Geekbang. 极客邦科技 InfoQ

QCon 全球软件开发大会【北京站】2016

点线面，一个安全人员的漏洞世界

张祖优(Fooying)

Intemational Software Development Conference

关于我

Fooying

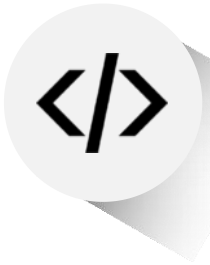
来自知道创宇安全研究团队404
安全研究员，产品经理

微博：http://weibo.com/fooying
知乎专栏：http://zhuanlan.zhihu.com/fooying

关于我

安全研究人员

08年接触黑客与安全，4年安全行业工作经验
在 KCon、WOT2014、ISF 等会议上做过安全相关演讲，给腾讯、微软、阿里等报送过漏洞



程序猿

软件技术专业毕业，学过.net、PHP等，
Pythoner，自学会点前端、会点 PS 等

半吊子产品经理

负责知道创宇漏洞社区，是Seebug.org 产品经理，同步算是ZoomEye.org、Kcon 官网等平台产品经理

目录

黑客与黑客思维

那些被忽略的安全问题

你不知道的点到面的攻击

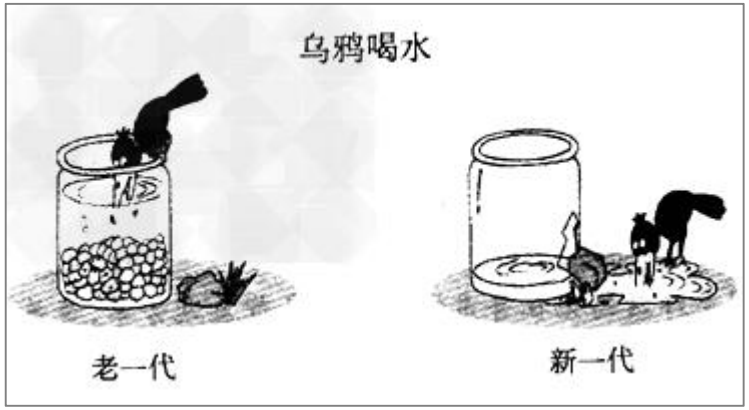
成为一名黑客

01 黑客与黑客思维

什么是黑客？

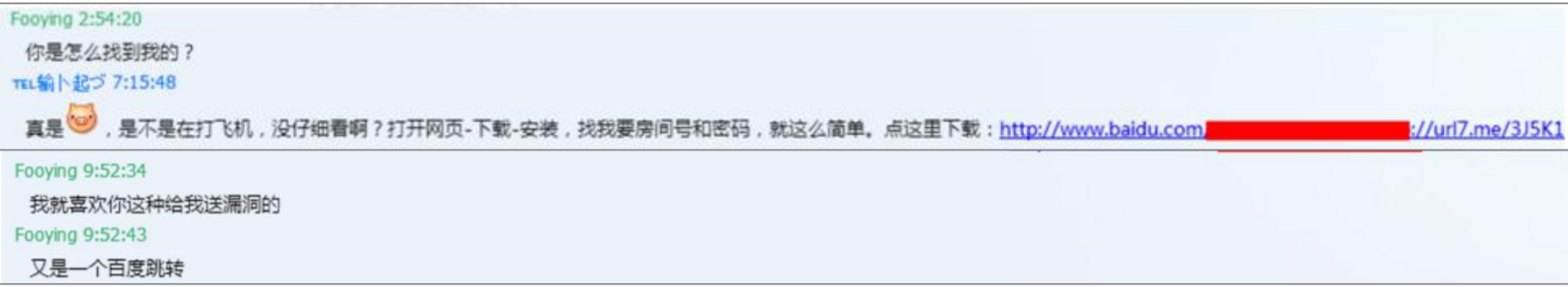
创造与突破，守正出奇

创造与突破



-折叠	2015-09-22 09:54:42	• location : http://kefu.game.corp.qihoo.net:8360/monitor_onlinework.html# • toplocation : http://kefu.game.corp.qihoo.net:8360/monitor_onlinework.html# • cookie : TD=t%3D1437139960%26s%3D2b35ce4fb5184c524046e38a5f69adb7%26a%3D1; QD=u%3Dlnatfra%26m%3Dlnatfra%40360.pa; kefu=3c612cc89141d1daf7fba11fee6da844; PS_LOGINLIST=-1; ExpirePage=; PS_TOKENEXPIRE=-1; PS_TOKEN=; svcUser=yangsen%40360.cn--CN%3DDomain Users%2CCN%3DUsers%2CDC%3Dcorp%2CDC%3Dqihoo%2CDC%3Dnet--yangsen--%E6%9D%A8%E6%A3%AE--61f9707208f9c21286c69c7675289274 • opener :	• HTTP_REFERER : http://kefu.game.corp.qihoo.net:8360/monitor_onlinework.html • HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.152 Safari/537.36 • REMOTE_ADDR : 182.150.21.238, 182.150.21.238	删除
-折叠	2015-09-22 08:57:07	• location : http://kefu.game.corp.qihoo.net:8360/monitor_onlinework.html • toplocation : http://kefu.game.corp.qihoo.net:8360/monitor_onlinework.html • cookie : TD=t%3D1437139960%26s%3D2b35ce4fb5184c524046e38a5f69adb7%26a%3D1; QD=u%3Dlnatfra%26m%3Dlnatfra%40360.pa; kefu=3c612cc89141d1daf7fba11fee6da844; PS_LOGINLIST=-1; ExpirePage=; PS_TOKENEXPIRE=-1; PS_TOKEN=; svcUser=yangsen%40360.cn--CN%3DDomain Users%2CCN%3DUsers%2CDC%3Dcorp%2CDC%3Dqihoo%2CDC%3Dnet--yangsen--%E6%9D%A8%E6%A3%AE--61f9707208f9c21286c69c7675289274 • opener :	• HTTP_REFERER : http://kefu.game.corp.qihoo.net:8360/monitor_onlinework.html • HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.152 Safari/537.36 • REMOTE_ADDR : 182.150.21.238, 182.150.21.238	删除


+全部
时间
接收的内容
Request Headers
操作
+展开
2015-09-23 13:23:27
location : http://www.coolpad.com/FFFa
HTTP_REFERER : http://www.coolpad.c
删除
+展开
2015-09-23 13:23:08
location : http://www.coolpad.com/FFFa
HTTP_REFERER : http://www.coolpad.c
删除
+展开
2015-09-22 09:54:42
location : http://kefu.game.corp.qihoo.ne
HTTP_REFERER : http://kefu.game.corp.
删除
+展开
2015-09-22 08:57:07
location : http://kefu.game.corp.qihoo.ne
HTTP_REFERER : http://kefu.game.corp.
删除
+展开
2015-02-08 19:54:45
location : http://www.coolpad.com/FFFa
HTTP_REFERER : http://www.coolpad.c
删除
+展开
2015-02-08 19:38:23
location : http://www.coolpad.com/FFFa
HTTP_REFERER : http://www.coolpad.c
删除
+展开
2015-01-11
location : http://118.145.22.73/juaicai-us
HTTP_REFERER : http://118.145.22.73/j
删除
看到框就想X
+展开
http://union.xyz.cn/uni
删除
+展开
http://union.xyz.cn/uni
删除
+展开
2014-08-29 16:18:54
location : http://union.xyz.cn/unionApi/in
HTTP_REFERER : http://union.xyz.cn/uni
删除
+展开
2014-08-29 11:19:42
location : http://admin.t.so.com:8361/ind
HTTP_REFERER : http://admin.t.so.com:
删除
+展开
2014-08-29 11:05:54
location : http://admin.t.so.com:8361/ind
HTTP_REFERER : http://admin.t.so.com:
删除
+展开
2014-08-28 15:01:38
location : http://admin.t.so.com:8361/ind
HTTP_REFERER : http://admin.t.so.com:
删除
+展开
2014-08-11 18:00:59
location : http://newadmin.mail.sina.co
HTTP_REFERER : http://newadmin.mail.
删除
+展开
2014-08-11 17:46:42
location : http://newadmin.mail.sina.co
HTTP_REFERER : http://newadmin.mail.
删除
+展开
2014-08-04 14:31:06
location : http://newadmin.mail.sina.co
HTTP_REFERER : http://newadmin.mail.
删除
+展开
2014-08-04
location : http://newadmin.mail.sina.co
HTTP_REFERER : http://newadmin.mail.
删除

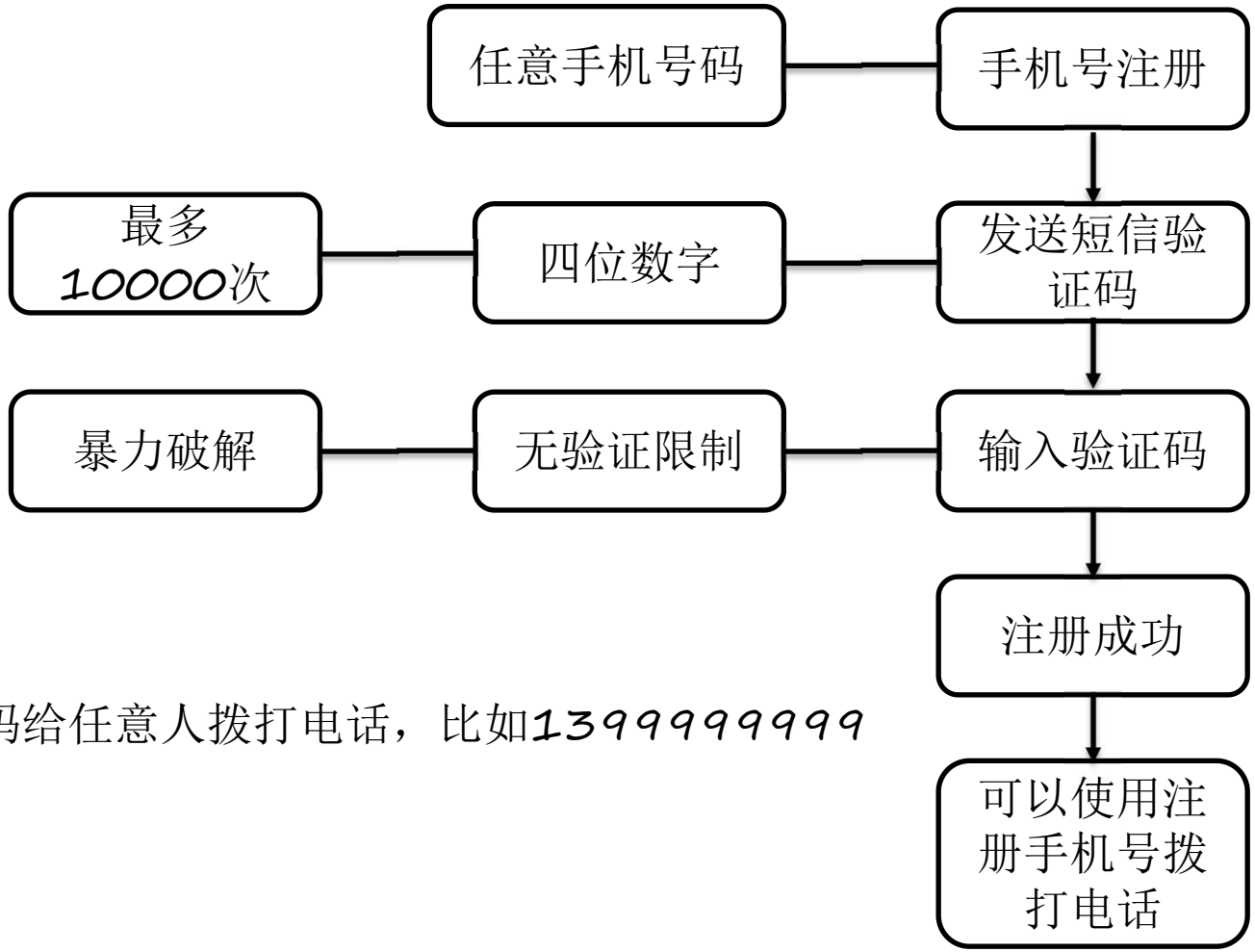

Fooying 2:54:20
你是怎么找到我的？
TEL输卜起づ 7:15:48
真是，是不是在打飞机，没仔细看啊？打开网页-下载-安装，找我要房间号和密码，就这么简单。点这里下载：http://www.baidu.com[redacted]://url7.me/3J5K1
Fooying 9:52:34
我就喜欢你这种给我送漏洞的
Fooying 9:52:43
又是一个百度跳转

