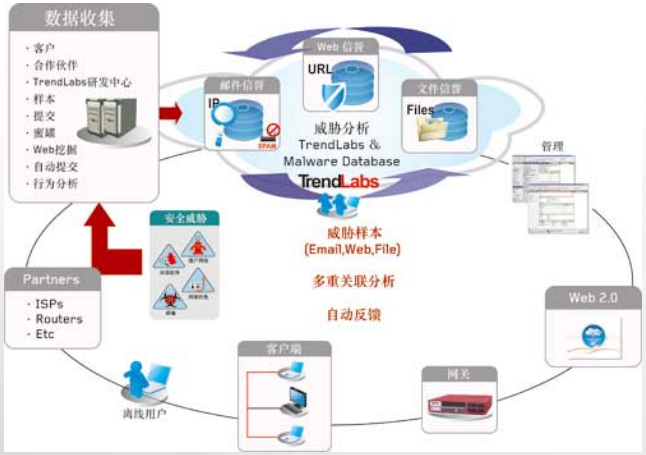
1988年以来的对抗演进

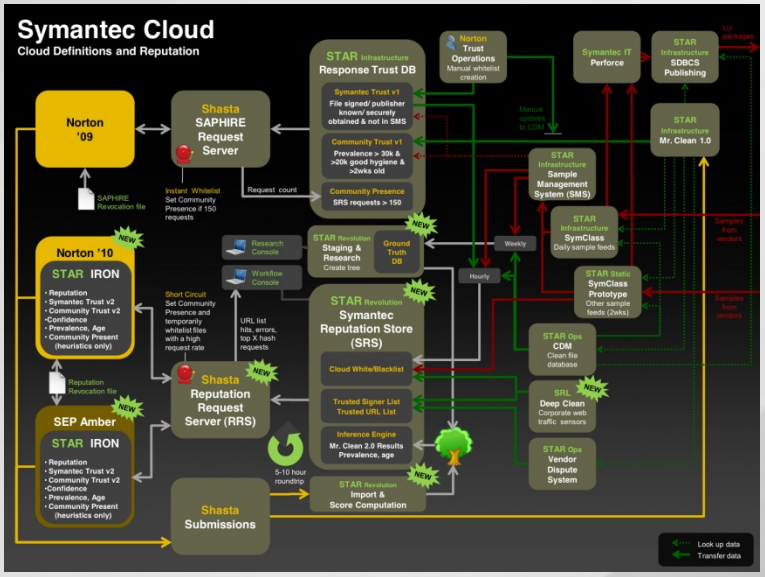
归一化对抗



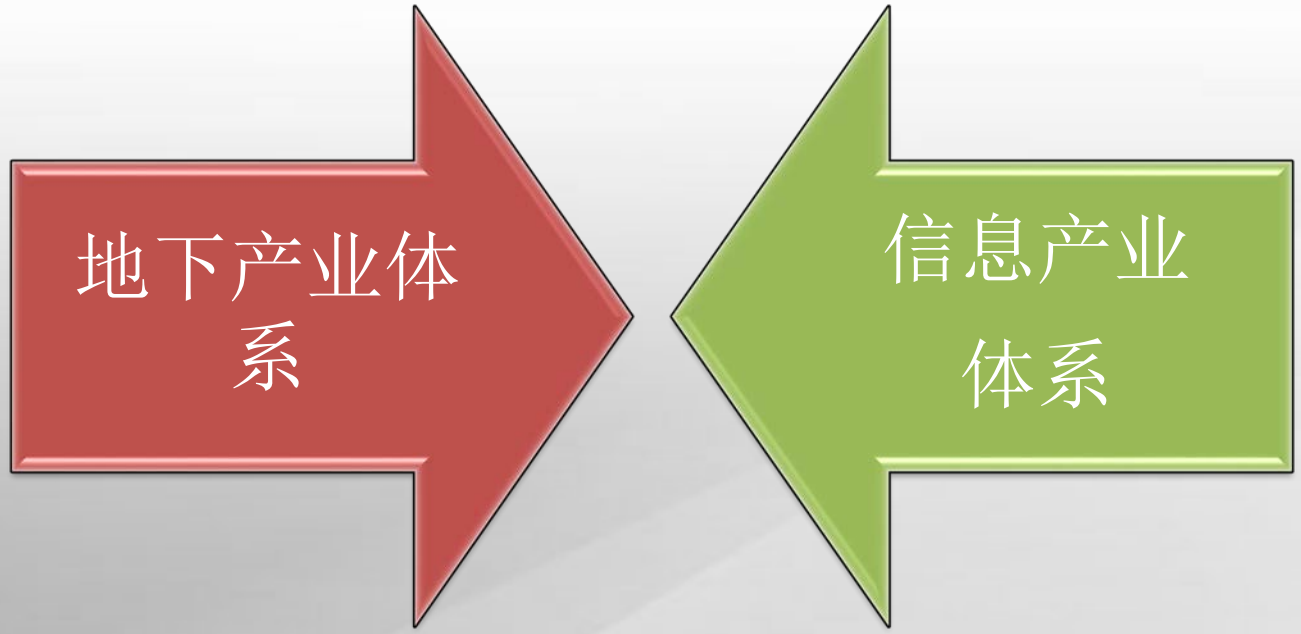
体系化对抗（2000～2005）



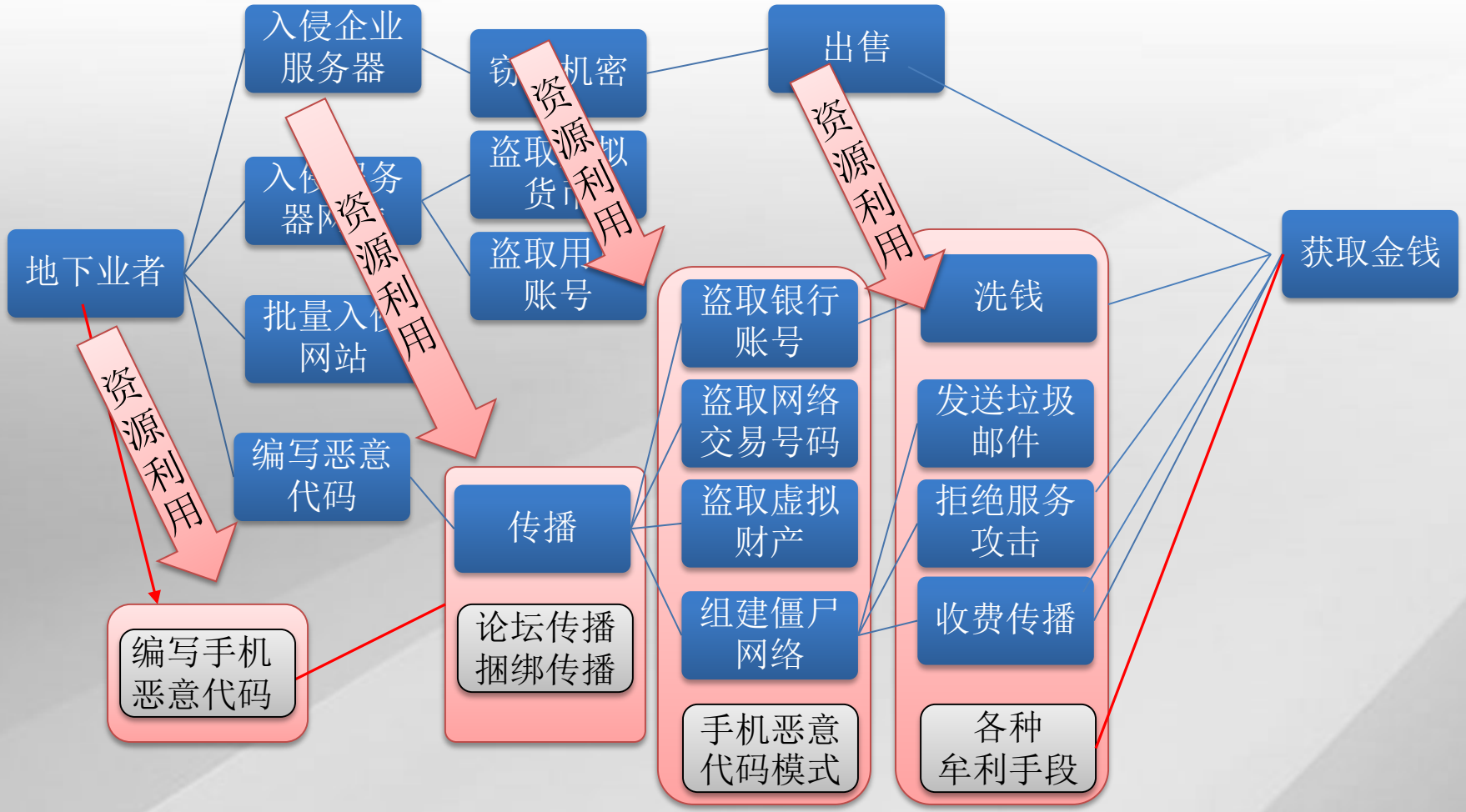




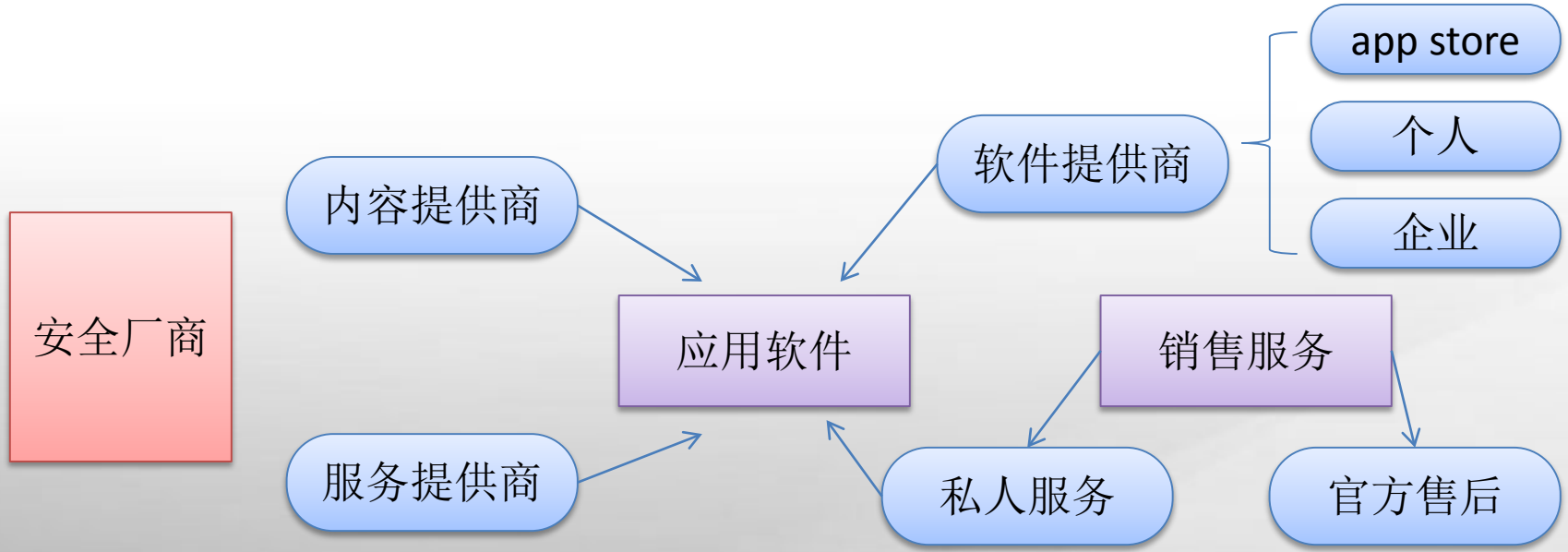
产业化对抗（2005～今）



地下产业链条


入侵企业服务器
盗取机密
出售
资源利用
资源利用
资源利用
入侵服务器网站
盗取虚拟货币
盗取用户账号
地下业者
获取金钱
批量入侵网站
资源利用
盗取银行账号
洗钱
盗取网络交易号码
发送垃圾邮件
编写恶意代码
传播
盗取虚拟财产
拒绝服务攻击
组建僵尸网络
收费传播
编写手机恶意代码
论坛传播
捆绑传播
手机恶意代码模式
各种牟利手段

移动产业链链条



基带芯片	解决方案	零部件	操作系统	生产制造	销售渠道
高通 TI	TechFaith 大唐 ……	ARM 内存 电池	Symbian、WM、 Macos、android、 palm……		行货、定制 水货、捆绑

