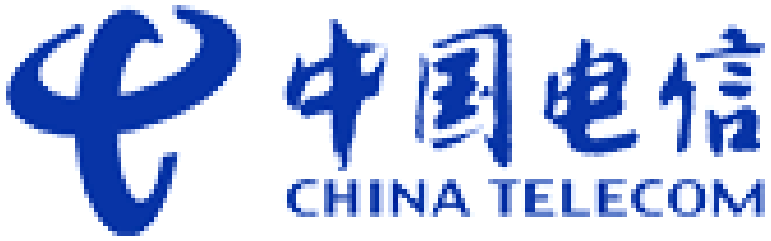


DNS安全的这些年，那些事...

刘紫千

中国计算机网络安全年会

汕头，2014-05-29

录

第一部分

DNS科普

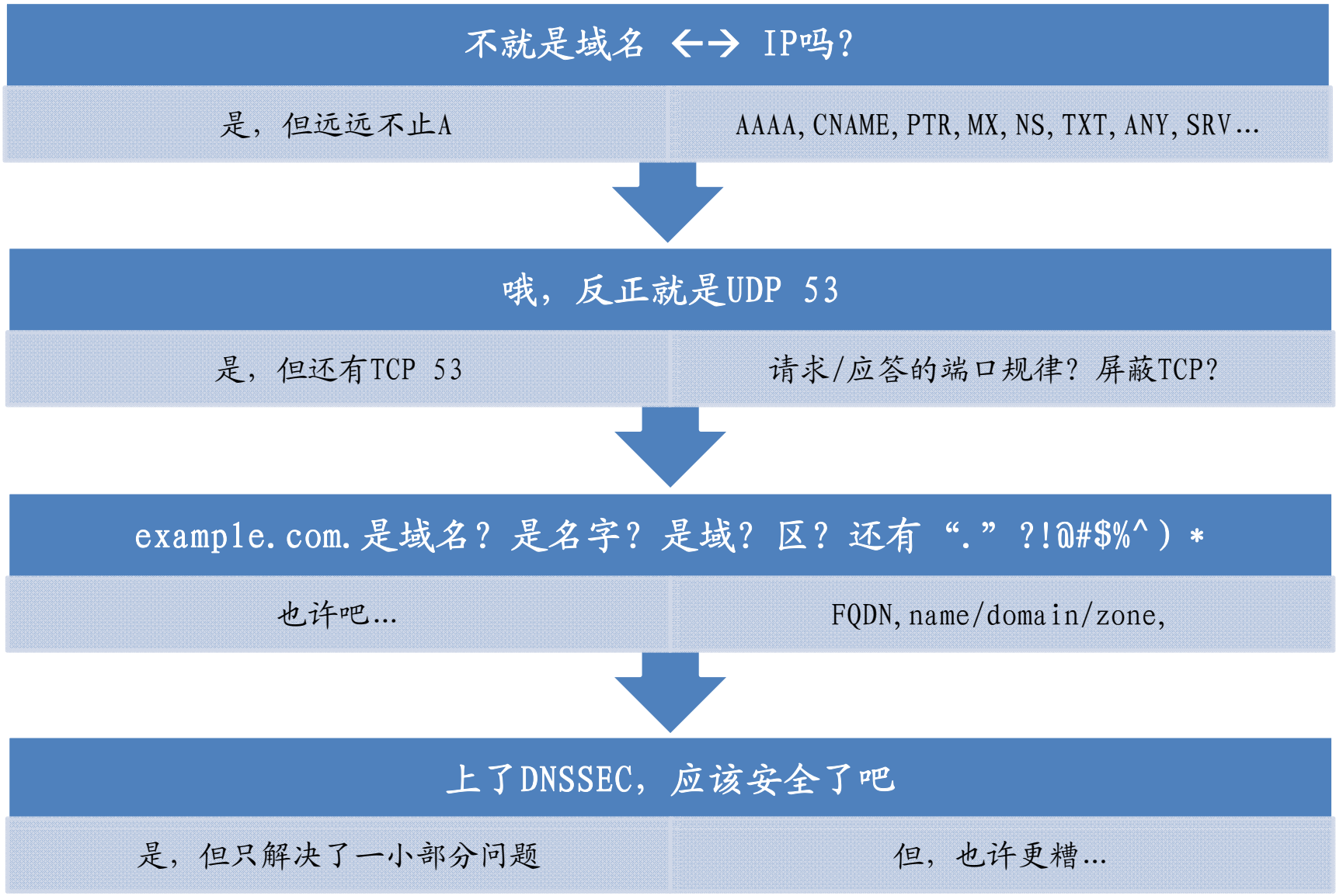
第二部分

这些年，那些事儿

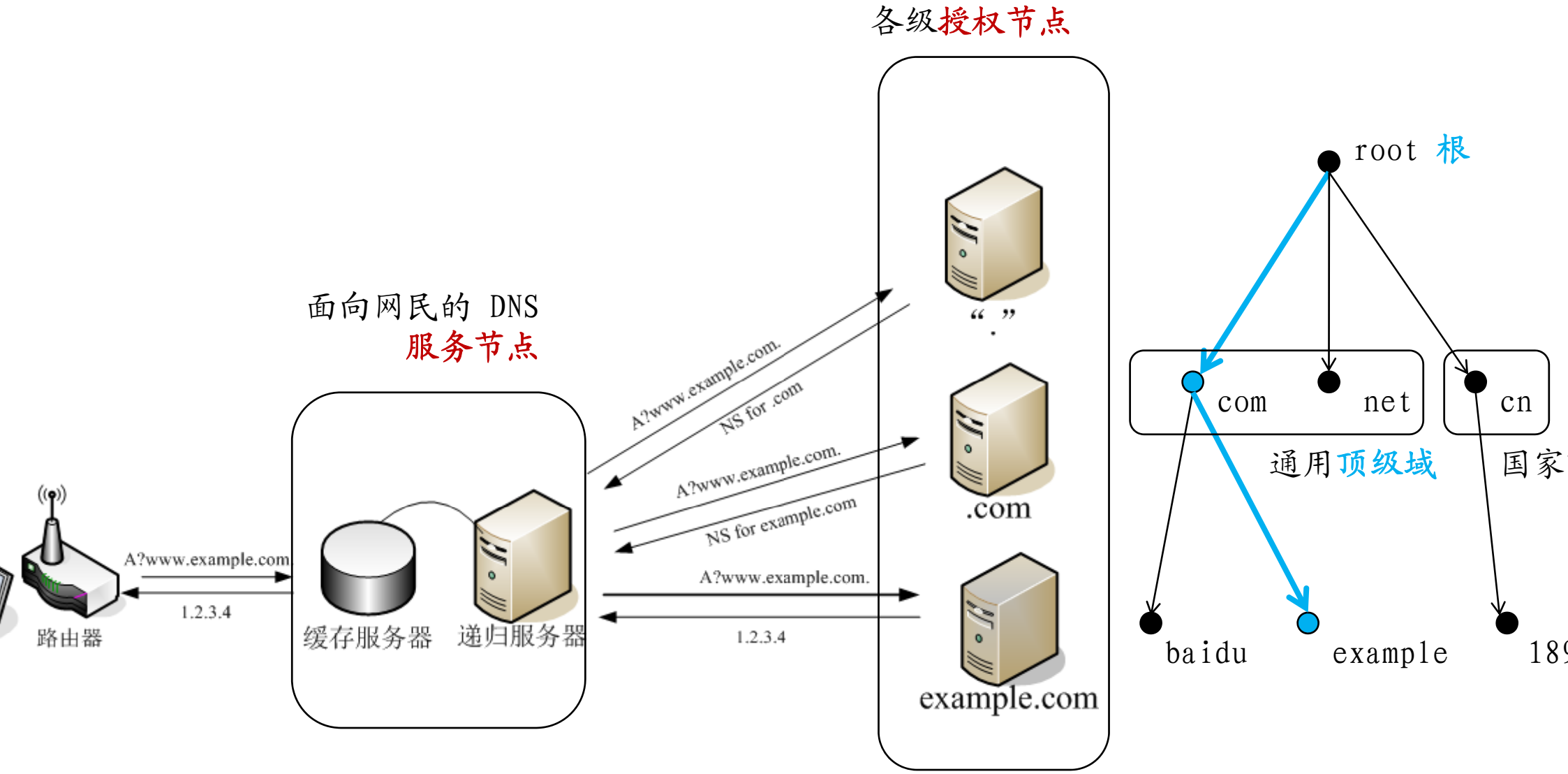
第三部分

DNS安全关注点

S科普 – 协议应用


不就是域名 ←→ IP吗?
是，但远远不止A
AAAA, CNAME, PTR, MX, NS, TXT, ANY, SRV…
哦，反正就是UDP 53
是，但还有TCP 53
请求/应答的端口规律？屏蔽TCP?
example.com.是域名？是名字？是域？区？还有“.”?!@#$%^）*
也许吧…
FQDN, name/domain/zone,
上了DNSSEC，应该安全了吧
是，但只解决了一小部分问题
但，也许更糟…

NS科普 – 系统角色


各级授权节点
面向网民的 DNS
服务节点
A?www.example.com.
NS for .com
A?www.example.com.
NS for example.com
A?www.example.com.
1.2.3.4
A?www.example.com
1.2.3.4
路由器
缓存服务器
递归服务器
“ ”
.com
example.com
root 根
com
net
cn
通用顶级域
国家
baidu
example