02 那些被忽略的安全问题

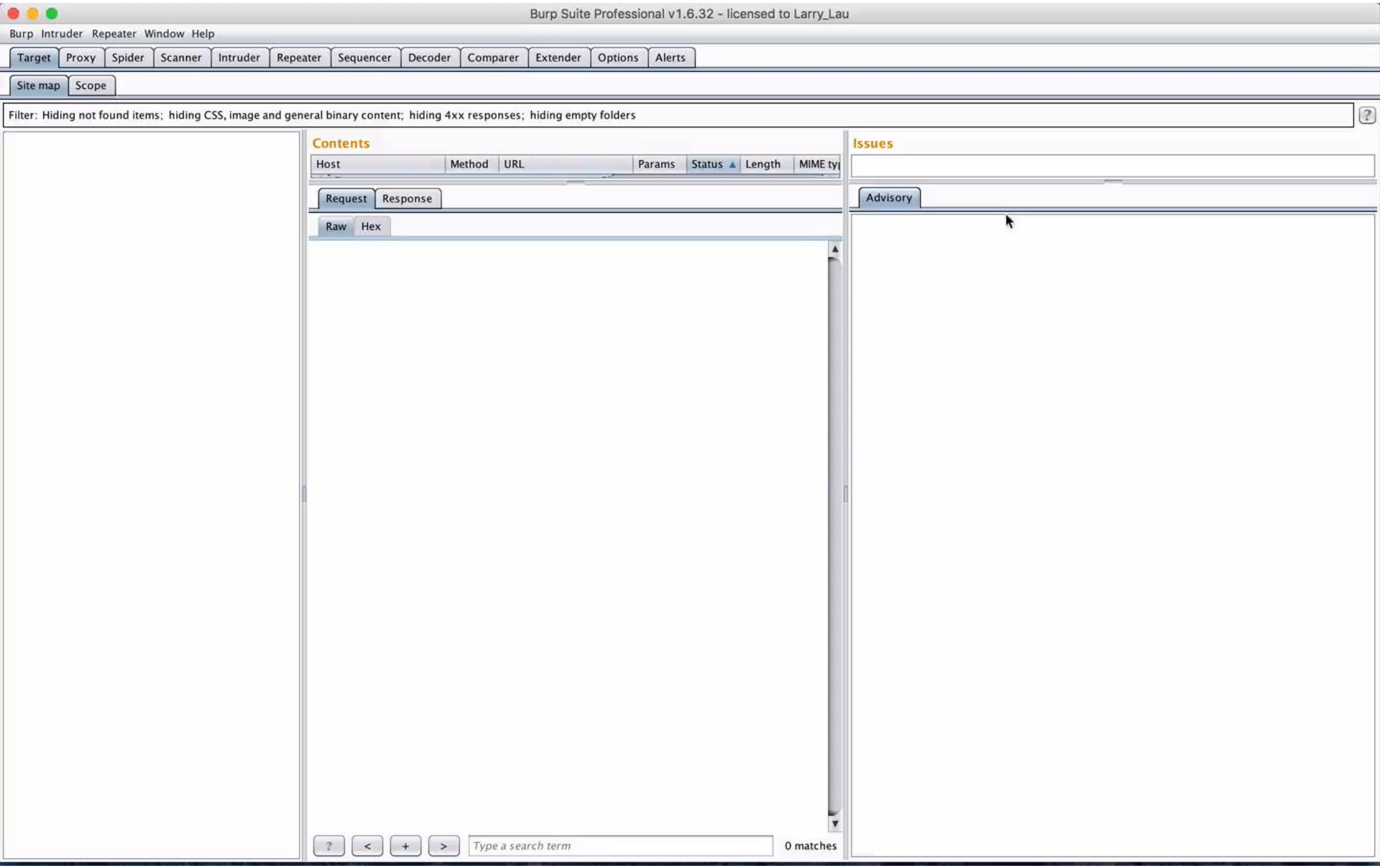
轻而易举突破的限制


只需15秒，手机号注册送36分钟话费！
手机注册
手机号：
手机号不能为空
验证码：
换一张
提交注册
我已阅读并同意 的<服务条款>
注册 网络电话：
国内长途低至5分，国际长途7分起
所有会员夜间通话完全免费
手机，电脑多方式随意拨打
and
已有 帐号？
直接登录>>
有问题？寻找帮助

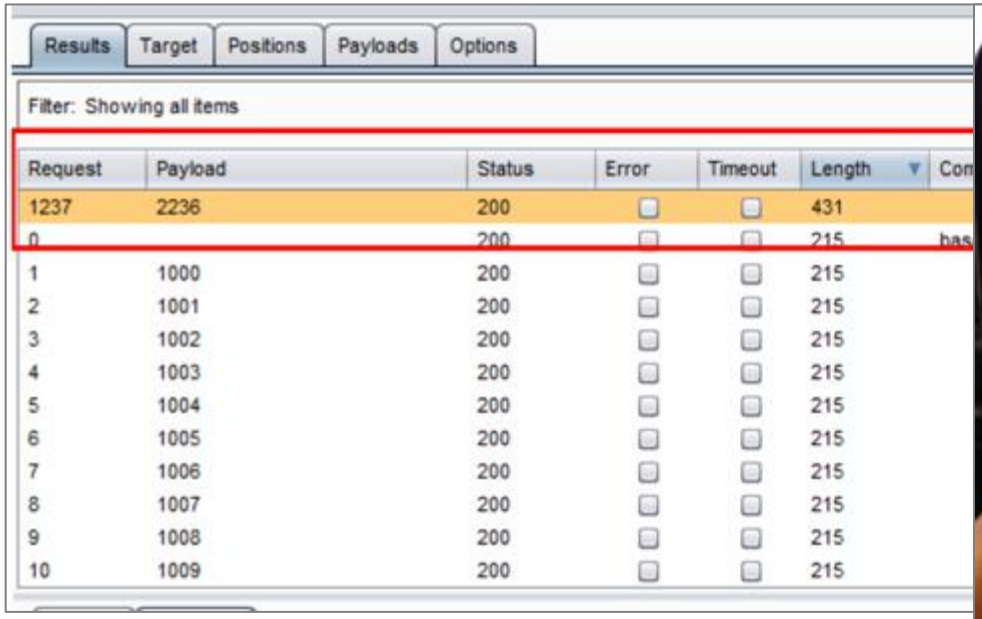
轻而易举突破的限制

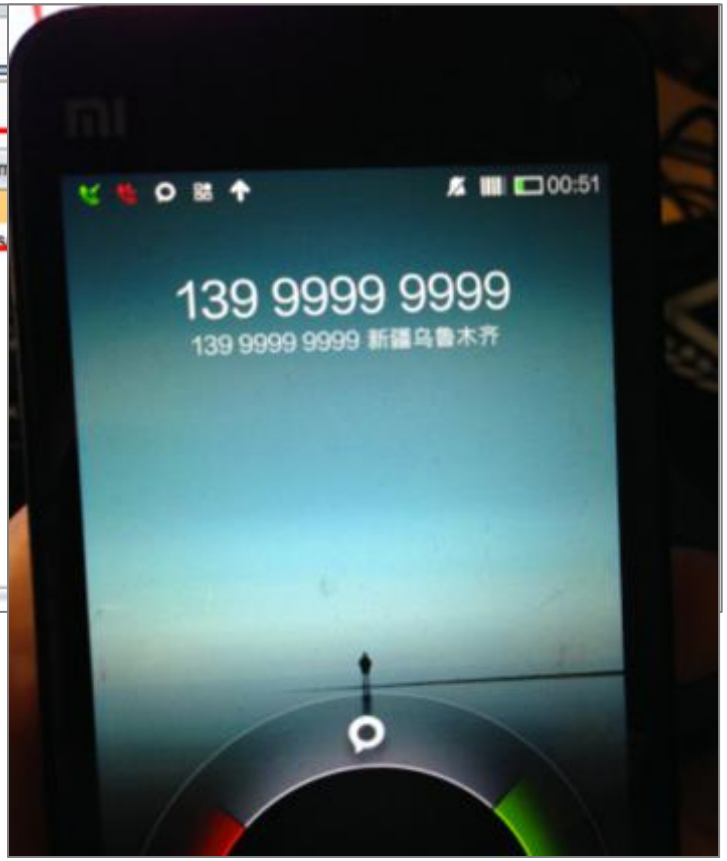


任意号码给任意人拨打电话，比如1399999999


Burp Suite Professional v1.6.32 - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Contents
Host Method URL Params Status Length MIME ty
Request Response
Raw Hex
Type a search term
0 matches
Issues
Advisory

利用流程

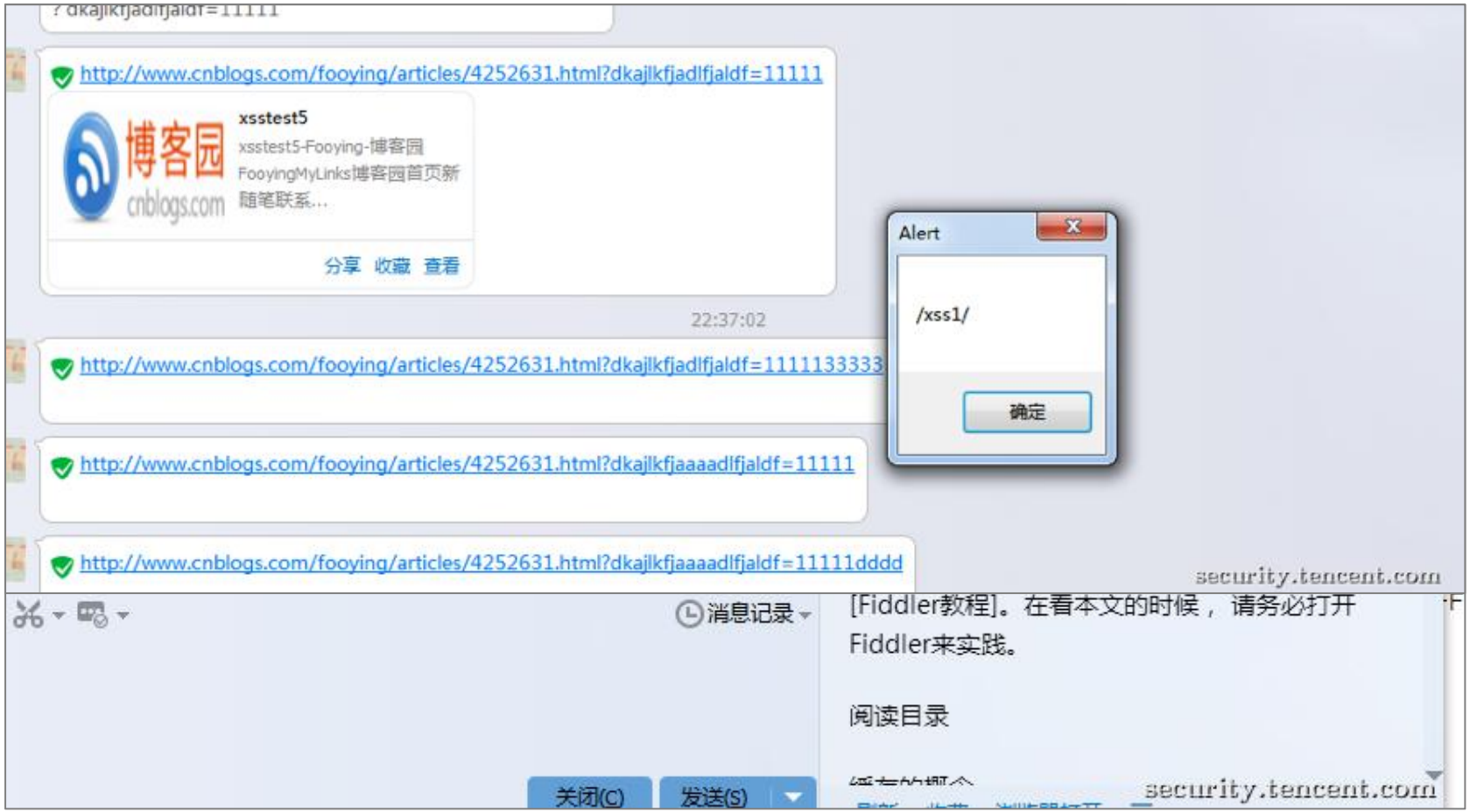

Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
1237 2236 200 431
0 200 215
1 1000 200 215
2 1001 200 215
3 1002 200 215
4 1003 200 215
5 1004 200 215
6 1005 200 215
7 1006 200 215
8 1007 200 215
9 1008 200 215
10 1009 200 215