谁决定移动安全的走向

传统反病毒方法面临挑战

蜜罐

诱饵信箱

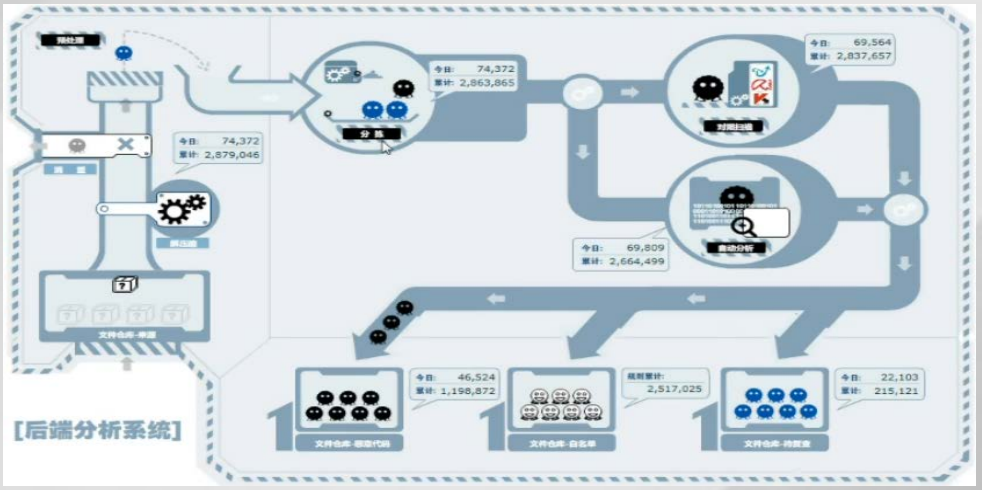

自动上报


用户上报


流量捕获


主机产品

安全设备



传统困境之样本捕获

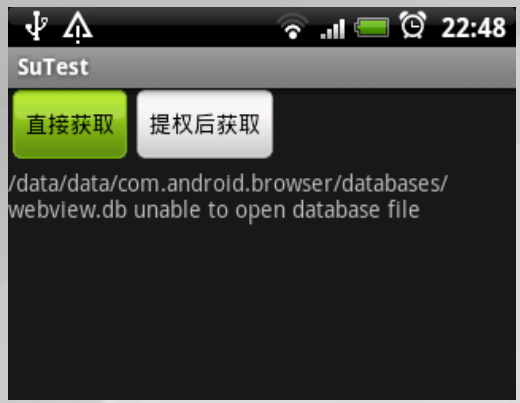
终端样本捕获	• 流量资费 • 用户隐私 • 终端覆盖率
蜜罐技术	• 部署成本 • 捕获效力 • 采集困难
用户上报	• 用户上报意识 • 用户鉴别能力 • 样本的采集方法
网络捕获	• 捕获基础建设 • 设备部署 • 运营商配合 • 用户隐私

传统困境之终端权限

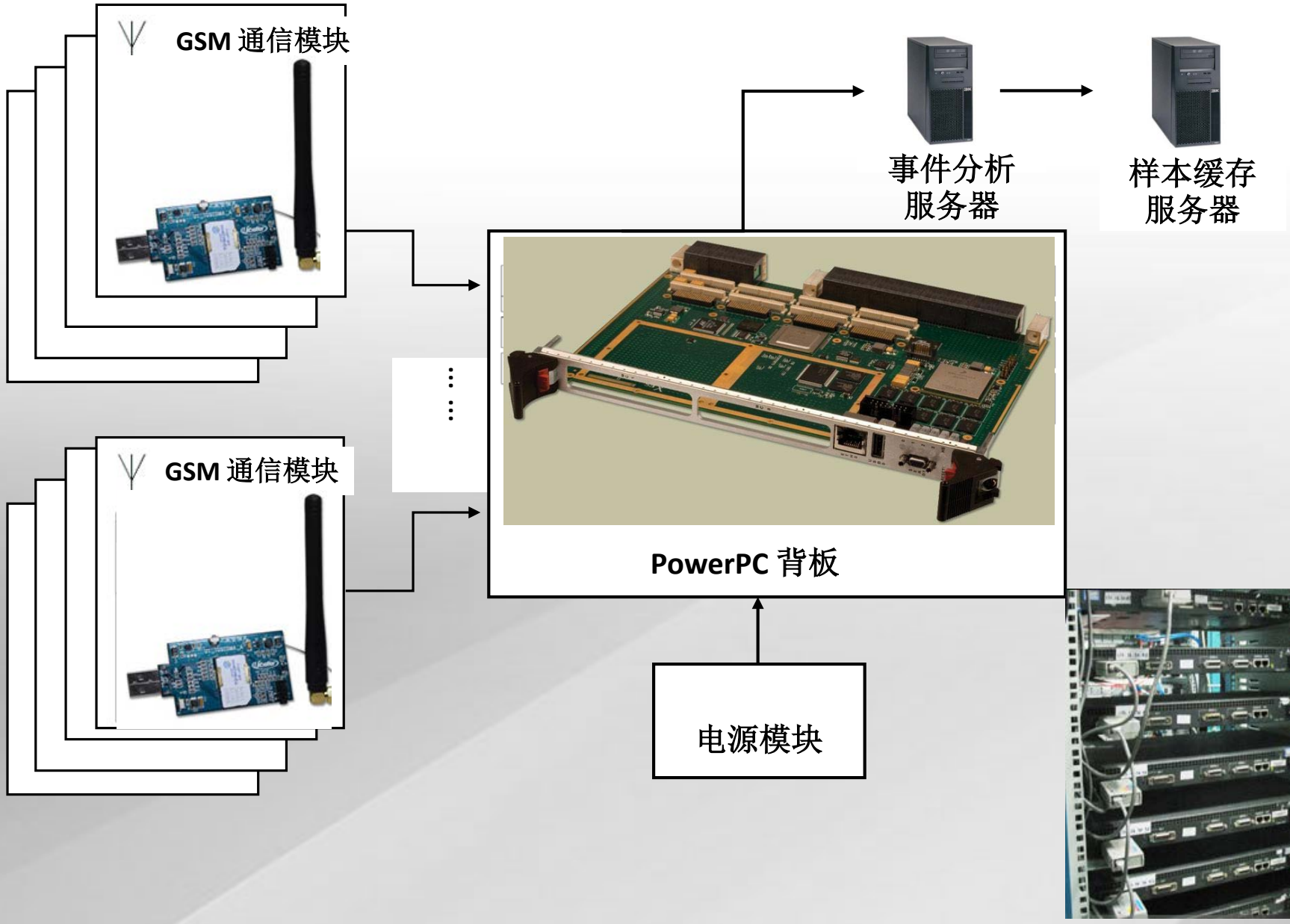
- 利用系统漏洞
- 可以获得极高权限
- 可以获得其他程序的隐私信息

手机操作系统 → 破解、提权 →
- 更开放的系统环境
- 更多安全隐患和漏洞
- 更易受控的移动节点

_id	name	address	date	subject	body
1	朱	+8615827[redacted]7	1285846454697		[redacted]
2	朱	+8615827[redacted]7	1285846048856		[redacted]
3	朱	+8615827[redacted]7	1281412586124		[redacted]
4	朱	+8615827[redacted]7	1280679178598		现在忙，稍后给您回电。

