乌云笼罩下的互联网金融

赖东方
任职：绿盟科技高级安全顾问
深圳互联网金融安全研究负责人
NSTRT安全团队核心成员
专长：黑客攻防、代码审计、开发安全咨询

黑客篡改用户账号盗取1600万

7月24日9时，深圳市公安局反信息诈骗咨询专线接到一事主报案称：其经营一家互联网公司，7月23下午突然接到客户询问，称有多笔资金未按时到帐。经公司财务核对，需向客户支付的款项早已汇出。经过询问，事主发现有8个商户帐户资料被嫌疑人通过网络入侵篡改成嫌疑人银行账号，该公司财务向8个陌生账号汇去款项共计1600万元。

深圳警方：一事主遇黑客

gd.qq.com/a/20150729/045982.htm?ADUIN=540010550&ADSESSION=1438165277&ADTAG

娱乐 房产 汽车 财经 数码 时尚 旅游 美食 健康 社区 更多

深圳警方：一事主遇黑客入侵转账1600万

政务聚焦 | 腾讯大粤网 2015-07-29 17:47 | 我要分享 107

[摘要]近日，深圳市公安局反信息诈骗中心接到报案不到15分钟，成功拦下了被骗款共计1456万元，帮助事主挽回了大部分被骗资金。

近日，深圳市公安局反信息诈骗中心接到报案不到15分钟，成功拦下了被骗款共计1456万元，帮助事主挽回了大部分被骗资金。

7月24日9时许，深圳市公安局反信息诈骗咨询专线接到一事主报案称：其经营一家互联网科技公司，7月23下午突然接到客户询问，称有多笔资金未按时到帐。经公司财务核对，需向客户支付的款项早已汇出。经过询问，事主发现有8个商户帐户资料被嫌疑人通过网络

www.freebuf.com/news/67162.html

FREEBUF

香港中银、东亚银行遭遇DDoS攻击，攻击者勒索比特币

fber 2015-05-13 共16485人围观，发现5个不明物体 资讯

- 有人说，企业分为两种
  1. 知道自己被黑的
  2. 不知道自己被黑的

- 还有人说应该这样分
  1. 值得被黑的
  2. 不值得被黑的

安全风险：从漏洞说起

WooYun.org

NSFOCUS

2014 绿盟科技互联网金融安全报告

2014 Internet Finance Security Report

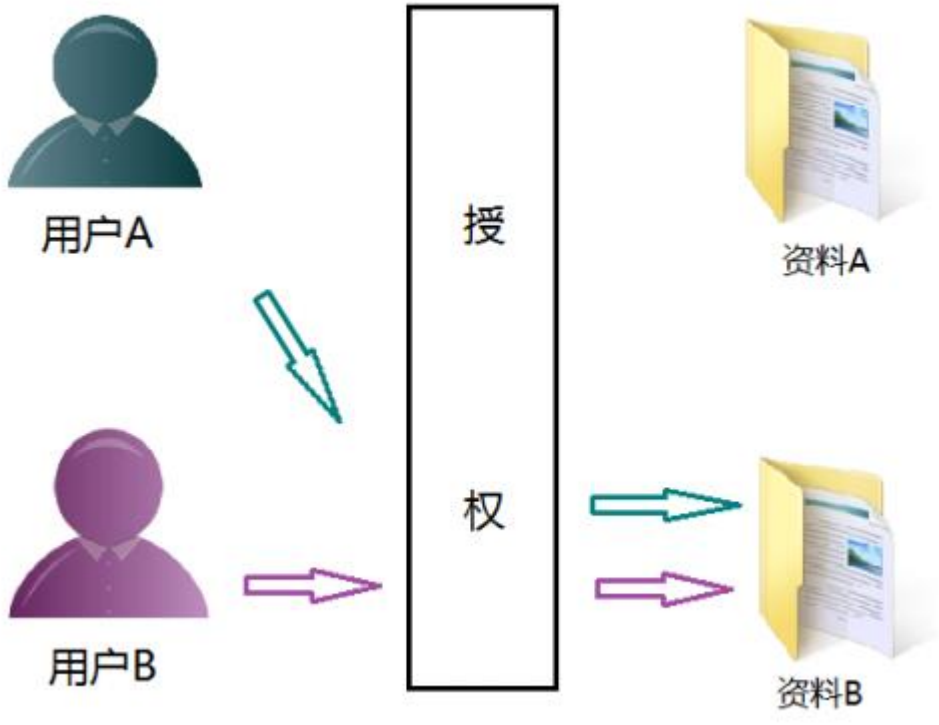
安全漏洞

按照漏洞类型的分类和数量统计，我们得出了最常见的 12 种漏洞类型，漏洞类型按照数量和风险值进行叠加后排序，得出如下漏洞数据分布：

互联网金融业务设计缺陷统计

平行越权查询	29%
平行越权修改	20%
垂直越权操作	7%
批量注册	7%
任意用户密码修改	7%
密码暴力破解	5%
平行越权下载	5%
身份伪造漏洞	2%
退出功能失效问题	2%
任意邮箱注册漏洞	2%
邮箱激活功能漏洞	2%
刷积分漏洞	2%
提现密码暴力破解	2%
邀请码暴力破解	2%
一号多户问题	2%
其它	4%

- 为何关于业务设计缺陷漏洞占比较高？
  - 传统漏洞的比重下降
  - 无法贴近业务场景是Web防护设备的短板
  - 业务漏洞涉及商业利益，攻击者感兴趣
    - 获取敏感数据
    - 盗取账号
    - 刷钱
    - 刷积分
    - 诈骗



薅羊毛，助你踏出理财第一步!

薅羊毛
haoyangmao8.com

深圳南山二手房 | 我想贷款1万 | 沙井房价
深圳二手房 | 开心贷 | 深圳沙井房价 | 比亚迪新车价
沙井二手房 | 银行卡代办 | 新秀丽拉杆箱 | 无抵押个

你我贷 投1元送体验金 5天收益13.5元 可提现

你我贷的体验金活动，之前举办过两期，信誉一直不错，这次是第三期，和之前一样，微信扫描二维码，参加

聚爱财 注册投资100元3天标 赚24元 可提现

通过玩赚乐注册聚爱财，点击"试试手气"，一般都可以抽到8000以上体验

推荐新闻

满亿宝 完成注册绑卡 送7.5元 可直接提现

通过有赚网注册满亿宝，注册绑卡，送7.5元，审核通过后，赚网提现，没做过的朋友，可以去看看。活动时间：短期一

鑫合汇 注册投资100元2天标 送13.2元 可提现

鑫合汇和聚享游合作的活动，通过聚享游，注册鑫合汇，投的新手标，聚享游送13.2元，审核通过后，可提现，我上个

短信费是怎样用完的？


手机炸弹-短信攻击器
代理ip地址
链接速度
手机号码：
攻击次数：
代理地址：
开始获取代理
停止获取代理
开始攻击
停止攻击
联系QQ：530137417
BY：风雨无阻
警告！此软件不间断大量发送短信，可倒是对方手机卡死，以及电量耗尽，同时对短信平台造成资金损失。请谨慎使用！！！！
上面输入手机号，下面输入攻击次数。然后点击 开始攻击