00:51
139 9999 9999
139 9999 9999 新疆乌鲁木齐

不可信的安全来源

2015/02/15	QQ客户端页面预览XSS[复查异议][复查异议][复查异议]	已修复
2015/02/04	QQ客户端页面预览XSS[复查异议][复查异议]	已完成
2015/01/28	QQ客户端页面预览XSS[复查异议]	已完成
2015/01/23	QQ客户端页面预览XSS	已完成

不可信的安全来源


http://www.cnblogs.com/fooying/articles/4252631.html?dkajlkfjadlfjaldf=11111
xsstest5
xsstest5-Fooying-博客园
FooyingMyLinks博客园首页新
随笔联系...
分享 收藏 查看
22:37:02
http://www.cnblogs.com/fooying/articles/4252631.html?dkajlkfjadlfjaldf=1111133333
http://www.cnblogs.com/fooying/articles/4252631.html?dkajlkfjaaaadlfjaldf=11111
http://www.cnblogs.com/fooying/articles/4252631.html?dkajlkfjaaaadlfjaldf=11111dddd
Alert
/xss1/
确定
security.tencent.com
消息记录
[Fiddler教程]。在看本文的时候， 请务必打开
Fiddler来实践。
阅读目录
关闭(C)
发送(S)
security.tencent.com

不可信的安全来源


Alert
1
确定
应用
更多
相册
文件
投票
签到
群成员(2/2)


通知中心
视频 "><img src=1 onerror=alert(

不可信的安全来源

1、登录注册跳转链接的可替换导致的XSS

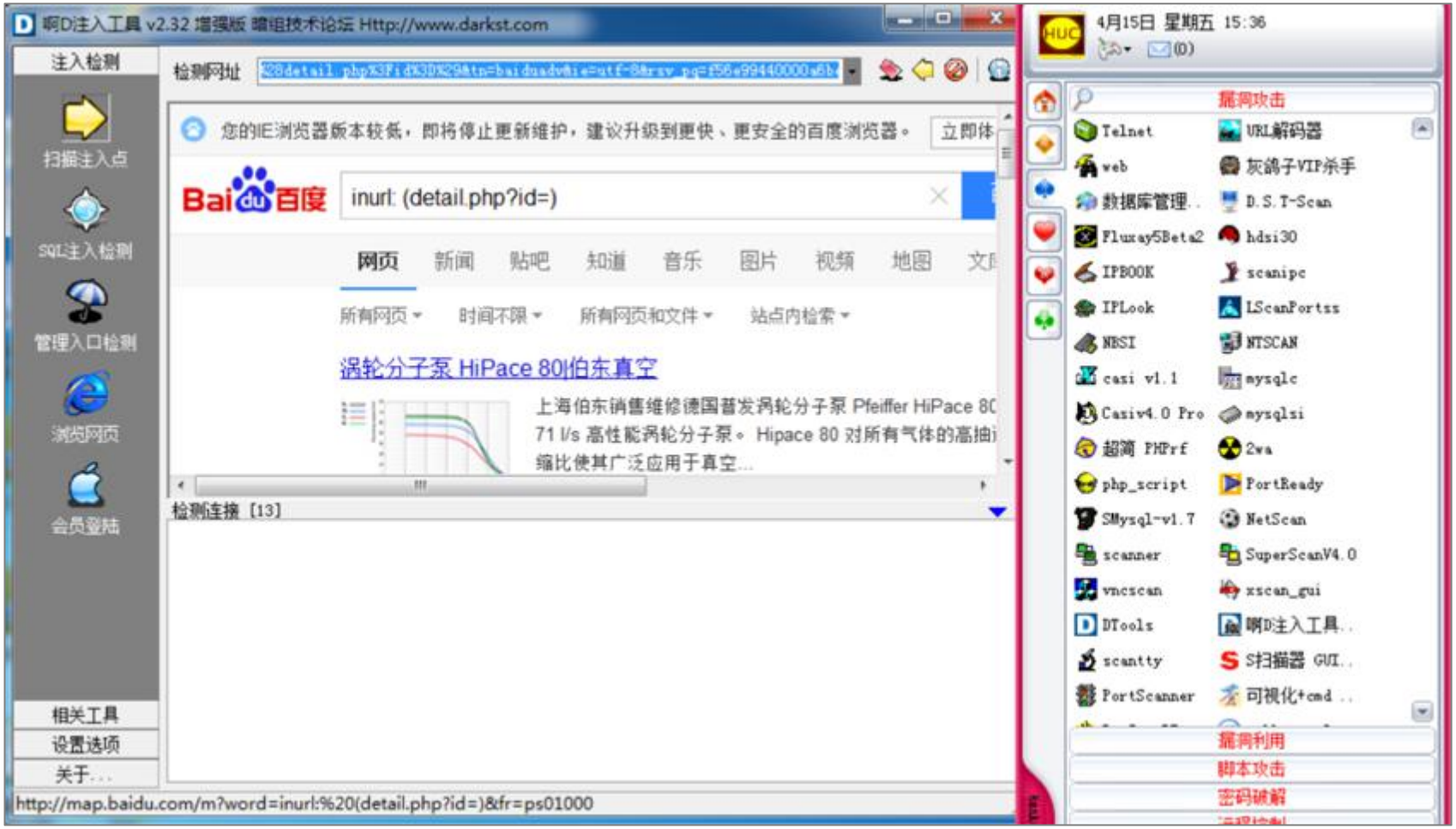
2、拍拍网店存储型XSS利用QQ昵称构造 Payload

…

失效的权限控制

http://www.example.com/detail.php?userid=123

那些被忽略的安全问题


啊D注入工具 v2.32 增强版 暗组技术论坛 Http://www.darkst.com
注入检测
检测网址
扫描注入点
SQL注入检测
管理入口检测
浏览网页
会员登陆
相关工具
设置选项
关于...
您的IE浏览器版本较低，即将停止更新维护，建议升级到更快、更安全的百度浏览器。
立即体
Bai du 百度
inurl: (detail.php?id=)
网页 新闻 贴吧 知道 音乐 图片 视频 地图
所有网页 时间不限 所有网页和文件 站点内检索
涡轮分子泵 HiPace 80|伯东真空
上海伯东销售维修德国普发涡轮分子泵 Pfeiffer HiPace 80
71 l/s 高性能涡轮分子泵。 Hipace 80 对所有气体的高抽
缩比使其广泛应用于真空...
检测连接 [13]
http://map.baidu.com/m?word=inurl:%20(detail.php?id=)&fr=ps01000
4月15日 星期五 15:36
漏洞攻击
Telnet
URL解码器
web
灰鸽子VIP杀手
数据库管理..
D.S.T-Scan
Fluxay5Beta2
hdsi30
IPBOOK
scanipc
IPLook
LScanPortss
NBSI
NTSCAN
casi v1.1
mysqlc
Casiv4.0 Pro
mysqlsi
超简 PHPrf
2wa
php_script
PortReady
SMysql-v1.7
NetScan
scanner
SuperScanV4.0
vncscan
xscan_gui
DTools
啊D注入工具..
scantty
S扫描器 GUI..
PortScanner
可视化+cmd ..
漏洞利用
脚本攻击
密码破解