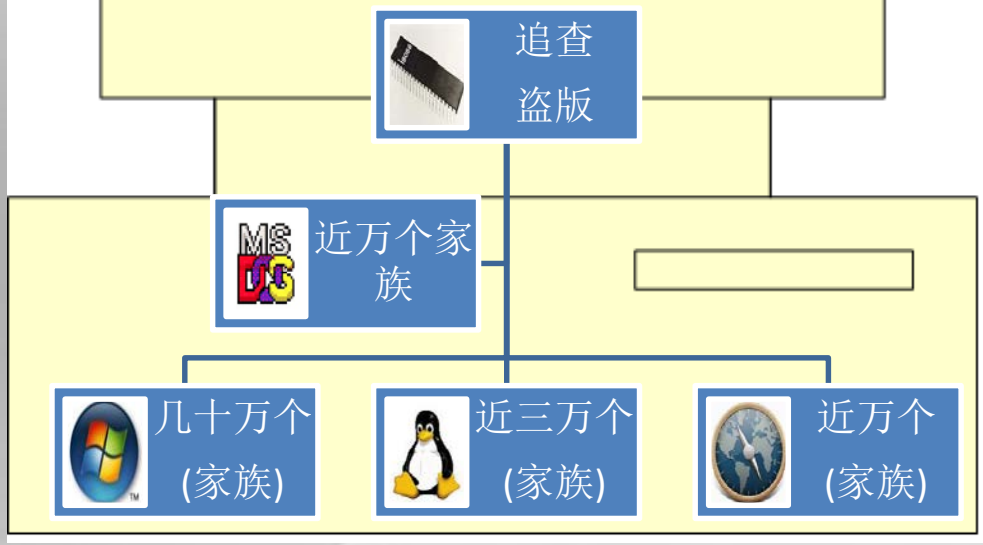


厂商的问题到运营商迎刃而解



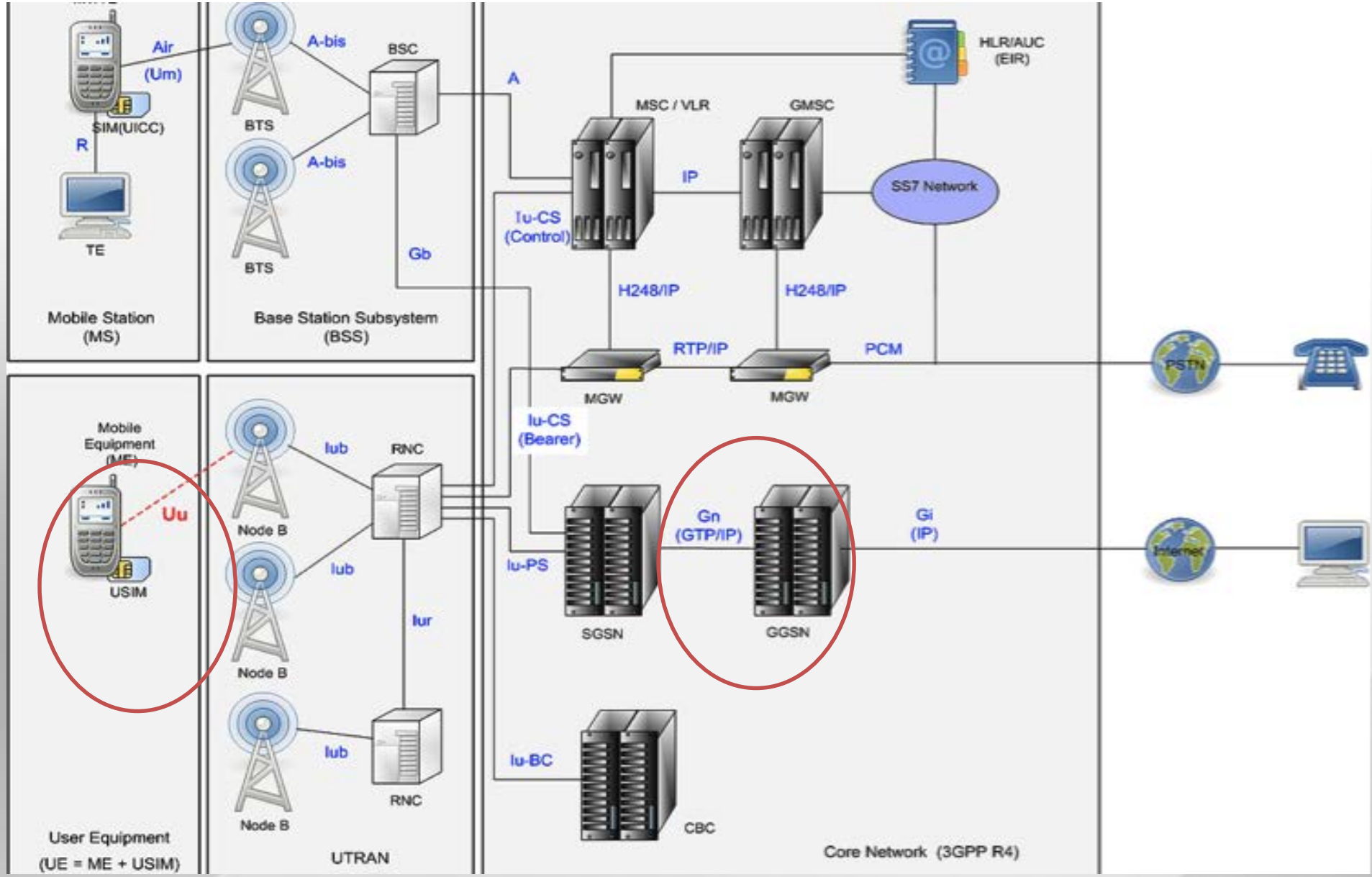
这是最坏的时代，亦是最好的时代

PC恶意代码发展至今，已经形成了总计几十万个病毒家族、近四百万独立命名和以亿计算的实体样本。

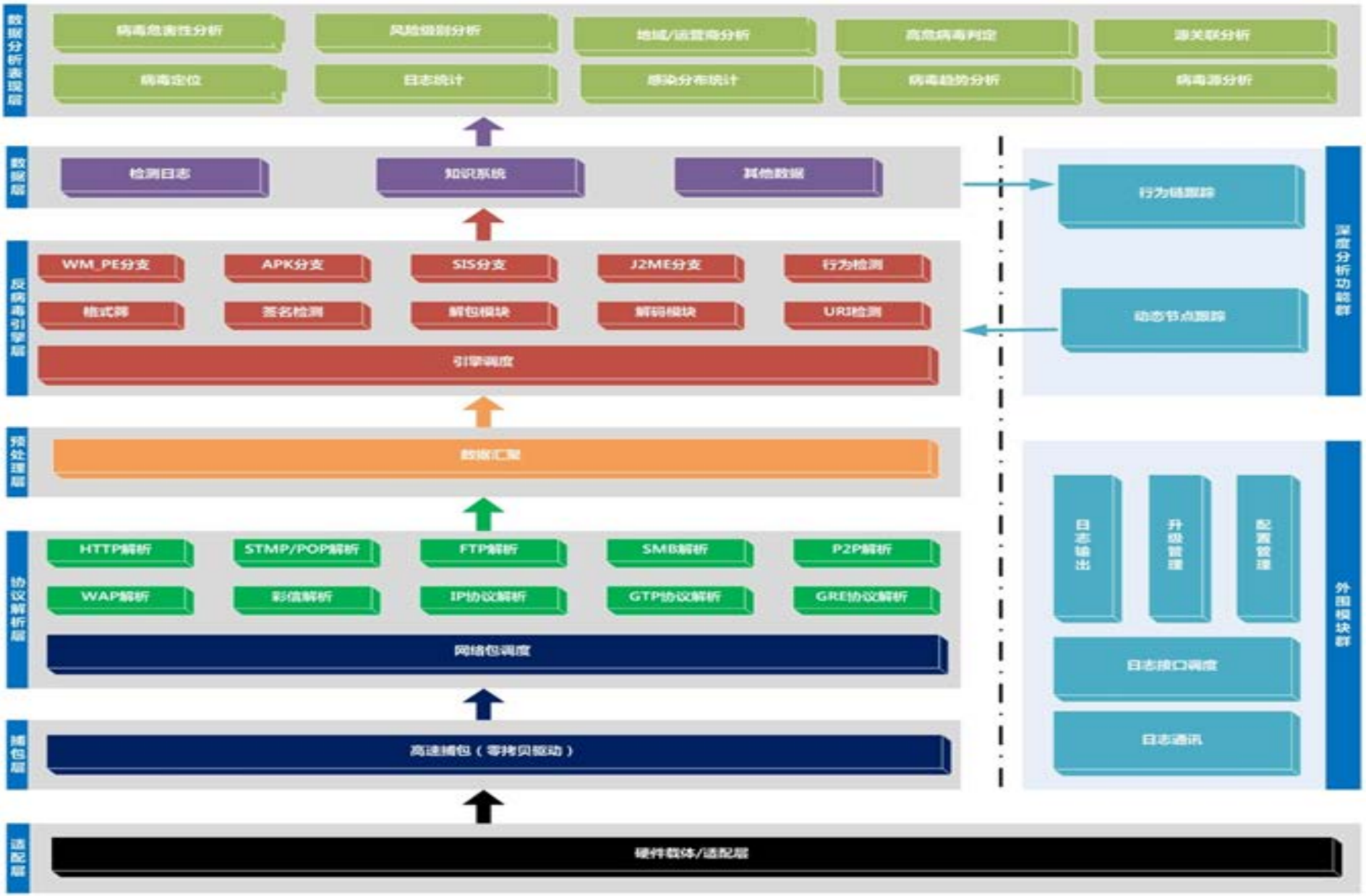


当前具有实际活性的手机恶意代码家族数还不过百，种类数不过万，实体样本数仍为万数量级。

移动用户与PC用户的不同



局端大有可为


数据分析表现层
病毒危害性分析
风险级别分析
地域/运营商分析
高危病毒判定
源关联分析
病毒定位
日志统计
感染分布统计
病毒趋势分析
病毒源分析
数据层
检测日志
知识系统
其他数据
反病毒引擎层
WM_PE分支
APK分支
SIS分支
J2ME分支
行为检测
格式等
签名检测
解包模块
解码模块
URI检测
引擎调度
预处理层
数据汇聚
协议解析层
HTTP解析
STMP/POP解析
FTP解析
SMB解析
P2P解析
WAP解析
彩信解析
IP协议解析
GTP协议解析
GRE协议解析
网络包调度
捕包层
高速捕包（零拷贝驱动）
适配层
硬件载体/适配层
行为链跟踪
动态节点跟踪
深度分析功能群
日志输出
升级管理
配置管理
日志接口调度
日志通讯
外围模块群