录

第一部分

DNS科普

第二部分

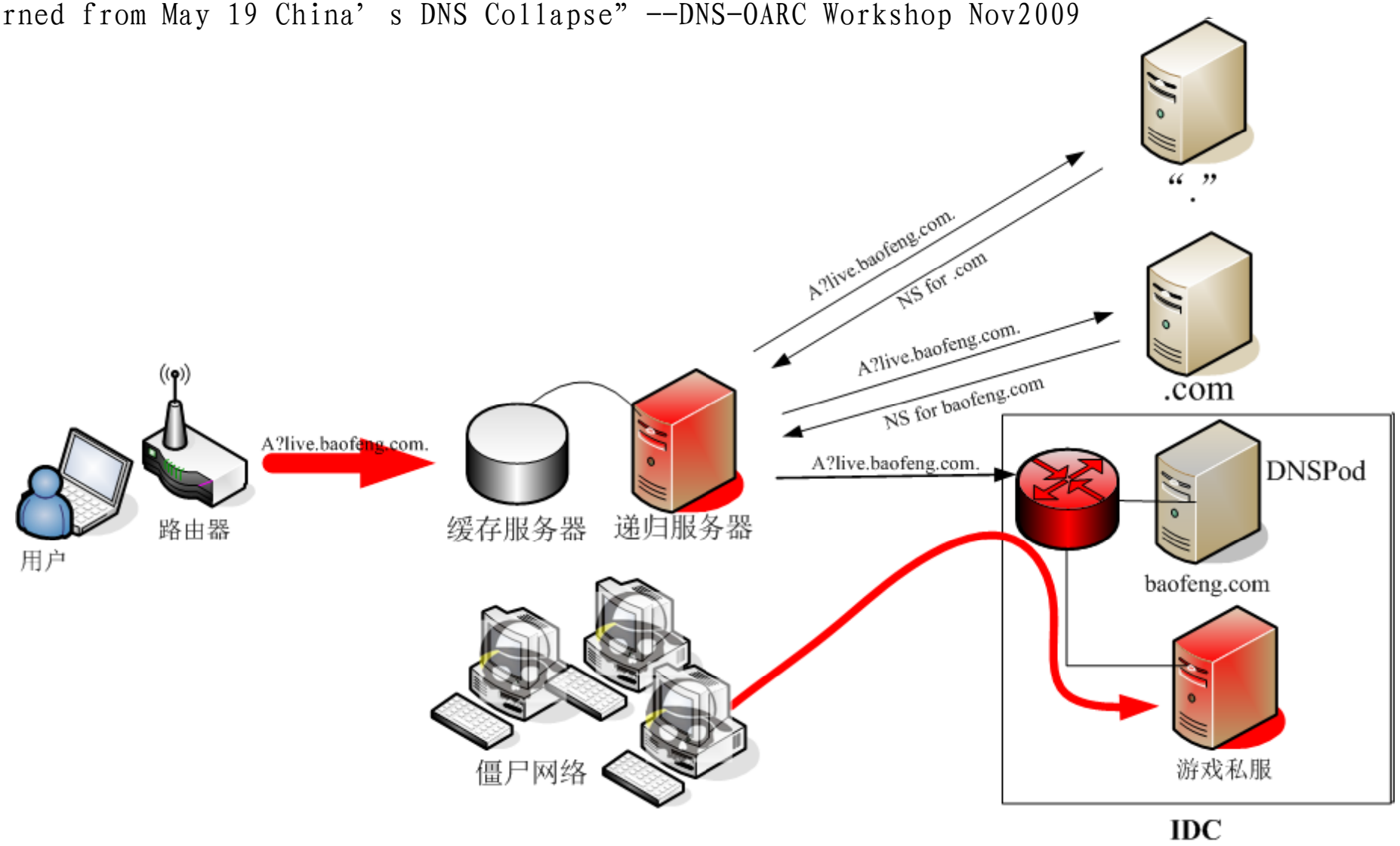
这些年，那些事儿

第三部分

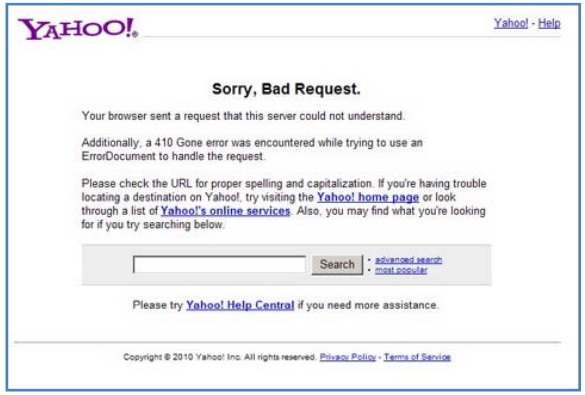
DNS安全关注点

09-05-19 暴风影音

ssons Learned from May 19 China’ s DNS Collapse” --DNS-OARC Workshop Nov2009



10-01-12 百度




```
domain name: baidu.com
registrar: register.com, inc.
whois server: whois.register.com
referral url: http://www.registe
name server: yns1.yahoo.com
name server: yns2.yahoo.com
status: clienttransferprohibited
updated date: 11-jan-2010
creation date: 11-oct-1999
expiration date: 11-oct-2014
```