短信费是怎样用完的？


phone
第 45 条，共 228 条
Message&xajaxargs%5B%5D=%3Cxjxquery%3E%3Cq%3Emobile%3Dd$%3C
axr=1363500615734", _
"https://passport.jd.com/emReg/sendMobileCode?mobile=%phone_number%&r=0.9010949897739119", _
"https://member.suning.com/emall/SNCellPhoneRegisterCmd?actionType=reSendValCode&logonId=%phone_nu
L=SNUserRegisterComfirmView&_=1363500974671", _
"http://account.iqiyi.com/security/secret/mobile/adm.action?time=1363501090218&mobile=%phone_numbe
"http://www.skywldh.com/registerForMobileForCode.act?mobileNo=%phone_number%&smSecurityCode=", _
"http://wap.skywldh.com/index.php?register&flag=flag&phone=%phone_number%&mss=on", _
"http://zg51.net/web/customer/forgetPwd_up.asp?customermobile=%phone_number%&verify=01f735f97f1af9
codeflag=1", _
"http://www.qqvoice.com/free/getExpCode.do?_isAjaxRequest=true&phonemail=%phone_number%&type=1&ran
, _
"http://www.feiin.com/findAccountInfoByAccount.act?mobile=%phone_number%", _
"http://wap.feiin.cn/index.php?register?phone=%phone_number%", _
"http://www.feiin.cn/bindMobileCode.act?account=%phone_number%&quhao=0086", _
"http://www.139talk.com/user/regnum.html?phone=%phone_number%&type=1&key=ofoedsv0oeg6aari1m3ig0nsc
"http://www.139talk.com/invite/invitesms.html?phone=%phone_number%&key=ofoedsv0oeg6aari1m3ig0nsc5"
"http://www.139talk.com/invite/regnum.html?phone=%phone_number%&type=1&key=ofoedsv0oeg6aari1m3ig0n

命运多舛的安全功能：短信校验

- 手机短信：经常带来安全风险的安全功能
  - 短信炸弹
  - 短信钓鱼（短信内容操纵、伪基站）
  - 短信验证码破解
  - 短信验证绕过
  - 短信重复利用
  - ……

安全功能之重灾区：登录功能

- ✓账户名猜测
- ✓密码破解
- ✓利用第三方账号
- ✓注册覆盖
- ✓任意用户密码重置
- ✓短信校验绕过
- ✓弱口令
- ✓登录流程绕过
- ✓批量账号锁定
- ✓信息泄露
- ✓传输劫持
- ✓XSS钓鱼