03 你不知道的点到面的攻击

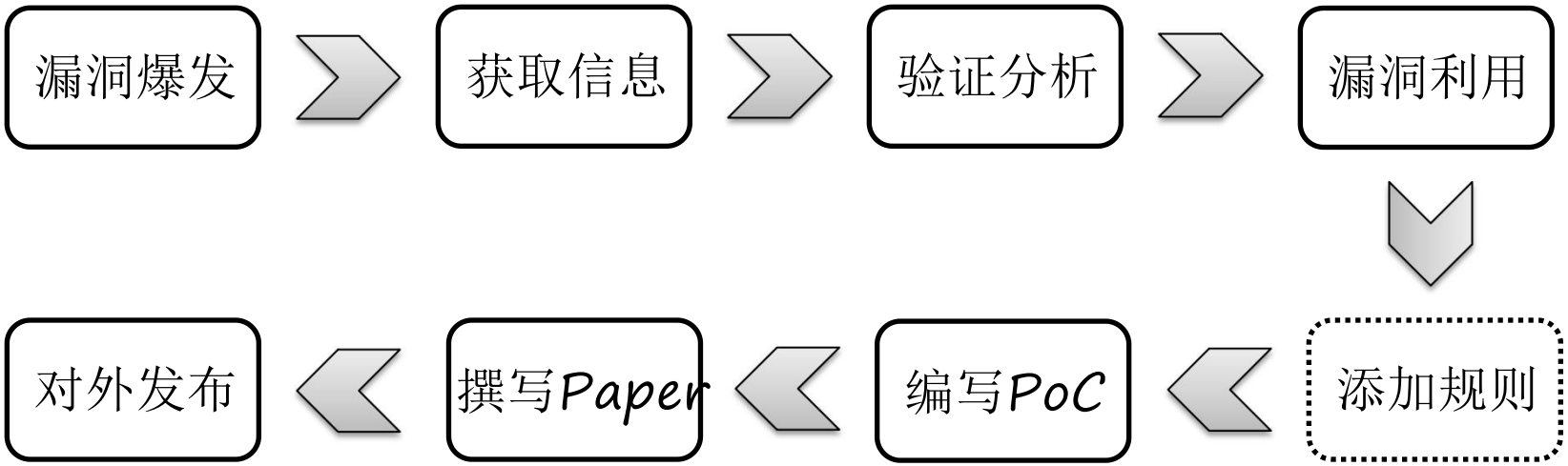
漏洞应急与研究

黄金应急时间

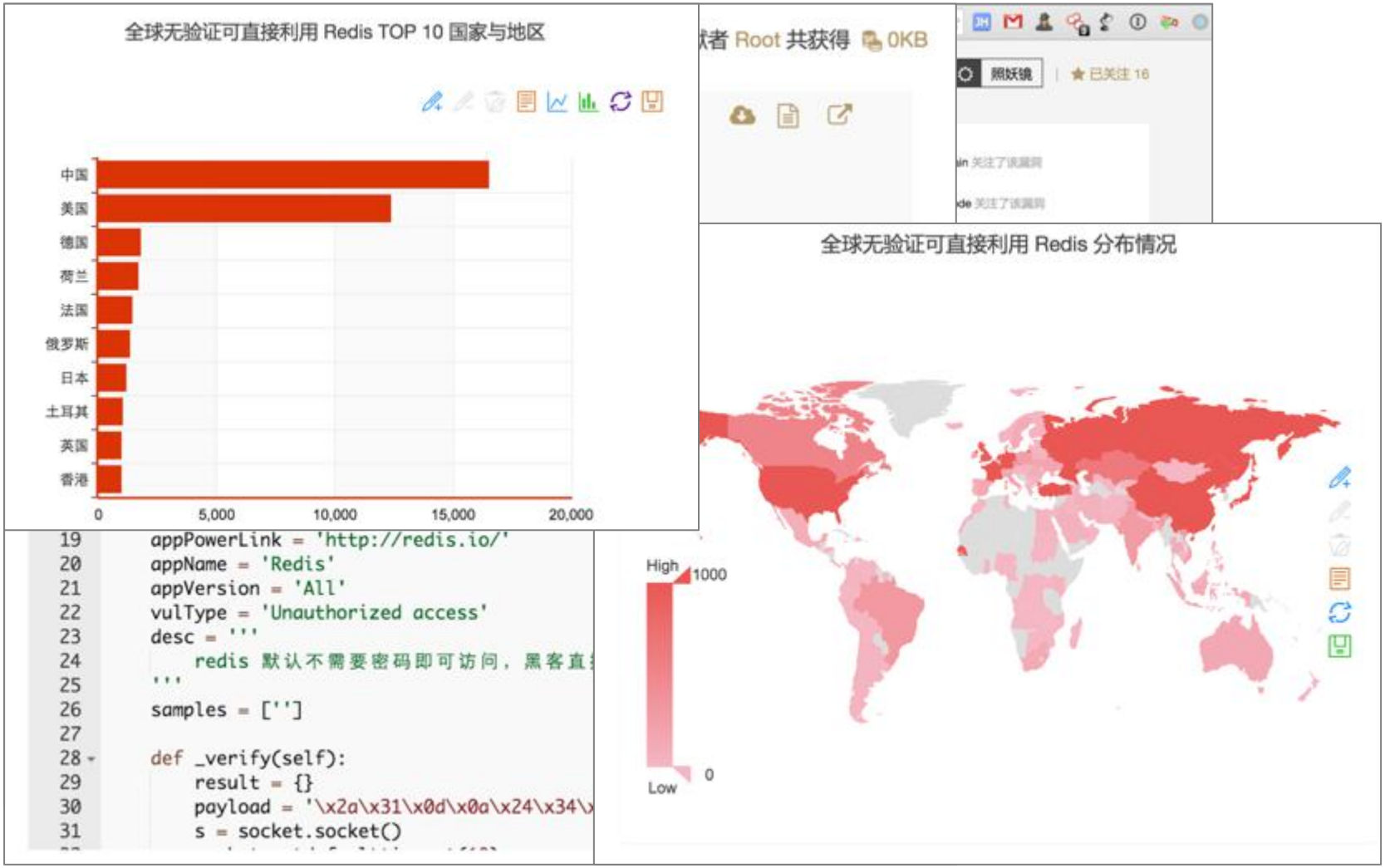
〔 1h 〕 〔 6h 〕 〔12h〕 〔24h〕

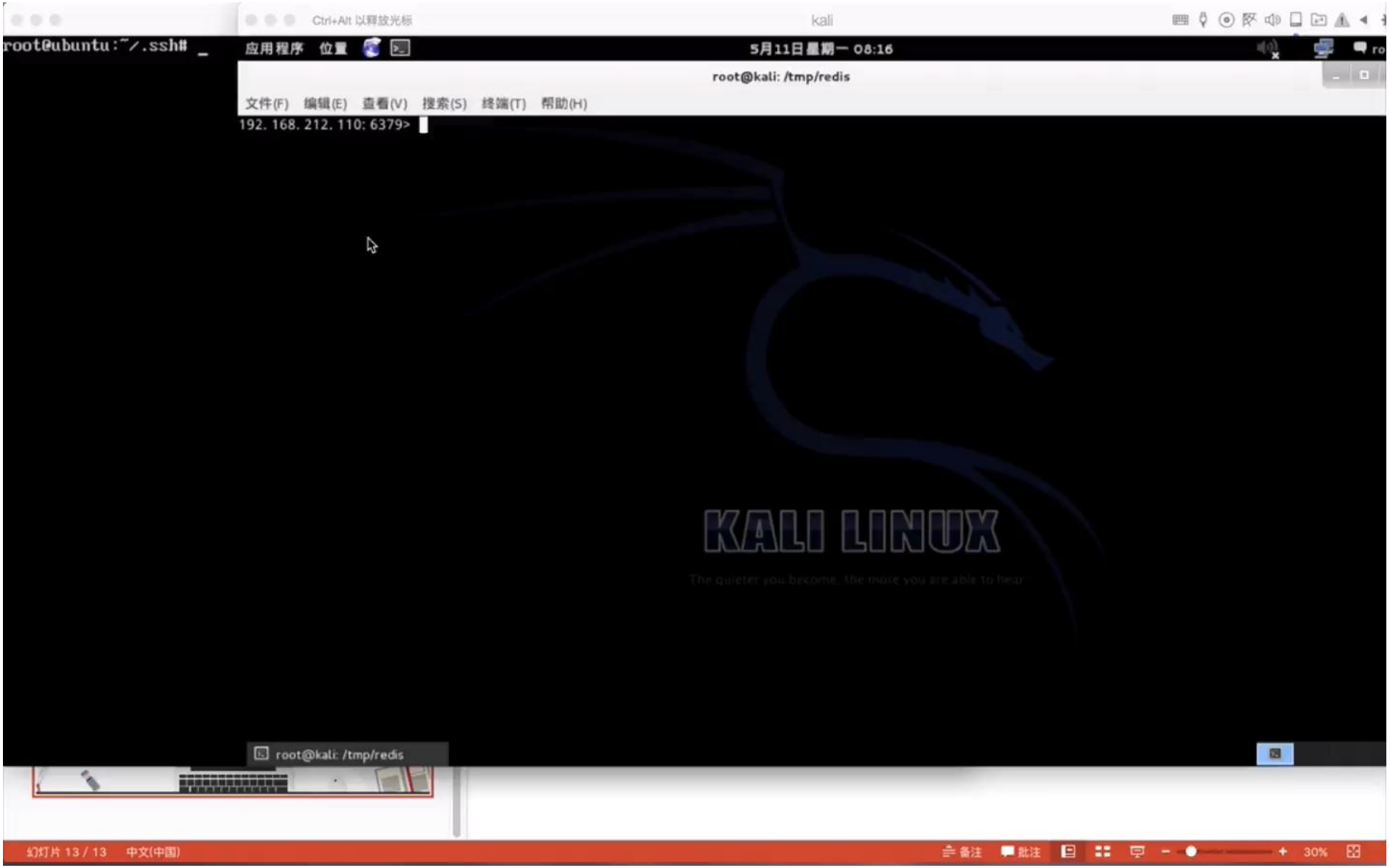
漏洞应急与研究

应急流程



漏洞应急与研究


全球无验证可直接利用 Redis TOP 10 国家与地区
中国
美国
德国
荷兰
法国
俄罗斯
日本
土耳其
英国
香港
0
5,000
10,000
15,000
20,000
者 Root 共获得 0KB
照妖镜
已关注 16
全球无验证可直接利用 Redis 分布情况
High
1000
0
Low
appPowerLink = 'http://redis.io/'
appName = 'Redis'
appVersion = 'All'
vulType = 'Unauthorized access'
desc = '''
redis 默认不需要密码即可访问，黑客直
'''
samples = ['']
def _verify(self):
result = {}
payload = '\x2a\x31\x0d\x0a\x24\x34\
s = socket.socket()

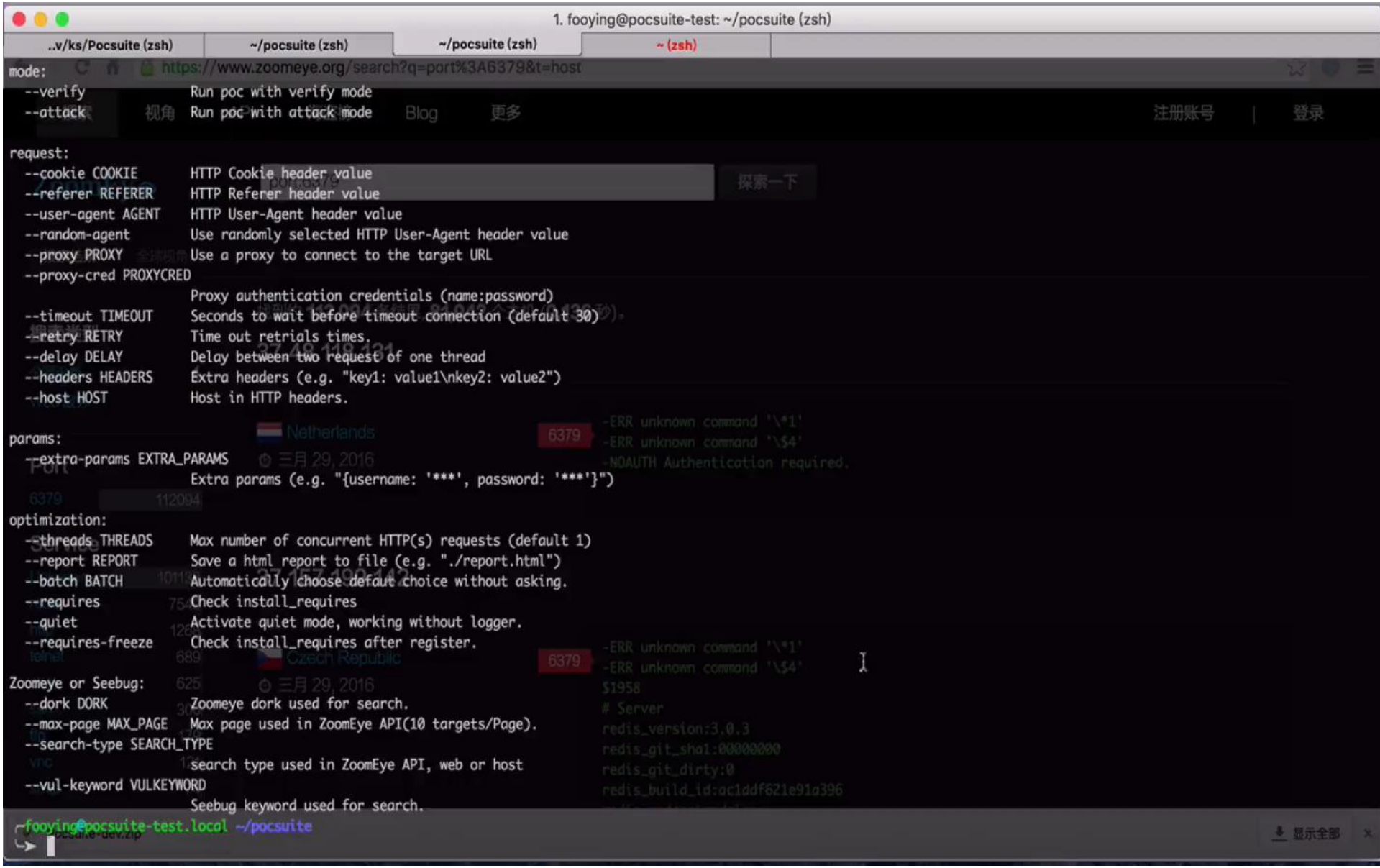

root@ubuntu:~/.ssh#
Ctrl+Alt 以释放光标
kali
应用程序 位置
5月11日星期一 08:16
root@kali: /tmp/redis
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
192.168.212.110:6379>
KALI LINUX
The quieter you become, the more you are able to hear
root@kali: /tmp/redis
幻灯片 13 / 13
中文(中国)
备注
批注
30%