11-Q2 DNS隧道和递归攻击 – 场景III

S递归攻击中的查询特点:

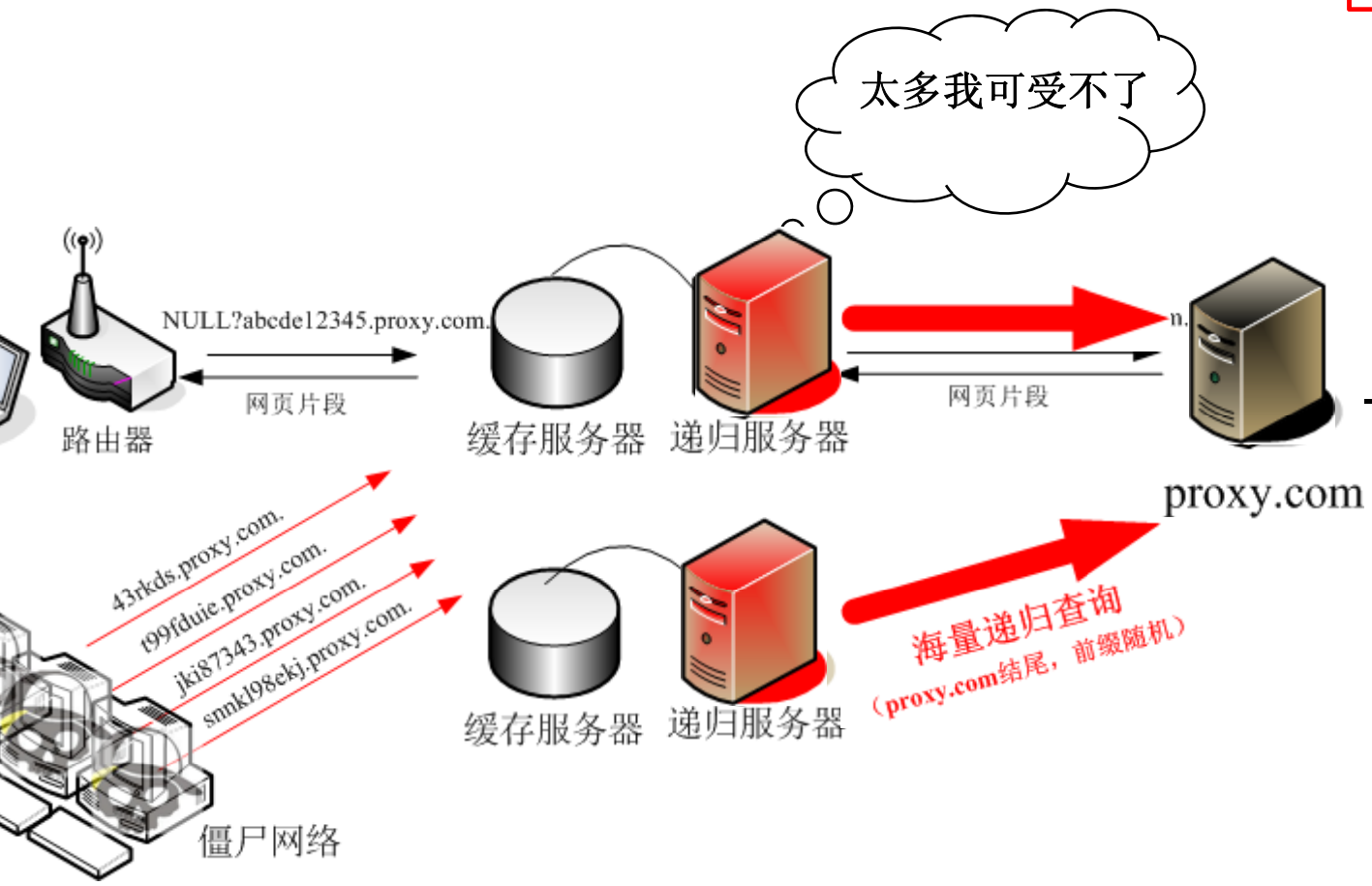
后缀：稳定，一致

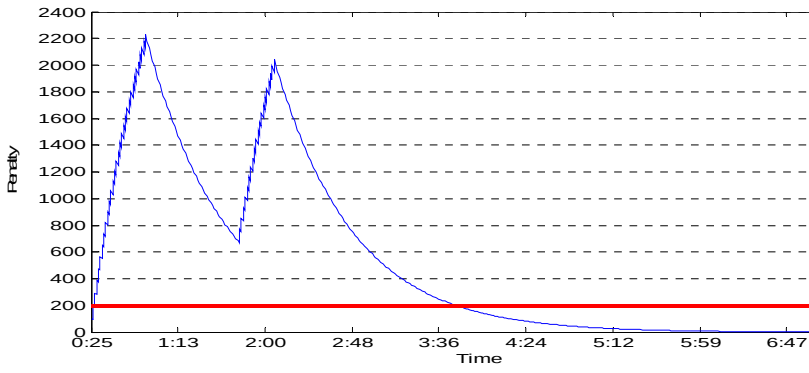
前缀：频繁变化、唯一、NXdomain

递归攻击的智能防护
SM/RFC算法（DNSEASY2011）

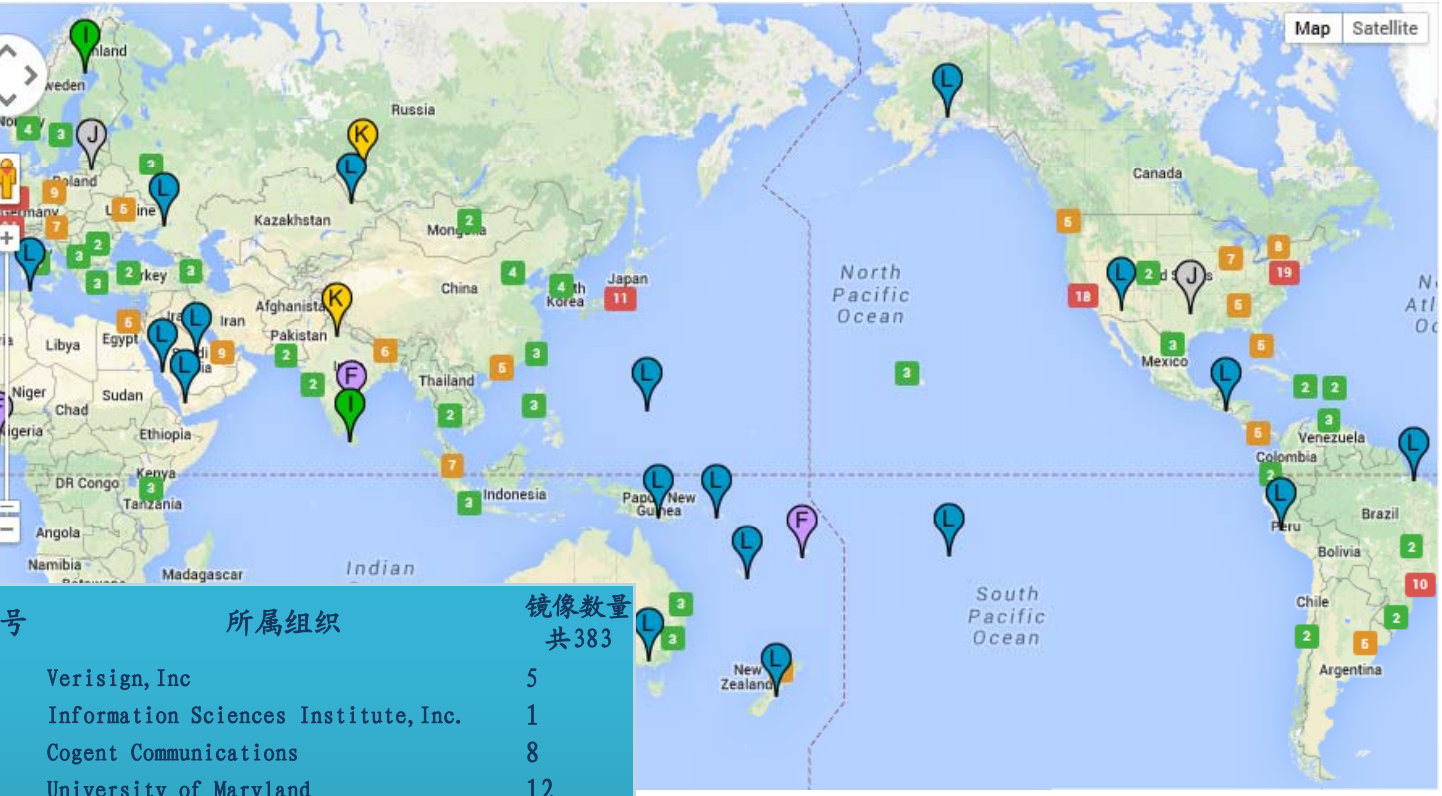
某省级DNS节点24小时监测结果

