2016乌云白帽大会・不插电

入侵对抗体系建设漫谈

江虎

2016.7

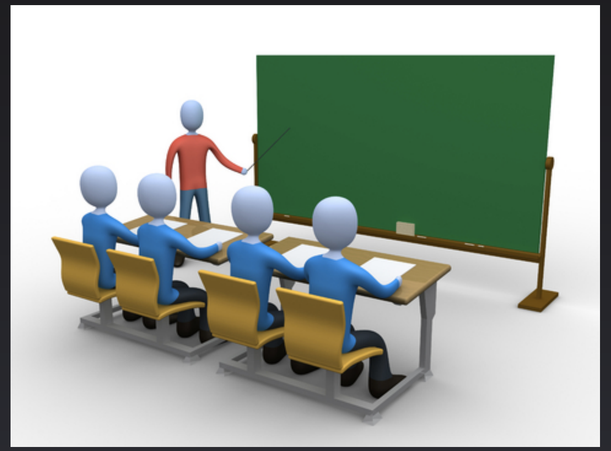
自我简介

网络ID:xti9er 十六年安全研究与工作经验
曾混迹于黑盟、灰色轨迹、幻影等社区

久游 → 腾讯 → 阿里巴巴
负责集团安全体系架构

专注入侵检测体系建设、取证分析研究
《互联网企业高级安全指南》

HOW TO …



hids

waf

RASP

Big data

rules

Kill chain

WHY?