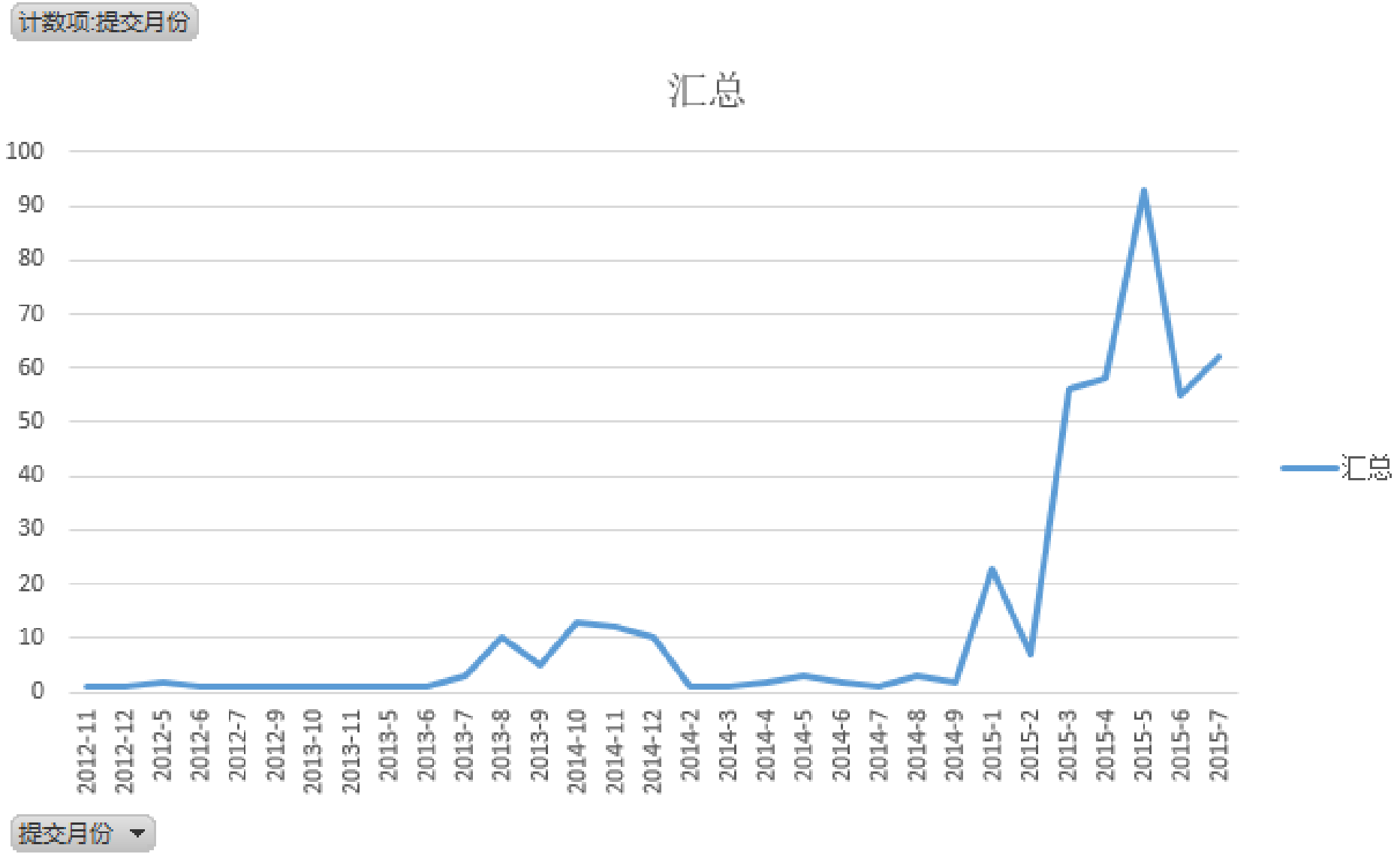
WooYun.org

互联网厂商： 网络边界/基础架构 系统运维/服务设置 应用程序/应用漏洞 业务安全/运营风险 安全事件/安全情报

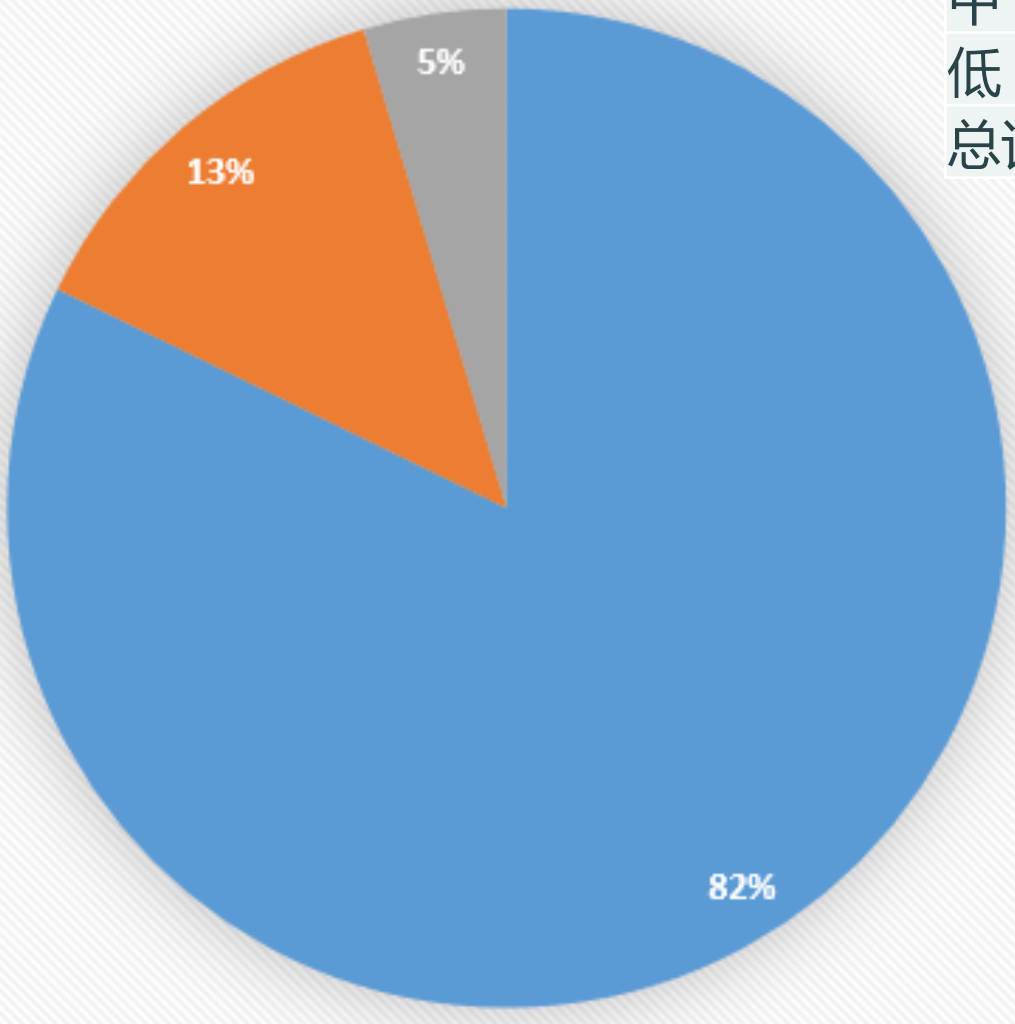
传统应用厂商： 网络设备/硬件设施 操作系统/系统服务 基础组件/开发框架 建站软件/web应用 常用软件/客户端应用

提交日期	漏洞名称
2015-08-07	国美某系统沦陷涉及全国运单信息
2015-08-07	深圳某宽带系统SQL注射（泄露几百万用户套餐信息+宽带充值业务记录）
2015-08-07	8个省份"工农建商"等银行报修系统后台缺陷可查设备参数等内容工程师信息等（各个地区支行IP网关信息泄漏）
2015-08-07	北斗卫星某市车辆定位监控系统后台缺陷泄漏（公司/出租/敏感部门等信息以及个人数据）
2015-08-07	游奇网络半夜捣入后台(可封禁100多万用户/官方任意消息推送/屌丝福音之礼包随意发和土豪账号随意登陆)