被抑制解析的聚类域	聚类域查询次数	最大的每分钟查询数	抑制解析总时长 最大连续抑制时 / 抑制次数
www-geme456.net	6937090	98093	173/173/1
vwvvw-garne456.com	3402737	141704	200/200/1
emga456.com	2198819	305873	77/77/1
vvwvw-garne456.com	1735165	258406	97/57/2
214sp.com	844037	171130	62/62/1
qamer456.com	564760	250660	40/40/1
gamenc456.com	411593	203801	30/30/1
18wsm.com	333293	21499	131/120/2
qamea456.com	158022	135165	17/17/1
000390.com	155954	22346	82/82/1
at5.com.cn	115219	15710	67/67/1
337070.com	51996	26739	6/6/1



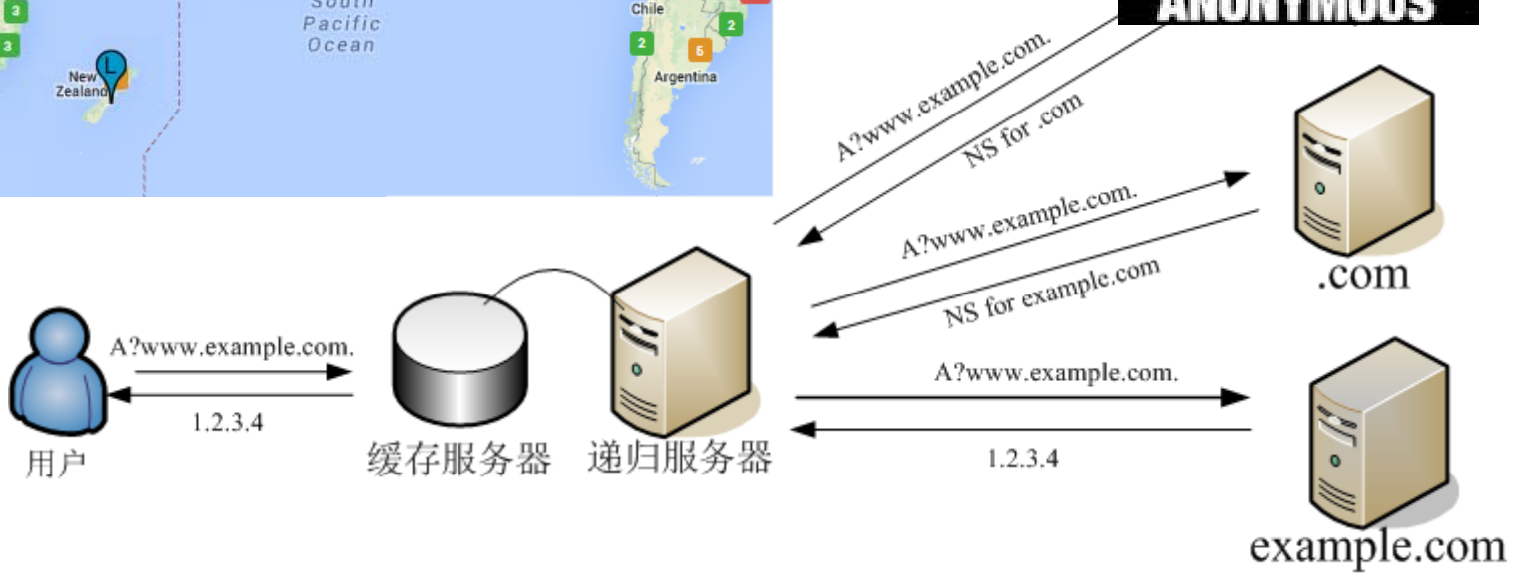


12-03-31 “攻击DNS根？”