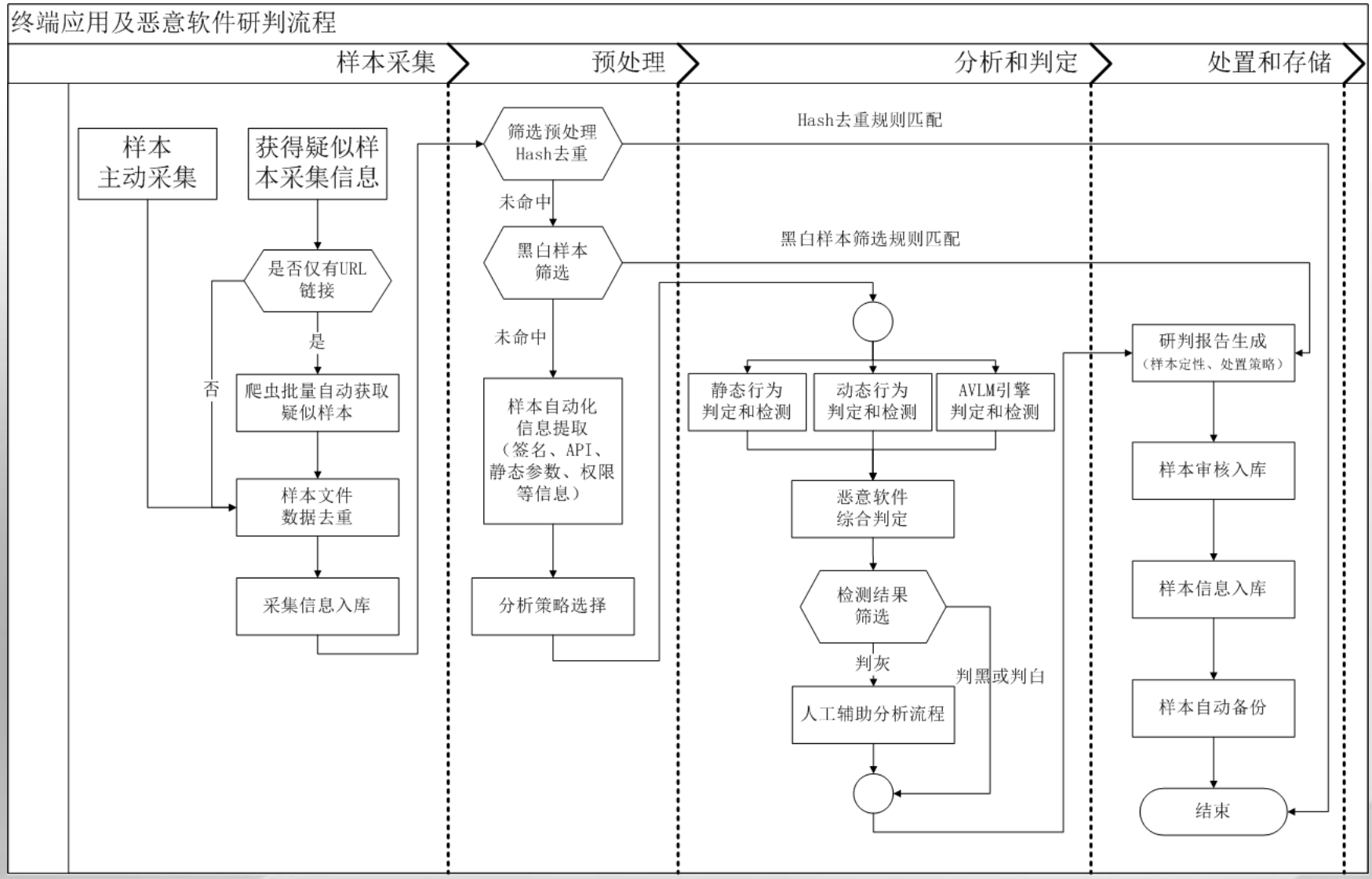
局端疫情呈现


首页
病毒监测
统计报表
系统配置
地区监测汇总
实时病毒监测
病毒预警信息
Top10病毒
FusionCharts v3.2 Evaluation
出现频度最高的10个病毒
2011-08-19
20
14
8
6
6
5
3
2
Trojan/Android.MainService.a
Trojan/Symbian.AhElla.a
Trojan/Symbian.DumusicPlay.a
Trojan/Symbian.SysSer.a
Trojan/Symbian.MdiMServer.a
Trojan/Android.Kongfu.a
Trojan/Android.Deduction.a
Trojan/Symbian.NokConsult.a
时间
病毒名
病毒类型
危害级别
感染手机号
用户手机系统
URL/IP
详细


首页
病毒监测
统计报表
系统配置
病毒分类统计
病毒事件统计
2011-08-19
SUBMIT
FusionCharts v3.2 Evaluation
病毒协议统计
2011-08-19
HTTP
FusionCharts v3.2 Evaluation
监测类型统计
2011-08-19
FusionCharts v3.2 Evaluation
病毒分类小时统计
2011-08-19


首页
病毒监测
统计报表
系统配置
地区监测汇总
实时病毒监测
病毒预警信息
Top10病毒
FusionCharts v3.2 Evaluation
病毒趋势统计
2011-07 ~ 2011-08
2011-08
2011-07
病毒名
病毒类型
危害级别
检出次数
Trojan/Android.MainService.a
Trojan/Symbian.AhElla.a
Trojan/Symbian.DumusicPlay.a
Trojan/Symbian.MdiMServer.a
Trojan/Symbian.SysSer.a
Trojan/Android.Kongfu.a
Trojan/Android.Deduction.a
Trojan/Symbian.NokConsult.a

后端研判

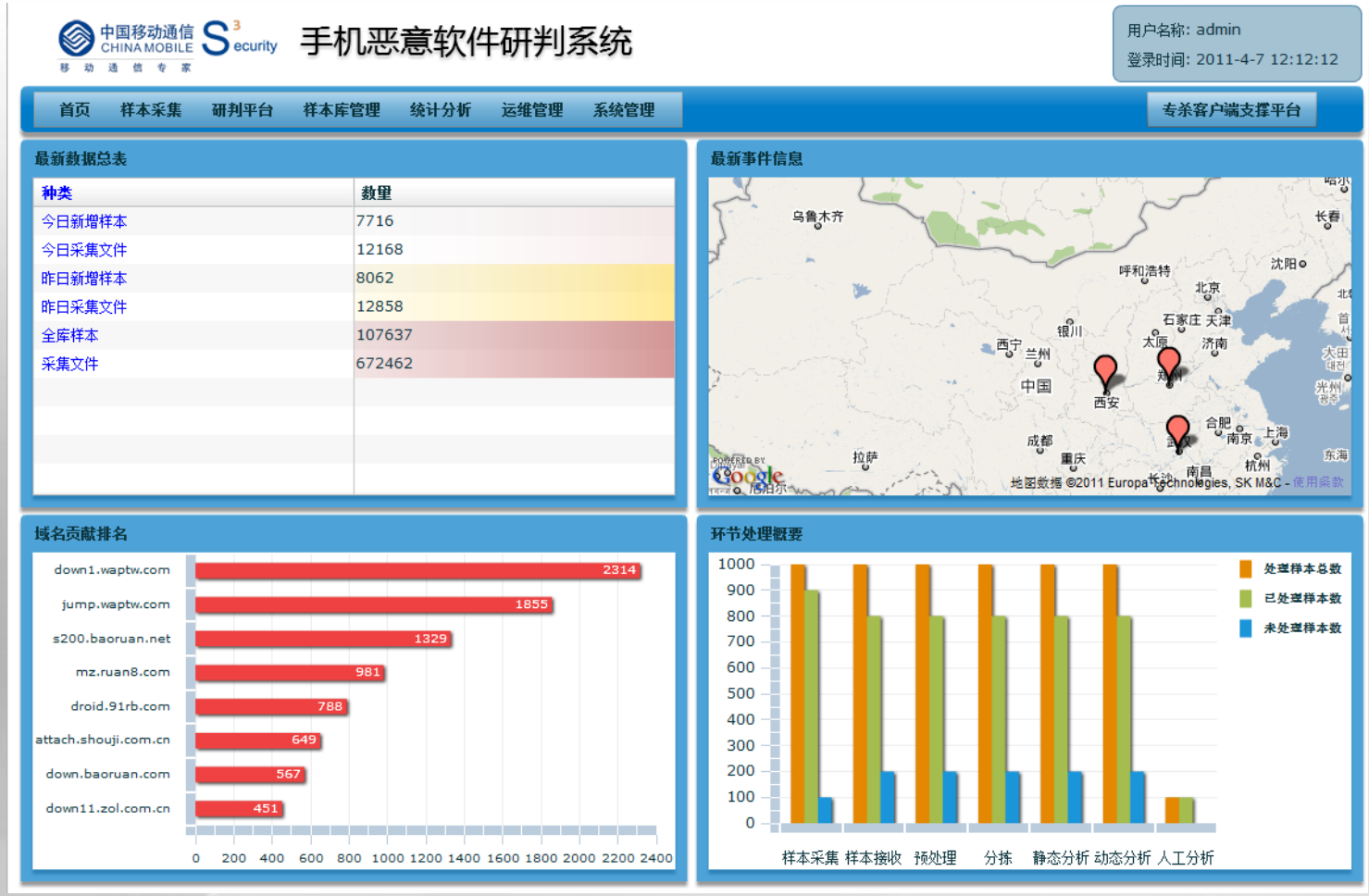

终端应用及恶意软件研判流程
样本采集
预处理
分析和判定
处置和存储
样本
主动采集
获得疑似样
本采集信息
是否仅有URL
链接
是
否
爬虫批量自动获取
疑似样本
样本文件
数据去重
采集信息入库
筛选预处理
Hash去重
Hash去重规则匹配
未命中
黑白样本
筛选
黑白样本筛选规则匹配
未命中
样本自动化
信息提取
（签名、API、
静态参数、权限
等信息）
分析策略选择
静态行为
判定和检测
动态行为
判定和检测
AVLM引擎
判定和检测
恶意软件
综合判定
检测结果
筛选
判灰
判黑或判白
人工辅助分析流程
研判报告生成
（样本定性、处置策略）
样本审核入库
样本信息入库
样本自动备份
结束