面的攻击

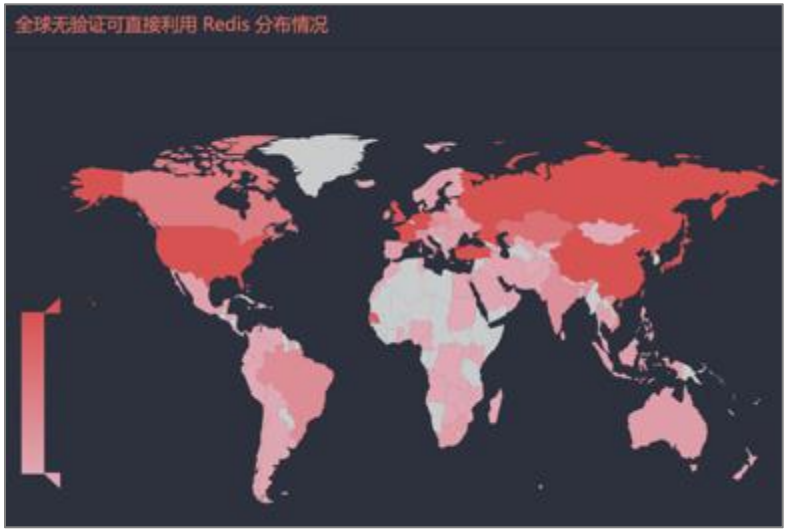
1、自动化的获取存在该漏洞的目标

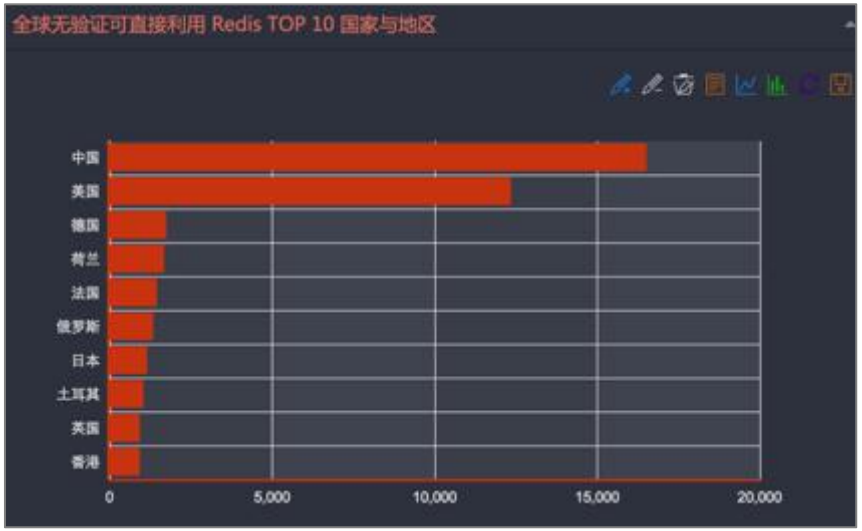
2、漏洞验证脚本

3、自动化的获取目标+调用验证脚本


1. fooying@pocsuite-test: ~/pocsuite (zsh)
..v/ks/Pocsuite (zsh)
~/pocsuite (zsh)
~/pocsuite (zsh)
~ (zsh)
https://www.zoomeye.org/search?q=port%3A6379&t=host
mode:
--verify Run poc with verify mode
--attack Run poc with attack mode
request:
--cookie COOKIE HTTP Cookie header value
--referer REFERER HTTP Referer header value
--user-agent AGENT HTTP User-Agent header value
--random-agent Use randomly selected HTTP User-Agent header value
--proxy PROXY Use a proxy to connect to the target URL
--proxy-cred PROXYCRED
Proxy authentication credentials (name:password)
--timeout TIMEOUT Seconds to wait before timeout connection (default 30)
--retry RETRY Time out retrials times.
--delay DELAY Delay between two request of one thread
--headers HEADERS Extra headers (e.g. "key1: value1\nkey2: value2")
--host HOST Host in HTTP headers.
params:
--extra-params EXTRA_PARAMS
Extra params (e.g. "{username: '***', password: '***'}")
optimization:
--threads THREADS Max number of concurrent HTTP(s) requests (default 1)
--report REPORT Save a html report to file (e.g. "./report.html")
--batch BATCH Automatically choose defaut choice without asking.
--requires Check install_requires
--quiet Activate quiet mode, working without logger.
--requires-freeze Check install_requires after register.
Zoomeye or Seebug:
--dork DORK Zoomeye dork used for search.
--max-page MAX_PAGE Max page used in ZoomEye API(10 targets/Page).
--search-type SEARCH_TYPE
search type used in ZoomEye API, web or host
--vul-keyword VULKEYWORD
Seebug keyword used for search.
fooying@pocsuite-test.local ~/pocsuite
注册账号
登录
探索一下
Netherlands
6379
三月 29, 2016
-ERR unknown command '*1'
-ERR unknown command '\$4'
-NOAUTH Authentication required.
Czech Republic
6379
三月 29, 2016
-ERR unknown command '*1'
-ERR unknown command '\$4'
$1958
Server
redis_version:3.0.3
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:ac1ddf621e91a396
显示全部

面的攻击





根据 ZoomEye 最新于2015年11月12日0点探测结果显示：
总的存在无验证可直接利用 Redis 服务的目标全球有49099，其中中国有16477。其中已经被黑的比例分别是全球65%（3.1万），中国67.5%（1.1万）。

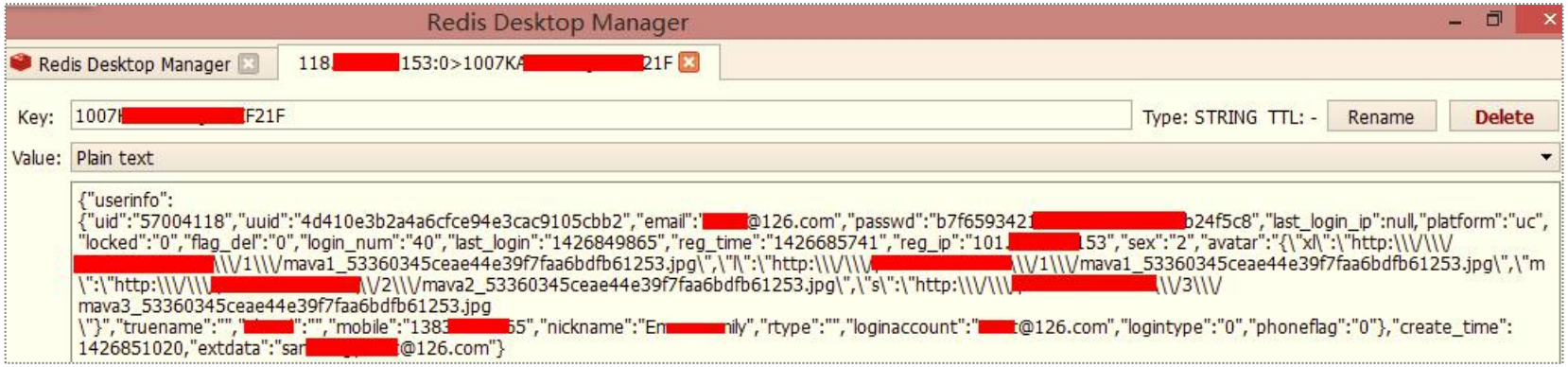
面的攻击

RedisDDoS——第一个利用Redis漏洞的僵尸网络出现

2015-11-18 启明星辰 ADLab

自从Redis漏洞公布之后，网络空间出现了大量利用该漏洞进行攻击的事件，启明星辰ADLab捕获到一款新的僵尸程序，这款僵尸程序已经渗透进入大量服务器中，并利用这些服务器资源进行大规模的DDoS攻击。

启明星辰ADLab通过对攻击源主机的查证，发现这是一款专门为Redis漏洞定制的僵尸程序，该僵尸除了具有DDoS攻击的功能外还具有下载任意程序执行以及执行任意远程命令的功能，并可随时进行样本更新，目前捕获到的样本控制端来自于广东省潮州市。



面的攻击

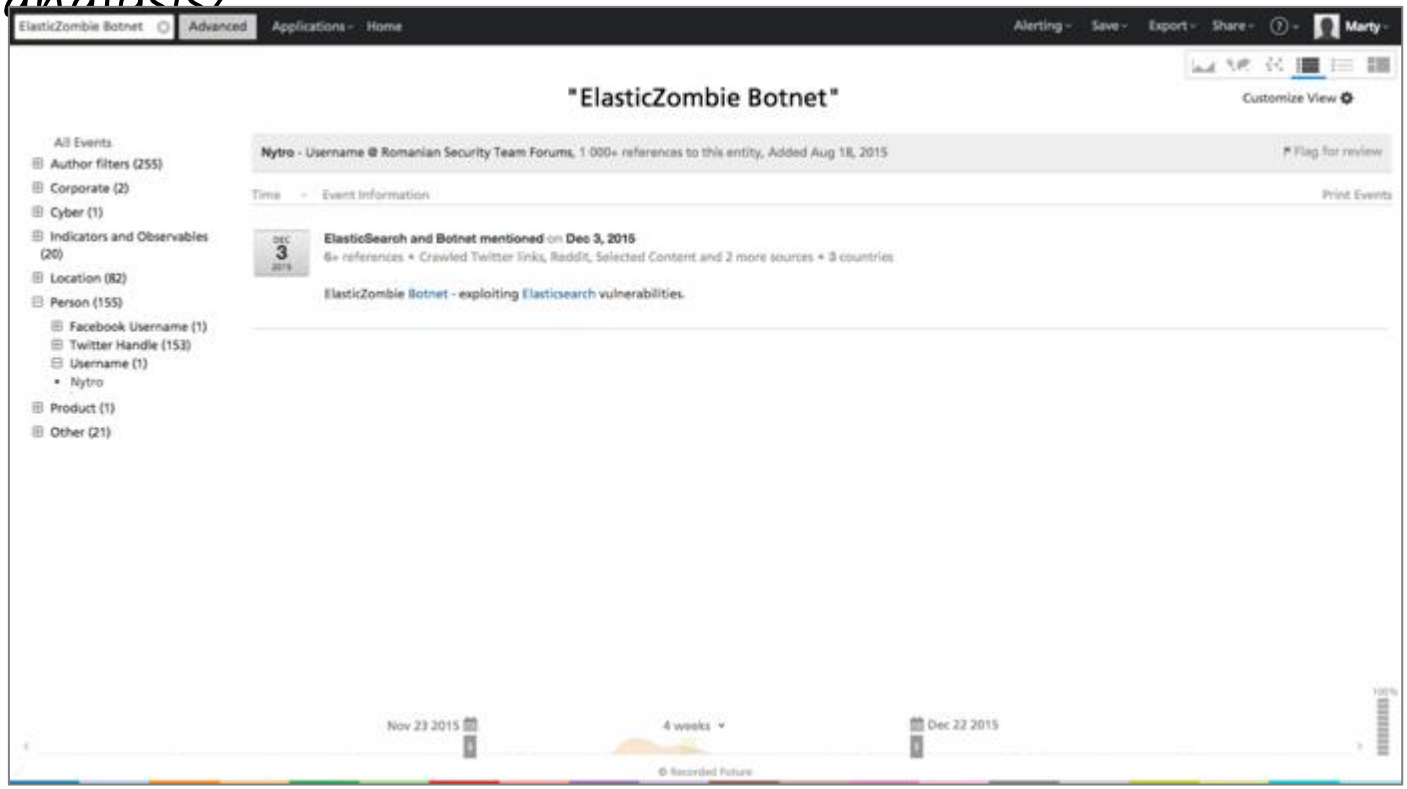
面，思考其他NoSQL

Memcached、ElasticSearch、 MongoDB …

面的攻击

ElasticZombie

https://www.recordedfuture.com/elasticzombie-botnet-analysis/



面的攻击

ElasticZombie

210 阅读 0 回复

[系统和服务器安全]ElasticSearch命令执行漏洞：通过perl进行反弹shell [复制链接]

黑手_疯子

我是疯子我怕谁

级别：管理员

发帖 49699
金钱 56123
威望 19640
贡献值 16212
在线时间 9375小时

加关注 发消息

楼主 发表于: 03-06 只看楼主 倒序阅读 使用道具

关键词： ElasticSearch perl 命令执行漏洞 shell

ElasticSearch是一个基于Lucene的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful web接口。Elasticsearch是用Java开发的，并作为Apache许可条款下的开放源码发布，是第二最流行的企业搜索引擎。设计用于云计算中，能够达到实时搜索，稳定，可靠，快速，安装使用方便。目前网络公开部署Elasticsearch大概有数万台服务器，内部网络部署就不计其数了。Elasticsearch用了两个危险性的脚本MVEL和Groovy。2014年5月MVEL爆出来命令执行漏洞，这次轮到Groovy了，Elasticsearch 1.3.0-1.3.7 和 1.4.0-1.4.2的Groovy 脚本引擎存在漏洞。这个漏洞允许攻击者构造Groovy脚本绕过沙箱检查执行shell命令，已修复的版本是Elasticsearch 1.3.8 和 1.4.3。 这个漏洞不亚于Java Struct执行命令漏洞，对与Linux和Windows平台都适用，在实际测试中也有授权为最高权限root或者system权限的，可以获取webshell和最高系统权限。

受影响版本：

cpe:/a:elasticsearch:elasticsearch:1.4.2

cpe:/a:elasticsearch:elasticsearch:1.4.0

cpe:/a:elasticsearch:elasticsearch:1.3.7

cpe:/a:elasticsearch:elasticsearch:1.4.0:beta1

cpe:/a:elasticsearch:elasticsearch:1.4.1

(一)可利用POC

Export Share Marty

Customize View

Elasticsearch CVE-2015-5377.