体系初建

- 风险分析
- 工程化建设
- 运营能力建设

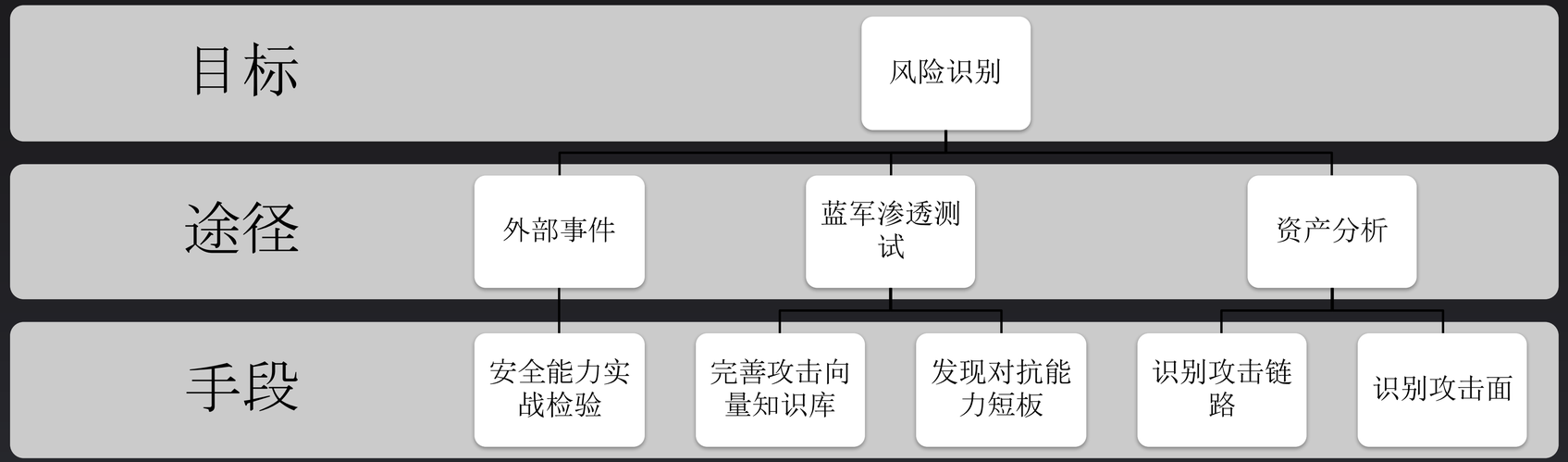
数据hack

- 我们在对抗什么？
- 数据化的安全能力建设

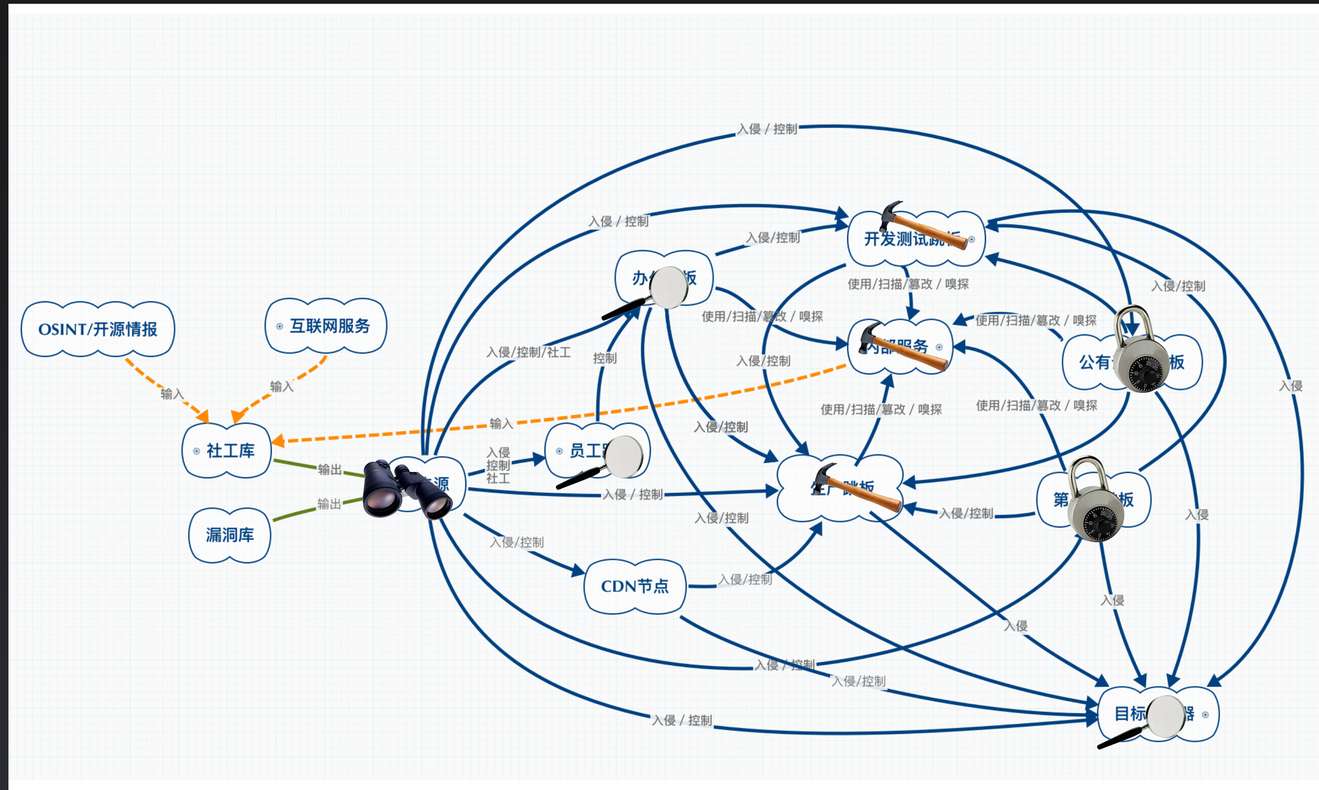
成熟度模型

- 我理想中的入侵检测成熟度模型

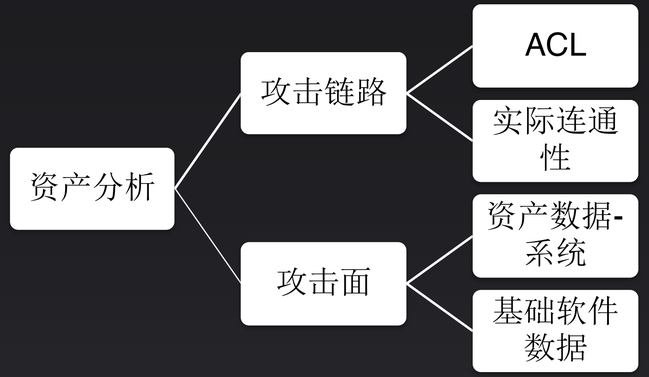
知己-风险识别

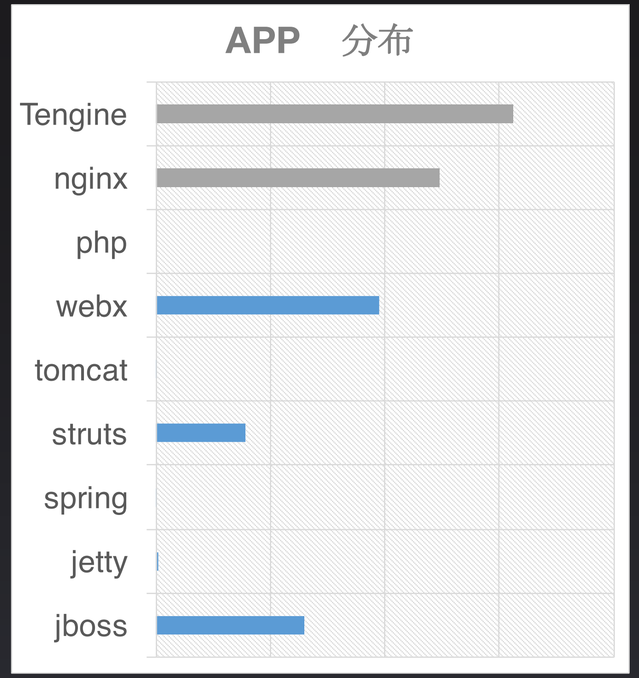

目标
风险识别
途径
外部事件
蓝军渗透测试