每个月出现的安全漏洞数量

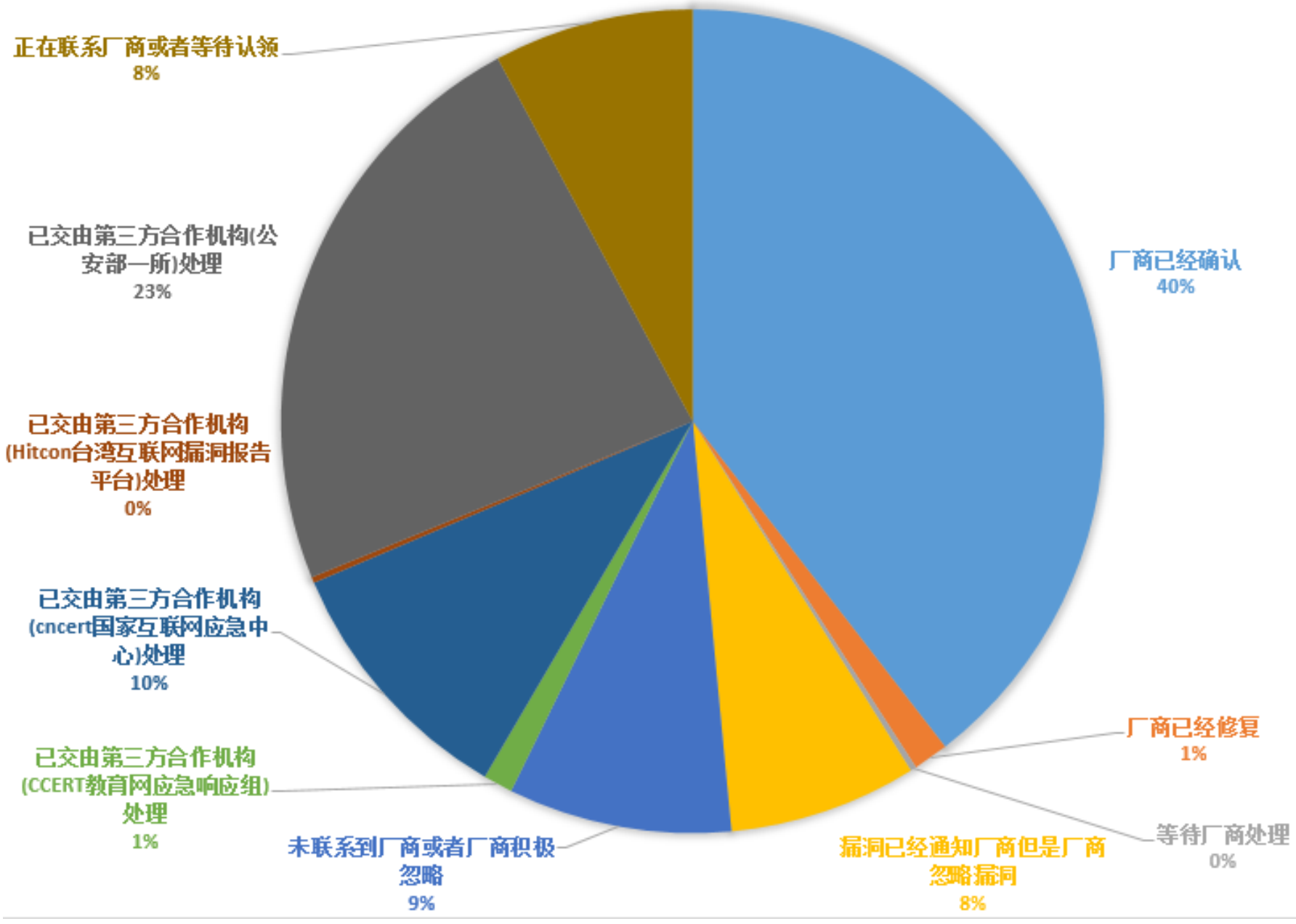


高风险漏洞占82%



危害等级	汇总
高	356
中	57
低	20
总计	433

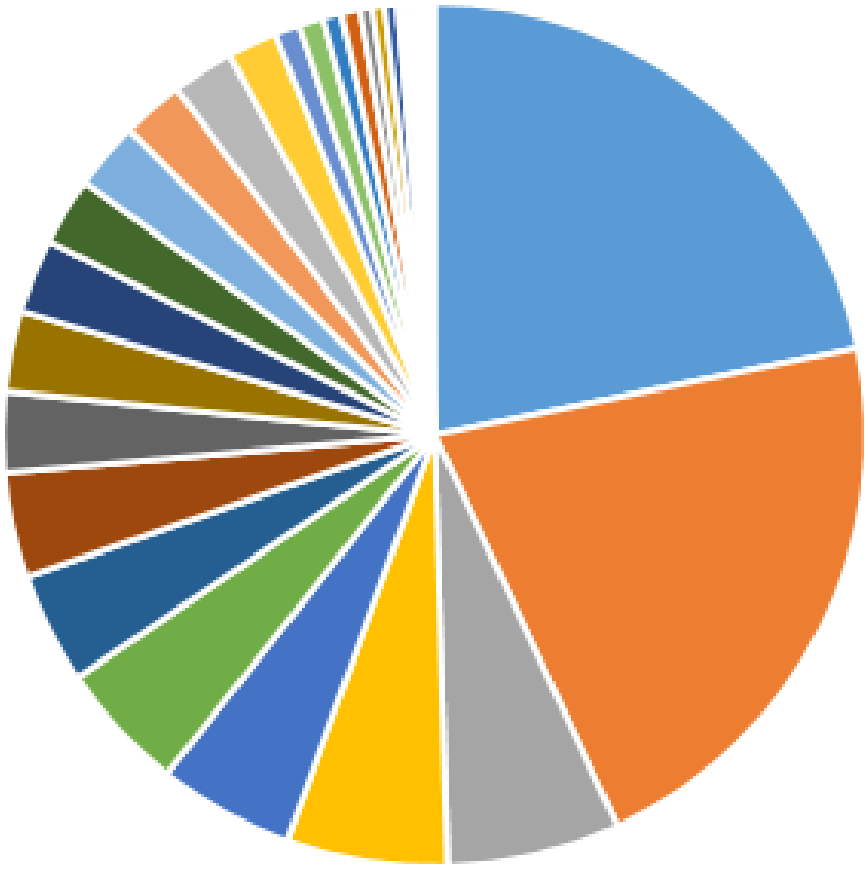
漏洞状态


正在联系厂商或者等待认领
8%
已交由第三方合作机构(公安部一所)处理
23%
已交由第三方合作机构(Hitcon台湾互联网漏洞报告平台)处理
0%
已交由第三方合作机构(cncert国家互联网应急中心)处理
10%
已交由第三方合作机构(CCERT教育网应急响应组)处理
1%
未联系到厂商或者厂商积极忽略
9%
漏洞已经通知厂商但是厂商忽略漏洞
8%
等待厂商处理
0%
厂商已经修复
1%
厂商已经确认
40%

厂商确认只占40%

漏洞状态	汇总
厂商已经确认	171
厂商已经修复	6
等待厂商处理	1
漏洞已经通知厂商但是厂商忽略漏洞	32
未联系到厂商或者厂商积极忽略	38
已交由第三方合作机构(CCERT教育网应急响应组)处理	5
已交由第三方合作机构(cncert国家互联网应急中心)处理	44
已交由第三方合作机构(Hitcon台湾互联网漏洞报告平台)处理	1
已交由第三方合作机构(公安部一所)处理	101
正在联系厂商或者等待认领	34
总计	433

漏洞类型排行



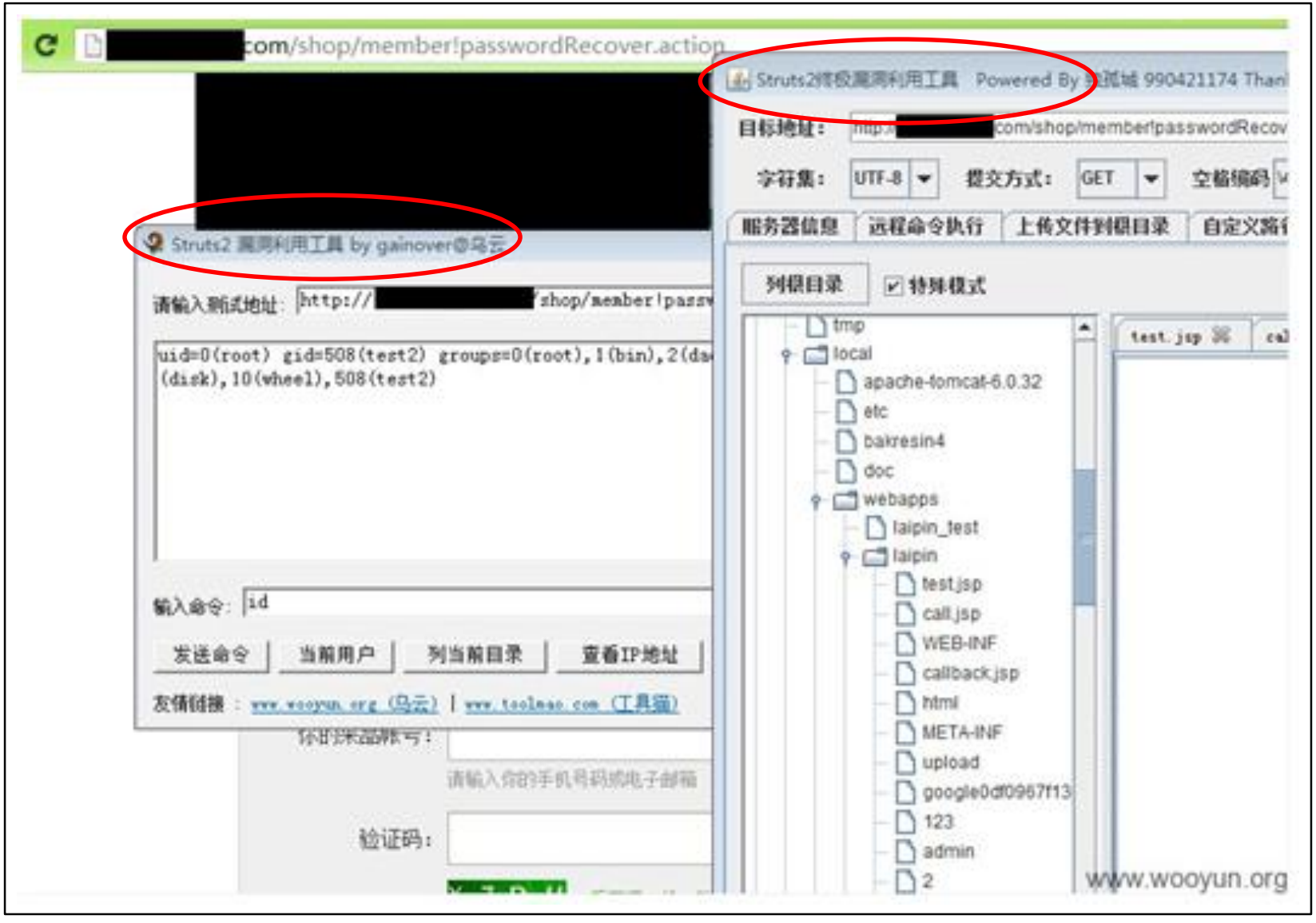
漏洞类型

- 设计缺陷/逻辑错误
- SQL注射漏洞
- 账户体系控制不严
- 敏感信息泄露
- 后台弱口令
- 命令执行
- 未授权访问/权限绕过
- 系统/服务运维配置不当
- 成功的入侵事件
- 重要敏感信息泄露
- 任意文件遍历/下载
- 文件上传导致任意代码执行
- 应用配置错误
- 服务弱口令
- xss跨站脚本攻击
- 内部绝密信息泄漏
- 系统/服务补丁不及时
- 设计错误/逻辑缺陷
- 用户资料大里泄漏
- 基础设施弱口令
- 默认配置不当
- 网络设计缺陷/逻辑错误
- 非授权访问/权限绕过
- 非授权访问/认证绕过
- CSRF