ElasticSearch-Botnet C&C-Master DNS-Names.

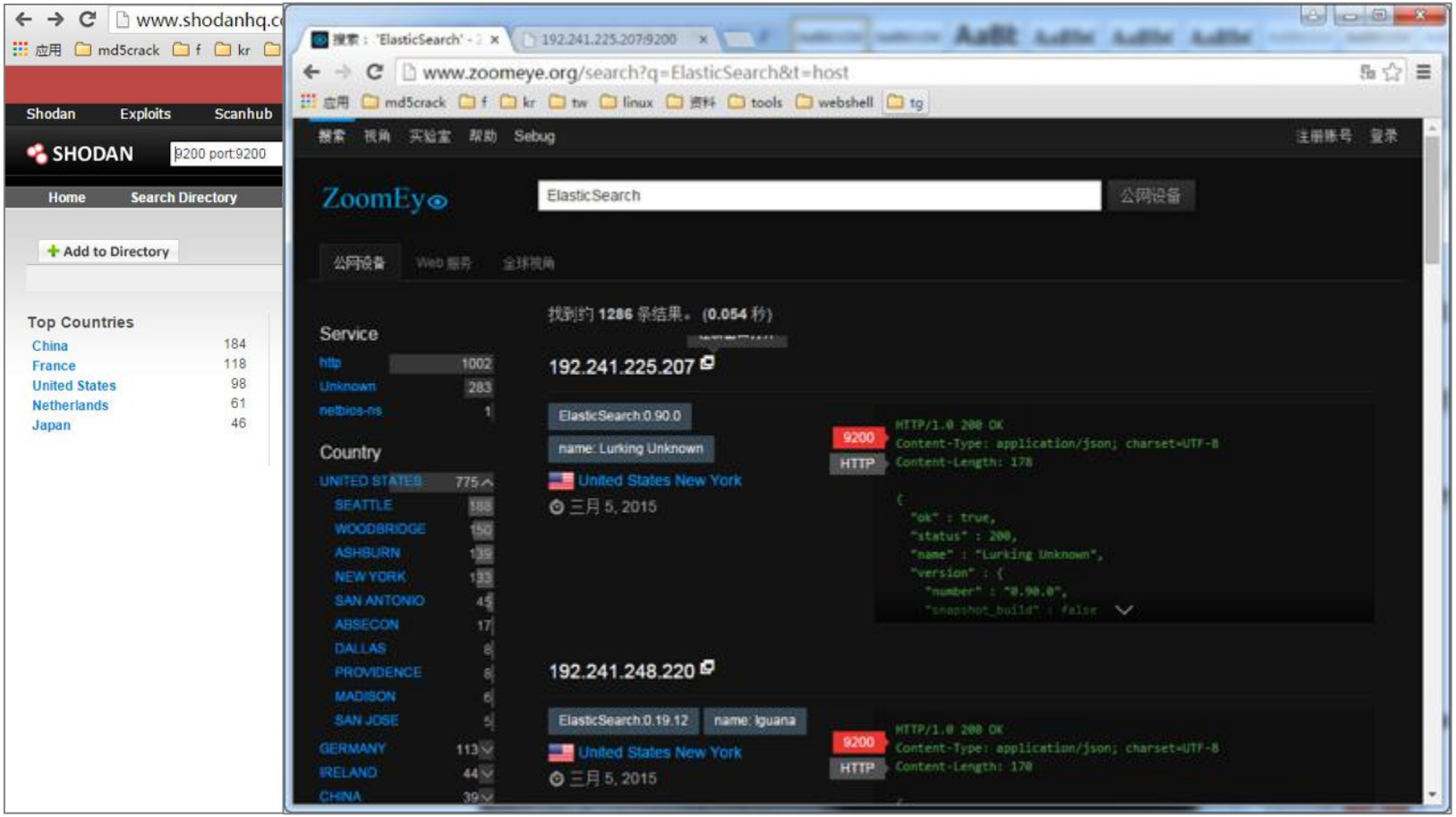
ElasticZombie Botnet - exploiting Elasticsearch vulnerabilities.

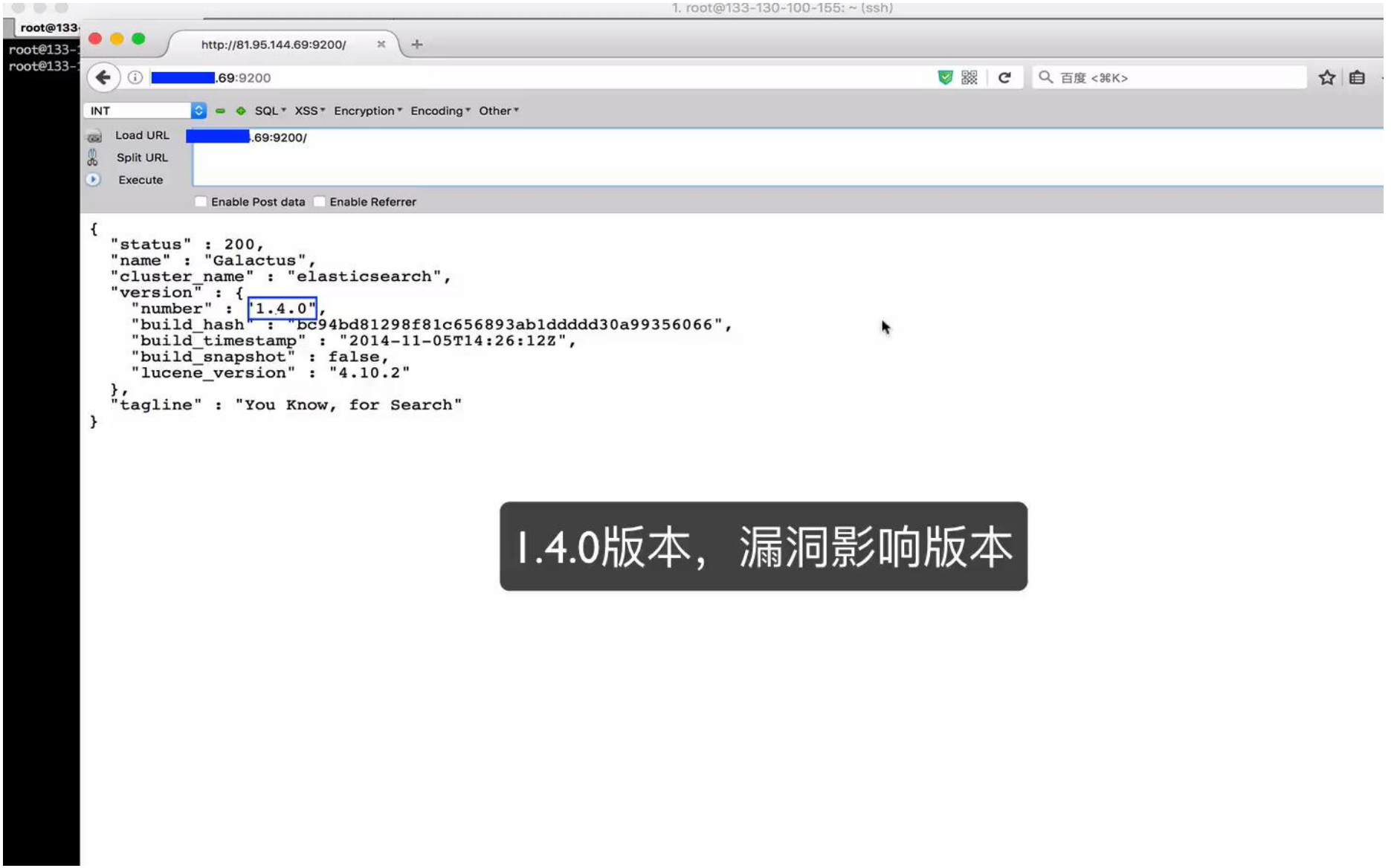
[webapps] - ElasticSearch 1.6.0 - Arbitrary File Download.

Sep Oct Nov Dec

面的攻击

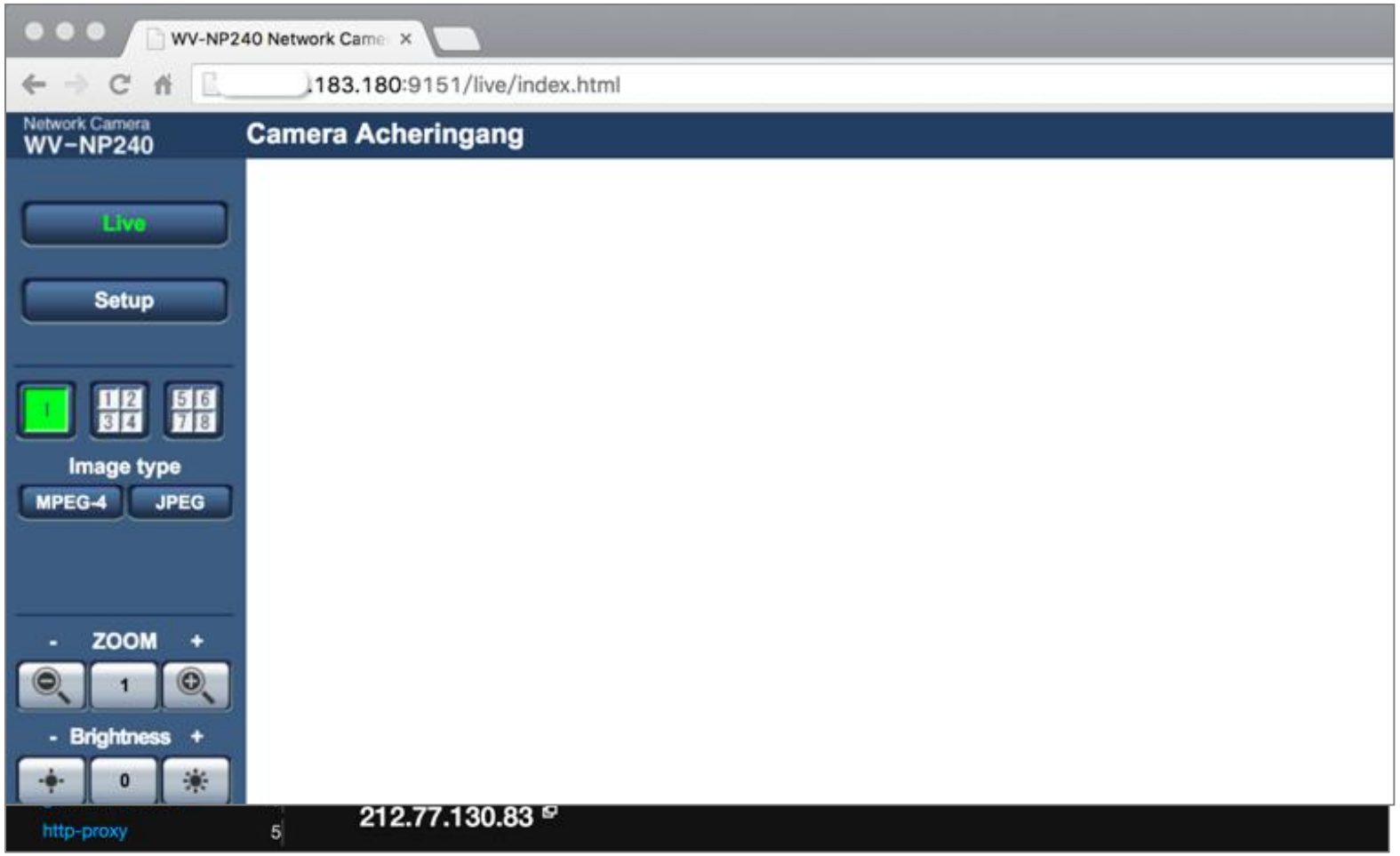
ElasticZombie




1. root@133-130-100-155: ~ (ssh)
http://81.95.144.69:9200/
[redacted].69:9200
百度 <⌘K>
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
[redacted].69:9200/
Split URL
Execute
Enable Post data
Enable Referrer
{
"status" : 200,
"name" : "Galactus",
"cluster_name" : "elasticsearch",
"version" : {
"number" : "1.4.0",
"build_hash" : "bc94bd81298f81c656893ab1ddddd30a99356066",
"build_timestamp" : "2014-11-05T14:26:12Z",
"build_snapshot" : false,
"lucene_version" : "4.10.2"
},
"tagline" : "You Know, for Search"
}
1.4.0版本，漏洞影响版本