资产分析
手段
安全能力实战检验
完善攻击向量知识库
发现对抗能力短板
识别攻击链路
识别攻击面

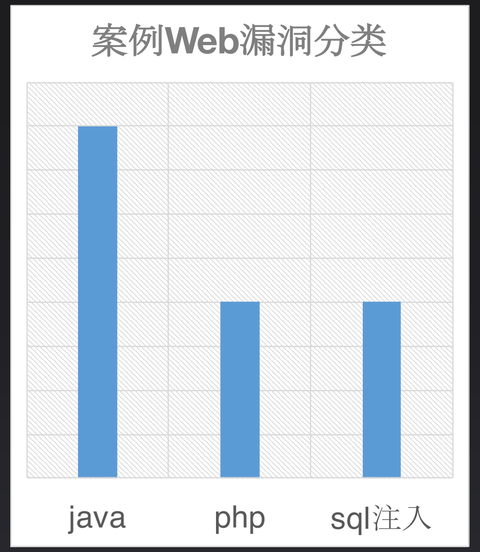
风险识别-攻击链



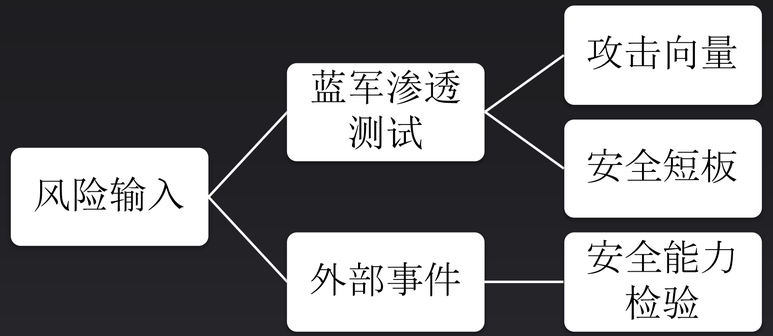
风险识别-资产分析-攻击面







风险识别-案例-攻击向量



业务逻辑
- 欺诈
- 数据盗取

PHP
- sqlinject
- webshell

JAVA
- RCE
- webshell

Other GGI
- RCE
- webshell