有时候，一个漏洞可以打死一片

开发框架风险：某网贷Struts2远程命令执行

- 某网贷网站struts2远程命令执行漏洞，轻松获得root权限



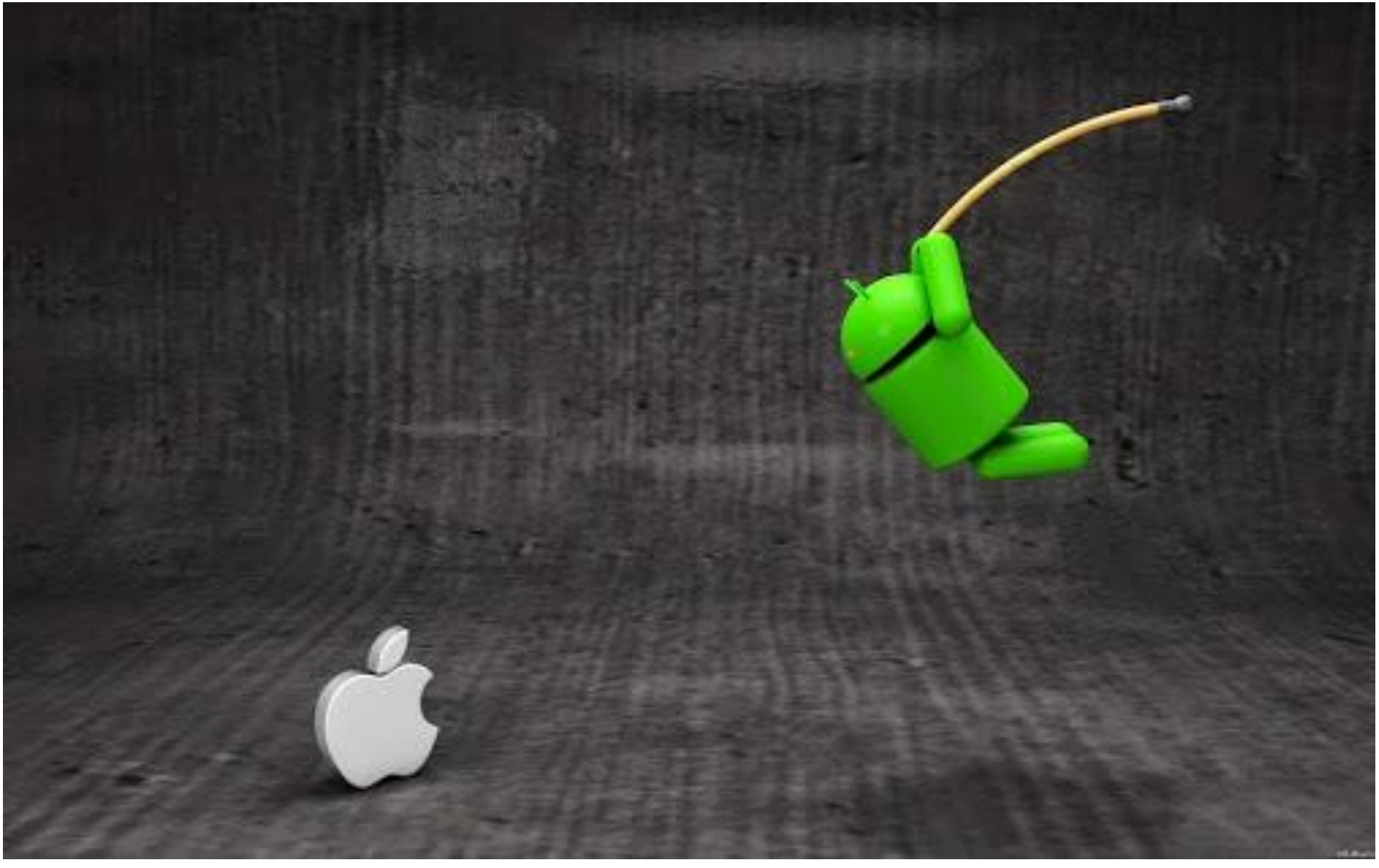
NSFOCUS

最新提交

提交日期	漏洞名称
2013-07-17	多玩多个分站远程命令执行漏洞
2013-07-17	百度某分站最新Struts命令执行漏洞
2013-07-17	土豆某后台struts2任意命令执行（E
2013-07-17	PHPCMS V9 鸡肋注射漏洞2
2013-07-17	网易某分站存在命令执行漏洞已执行
2013-07-17	百度某分站struts2命令执行漏洞（E
2013-07-17	PHPCMS V9 鸡肋注入漏洞
2013-07-17	淘宝某业务存在命令执行
2013-07-17	工信部备案查询系统struts2最新洞
2013-07-17	百度某分站最新Struts命令执行漏洞
2013-07-17	百度某业务命令执行
2013-07-17	腾讯某业务struts2命令执行
2013-07-17	京东商城几处struts2命令执行漏洞
2013-07-17	淘宝某分站最新Struts命令执行漏洞
2013-07-17	国美最新struts2命令执行漏洞
2013-07-17	淘宝某分站最新Struts命令执行漏洞

最新提交

提交日期	漏洞名称
2013-07-18	联众世界某分站Struts2命令执行漏洞(root权限可shell)
2013-07-18	人人网某站点Struts2命令执行漏洞
2013-07-18	中国移动struts2漏洞大礼包
2013-07-18	一个短信引发的xss挖出黑产网站
2013-07-18	天极传媒集团商场命令执行可拿shell
2013-07-18	中国电信某分站struts2命令执行
2013-07-18	某省特种设备安全工作专网源码备份泄漏致整个服务器沦陷
2013-07-18	中国科学院某分站struts2漏洞
2013-07-18	某市银行网站存在严重的上传漏洞导致全站沦陷
2013-07-18	库巴网struts2任意执行命令漏洞
2013-07-18	中国移动某分站存在st2远程执行命令漏洞
2013-07-18	天极网某子站漏洞可getshell
2013-07-17	中国银行某省分行信用卡网站任意执行命令
2013-07-17	中国民生银行信用卡商城命令执行漏洞
2013-07-17	京东商城销售联盟命令执行漏洞
2013-07-17	联通某站命令执行漏洞
2013-07-17	中国银联命令执行漏洞
2013-07-17	中国联通某分站struts命令执行
2013-07-17	京东某分站命令执行漏洞



手机App安全风险点

- 移动终端安全
  - 基础环境安全
    - 逆向分析/反编译
    - 进程注入
    - 键盘纪录
    - 屏幕截取
  - 数据安全
    - 客户端本地信息存储
    - 敏感信息输入保护
    - 敏感信息上传
    - 日志信息/调试信息
    - 内存敏感数据
    - 硬编码
  - 通讯安全
    - 通讯加密算法、强度
    - 客户端证书验证
  - 程序安全
    - 界面劫持
    - 调试接口
    - 组件权限暴漏
    - 第三方库安全
  - 交互端常规WEB安全
  - 交互端逻辑安全
  - 交互端业务安全

安全不是一个网站的事情

- 从脱库到撞库
  - 安全已经不是一个人的事
  - 也不是一个网站的事

12306信息泄露系撞库攻击，窃密者已被抓获（全文）

2014-12-26 02:19:43 来源: 21世纪经济报道(广州)

