RSA CONFERENCE
CHINA 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

中国域名安全分析、研究与实践

演讲人姓名　陈钟

演讲人单位　北京大学

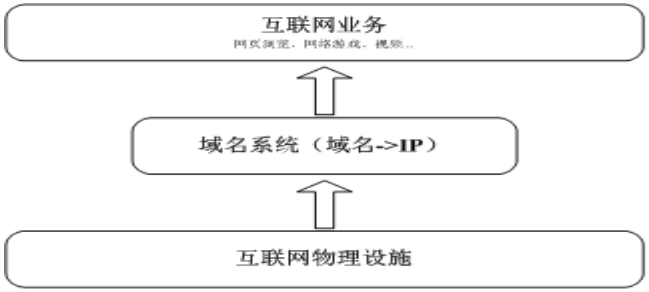
RSA CONFERENCE CHINA 2012

目录

域名系统安全的重要性

定义

- 域名系统(Domain Name System,DNS)是互联网的重要组成部分，主要用于提供域名到IP地址的翻译转换服务，是现有多数互联网业务的基础设施。



重要性

- 域名系统是互联网应用的寻址方式；
- 域名技术丰富了互联网应用；
- 域名是互联网上不可重复的标识资源；
- 域名是标识一国主权的国家战略资源

安全必要性

- 大多数攻击类型都与域名有着直接或间接的联系;
- 域名系统受到攻击很容易产生“蝴蝶效应”,引发大规模连锁反应；
- 可能会造成企业或个人经济损失、商业影响；国家造成政治影响。

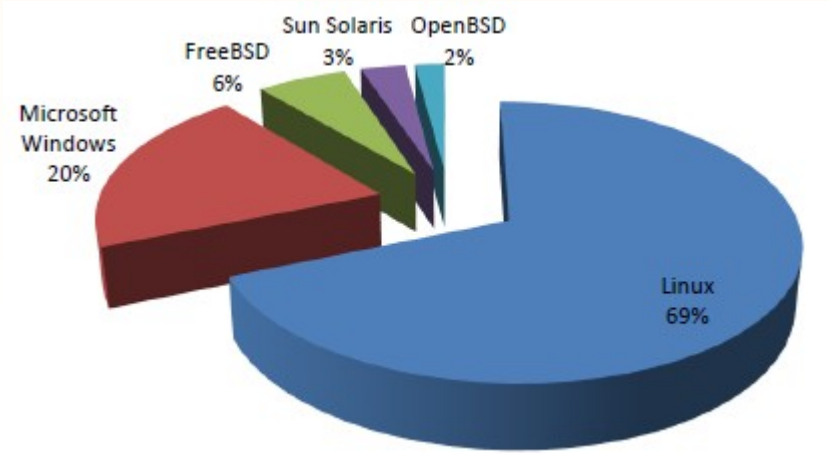
顶级域名服务分类


根据国际互联网域名体系的构成
顶级域名分为三类
通用顶级域名
组织主办类(Sponsored)14个；
通用类(Generic)4个；
限制通用类(Generic-restricted)3个
国家和地区顶级域名
国家与地区顶级域名291个；
实验性顶域11个
基础设施顶级域名
目前仅有.Arpa;

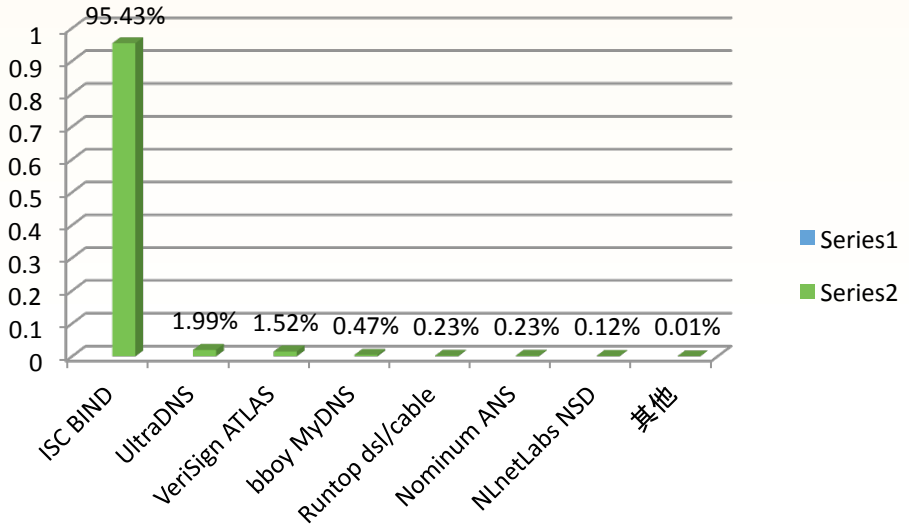
顶级域名系统及软件统计

RSA CONFERENCE CHINA 2012

顶级域名服务系统操作系统类型分布



顶级域名服务系统解析软件分类

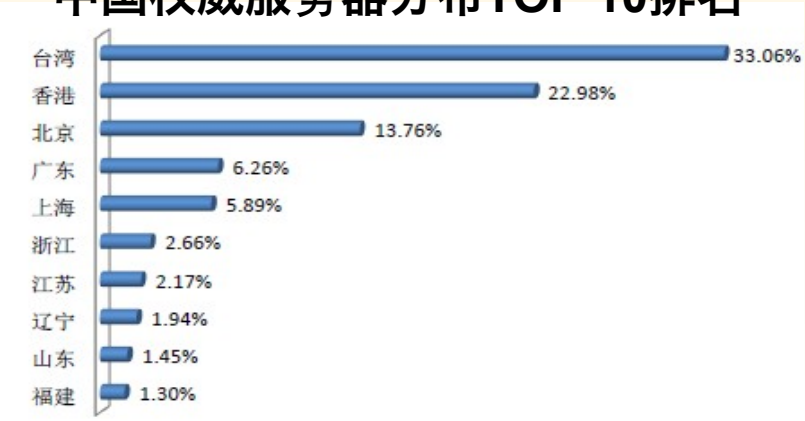


注：以上数据来自北龙中网《2011年中国域名服务及安全现状报告》

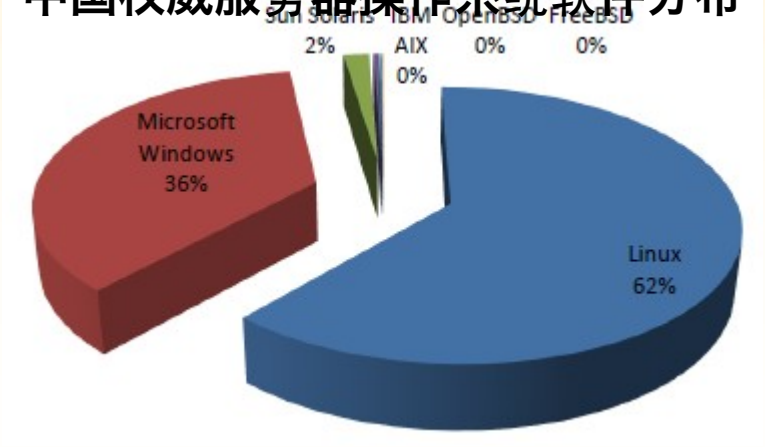
中国二级及以下权威域名服务系统分析

RSA CONFERENCE CHINA 2012

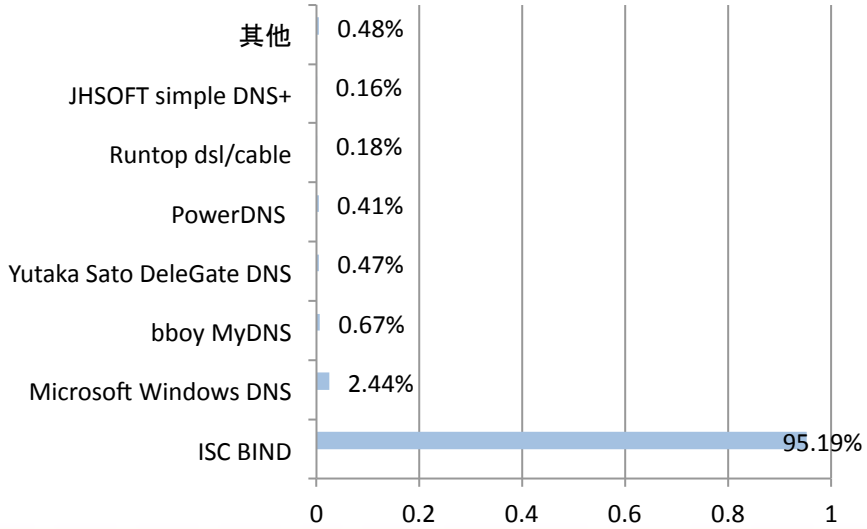
中国权威服务器分布TOP 10排名



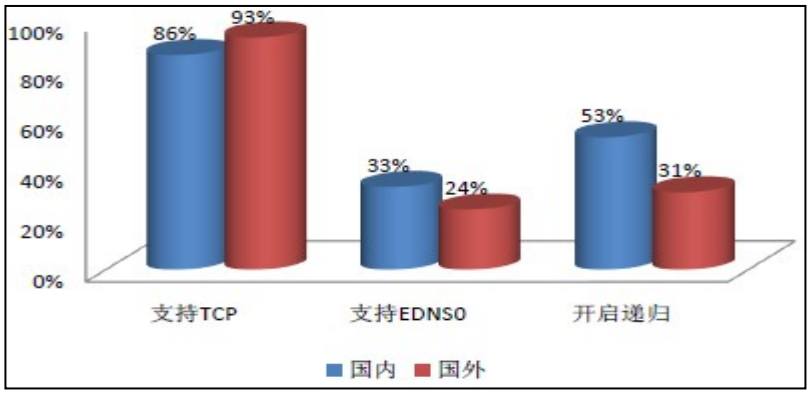
中国权威服务器操作系统软件分布



中国权威服务器解析软件分布



中国权威服务器协议支持程度分布



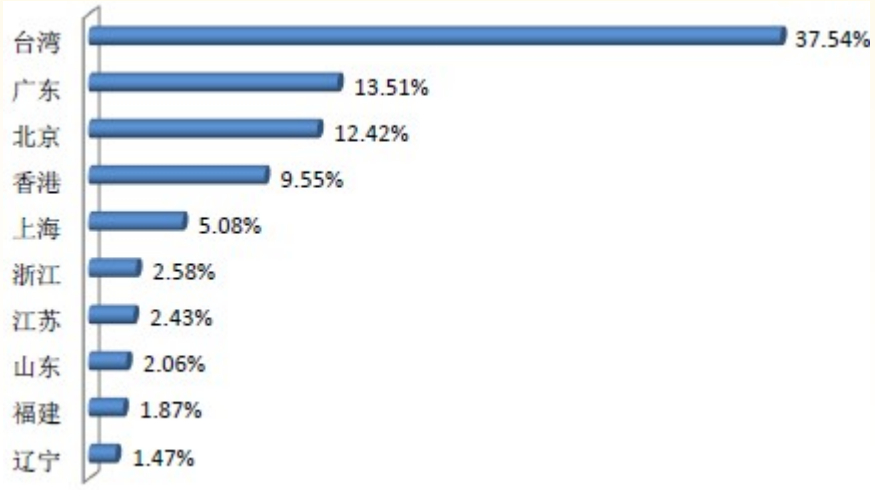
说明：中国各级权威服务器开启递归的比例远远大于国际水平，存在安全隐患，说明中国各级域名配置方式存在问题。