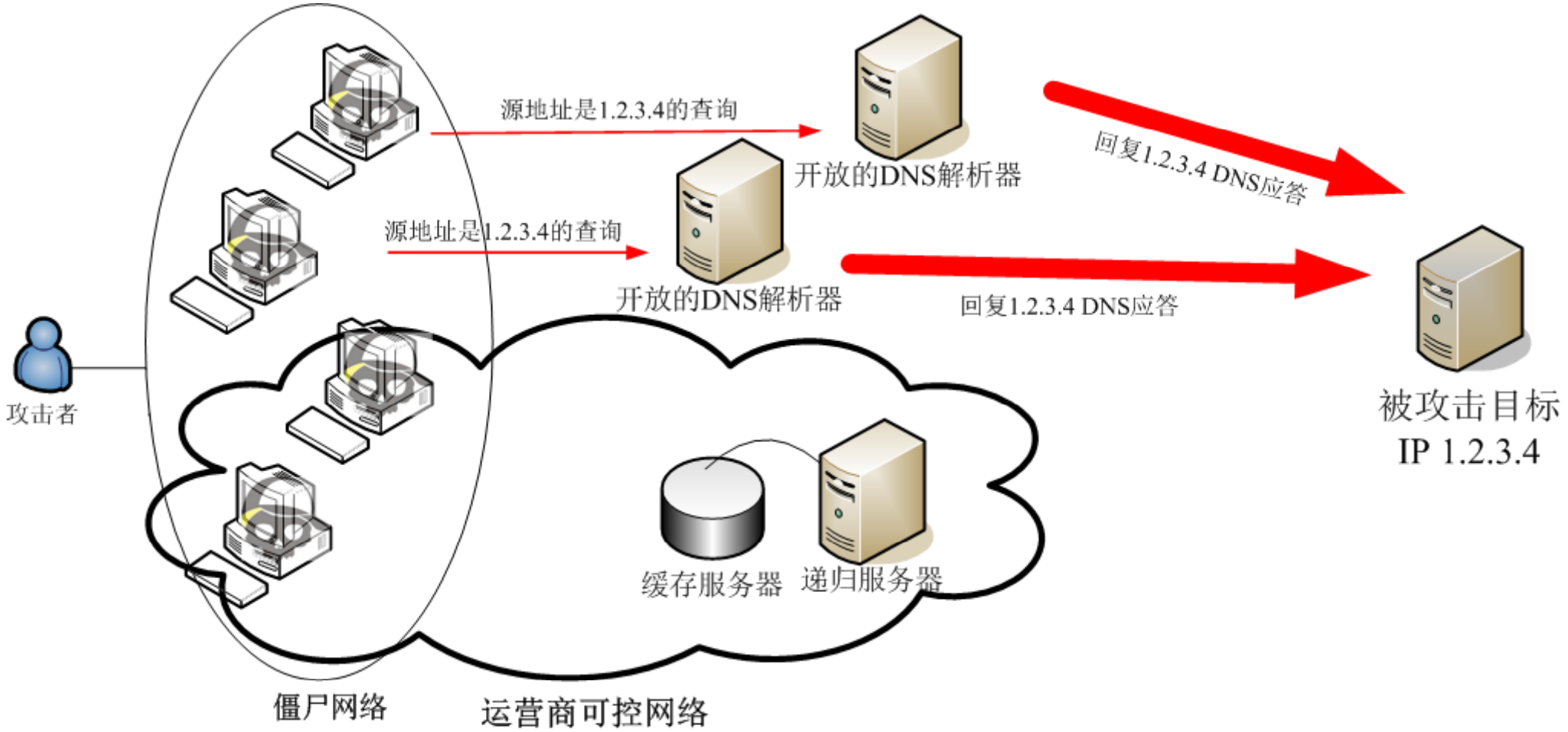
号	所属组织	镜像数量 共383
	Verisign, Inc	5
	Information Sciences Institute, Inc.	1
	Cogent Communications	8
	University of Maryland	12
	NASA Ames Research Center	12
	Internet Systems Consortium	55
	U.S. DOD Network Information Center	6
	U.S. Army Research Lab	2
	Netnod (formerly Autonomica)	41
	Verisign, Inc.	73
	RIPE NCC	17
	ICANN	144
	WIDE Project	7