后端研判（能力）

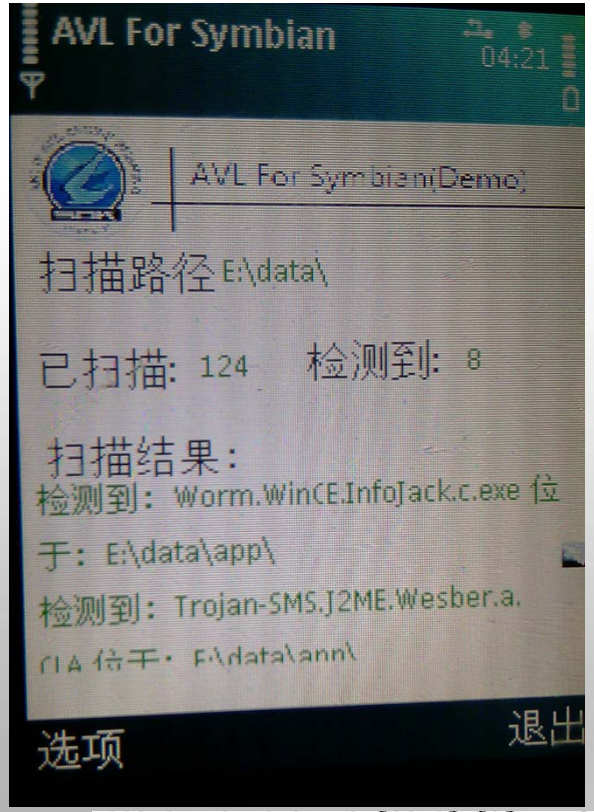
```
<?xml version="1.0"?>
<root>
  <MSampleBasic>
    <SourceID>0</SourceID>
    <Source/>
    <FileFormatID>7</FileFormatID>
    <FileFormatDes>ANDROID APK</FileFormatDes>
    <HASH>
      <MD5>377002954FC3D6858CDD61611BBA83EB</MD5>
      <SHA1>A3D6A1DFF4490B4C3CD46C5B782B51E72EFCD8D1</SHA1>
      <CRC32>9B4BCD64</CRC32>
    </HASH>
  </MSampleBasic>
  <MPackage>
    <APK>
      <EXFILE>
        <HASH>
          <MD5>CB19731DA1CEFDAF48AB27D87EC8BC3D</MD5>
        </HASH>
        <TYPEID>40</TYPEID>
      </EXFILE>
      <EXFILE>
        <HASH>
          <MD5>5E3375778BBFB4BC798FD3E155D482C9</MD5>
        </HASH>
        <TYPEID>41</TYPEID>
      </EXFILE>
      <EXFILE>
        <HASH>
          <MD5>A40A545B5F91F017CF940FC80E66ECE3</MD5>
        </HASH>
```

```
<?xml version="1.0" encoding="utf-8"?>
<root>
  <MSampleBasic>
    <SourceID>1</SourceID>
    <Source>377002954FC3D6858CDD61611BBA83EB</Source>
    <FileFormatID>6</FileFormatID>
    <FileFormatDes>ANDROID DEX</FileFormatDes>
    <HASH>
      <MD5>B44988D72EAE7976C311952CF856FE85</MD5>
      <SHA1>4E5BB32A9F5DA4FFE7941CE3341301D40FC858DE</SHA1>
      <CRC32>06DEB773</CRC32>
    </HASH>
  </MSampleBasic>
  <DEXFILE>
    <DefClasses>
      <Class>
        <Name>Lcom/android/AndroidActionReceiver;</Name>
        <DirMethod>&lt;init&gt;</DirMethod>
        <VirMethod>onReceive</VirMethod>
      </Class>
      <Class>
        <Name>Lcom/android/APKInstaller;</Name>
        <DirMethod>&lt;init&gt;</DirMethod>
        <DirMethod>exec</DirMethod>
        <DirMethod>install</DirMethod>
      </Class>
      <Class>
        <Name>Lcom/android/Base64;</Name>
        <DirMethod>&lt;init&gt;</DirMethod>
        <DirMethod>encode</DirMethod>
        <DirMethod>encode</DirMethod>
        <DirMethod>splitLines</DirMethod>
        <DirMethod>zeroPad</DirMethod>
      </Class>
```

⊙ 系统总揽


中国移动通信 CHINA MOBILE
Security
手机恶意软件研判系统
用户名称: admin
登录时间: 2011-4-7 12:12:12
首页
样本采集
研判平台
样本库管理
统计分析
运维管理
系统管理
专杀客户端支撑平台
最新数据总表
种类
数量
今日新增样本 7716
今日采集文件 12168
昨日新增样本 8062
昨日采集文件 12858
全库样本 107637
采集文件 672462
最新事件信息
乌鲁木齐
呼和浩特
北京
沈阳
长春
银川
西宁
兰州
中国
西安
石家庄
天津
太原
济南
郑州
合肥
南京
上海
成都
重庆
拉萨
南昌
杭州
地图数据 ©2011 Europa Technologies, SK M&C - 使用条款
域名贡献排名
down1.waptw.com 2314
jump.waptw.com 1855
s200.baoruan.net 1329
mz.ruan8.com 981
droid.91rb.com 788
attach.shouji.com.cn 649
down.baoruan.com 567
down11.zol.com.cn 451
0 200 400 600 800 1000 1200 1400 1600 1800 2000 2200 2400
环节处理概要
1000 900 800 700 600 500 400 300 200 100 0
处理样本总数
已处理样本数
未处理样本数
样本采集 样本接收 预处理 分拣 静态分析 动态分析 人工分析

