Day169　应急响应-战后溯源反制&社会工程学&IP&ID追踪&URL反查&攻击画像

蓝队应急-小迪安全

异常特征

- 主机安全
  - CPU满负载
  - 服务器莫名重启
  - 其它
- 网站安全
  - 被植入暗链
  - 出现Webshell
  - 网页文件被篡改
  - 其它
- 流量安全
  - 网络阻塞
  - 网络异常
  - 其它
- 数据安全
  - 泄露
  - 篡改
- 文件安全
  - 丢失
  - 异常
- 设备告警
  - 防火墙
  - 杀毒软件
  - 感知平台
  - 检测系统
  - 其它

处置流程

1. 准备阶段
   - 获取事件信息
   - 准备设备工具
2. 保护阶段
   - 断网
   - 备份
   - 数据恢复
   - 物理隔离
3. 检测阶段
   - 技术分析
4. 取证阶段
   - 确定攻击事件
   - 确定攻击时间
   - 确定攻击过程
   - 确定攻击对象
5. 处置阶段
   - 提出安全问题
   - 提出解决方案
   - 业务恢复
6. 总结阶段
   - 完整事件报告编写

问题排查

- 系统
  - Windows
    - 远控后门
      - 进程
      - 网络
    - 勒索病毒
      - 表现
    - 挖矿程序
      - 进程
      - 网络
    - 爆破攻击
      - 系统日志
    - DDOS攻击
      - 网络流量
      - CPU爆满
  - Linux
- Web
  - 源码
  - 数据库
  - 中间件
- 其他

工具平台

1.知识点

- 战后-社工篇-溯源攻击画像

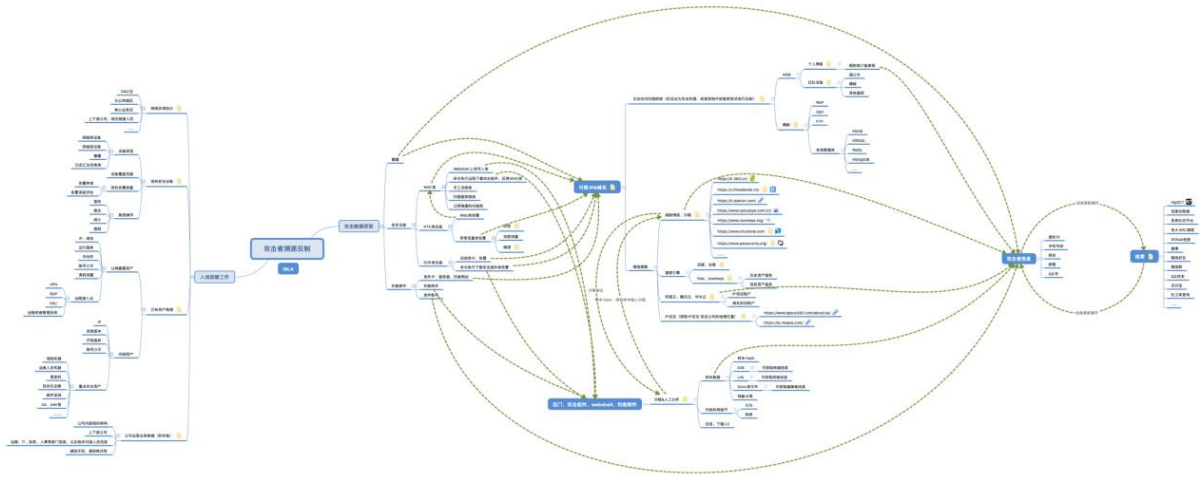
2.内容点

```
应急响应：
1、抗拒绝服务攻击防范应对指南
2、勒索软件防范应对指南
3、钓鱼邮件攻击防范应对指南
4、网页篡改与后门攻击防范应对指南
5、网络安全漏洞防范应对指南
6、大规模数据泄露防范应对指南
7、僵尸网络感染防范应对指南
8、APT攻击入侵防范应对指南
9、各种辅助类分析工具项目使用
```

```
朔源反制：
威胁情报，信息库追踪，设备反制，IDS&IPS等反制，工具漏洞反制，蜜罐钓鱼反制等
```

```
威胁情报相关平台：
Virustotal
深信服威胁情报中心
微步在线
venuseye
安恒威胁情报中心
360威胁情报中心
绿盟威胁情报中心
AlienVault
RedQueen安全智能服务平台
IBM X-Force Exchange
ThreatMiner
```

3.演示案例



```
ID追踪
(1) 百度信息收集："id" （双引号为英文）
(2) 谷歌信息收集
(3) src信息收集（各大src排行榜）
(4) 微博搜索（如果发现有微博记录，可使用tg查询weibo泄露数据）
```

(5) 微信ID收集：微信进行ID搜索（直接发钉钉群一起查）
(6) 如果获得手机号（可直接搜索支付宝、社交账户等）
注：获取手机号如信息不多，直接上报钉钉群（利用共享渠道对其进行二次工作）
(7) 豆瓣/贴吧/知乎/脉脉 你能知道的所有社交平台，进行信息收集
(8) 其他补充
在github，gitee，开源中国中查找
在社交平台上查找，（微信/微博/linkedin/twitter）
技术博客（csdn，博客园），src平台（补天）
在安全群/安全圈子里询问。

IP定位
https://www.opengps.cn/Data/IP/ipplus.aspx

网站URL，恶意样本
1、可利用网站：
https://x.threatbook.cn/
https://ti.qianxin.com/
https://ti.360.net/
https://www.venuseye.com.cn/
2、根据域名进行溯源
whois查询
备案查询
企查查/天眼查查询
zoomeye/fofa查询
3、样本特征字符密码等
如后门的密码，源码中的注释，反编译分析的特殊字符串等

社交帐号：
1、reg007
2、各种库子查询

```
36
37  手机号码：
38  1、支付宝转账 - > 确定姓名，甚至获取照片
39  2、微信搜索 ->  微信ID可能是攻击者的ID，甚至照片
40  3、各种裤子
41
42  攻击画像大概模型：
43  姓名/ID：
44  攻击IP：
45  地理位置：
46  QQ：
47  IP地址所属公司：
48  IP地址关联域名：
49  邮箱：
50  手机号：
51  微信/微博/src/id证明：
52  人物照片：
53  跳板机（可选）：
54  关联攻击事件：
```

3.1 溯源社工篇-日志提取-IP地址-攻击画像

```
1  日志上分析出攻击者IP地址
2  威胁感知-标签-社交-库搜搜-电话,其他信息等
```

3.2 内鬼提取-ID昵称溯源-攻击画像

```
1  某天Tg上有人贩卖课程，寻找内鬼开始
```

3.3 文件提取-恶意样本溯源-攻击画像

```
1  后门木马-IP-IP反查域名-域名收集-个人信息
```