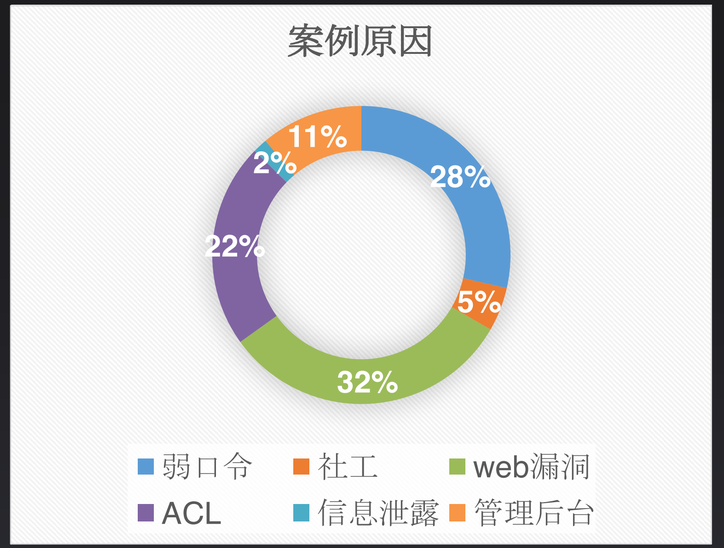
LIBC
- Buffer Overflow
- Other exploit

LIBPCAP
- sniffer
- Arpspoof

LIBXXX

OtherLIB

Linux Kernel
- Priviege Esclation
- Information Disclosure
- Other exploit



工程化-用户体验

安全大牛与运维大拿的不同视角

安全大牛：“你们这个方案太LOW了，分分钟绕过！”

运维大拿：“你们这个方案太大胆了，应用系统的XX都敢动！”