1193

中国铁路

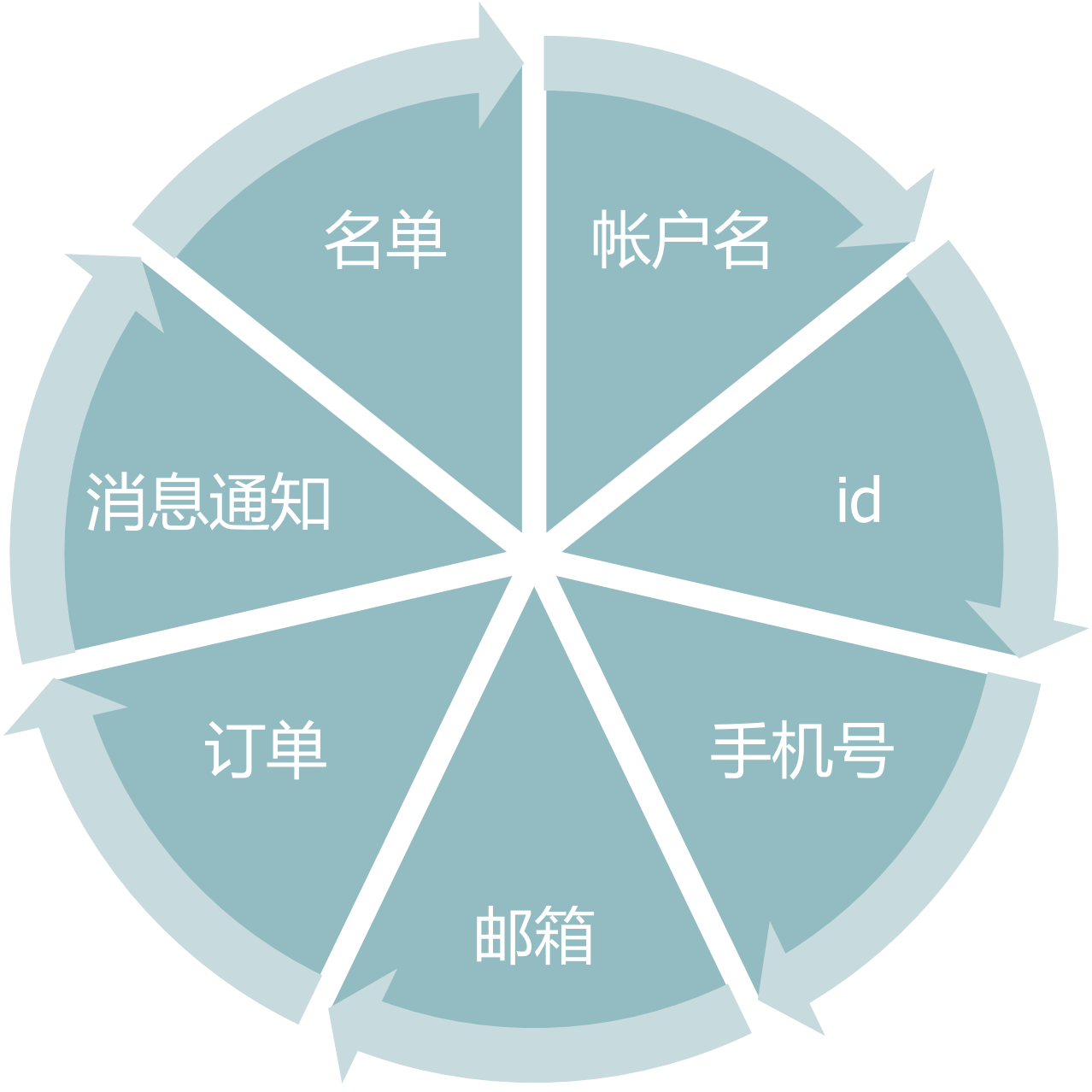
铁路公安机关
迅速抓获窃取他人电子信息的犯罪嫌疑人

铁路公安机关于2014年12月25日晚，将涉嫌窃取并泄露他人电子信息的犯罪嫌疑人抓获。经查，嫌疑人蒋某某、施某某通过收集互联网某游戏网站以及其他多个网站泄露的用户名加密码信息，尝试登陆其他网站进行“撞库”，非法获取用户的其他信息，并谋取非法利益。