注：以上数据来自北龙中网《2011年中国域名服务及安全现状报告》

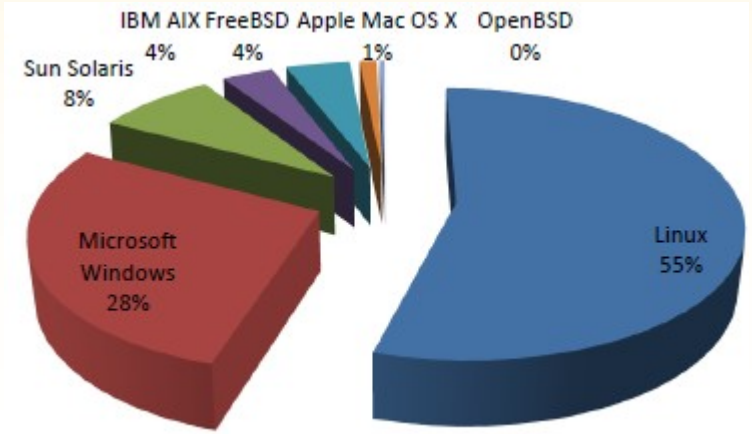
中国递归域名服务系统分析

RSA CONFERENCE CHINA 2012

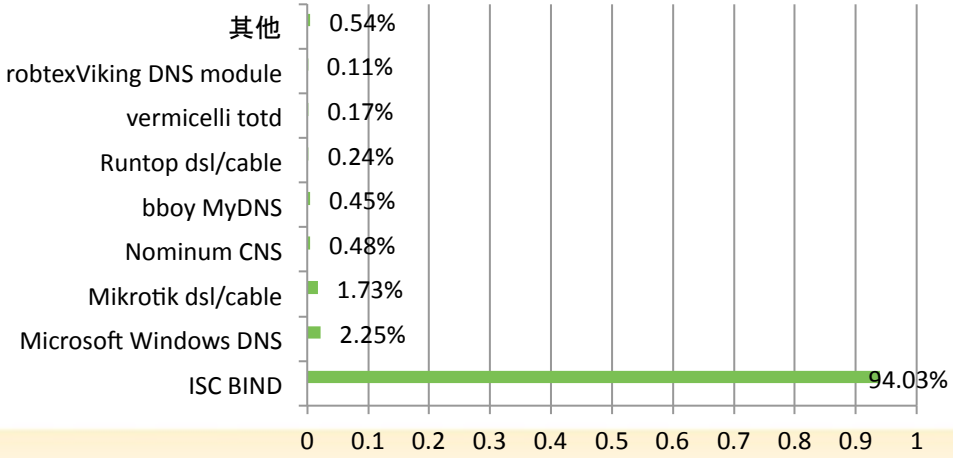
中国递归服务器分布TOP 10排名



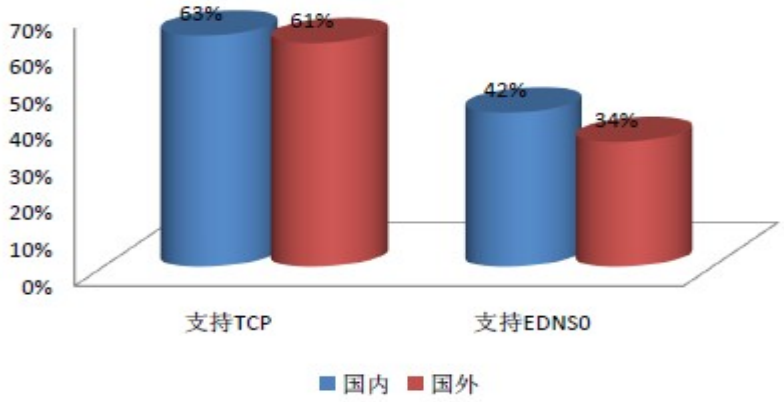
中国递归服务器操作系统软件分布



中国递归服务器解析软件分布

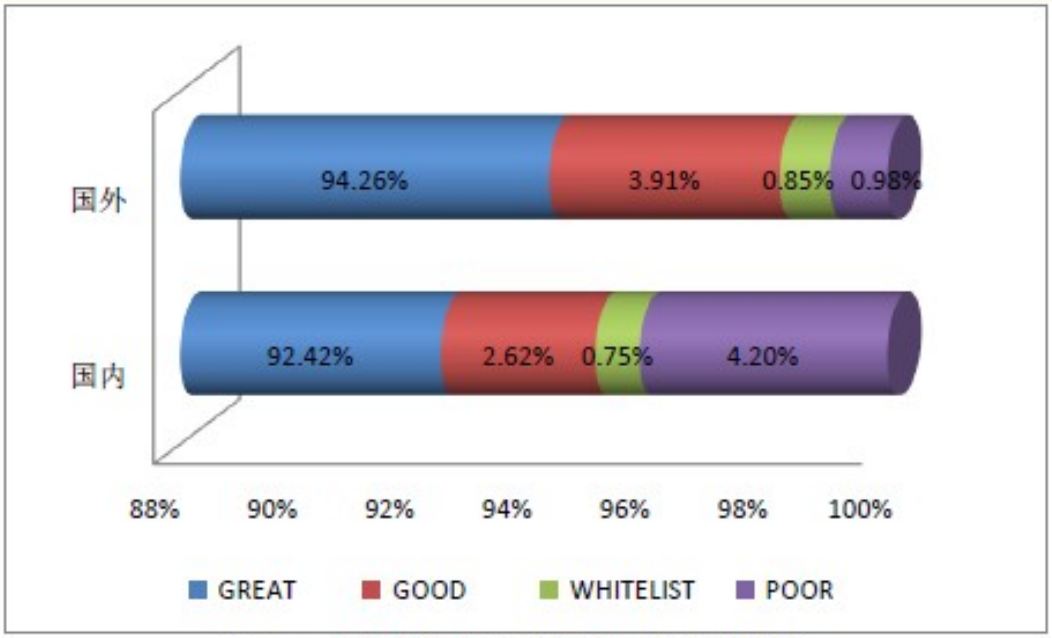


中国递归服务器协议支持程度分布



注：以上数据来自北龙中网《2011年中国域名服务及安全现状报告》

递归服务器端口随机性统计



递归域名服务系统端口随机程度分布

- 端口随机算法如果不够安全，容易遭受缓存中毒攻击；
- 中国超过4%的递归域名服务器端口随机性较差，远高于世界平均的0.98%；

近几年域名安全事故大事记

RSA CONFERENCE CHINA 2012

- **2009年5月19日，5.19事件，DNSPoD受到攻击，由暴风影音引发“蝴蝶效应”，导致6省大面积断网，二十几个省网络缓慢。**
- 2009年6月，国内著名域名注册商新网公司DNS遭受攻击，20万域名无法解析
- 2009年8月，波多黎各主要的域名注册机构遭受长达几个小时的攻击，造成Google, Microsoft, Yahoo, Coca-Cola等多家大公司的网站被重定向到某恶意网站。
- 2009年10月，由于在日常维护中不正确的软件升级，瑞典国家顶级域名.se出现故障，导致整个瑞典互联网几乎完全瘫痪。
- 2009年12月，twitter上次域名被转向，百度和这次攻击有着惊人的相似之处
- 2009年12月，亚马逊所使用的UltraDNS遭DDoS攻击 瘫痪约一小时
- **2010年1月，百度在美国的域名服务商服务器授权记录遭到篡改，域名被劫持，造成百度数小时不能正常访问。**
- 2010年5月，德国国家顶级域de因配置错误，导致大量de域名无法访问；
- **2011年2月，中国电信DNS故障，导致全国各地网络同时出现问题，DNS大面积故障；**
- 2011年4月，著名DNS服务器提供商PowerDNS遭受DDoS攻击，造成服务延迟；
- 2011年5月，Microsoft提供的BPOS云解析服务由于DNS遭受攻击导致大量用户邮件发送延迟。