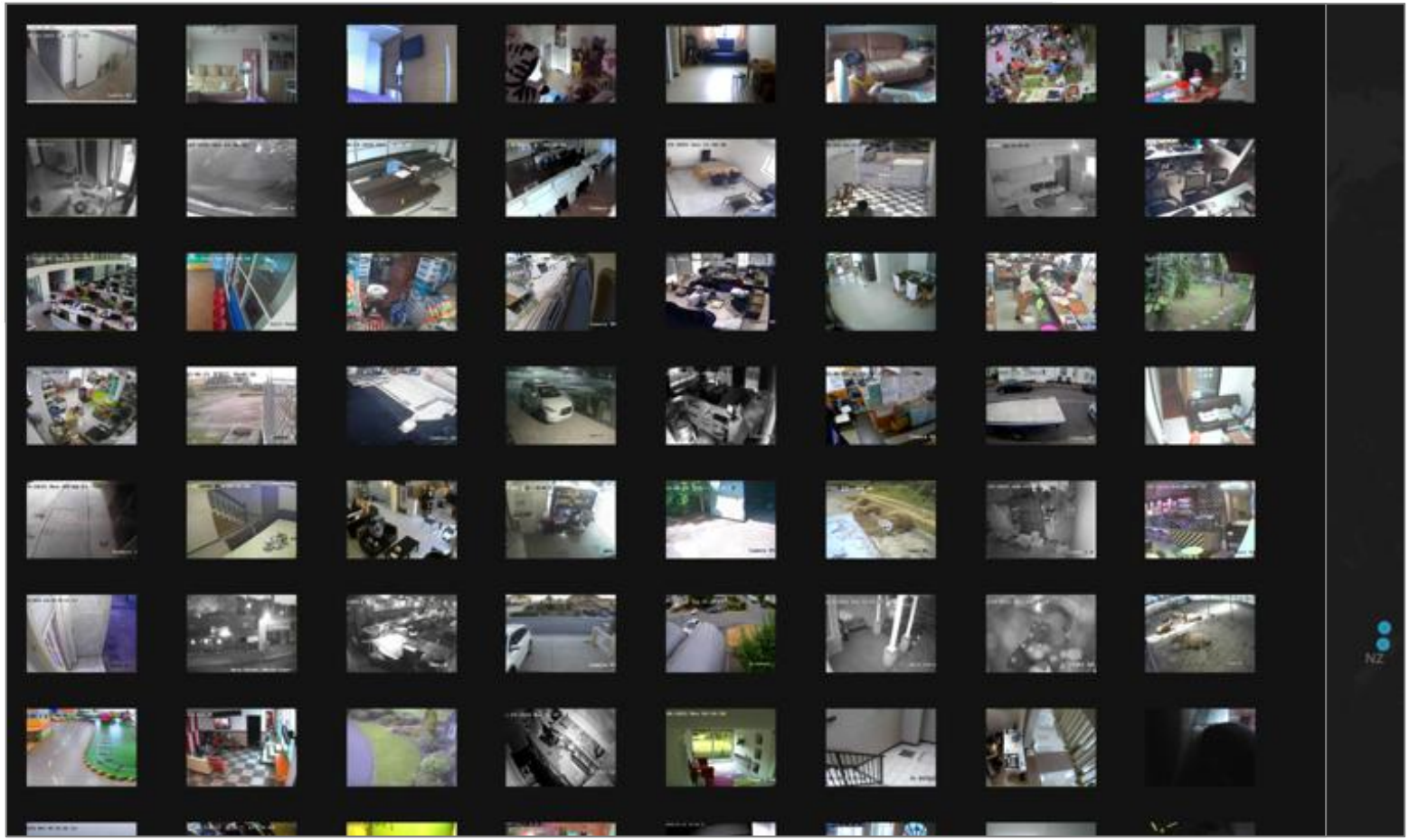
面的攻击

摄像头风险


WV-NP240 Network Came
183.180:9151/live/index.html
Network Camera
WV-NP240
Camera Acheringang
Live
Setup
Image type
MPEG-4
JPEG
- ZOOM +
1
- Brightness +
0
http-proxy
212.77.130.83