终端亦有可作为




```
2008-04-23 10:32:19 [8620] [9] DEBUG:    data: 89 53 01 40 c1 2a 11 1a 9d 34 de 03 7d 0c 08 c6   .S.@.*...4..}...
2008-04-23 10:32:19 [8620] [9] DEBUG:    data: 82 44 9c 24 7c e2 44 00 60 b0 8a c4 25 27 9d 00   .D.$|.D.`...%'..
2008-04-23 10:32:19 [8620] [9] DEBUG:    data: 76 76 2e 02 90 05 89 38 91 f8 c4 49 00 a0 65 b5   vv.....8...I..e.
2008-04-23 10:32:19 [8620] [9] DEBUG:    data: ca 3c a6 01 b0 01 a4 01 cc 01 81 90 07 37 00 10   .<...........7..
2008-04-23 10:32:19 [8620] [9] DEBUG:    data: f5 f0 06 40 46 1e 41 00 90 00 de 00 e4 e4 03 08   ...@F.A.........
2008-04-23 10:32:19 [8620] [9] DEBUG:    data: c0 18 95 1b 79 c0 03 48 a3 fa d1 2f ff ff ff ff   ....y..H.../....
2008-04-23 10:32:19 [8620] [9] DEBUG:    data: a2 01                                             ..
2008-04-23 10:32:19 [8620] [9] DEBUG: Octet string dump ends.
FOUND virus [Trojan.SymbOS.RommWar.a], antiy labs
2008-04-23 10:32:19 [8620] [9] ERROR: Couldn't fetch <http://10.0.19.118/Stoper.sis>
2008-04-23 10:32:19 [8620] [7] ERROR: WSP: HTTP lookup failed, oops.
2008-04-23 10:32:19 [8620] [1] DEBUG: WSP: machine 0x81e6c38, state CONNECTED, event S-MethodResult.req
```

移动反恶意代码支撑体系

监控和捕获

- 移动终端反恶意代码事件监控和捕获
- Gn口接入VDS设备（事件发现、样本捕获）

分析和研判

- 恶意代码采集
- 恶意代码自动化分析和定性
- 恶意代码处置策略生成

响应和处置

- 网络处置策略
- 移动终端专杀引擎支持

产业链条变化（昨天）

用户通道

Android Market

运营商

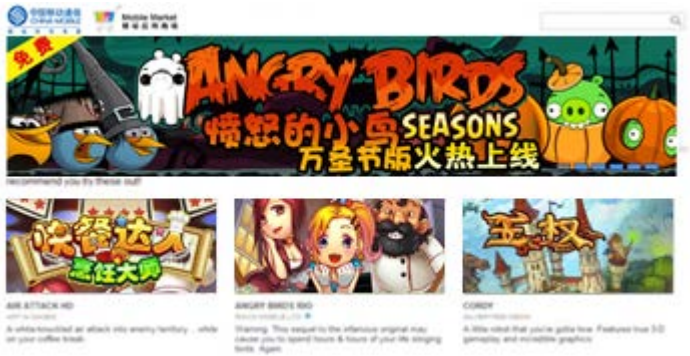
Google

消费者

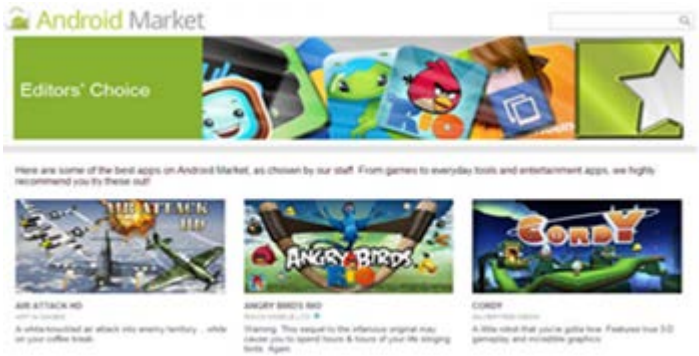
智能机厂商

手机分销商

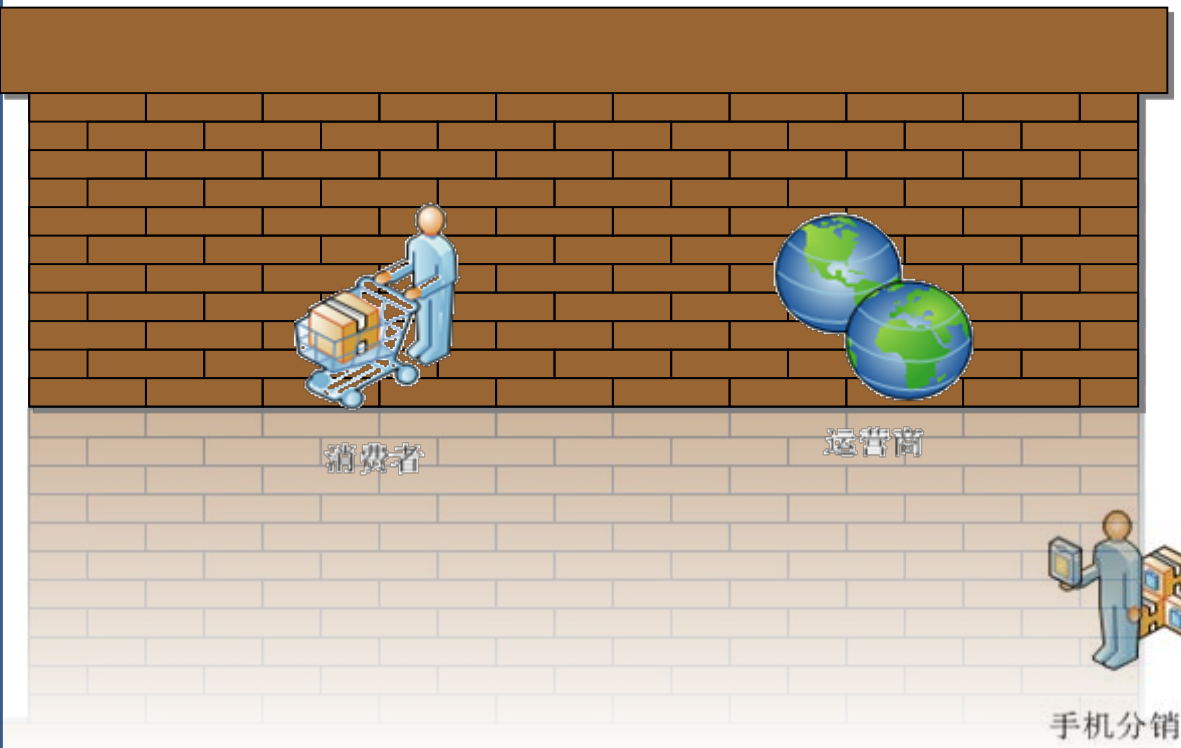
产业链条变化（明天）



中国移动MM商城



Android Market



Google

智能机厂商

结束语

- 恶意代码在蔓延至移动平台后，即是对安全现状的巨大挑战，也是建设全新安全境界的巨大机遇。由于与固网的差异，传统安全厂商的角色将在移动安全体系中逐步成为配角的角色，运营商必然为造就自身的安全新境界起到主导作用。
- 安天愿能在这种变革中助动一点自己的力量。

创造就是我们的脚步

- 谢谢各位尊敬的专家领导。

- seak@antiy.com