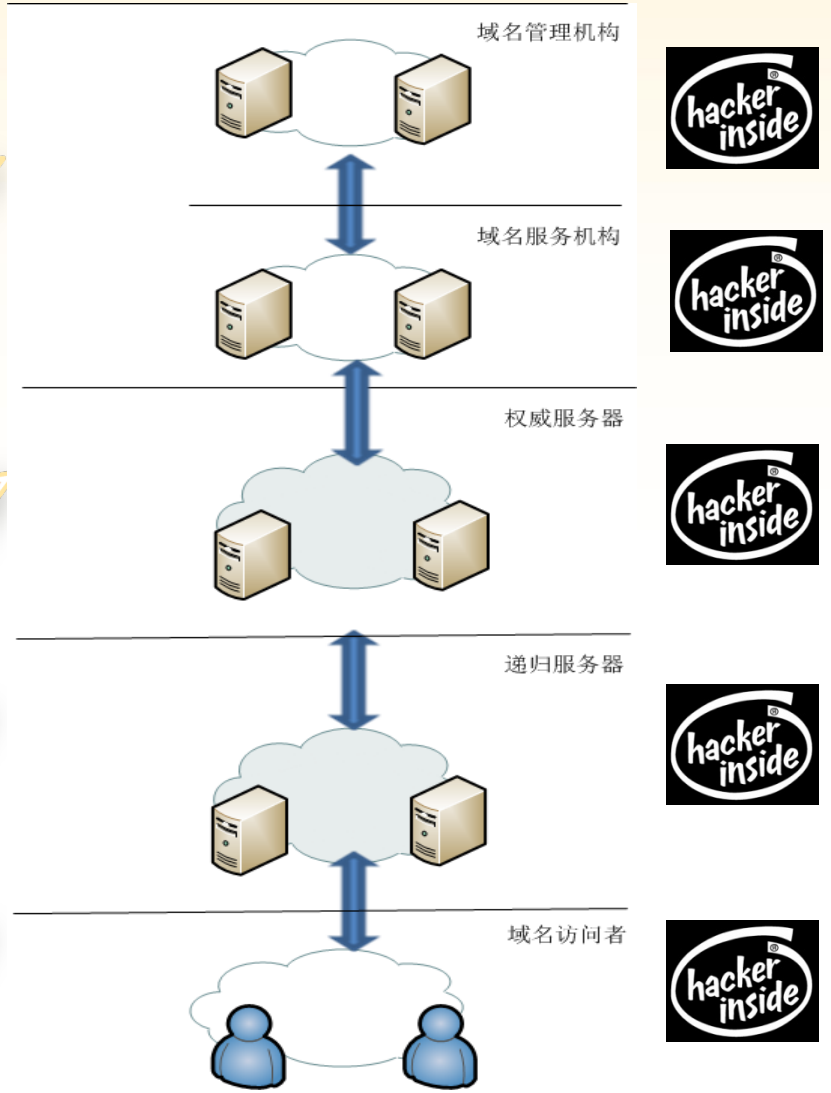
草木皆可成兵，危险无处不在

管理不善、系统漏洞造成信息泄露

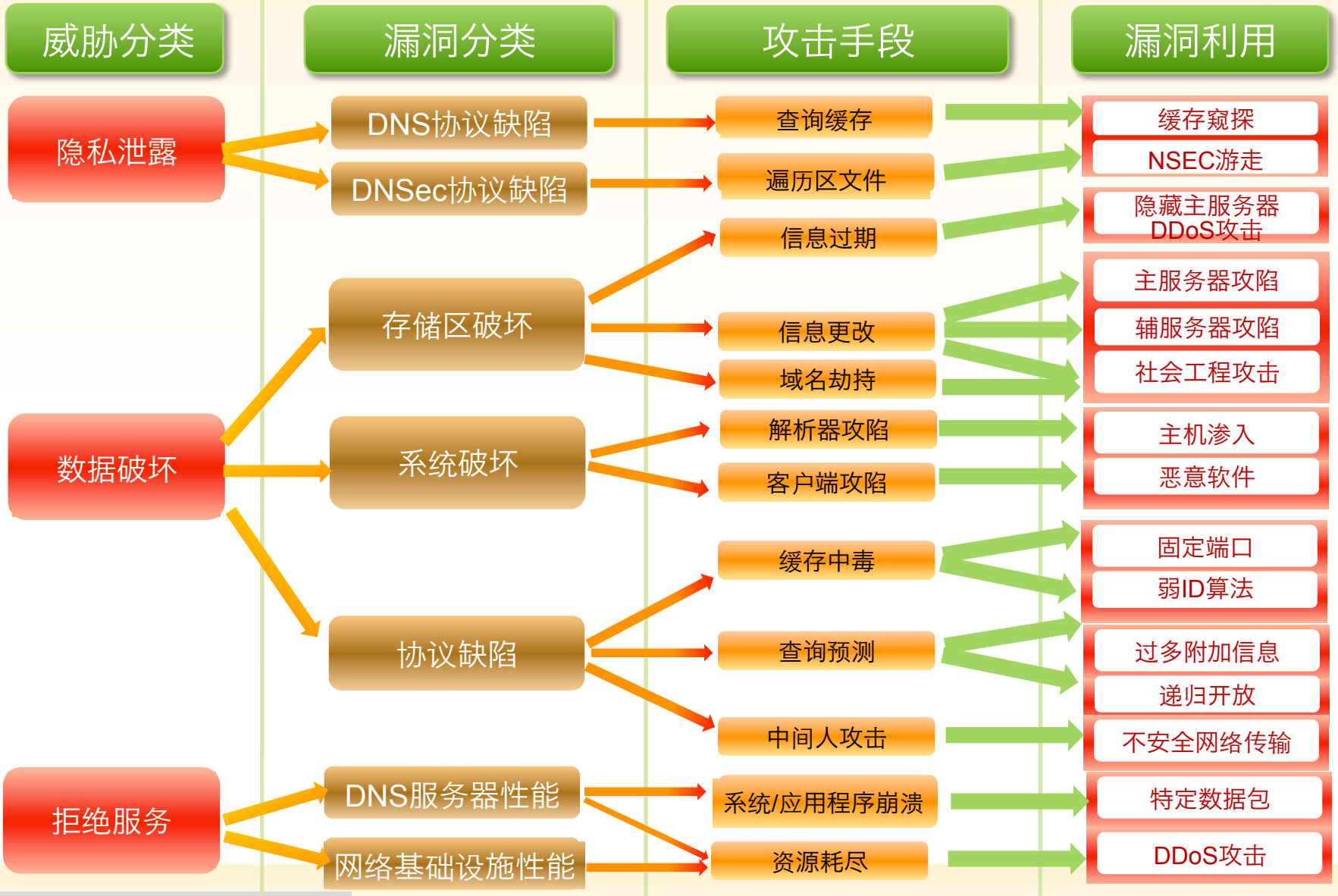
DNS软件漏洞、DDoS攻击

DNS软件漏洞、DDoS攻击

客户端系统和网络漏洞



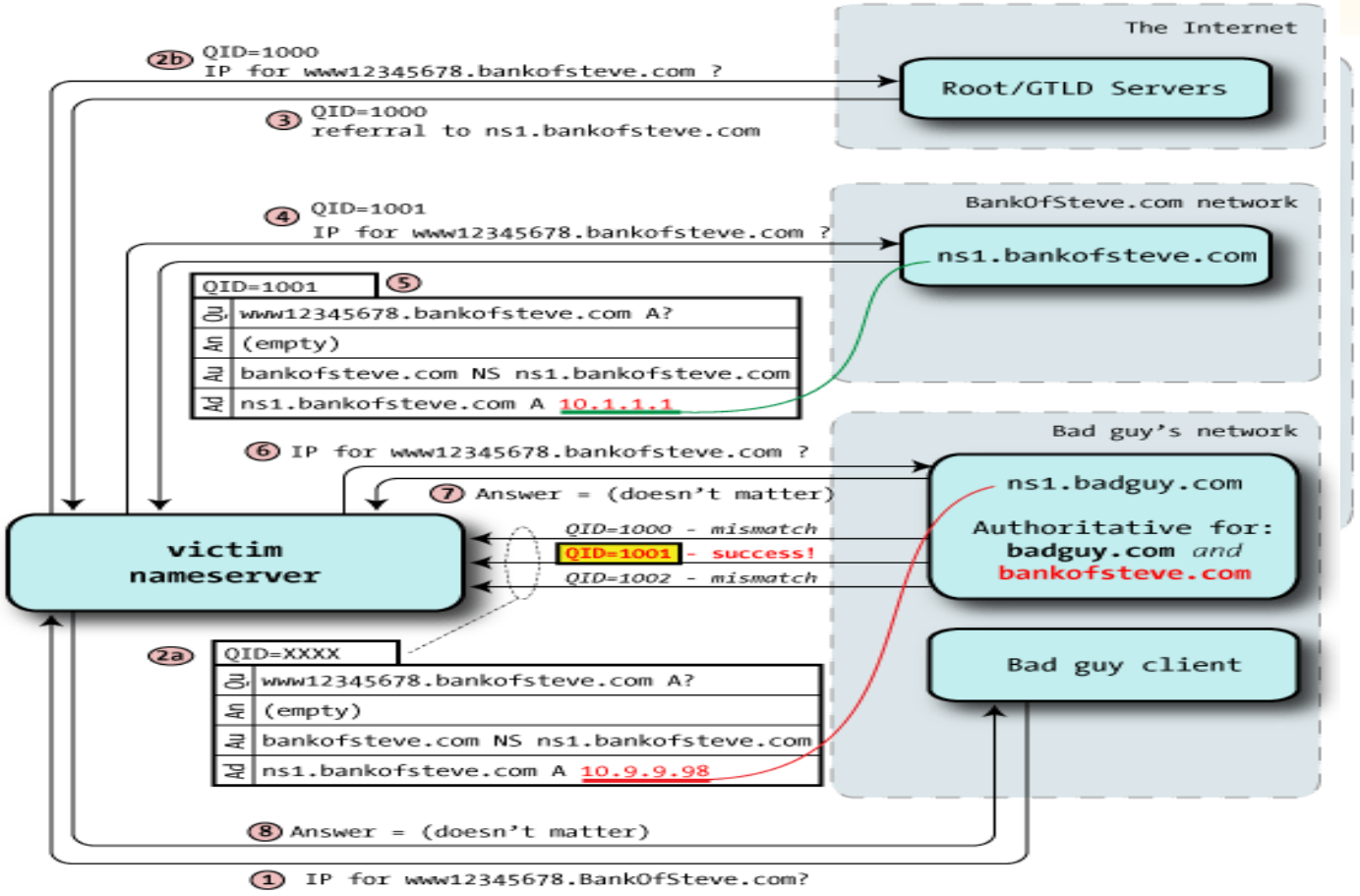
攻击形式多种多样


威胁分类
漏洞分类
攻击手段
漏洞利用
隐私泄露
数据破坏
拒绝服务
DNS协议缺陷
DNSec协议缺陷
存储区破坏
系统破坏
协议缺陷
DNS服务器性能
网络基础设施性能
查询缓存
遍历区文件
信息过期
信息更改
域名劫持
解析器攻陷
客户端攻陷
缓存中毒
查询预测
中间人攻击
系统/应用程序崩溃
资源耗尽
缓存窥探
NSEC游走
隐藏主服务器
DDoS攻击
主服务器攻陷
辅服务器攻陷
社会工程攻击
主机渗入
恶意软件
固定端口
弱ID算法
过多附加信息
递归开放
不安全网络传输
特定数据包
DDoS攻击

DNS缓存投毒

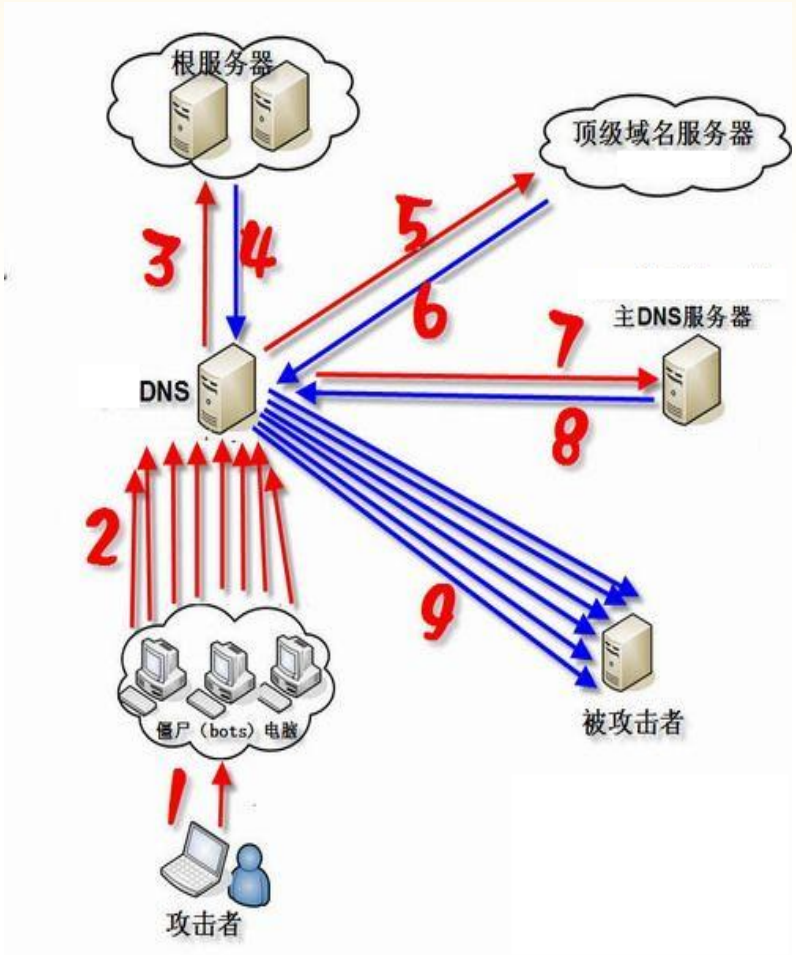
- DNS Cache Poisoning(DNS缓存投毒技术)就是通过技术手段，用伪造的域名解析记录，替换域名服务器系统的正确域名解析记录，以达到域名劫持的目的。**其针对的是DNS协议本身的安全缺陷**。