“Two days in the life of the DNS anycast r servers” -- PAM2007



13-03-27 Spamhaus被攻击

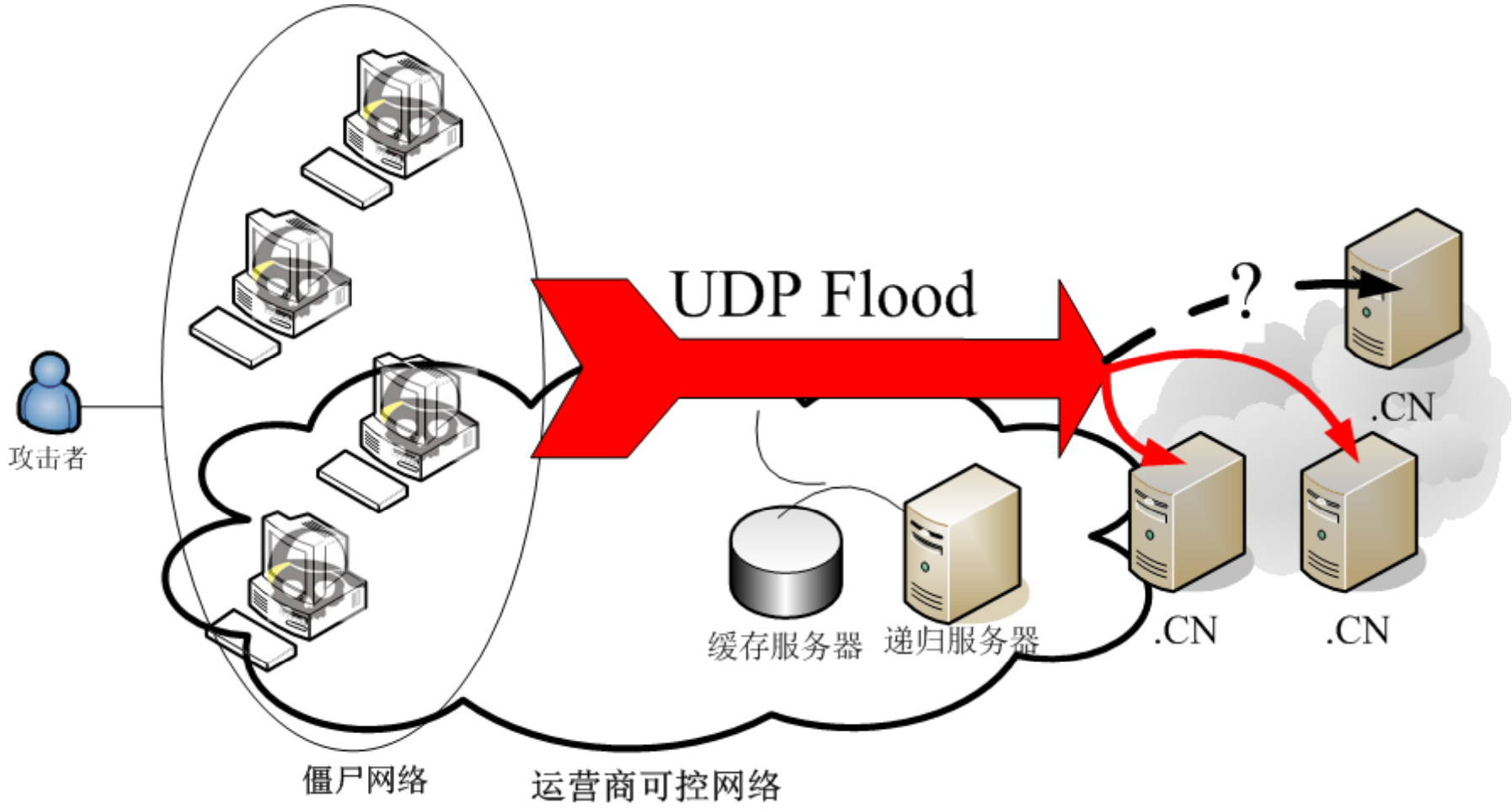
放的DNS解析器 → DNS反射放大 → 对互联网带宽压力 → 可控的运营商DNS → 虚假源地址流量管控



13-Q2 家用路由器DNS劫持

```
://admin:admin@192.168.1.1
rRpm/LanDhcpServerRpm.htm?
server=1&ip1=192.168.1.100
=192.168.1.199&Lease=30&ga
y=192.168.1.1&domain=&dnss
r=0.0.0.0&dnsserver2=0.0.0
ave=%B1%A3+%B4%E6
```

13-08-25 .CN



! ? !!

...

录

第一部分

DNS科普

第二部分

这些年，那些事儿

第三部分

DNS安全关注点

议安全

DNSSEC解决几个问题，放大一堆问题

- 数据是否完整，来源是否真实，主机是否真的不存在
- 信任锚，信任链，密钥的保管和分发
- 查询包大，响应包更大，递归的压力
- 离全体系部署还有多远 ？别忽悠，认真试点！

BIND9问题频发，BIND10表现何如

- 选择商用解析软件/其他开源软件进行异构

用安全

递归服务遭受正规互联网应用的滥用

- 多媒体软件、DNS隧道、ENUM、云资源定位、RFID…

DNS查询/应答被恶意代码利用

- 递归攻击、反射攻击、僵尸控制

权威服务器的安全管控

- 注册商、托管商、拥有者自己…

开放解析器

- 开放 → 失控

构安全

集中式 vs 分布式

- 节点内外的Anycast
- 一次有趣的交锋

授权-缓存-递归功能的物理分离

- 角色的差异决定了流量行为的差异和安全防护手段的差异
- 主授权的重要性和隐蔽性
- 缓存的高能力，控制的灵活性和对异常的控制颗粒度
- 递归的收敛度、资源消耗控制，可舍弃程度，CDN友好

中立性 vs 倾向性

- 互联网巨头之间的恩怨
- 运营商的功利性
- 运营商的中立性

经过这些年，那些事 … 我们努力让DNS更加安全