理想与现实的差距

工程化-项目运作

重点是解决问题，而非炫技

贪多嚼不烂

工程化-纵深防御

- 攻击面
  - 安全系统，交叉覆盖
- 攻击向量
  - 行为数据模型
  - 检测能力纵深
  - 高维防守

运营能力建设

- **技术**
- 攻防场景的技术研究与深刻理解是设计基础
- 产品代码的强壮性是生死存亡的关键

- **项目**
- 项目化运作
- 执行力

- **产品**
- 用户体验是项目推动的助推器
- 更新迭代进化能力是项目效果能力的关键

“数据hack” 数据化对抗

知其然（攻击手法），知其所以然（背景知识）
源于攻防，但不止于此
宏观数据趋势分析、微观数据技术分析

对抗方式的选择

技术情节，陷入了与黑客单纯比拼黑客技术的怪圈。

知识库更新滞后

- 基于业务场景的通用解决方案
- 源于技术对抗，不止于此

对业务更熟悉

- 丰富的业务数据，刻画黑白模型
- 聚焦解决业务面临的风险

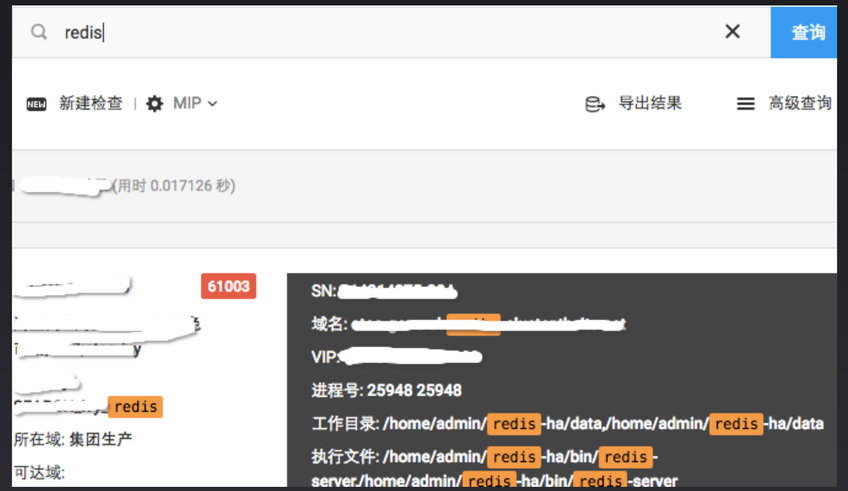
我们在对抗什么？

“苍蝇不叮无缝的蛋”