缓存毒药攻击示例



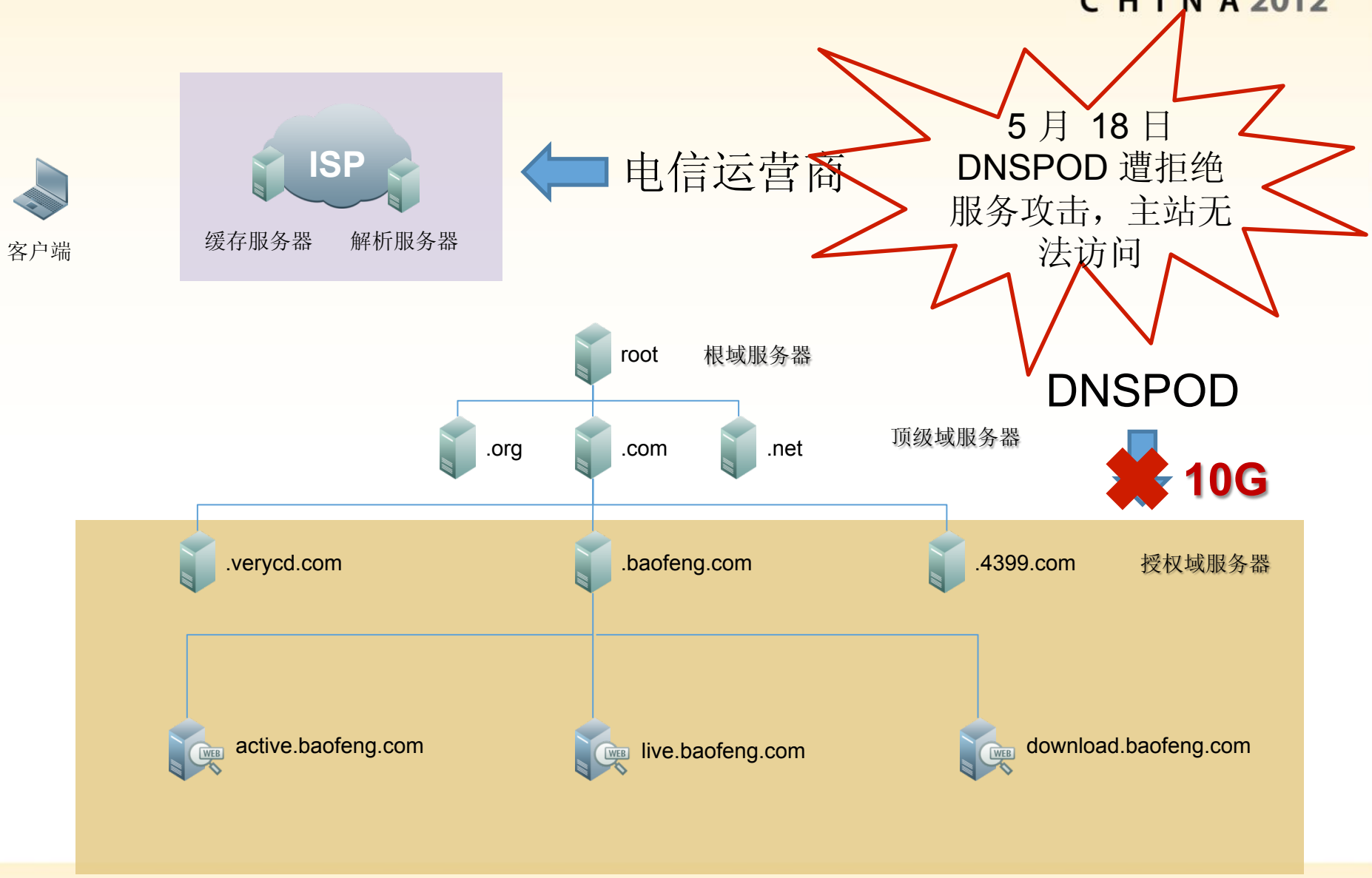
Spoof和放大类攻击检测

- 通过向被攻击目标倾泻大量的解析服务请求数据，消耗被攻击目标的系统及网络资源，最终达到拒绝服务的目的

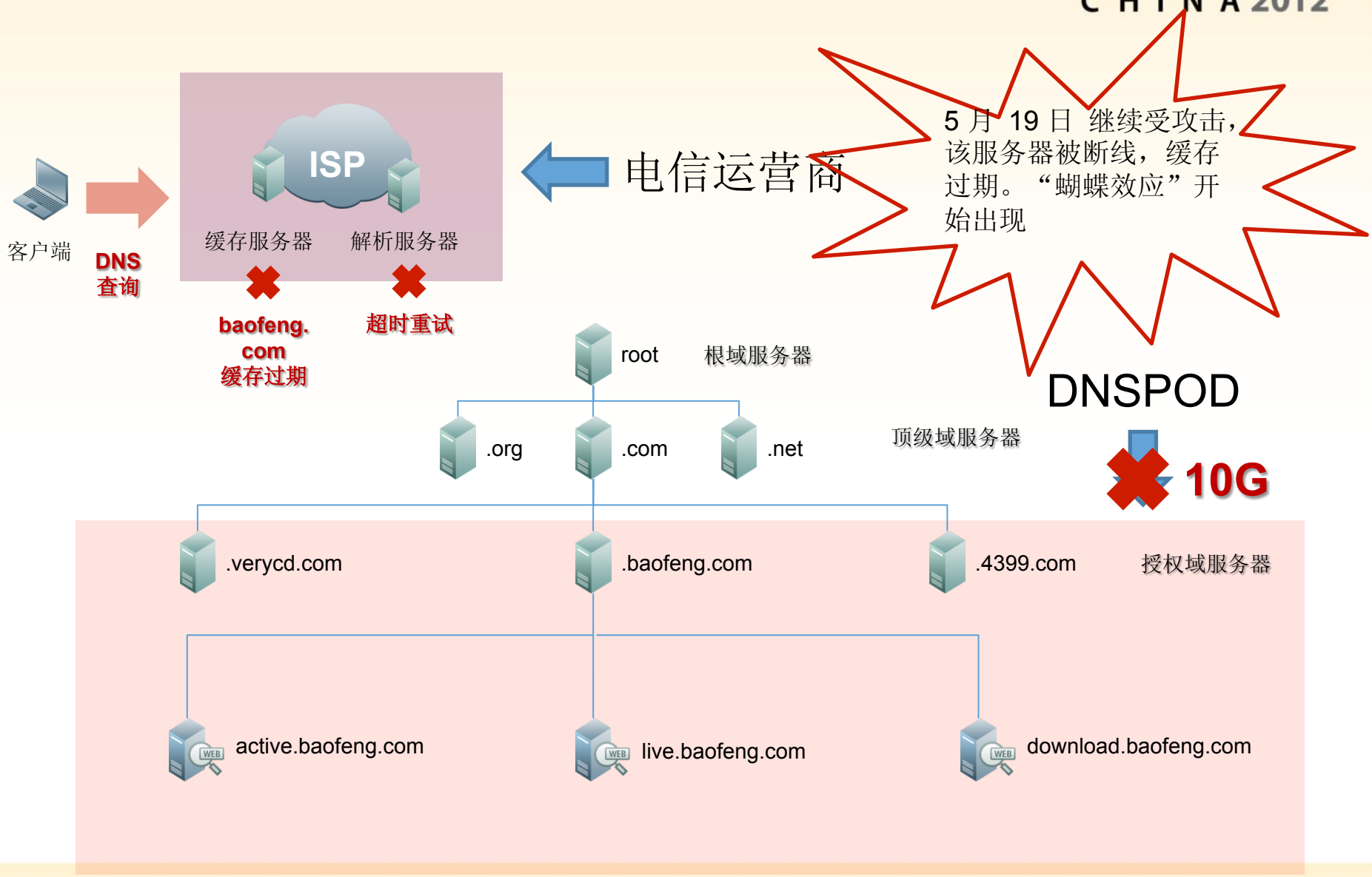


在2005年之前，利用DNS的放大攻击主要依靠对DNS发送60个字节左右的查询，回复最多可达512个字节，从而使通讯量放大8.5倍。然而当前许多DNS服务器支持EDNS。EDNS是DNS的一套扩大机制，如果请求者指出它能够处理大于512字节的DNS查询，一些选项能够让DNS服务器回复超过512字节并且仍然使用UDP。攻击者利用这种方法可以产生大量的通讯。通过发送一个60个字节的查询来获取一个大约4000个字节的记录，攻击者能够把通讯量放大66倍。DNS Amplification攻击的同时加之IP spoof攻击，利用TCP/IP协议的缺陷，伪造目标的源地址，利用DNS服务器的响应对目标进行攻击。使得攻击者制造流量的能力有了大幅度的提升。

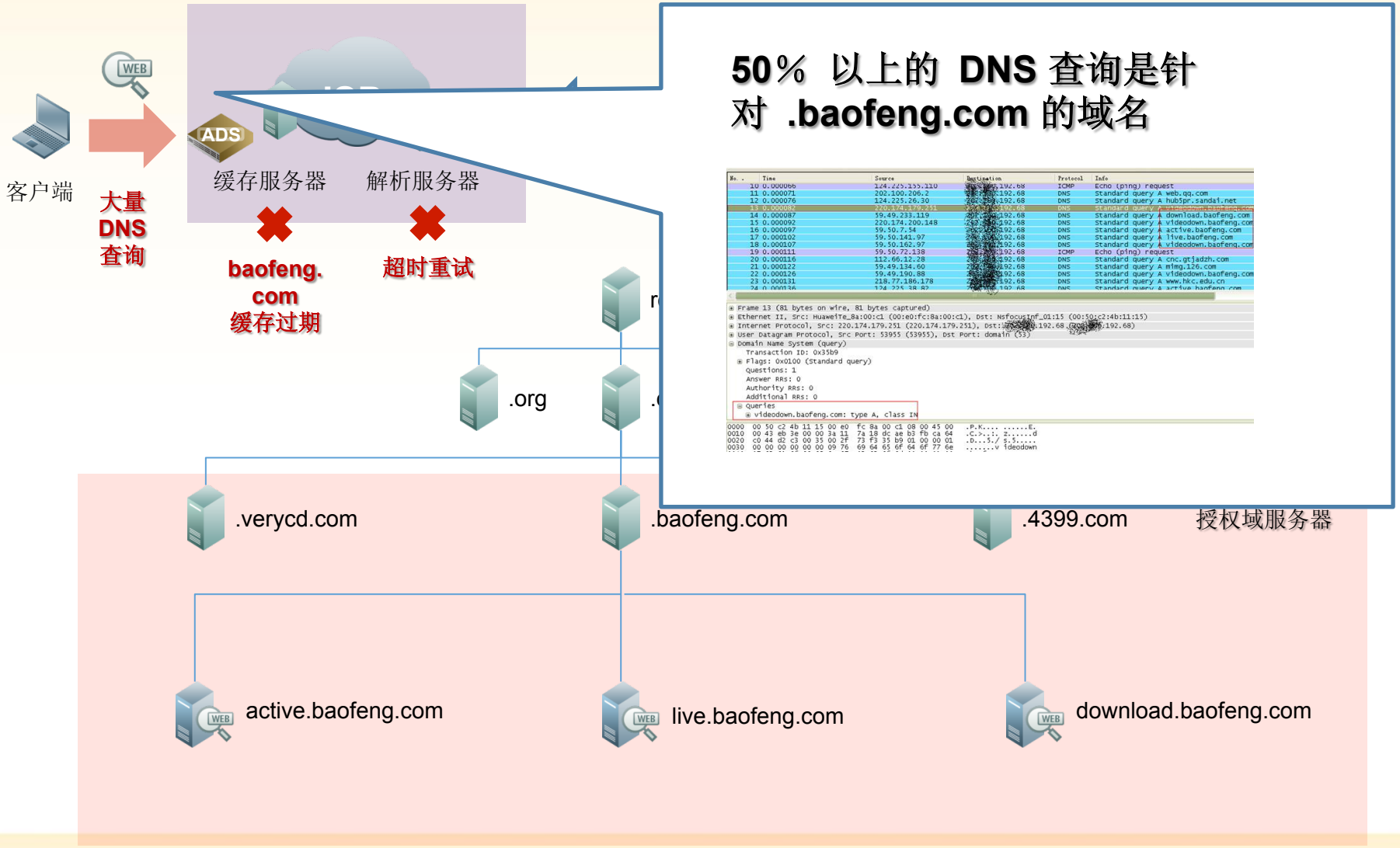
“5·19”断网事件 —— 前奏


客户端
ISP
缓存服务器
解析服务器
电信运营商
5 月 18 日
DNSPOD 遭拒绝
服务攻击，主站无
法访问
DNSPOD
10G
root
根域服务器
.org
.com
.net
顶级域服务器
.verycd.com
.baofeng.com
.4399.com
授权域服务器
active.baofeng.com
live.baofeng.com
download.baofeng.com