坏人都是不讲原则的

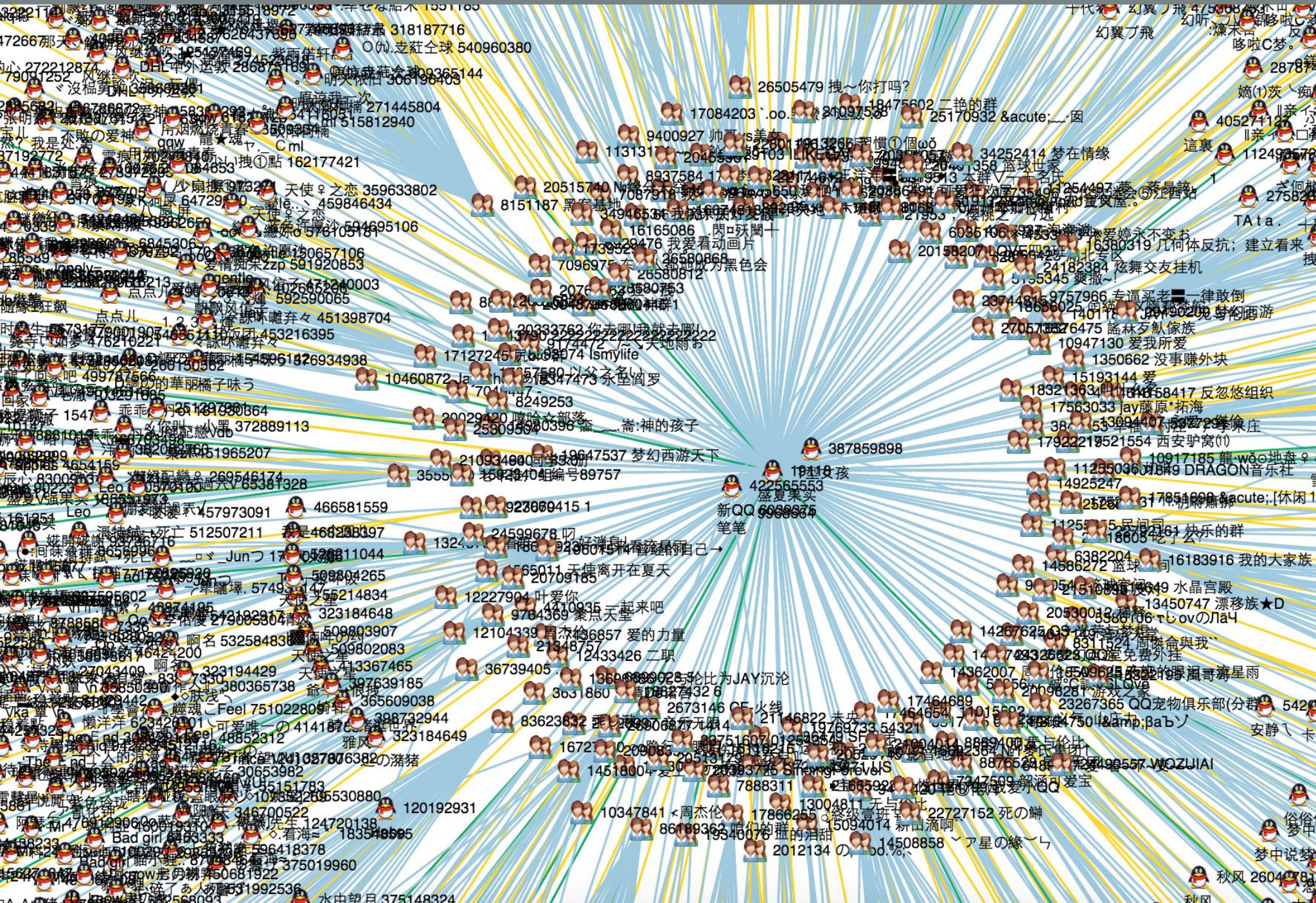
某黑客惨遭社工，银行卡手机金钱被盗

敏感数据相关风险



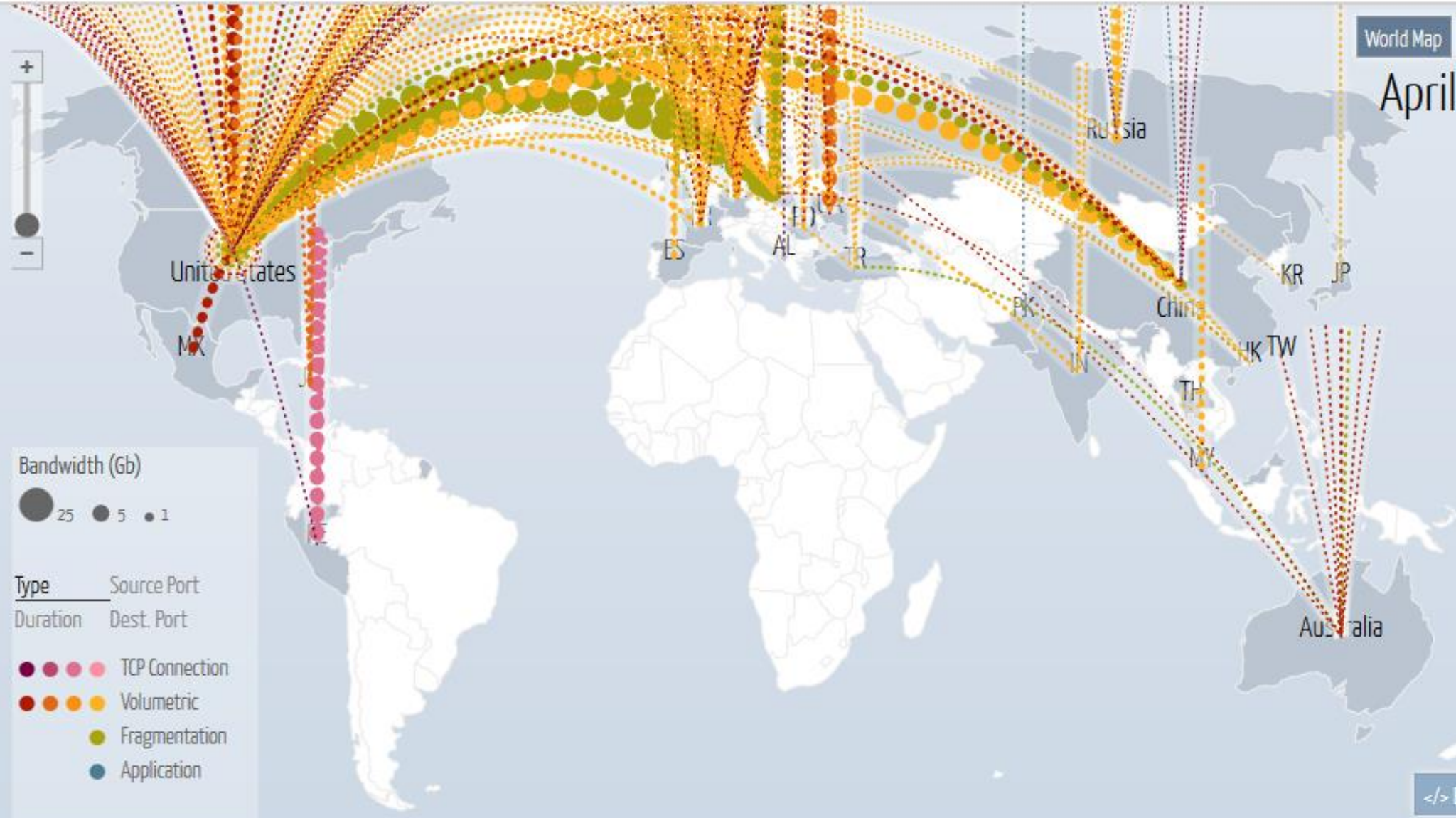
NSFOCUS

安全不是一个人的事情



Digital Attack Map

Top daily DDoS attacks worldwide



Type of Attack

between two countries

internal

Total Attack Bandwidth (All Countries), Gb

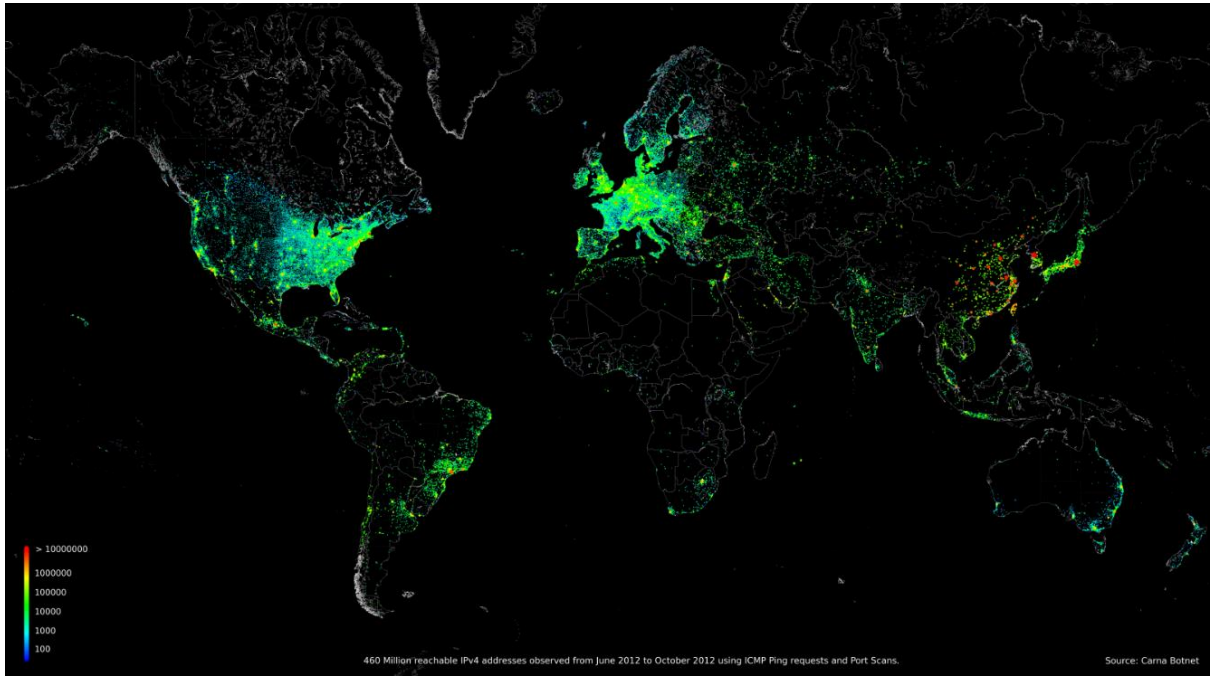
Dates are shown in GMT

Data shown represents the top ~2% of reported

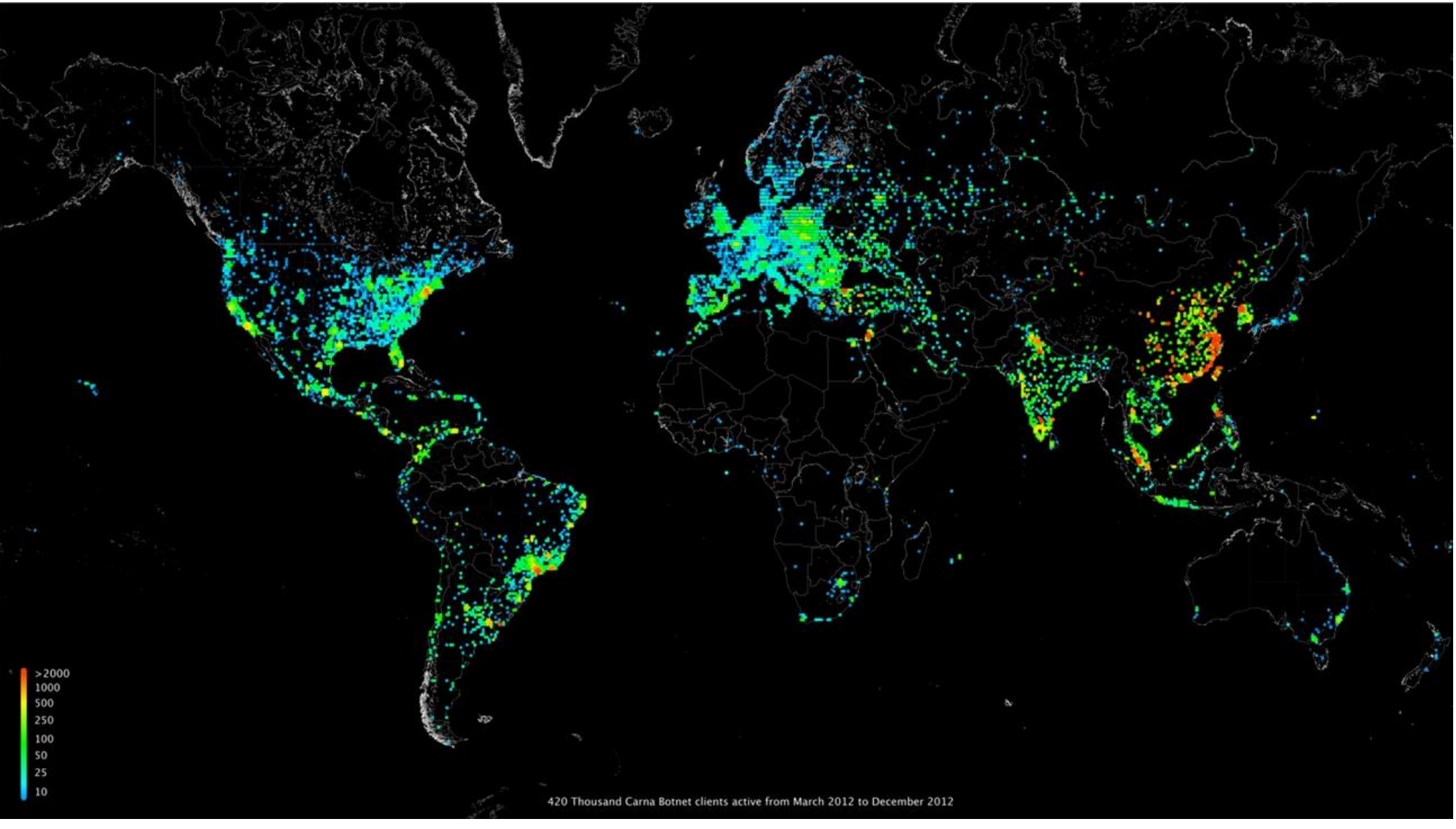
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS

研究人员利用42万僵尸节点创建全球IPv4地图

在IPv6即将大面积推广之际，某研究人员利用非常规手段，绘制了一份IPv4地球全图。此图造成了一个42万以上节点的僵尸网络。9TB的数据量已经开放下载。

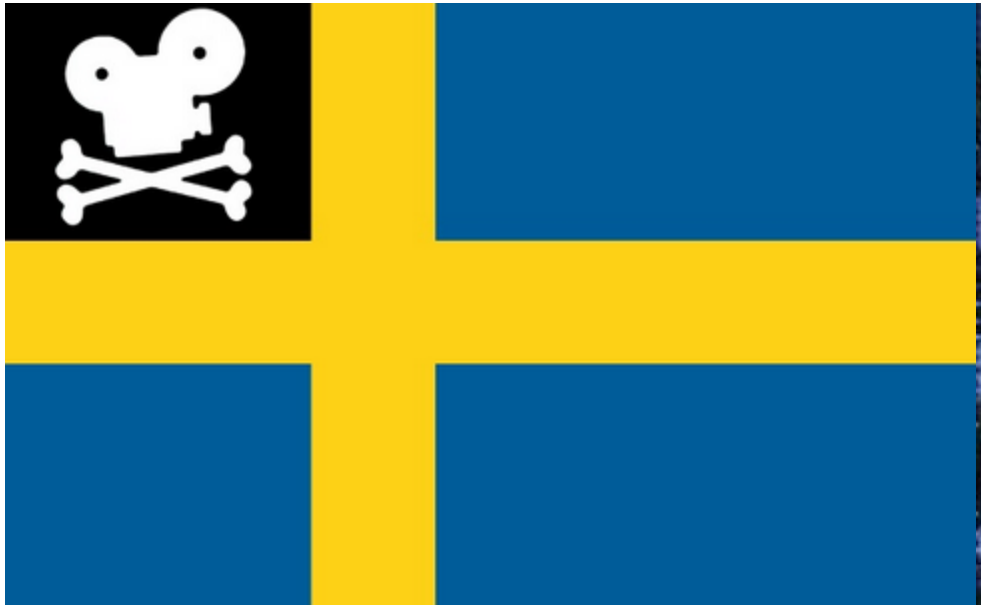


http://internetcensus2012.bitbucket.org/paper.html


>2000
1000
500
250
100
50
25
10
420 Thousand Carna Botnet clients active from March 2012 to December 2012

2013年：300Gbps！史上最大规模DDos攻击

反垃圾邮件组织Spamhaus 将荷兰网站托管公司 Cyberbunker 加入到垃圾邮件黑名单后，Spamhaus遭到了前所未有的DDOS攻击，这次攻击流量竟然超过了300Gbps，这是互联网史上最大规模的Ddos攻击。