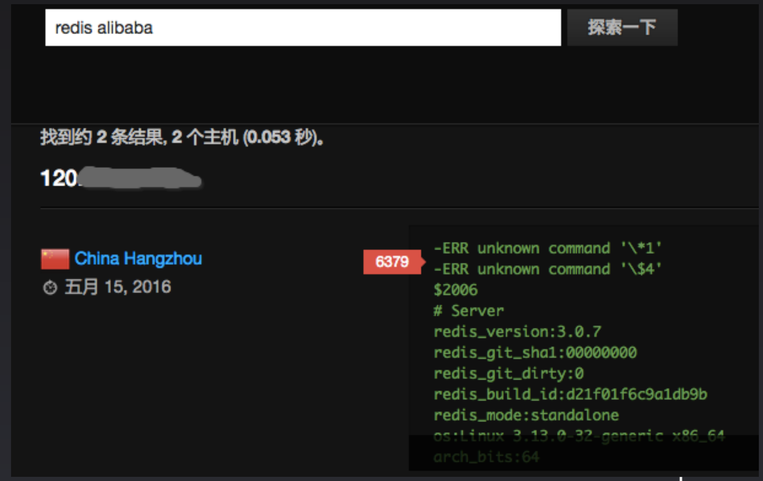
我们并非在对抗黑客，而是在解决我们犯的错

*更快更准更全的风险数据运营*能在对抗开始占得先机

资产分析 + 威胁情报 → 风险大图

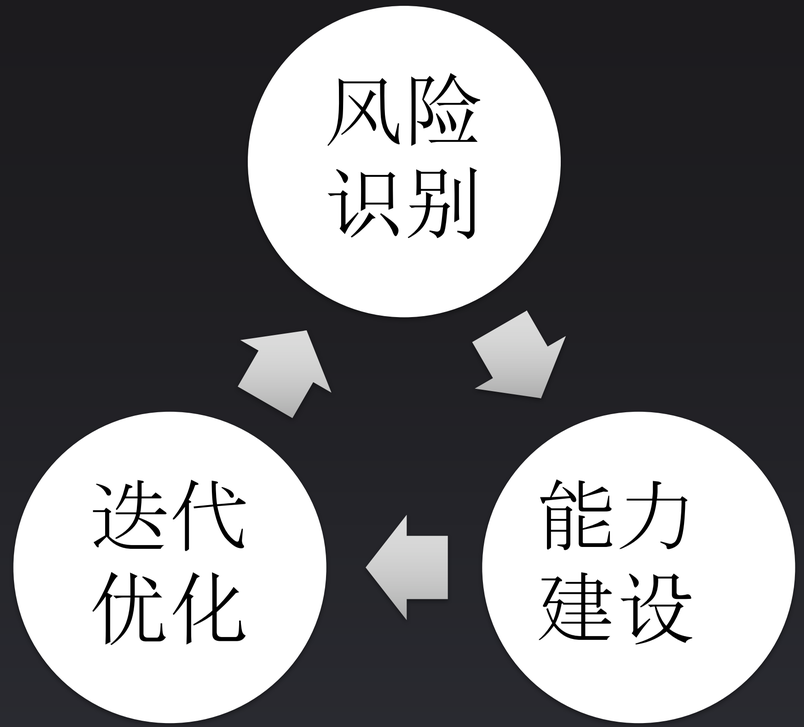


>

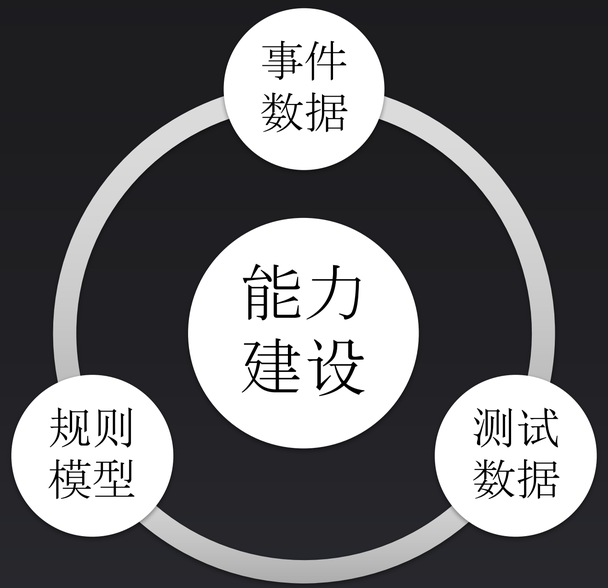


数据化的安全能力建设

数据的分析运营融入每个建设和能力迭代阶段



能力建设




```
{
    "exp":"exploit/multi/http/struts_dev_mode ",
    "http_request": {
        "method": "GET",
        "request_uri": "/struts2-blank/example/HelloWorld.action",
        "query_string": "debug=command&expression=%23f%3d%23_memberAccess.getCl
        "remote_addr": "1.1.1.1",
    },
    "context": [
        {
            "reason": "WRITE_FILE",
            "severity": 0,
            "stack_trace": [
                {
                    "clazz": "java.io.FileOutputStream",
                    "method": "<init>"
                },
                {
                    "clazz": "sun.reflect.NativeConstructorAccessorImpl",
                    "method": "newInstance0"
                },
                {
                    "clazz": "ognl.OgnlRuntime",
                    "method": "callConstructor"
                },
                {
                    "clazz": "com.opensymphony.xwork2.DefaultActionInvocation",
                    "method": "invoke"
                }
            ],
            "params": [
                "Kf5zhB.jar"
            ]
        }
    ]
}
```

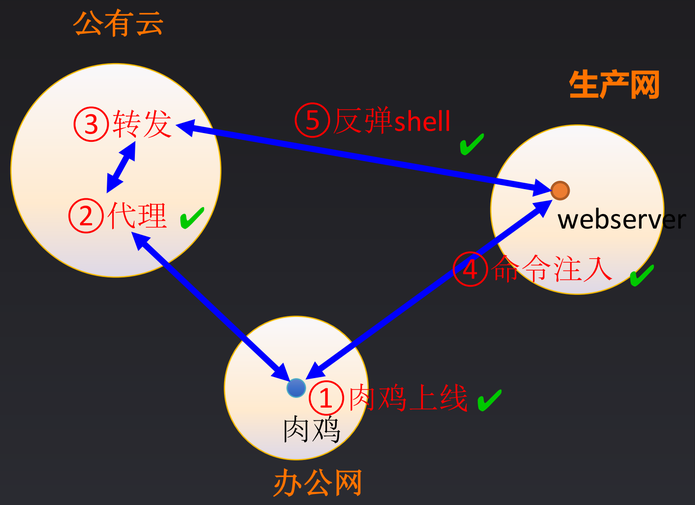
```
{
    "clazz": "java.io.FileOutputStream",
    "method": "<init>"
},
{
    "clazz": "metasploit.Payload",
    "method": "writeEmbeddedFile"
},

{
    "clazz": "java.lang.reflect.Method",
    "method": "invoke"
},

{
    "clazz": "ognl.ObjectMethodAccessor",
    "method": "callMethod"
}
```