“5·19”断网事件 —— 断网


客户端
DNS
查询
ISP
缓存服务器
解析服务器
baofeng.
com
缓存过期
超时重试
电信运营商
5 月 19 日 继续受攻击，该服务器被断线，缓存过期。“蝴蝶效应”开始出现
DNSPOD
10G
root
根域服务器
.org
.com
.net
顶级域服务器
.verycd.com
.baofeng.com
.4399.com
授权域服务器
active.baofeng.com
live.baofeng.com
download.baofeng.com

“5·19”断网事件 —— 发酵


客户端
大量
DNS
查询
ADS
缓存服务器
解析服务器
baofeng.
com
缓存过期
超时重试
.org
.verycd.com
.baofeng.com
.4399.com
授权域服务器
active.baofeng.com
live.baofeng.com
download.baofeng.com
50% 以上的 DNS 查询是针对 .baofeng.com 的域名

百度域名事件

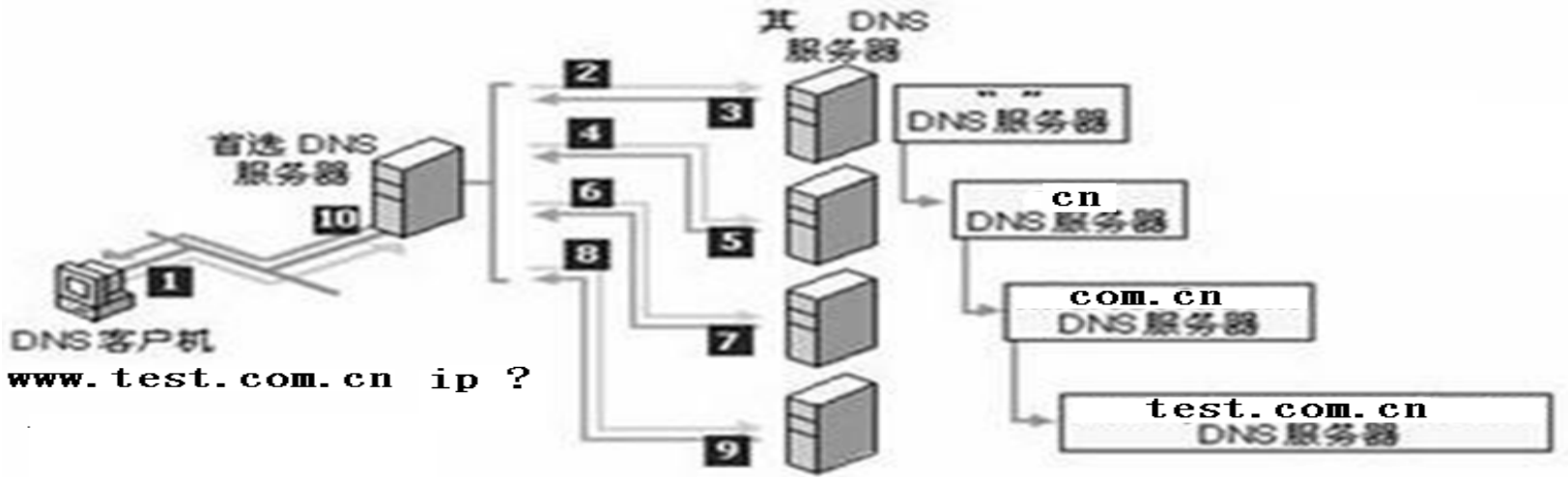
RSA CONFERENCE CHINA 2012

DNS查询式攻击

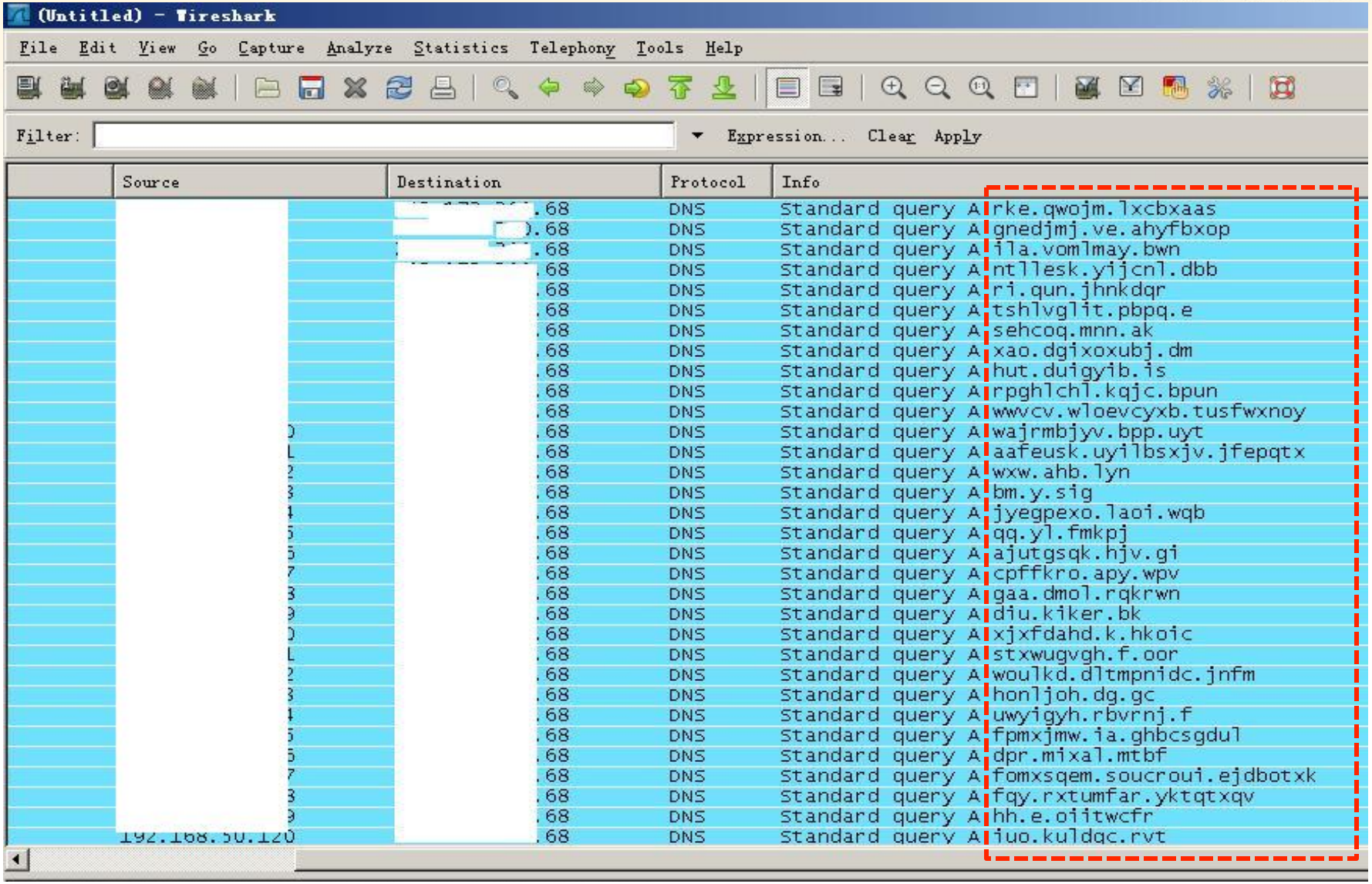
RSA CONFERENCE CHINA 2012

DNS 服务器的脆弱性

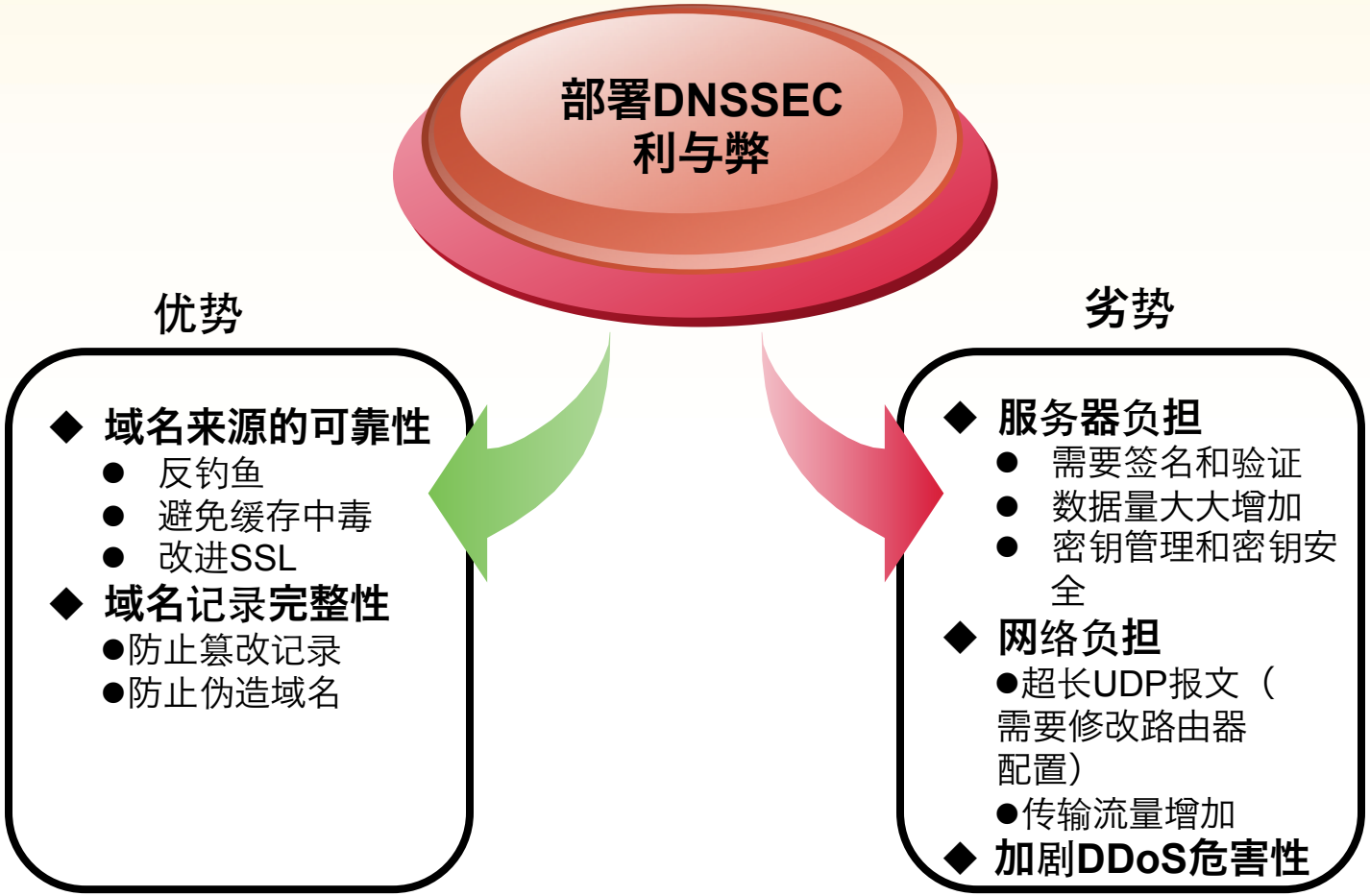
- 字符串匹配查找是DNS服务器的主要负载
- 普通单核CPU的DNS服务器，理论最佳每秒可以支撑近4万次正常查询
- 一台普通笔记本可以很轻易地发出每秒20万以上个请求
- 根据调研，运营商DNS服务器，经常有部分域名突然查询异常；或有大量异常域名查询；导致服务器负载过高