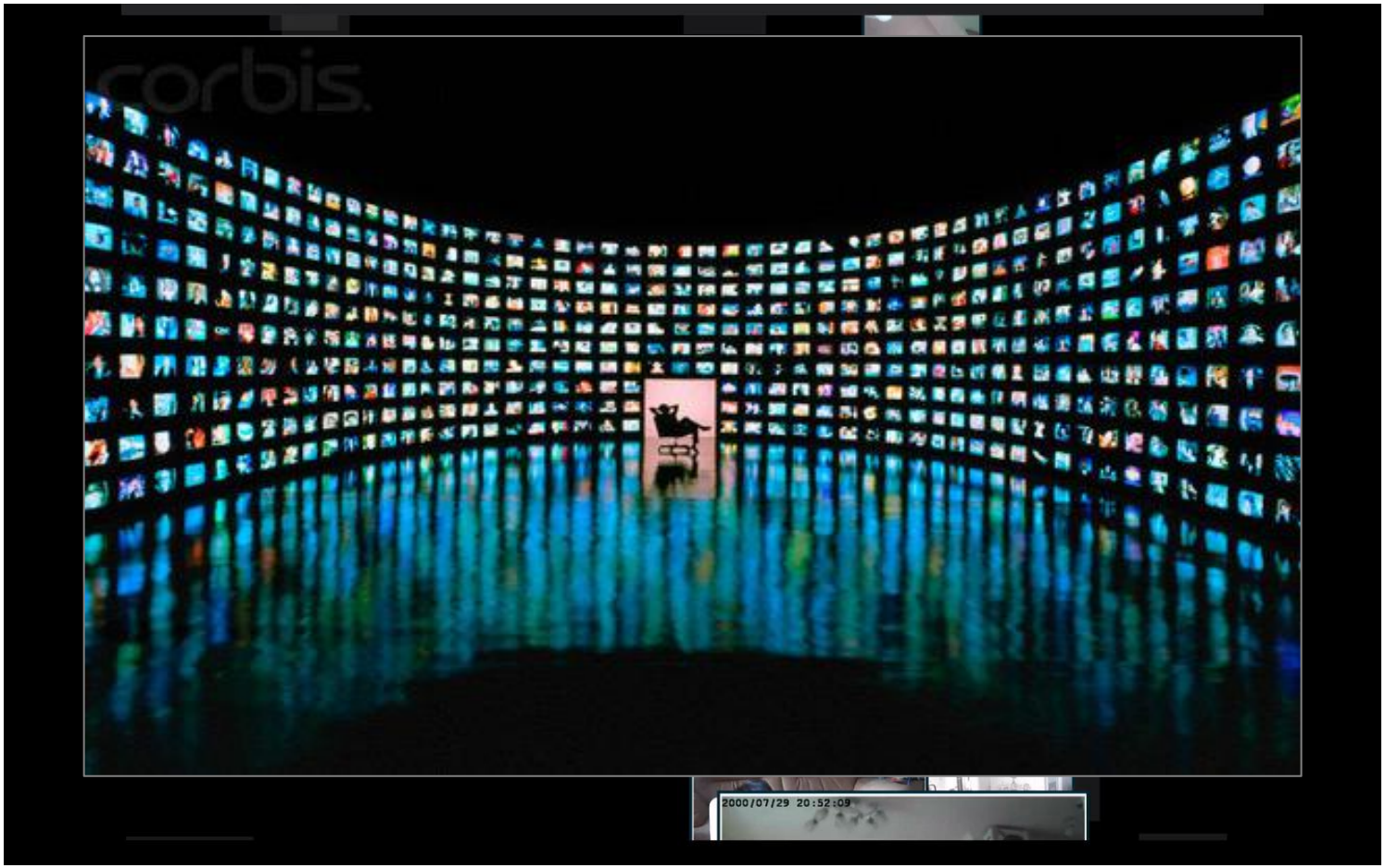
面的攻击

摄像头风险



面的攻击

摄像头风险



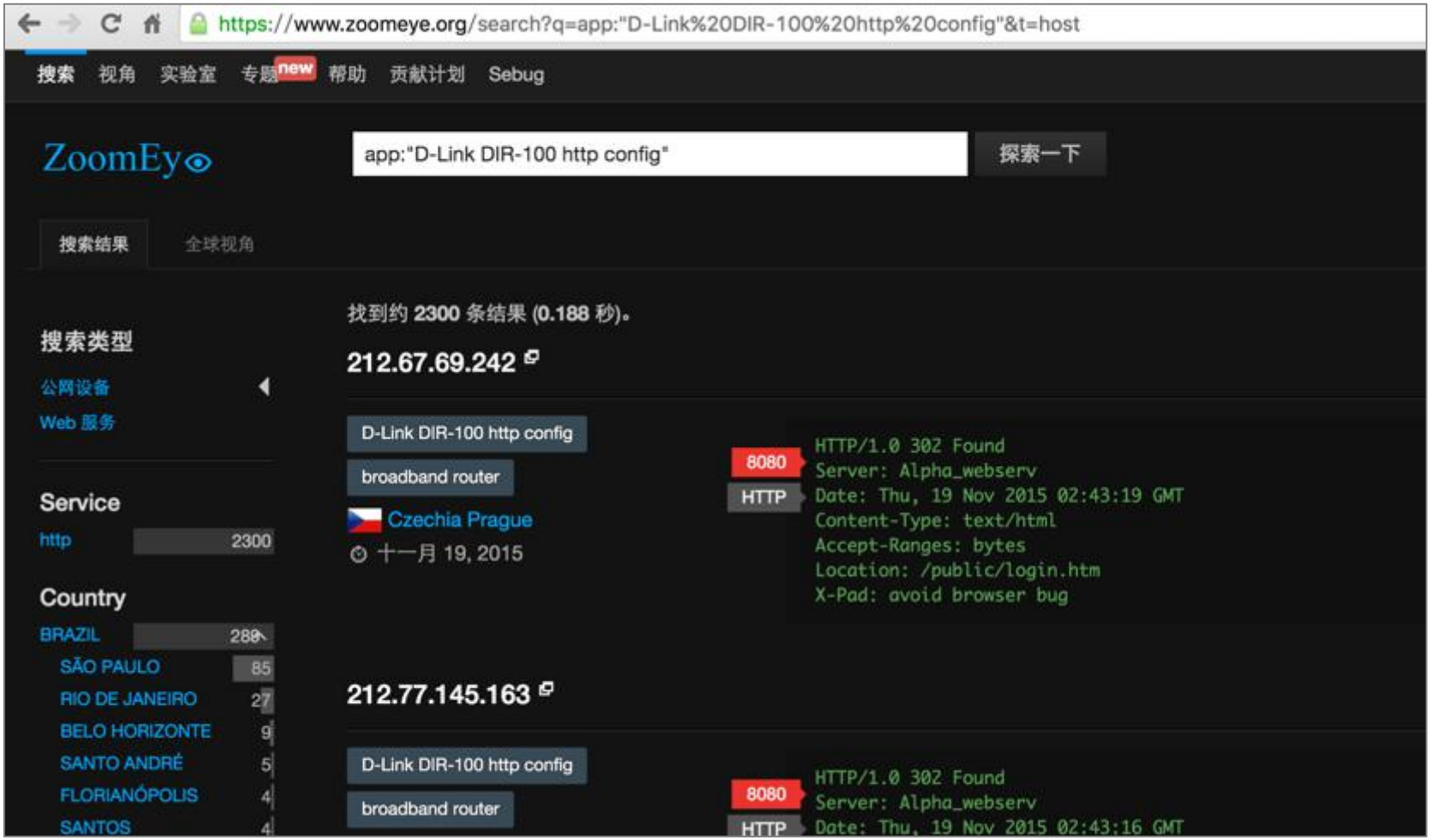
面的攻击

路由器威胁

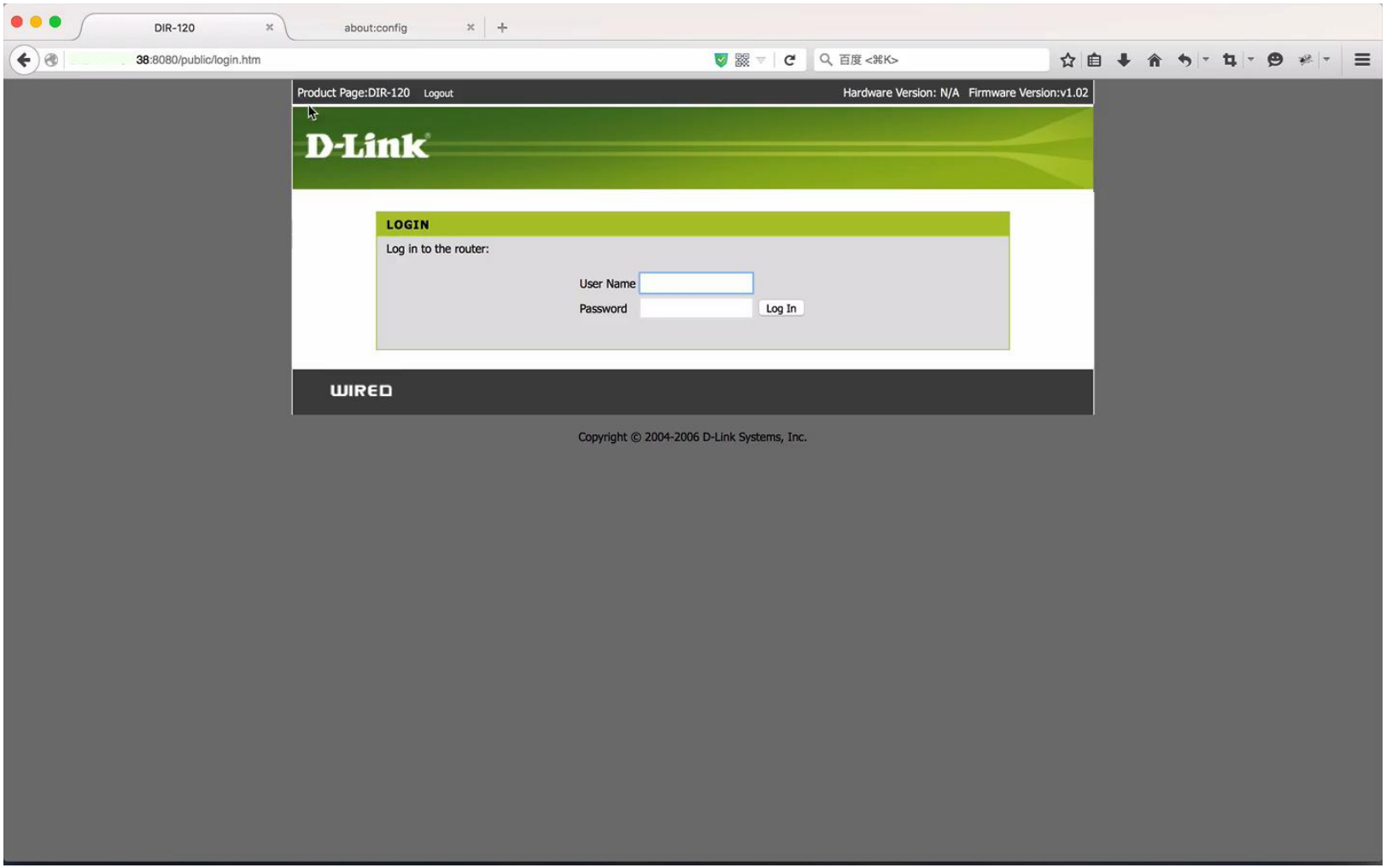
ZoomEye 路由器专题
https://www.zoomeye.org/project/router

面的攻击

D-Link 后门



D-Link 后门


DIR-120
about:config
38:8080/public/login.htm
百度 <⌘K>
Product Page:DIR-120 Logout
Hardware Version: N/A Firmware Version:v1.02
D-Link
LOGIN
Log in to the router:
User Name
Password
Log In
WIRED
Copyright © 2004-2006 D-Link Systems, Inc.

面的攻击


全球影响
There were about 67,000 affected devices worldwide. Only part of pins are shown due to browser performance.
+
−
0
5000
10000
15000
20000
25000

面的攻击

磊科(NetCore)路由器 后门

2014/8/25，趋势科技研究员Tim Yeh发文描述了磊科疑似后门的igdmptd程序，全球有200多万台磊科路由受影响

2014/10/3，Tim Yeh再次发文称磊科官方发布了新版固件，但新固件中只是默认关闭了「后门」程序，而并未将其删除。ShadowServer的统计受影响路由器仍有100多万台

2014/12/28，国内研究员h4ckmp发文详细分析了该「后门」

2014/12/31，ZoomEye Team进行了细节验证并发文

2015/9，ZoomEye Team的探测发现UDP 53413端口的IP总数约为140万，其中110万左右是存在后门的磊科路由器，占比近80%

其中95%在中国:(

面的攻击

工控安全


217.[redacted].100:81/cgi-bin/read.cgi?page=../../../etc/passwd
root:RM4.EMXm4X0.g:0:0:root:/:/bin/sh shutdown::6:0:shutdown:/bin:/bin/reboot
WAY
START NETWORK MODBUS STATUS ADMIN ABOUT
Status
Transparent Queries
Number of Connections 1
Valid Responses 10693
Serial Timeouts 30
CRC Errors 112
Buffer Overruns 0
Frame Errors 0
Exception Responses 131
clear
Anybus
close
bs InitialPage.asp
-S WebServer
ervice HTTPserv:00001
ge
eb Server/1.00
Modicon M340 CPU
PLC
Portal0000.htm

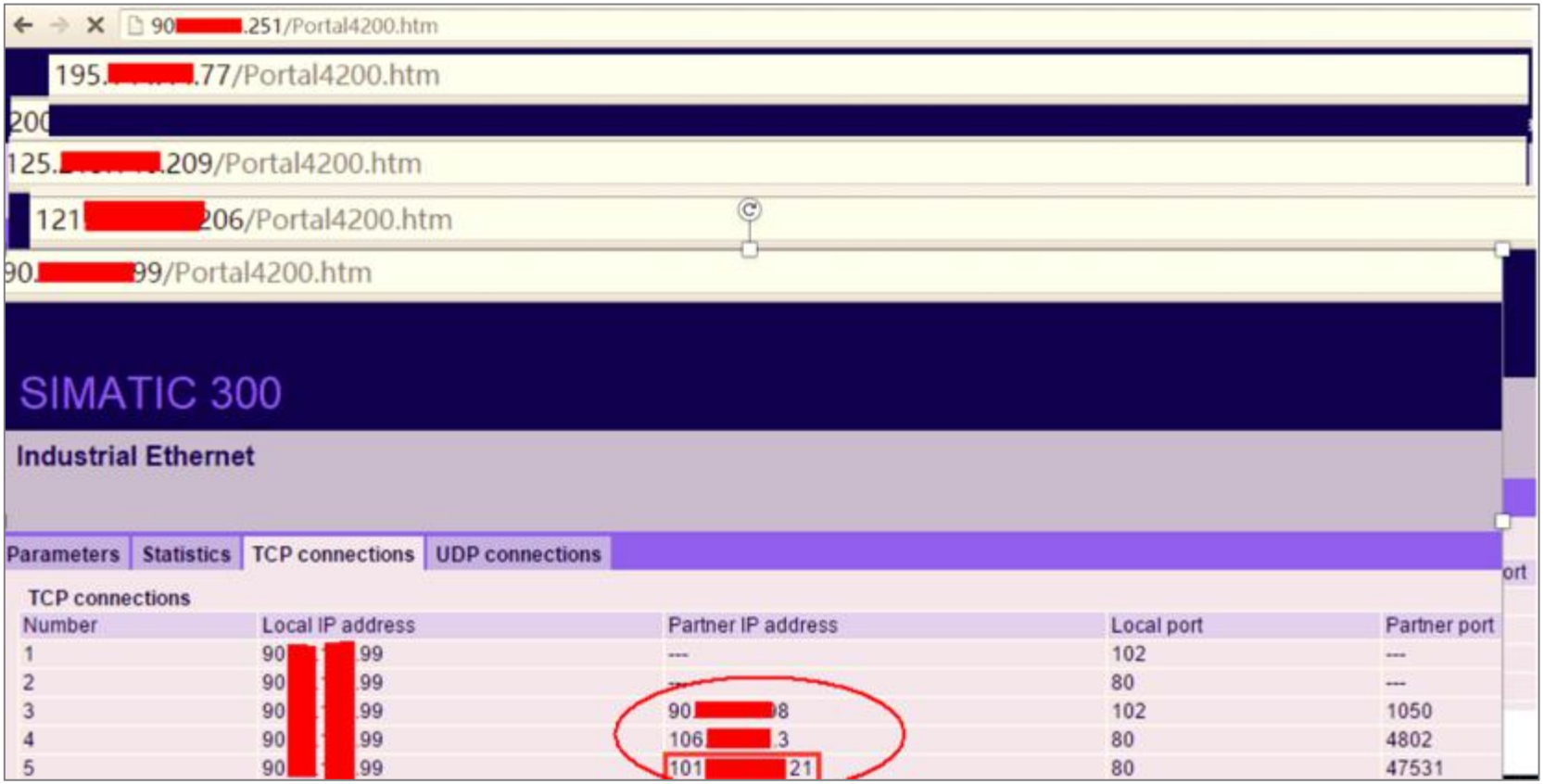
面的攻击

工控安全


HIKVISION
DS-7804HW-E1/M
预览
回放
日志
配置
English
05:29:19
Status
ESTABLISHED
LISTEN
LISTEN
ESTABLISHED
ESTABLISHED
ESTABLISHED
ESTABLISHED
SYN RECEIVED
ESTABLISHED
SYN RECEIVED
SYN RECEIVED
RTS Services
Generic
Generic
RTS SCADA Server

面的攻击

工控安全


90[redacted].251/Portal4200.htm
195.[redacted].77/Portal4200.htm
200
125.[redacted].209/Portal4200.htm
121[redacted]206/Portal4200.htm
90.[redacted]99/Portal4200.htm
SIMATIC 300
Industrial Ethernet
Parameters
Statistics
TCP connections
UDP connections
TCP connections
Number
Local IP address
Partner IP address
Local port
Partner port
1 90[redacted].99 --- 102 ---
2 90[redacted].99 80 ---
3 90[redacted].99 90[redacted]8 102 1050
4 90[redacted].99 106[redacted].3 80 4802
5 90[redacted].99 101[redacted]21 80 47531

04 成为一名黑客

如何成为一名黑客

1、保持你的好奇心

2、对一切都可以持怀疑态度

3、突破，转换思维，学会不同角度看待问题

守正出奇

Geekbang 极客邦科技 InfoQ

THANKS!