优化迭代

每一次的安全事件都是能力迭代更新 进化成长的机会！

优化迭代-事件分析

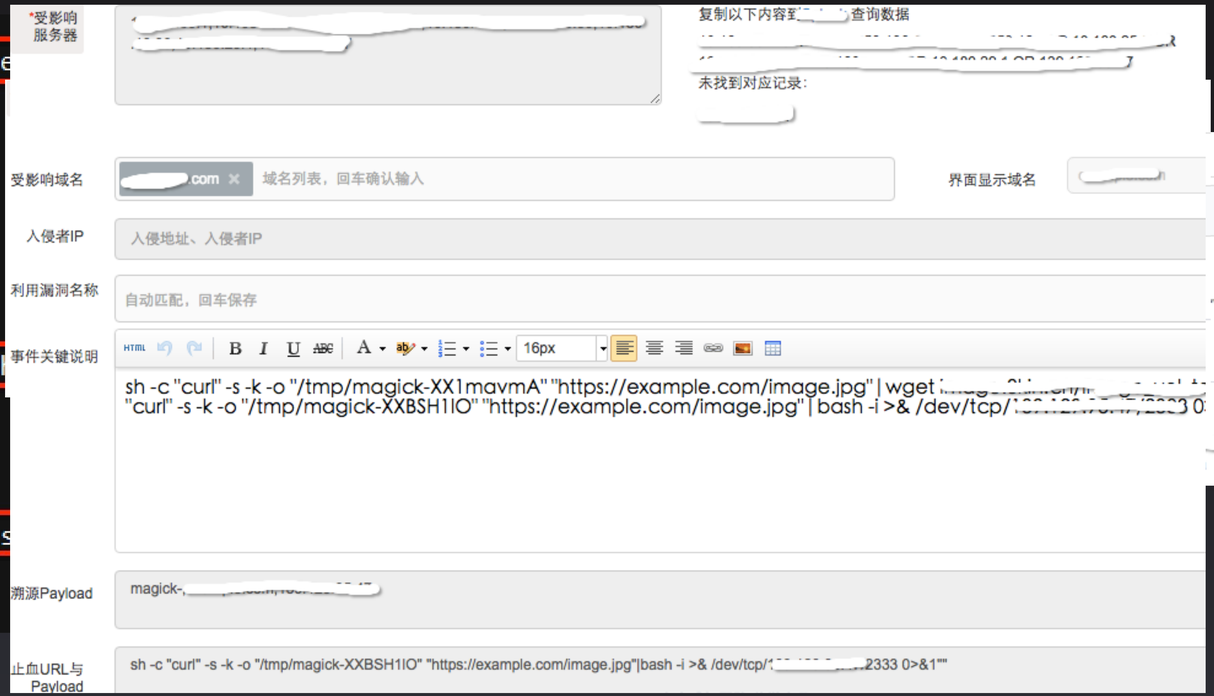
攻击链



攻击向量

```
{
    "clazz": "java.io.FileOutputStre
    "method": "<init>"
},
{
    "clazz": "metasploit.Payload"
    "method": "writeEmbeddedFile"
},

{
    "clazz": "java.lang.reflect.Met
    "method": "invoke"
},

{
    "clazz": "ognl.ObjectMethodAcces
    "method": "callMethod"
}
```

溯源定损



优化迭代-事件复盘-改进计划

入侵检测成熟度模型


资产数据覆盖度
100
80
60
40
20
0
资产风险识别能力
传感器部署覆盖
行为数据覆盖度
大数据处理能力
检测实时性
规则场景覆盖度
新型威胁响应速度
未知威胁检测能力
成熟
中期
初阶

总 结

建设

- 聚焦业务场景
- 实用不炫技

进化

- 充分利用数据运营
- 现在差不怕，可怕的是没有进化能力

理想

- 数据不能有盲点
- 业务风险解决方案不能有盲点

THANKS

乌云 WooYun | 乌云白帽大会 · 2016
不插电

Mail: xti9er@gmail.com