DNS查询式攻击数据包截图



部署DNSSEC的利与弊



域名系统安全防护思路

从用户层面到注册管理机构，需要从意识、制度和技术上全面进行防范。

意识是关键

- 提高安全意识；
- 养成安全的操作习惯；

制度是保障

- 定期的安全评估；
- 严格的安全管理；
- 标准的配置规范；

技术是手段

- 部署抗攻击设备；
- 实时的软件更新；
- 优化系统架构；
- 逐步实施DNSSec


业界关注重点
造成域名系统无法工作；
非法更改域名信息；
“针对”域名系统本身
“利用”域名恶意行为
合法利用域名解析；
实现非法目的；
呈现上升趋势
下面我们就探讨
如何利用域名进行恶意行为

目录

利用域名系统从事的各种恶意行为

网络钓鱼	相似域名， 如1cbc.com仿冒icbc.com.
僵尸网络控制	Fast-flux， Domain-flux
域名转嫁攻击	受攻击方恶意将DDoS攻击流量转嫁给无辜者.
恶意代码传播	经常会用到DDNS(Dynamic Domain Name System)

钓鱼网站如何钓鱼？

RSA CONFERENCE CHINA 2012

架设钓鱼网站

- 前台假冒网站：知名的金融机构、在线电子商务网站
- 后台脚本：收集、验证用户输入，并通过某种渠道转发给钓鱼者

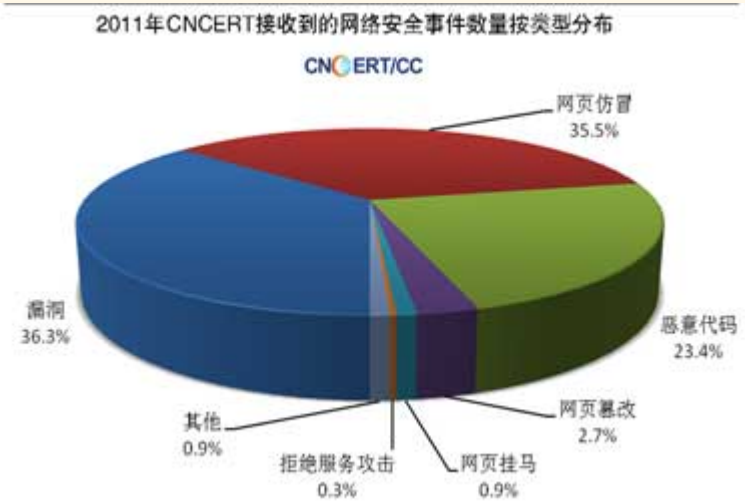
钓鱼欺骗方式

- 注册发音相近或形似的DNS域名；
- 真实链接中混杂指向假冒钓鱼网站的链接；或对链接URL进行编码和混淆；
- 利用僵尸网络发送欺骗信息；
- 利用木马和病毒
- ……

网络钓鱼范围

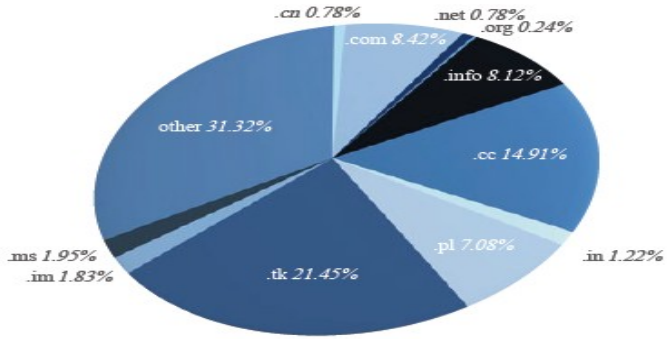
- 伪造银行网站，窃取用户账号和密码；
- 伪造交易网站，窃取交易信息
- 伪造大型网站，窃取邮箱、QQ等信息
- 伪造品牌企业或者机构，进行诈骗活动
- ……

中国钓鱼网站情况统计



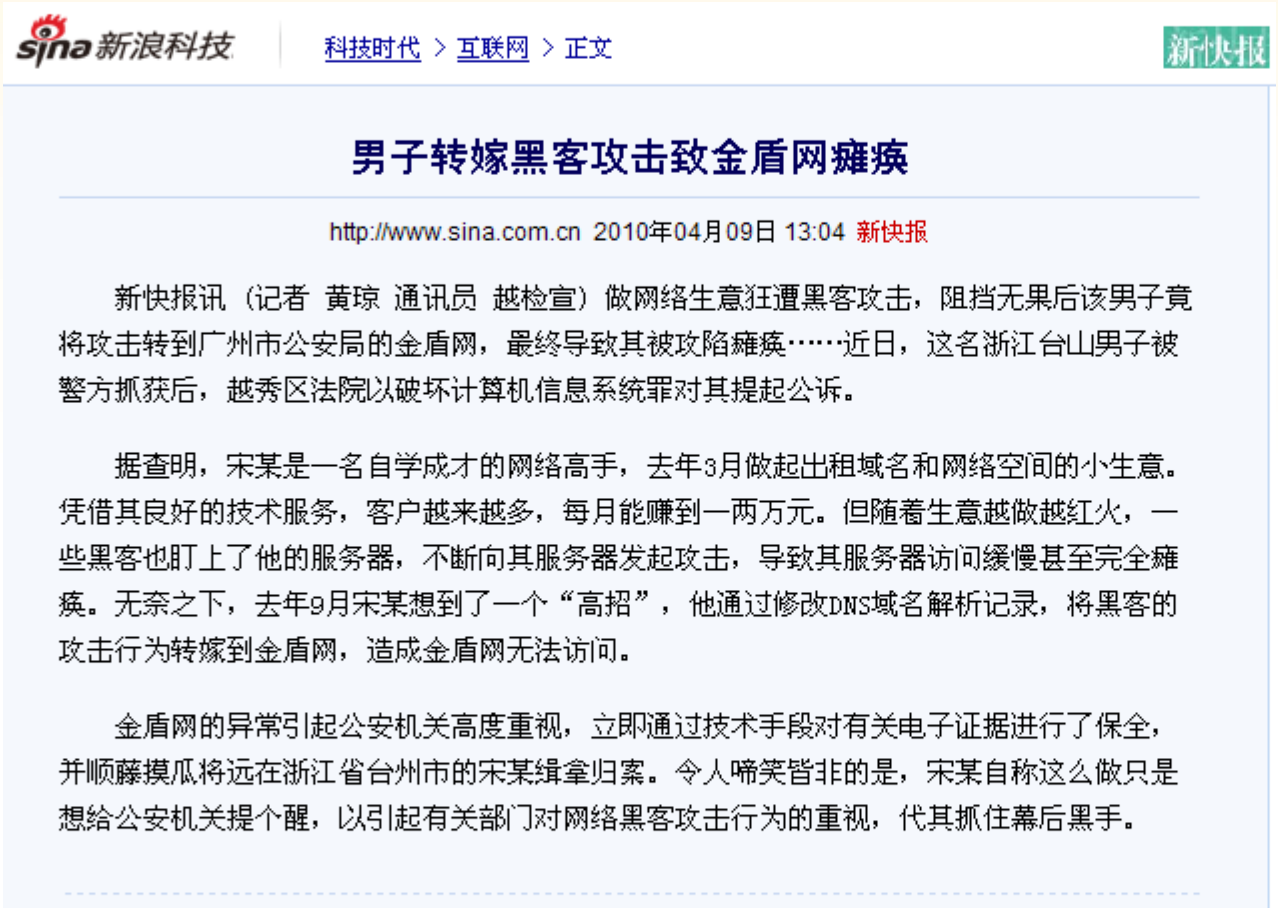
2011年针对网银用户名和密码、网银口令卡的网银大盗、Zeus等恶意程序较往年更加活跃, 3月-12月发现针对我国网银的钓鱼网站域名3841个。

中国反钓鱼网站联盟针对日益危害公众网络信息安全的钓鱼网站问题，建立快速处理机制，截至2011年12月31日，累计处理钓鱼网站75867个。



域名转嫁攻击

RSA CONFERENCE CHINA 2012



sina 新浪科技 | 科技时代 > 互联网 > 正文 新快报

男子转嫁黑客攻击致金盾网瘫痪

http://www.sina.com.cn 2010年04月09日 13:04 新快报

新快报讯（记者 黄琼 通讯员 越检宣）做网络生意狂遭黑客攻击，阻挡无果后该男子竟将攻击转到广州市公安局的金盾网，最终导致其被攻陷瘫痪……近日，这名浙江台山男子被警方抓获后，越秀区法院以破坏计算机信息系统罪对其提起公诉。

据查明，宋某是一名自学成才的网络高手，去年3月做起出租域名和网络空间的小生意。凭借其良好的技术服务，客户越来越多，每月能赚到一两万元。但随着生意越做越红火，一些黑客也盯上了他的服务器，不断向其服务器发起攻击，导致其服务器访问缓慢甚至完全瘫痪。无奈之下，去年9月宋某想到了一个“高招”，他通过修改DNS域名解析记录，将黑客的攻击行为转嫁到金盾网，造成金盾网无法访问。

金盾网的异常引起公安机关高度重视，立即通过技术手段对有关电子证据进行了保全，并顺藤摸瓜将远在浙江省台州市的宋某缉拿归案。令人啼笑皆非的是，宋某自称这么做只是想给公安机关提个醒，以引起有关部门对网络黑客攻击行为的重视，代其抓住幕后黑手。