CloudFlare公司的CEO Prince称，“我们发现在攻击者的武器库里充满了各种各样的攻击手段和工具”，Prince说，“好像一个攻击者俱乐部，俱乐部的成员们把所有的工具 都拿出来使用，一个不行换一个，直到有效为止”。

http://www.freebuf.com/news/8102.html

2014年：453.8G ！！

tech.sina.com.cn/it/2014-12-25/04199908780.shtml

阿里云称遭互联网史上最大规模DDoS攻击

2014年12月25日 04:19 京华时报 微博 收藏本文

京华时报讯(记者祝剑禾)昨天，阿里云计算发布声明称，12月20日-21日，部署在阿里云上的一家知名游戏公司，遭遇了全球互联网史上最大的一次DDoS攻击，攻击时长14个小时，攻击峰值流量达到每秒453.8G。

DDoS是DistributedDenialofService的缩写，翻译成中文是分布式拒绝服务。DDoS攻击就是指以分散攻击源来黑进指定网站的黑客方式。DDoS的攻击方式有很多种，最基本的攻击就是利用合理的服务请求来占用过多的服务器资源，从而使合法用户无法得到服务器响应。阿里云称，第一波DDoS共计从12月20日19点左右开始，一直持续到21日凌晨，第二天黑客又再次组织大规模攻击，共持续了14个小时。阿里云安全防护产品“云盾”，结合该游戏公司的“超级盾防火墙”，帮助用户成功抵御了此次攻击。

- 迄今为止，**全球互联网史上最大的一次DDoS攻击是去年底部署在阿里云的某游戏公司，攻击流量峰值达每秒453.8Gb**。目前而言，黑客甚至对攻击进行明码标价， **打1G的流量到一个网站一小时，只需50块钱**。

拒绝服务攻击现状

- 频率更高
- 产业链依然活跃
- 利益驱动明显
- 攻击类型混杂化
- 攻击手段更加灵活

拒绝服务攻击的发展

目标

- 网站-〉网络基础设施（路由器/交换机/DNS等）

流量

- 从几百兆-〉几十G-〉几百G甚至更高

技术

- 真实IP地址-〉IP欺骗技术
- 单一攻击源-〉多个攻击源
- 简单协议承载-〉复杂协议承载
- 智能化，试图绕过IDS或FW

形式

- DRDoS/ACK Flood
- Zombie Net/BOTNET
- Proxy Connection Flood
- DNS Flood

谢谢！


此致
敬礼