自己遭受攻击

修改自己的DNS服务器域名与IP对应记录

将攻击流量引向修改后的IP

僵尸网络

僵尸网络定义

通过各种手段在大量计算机中植入特定的恶意程序，使控制者能够通过相对集中的若干计算机直接向大量计算机发送指令的攻击网络。

僵尸网络类型

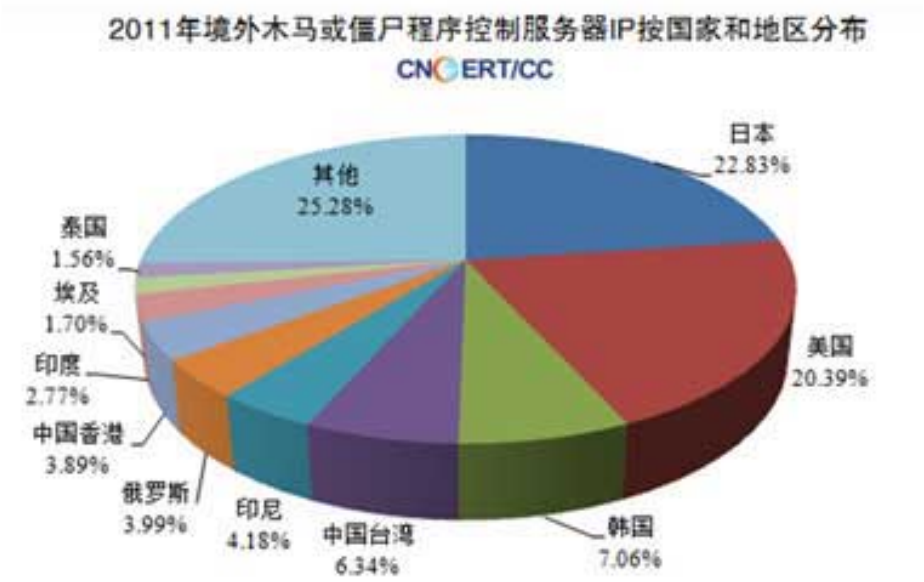
分类	类型	知名僵尸网络
集中式	IRC僵尸网络	Sdbot,Agobot,GT-Bot,Rbot
	HTTP僵尸网络	Rustock,Clickbot, Naz, Zeus, Conficker,Torpig
	自定义协议僵尸网络	MegaD, Mariposa
分布式	结构化P2P僵尸网络	Phatbot
	无结构P2P僵尸网络	Sinit, Nugache
	层次化僵尸网络	Koobface, Storm, Waledac

僵尸网络危害性


网络钓鱼
窃取秘密
- 窃取用户个人敏感信息
- 窃取网络流量中的秘密
滥用资源
- 滥用僵尸主机资源
- 消耗受害者网络资源
发动拒绝服务
- 规模大
- 难以溯源
发送垃圾邮件
- 数量大
- 隐蔽性好
利用
僵尸网络
1
2
3
4
5

中国僵尸网络现状

RSA CONFERENCE CHINA 2012



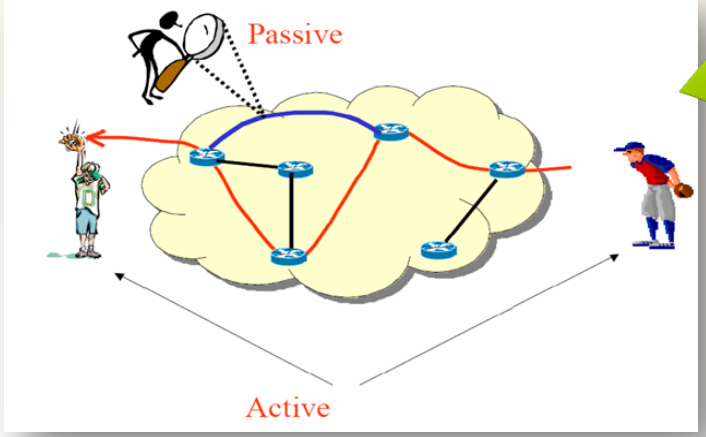
2011年，境外有近4.7万个IP地址作为木马或僵尸网络控制服务器控制我国境内主机，数量较2010年的22.1万大幅下降。

境内受控主机数量大幅增长，由2010年的近500万增加至近890万。美国以9528个IP地址控制着我国境内近885万台主机，控制我国境内主机数高居榜首。

目录

分析监测方法

主动监测与被动监测技术相结合

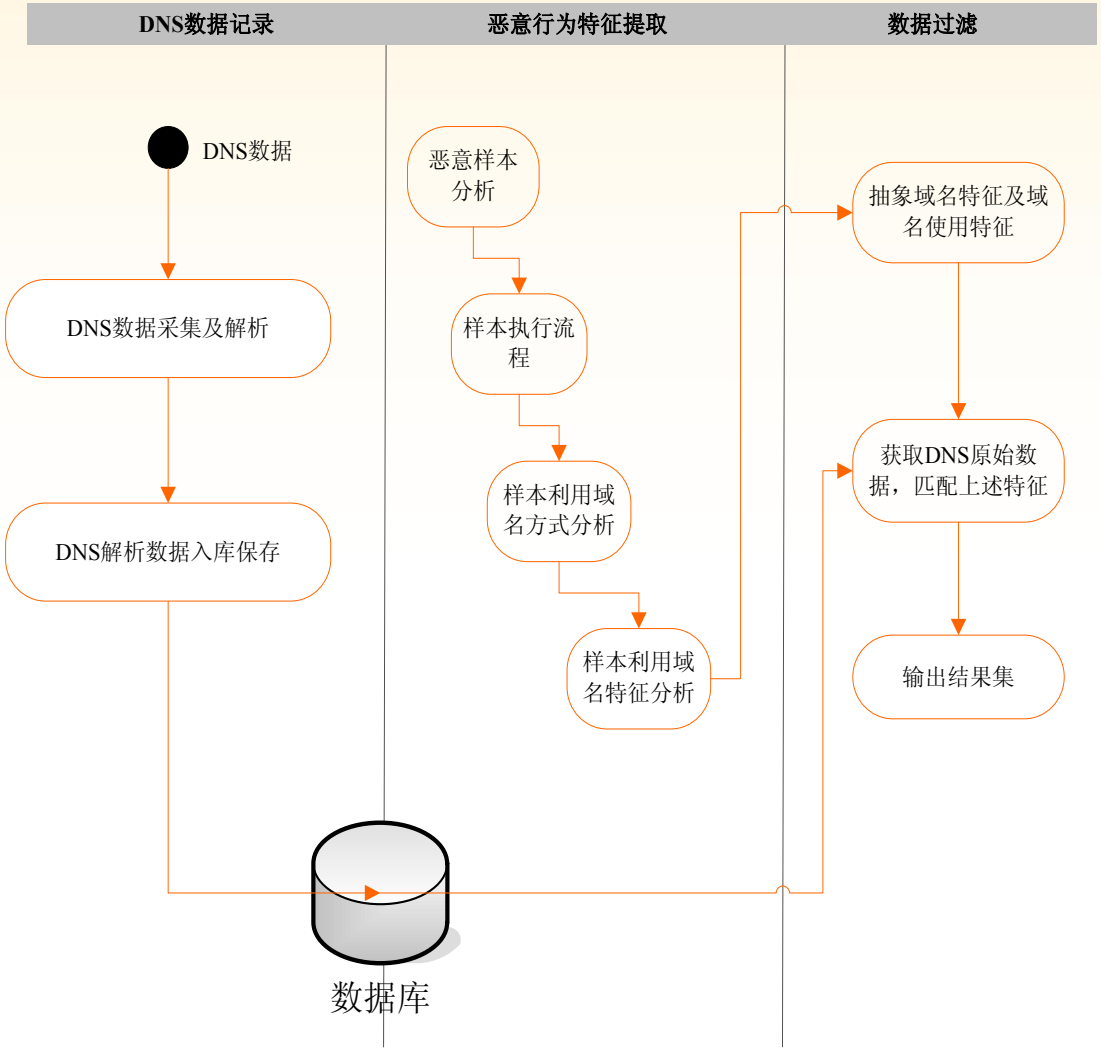


分布式监测与集中式监测并举

充分利用数据挖掘、机器学习等技术

检测利用域名的恶意活动

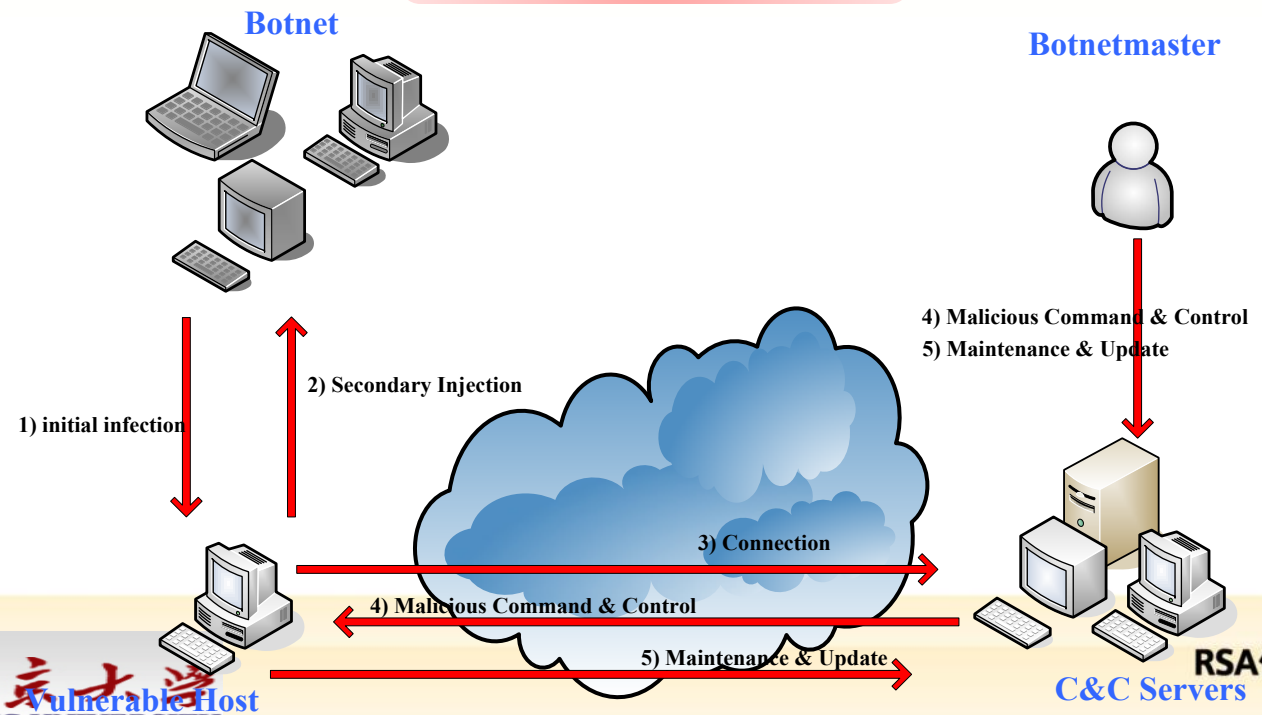
- 域名的恶意利用，流量夹杂在正常的域名流量中
- 根据不同恶意行为的特点，确定其域名本身的特征和访问请求的特征
- 将DNS数据记录下来，根据上述特征，在记录数据中筛选出恶意行为所利用的域名



利用域名隐藏自己的僵尸网络

- 僵尸网络对域名系统的利用，主要是动态域名（Dynamic DNS, DDNS）技术，其后fast flux及domain flux等技术用来标识控制服务器，以隐蔽和迁移控制服务器
- 利用domain-flux域名生成算法，可以生成大量的域名供botnet使用。域名使用具有随机性，即按照某种规则在所生成的域名集合中，挑选部分域名进行注册并使用，从而延长botnet生存时间

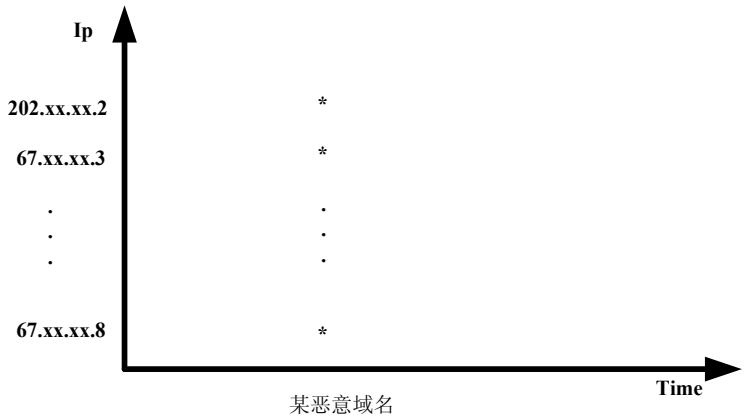
Botnet生命周期



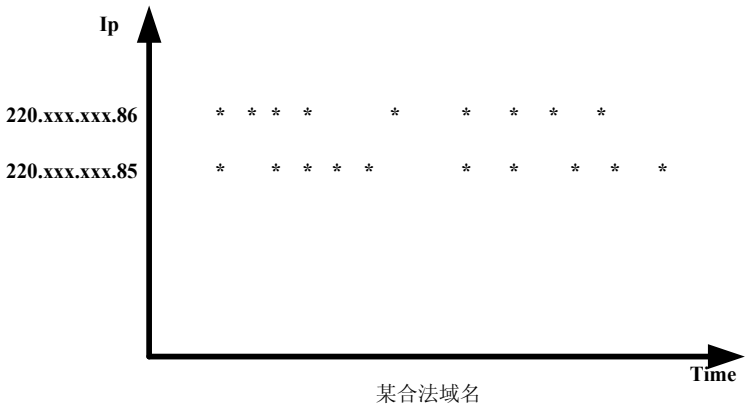
僵尸网络的行为特征

- 自动生成的域名主要任务是作为内部联络的途径，在域名使用的请求方面，表现出明显区别于正常域名的访问的特征：正常域名持续有解析访问，Domain Flux域名只在某段时间有访问
- 横轴表示时间，纵轴为域名解析出的ip，星号表示在某时刻此ip被客户端请求解析

域名活跃情况对比



某恶意域名



某合法域名

检测原理

- 随着时间的推移，恶意域名下，不断有新的子域名被请求解析，每一子域名的活跃时间不同，且不相交，但其活跃时间长度类似
- 对于domain-flux僵尸网络所生成的每个域名，各域名活跃时间在整个botnet的存活周期中，只占其中的一段
- 对于各域名，由于其使用方式是一样的，且其解析出的ip也属于同一ip集合。按照二级或三级域名并且解析ip属于同一集合这样的形式对域名进行归类

在某运营商网络中的检测效果验证

RSA CONFERENCE CHINA 2012

- 国际口的域名解析记录：5千万条/天
- 通过Domain Flux过滤得到1000个域名， 多数为不良网站：黄色网站、伪黄色网站、私服等
- 其中， 疑似僵尸网络结果数量：20条左右， 经验证：
  - ◆ 确定：50%以上
  - ◆ 误报：10%
  - ◆ 不确定：20~30%

返回

部分域名解析情况

域名	IP	过滤时间
2ac52kqx7rsgarhipseocdom7ou6sfhd.3wcde5lilmf4gmr9aigiw3lmmhlmp569.67.ujhvg.com	203.98.7.65	2011-11-14 00:00:00
n5drjcrfxaclwti2e8b68ocu7fwaxf6h.8diffntbvnikqhako9r8pw2fpfmiipsd.67.ujhvg.com	203.98.7.65	2011-11-14 00:00:00
9pqwtu4969aqh8tw7thxr884dmcji9nd.m9okajt46ilnhaajdkqos34nkm6qgo9x.67.ujhvg.com	46.82.174.68	2011-11-14 00:05:00
3uinaeg9deid9hcgpmcrn52dlswfgue5.mp96sfprkuvkctf3bgj4ec59mjc7gmv3.67.ujhvg.com	8.7.198.45	2011-11-14 00:10:00
lb59mjafh894ev895g7r63qcaiipjdhk.lu9d4u7gf2uejigvjsblruq6xjrhpe6c.67.ujhvg.com	203.98.7.65	2011-11-14 00:15:00
sj64rp24j4dwgj5484xhdtxvopo44ll6.nwahga9uvglcoa4sbq2cepll5p5jxg3v.67.ujhvg.com	159.106.121.75	2011-11-14 00:15:00
wd9lih3assadxexvdcbx2tul63mjomq9.mguoqh4erxqjn9xdat78ffst5hubv5bl.67.ujhvg.com	37.61.54.158	2011-11-14 00:20:00
xtmdn5vlbooo6jdeufn4aigd2bwguuwn.rbbwtnk6witngvxoeptsu2p39o2xavuw.67.ujhvg.com	37.61.54.158	2011-11-14 00:20:00
5wvw8rkq8d2idjqej7vclv7comsxv8u9.qhfgwnlio5p23wwi2mgpnt6tfd5v6kbt.67.ujhvg.com	93.46.8.89	2011-11-14 00:20:00
6cnkemtkr8ndxw2thvnl6kcgl69l562o.4fuq9a3dpo45f3l7mjolp52a7sihguwu.67.ujhvg.com	203.98.7.65	2011-11-14 00:25:00
in4323u6gqebkp4b4cmo3xn8co5vf23q.e9jj5lohffmhbn6iekua64xpl42ejpet.67.ujhvg.com	8.7.198.45	2011-11-14 00:25:00
tjk77fntemwhj4vxoh4dr8kftb44nake.7jr43asbdsdqto5hvfnm67p8jl9xntfg.67.ujhvg.com	78.16.49.15	2011-11-14 00:50:00

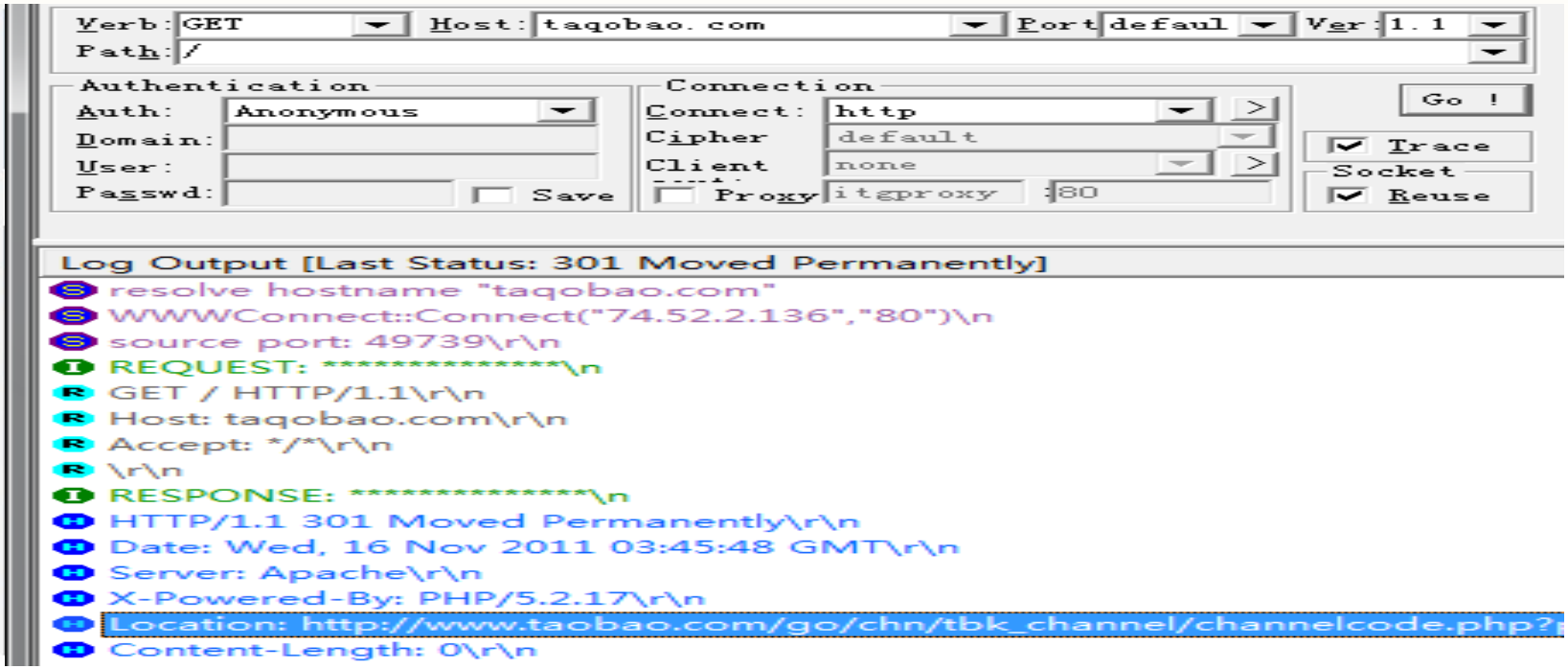
利用域名进行钓鱼攻击的检测原理

RSA CONFERENCE CHINA 2012

常用方法	钓鱼过程	检测原理
◆ URL混淆； ◆ 在URL中加入重定向； ◆ 使用社会网络攻击； ◆ 会话劫持； ◆ DNS投毒等	钓鱼网站域名与其仿冒的域名是非常相似的，并通过网站内容的相似进一步迷惑、引诱用户，以完成钓鱼过程	相似域名的过滤以及在此基础上的内容相似度计算

在运营商现网中的验证

- 利用相似算法，得到所监测域名的相似域名集合。基于字符串编辑距离的相似度判断
- 对疑似的域名，获取其网站首页内容，与所监测域名对应网站进行内容相似性对比，提高准确性。



小结

- 僵尸网络是目前互联网上最大的威胁之一，通过研究和实践提出了一种基于Domain Flux域名的僵尸网络主动发现与鉴别技术；
- 钓鱼网站能够直接给受害者带来巨大的损失，通过研究和实践提出了几种通过被动域名监测来发现和鉴别钓鱼网站的方法；
- 北京大学和国家网络信息安全技术研究所以及中国移动、中国联通和中国电信一起合作，开展了域名安全相关的研究工作，发现了位于中国境内和境外的僵尸网络和钓鱼网站若干，取得了比较明显的效果。

谢谢

RSA CONFERENCE
CHINA 2012