ByteDance 字节跳动 | Security 安全与风控 × 安全范儿 BYTEDANCE SECURITY

攻击队视角评估业务安全

以攻促防

郑洋

雁行安全团队 攻防领域研究员

雁行安全团队核心成员，长期安全从业者，多年一线攻击队经验。擅长对抗下的实战攻防和工具开发，具有丰富的实战经验，擅长寻找安全建设下的盲点。

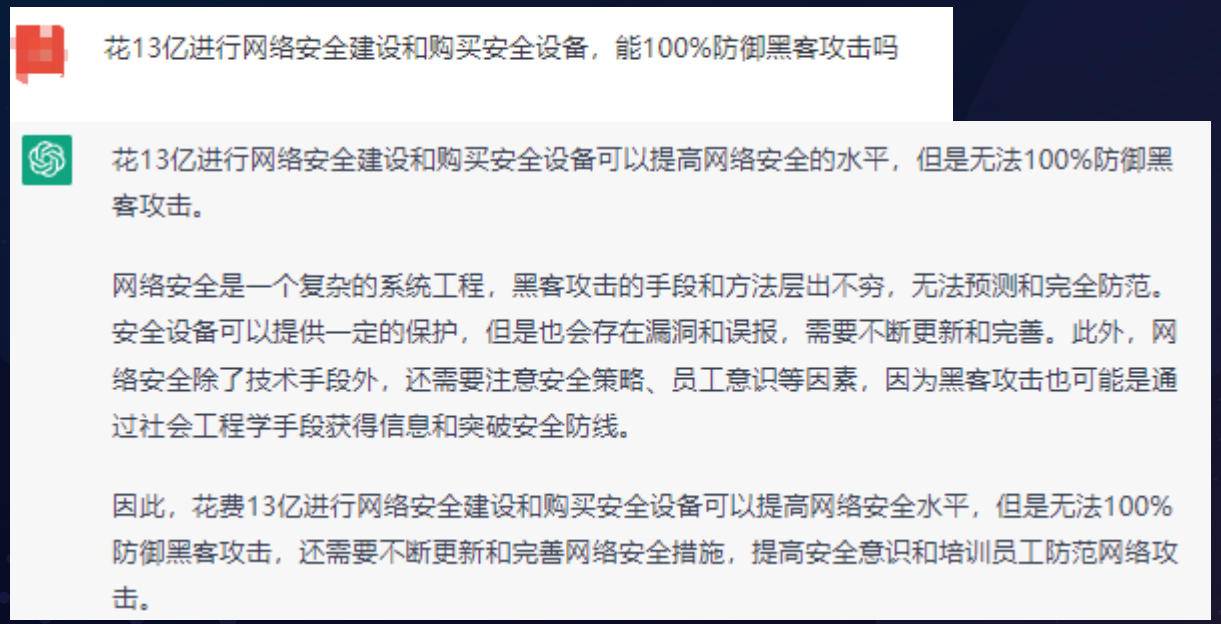
目录

一、实战驱动下的攻&防

背景&痛点

企业在安全建设上投入了很多精力，但还是出现了安全事件或者在模拟演练中失分，没达到想要的效果？

- 重点系统上了waf，做了漏洞挖掘，**攻击者**却从未知资产切入了
- web系统增加攻击流量监控，**黑客**又通过钓鱼打进来了
- 某国重点能源行业，被**某APT**组织持续入侵
- .....



为什么在安全布局中要关注攻击者的视角

One one

01

好的防守应该能够最大程度重现进攻，监控入侵行为，还原攻击路径。

Two two

02

对于模板套用和设备堆叠的防御体系来说，立体化攻击就如同降维打击一样。所以需要获得攻击者的视角，进行动态的主动防御。

Three three

03

知己知彼，以攻促防。攻击面管理（ASM）技术理念是符合当前生产环境刚需的。

攻击基本思路

主要资产正面硬刚

从主要资产入手，防护相对严密。漏洞少，防护多，难度大，收益高

上下游侧面入手

集团公司，下属单位，全资子公司

第三方机构扩展

供应链、开发商的针对性打击

边缘资产迂回靠近

监控缺少，未在严密管理下，攻击难度相对小

人员安全突破口

针对安全意识薄弱的员工进行钓鱼、社工攻击

近缘渗透

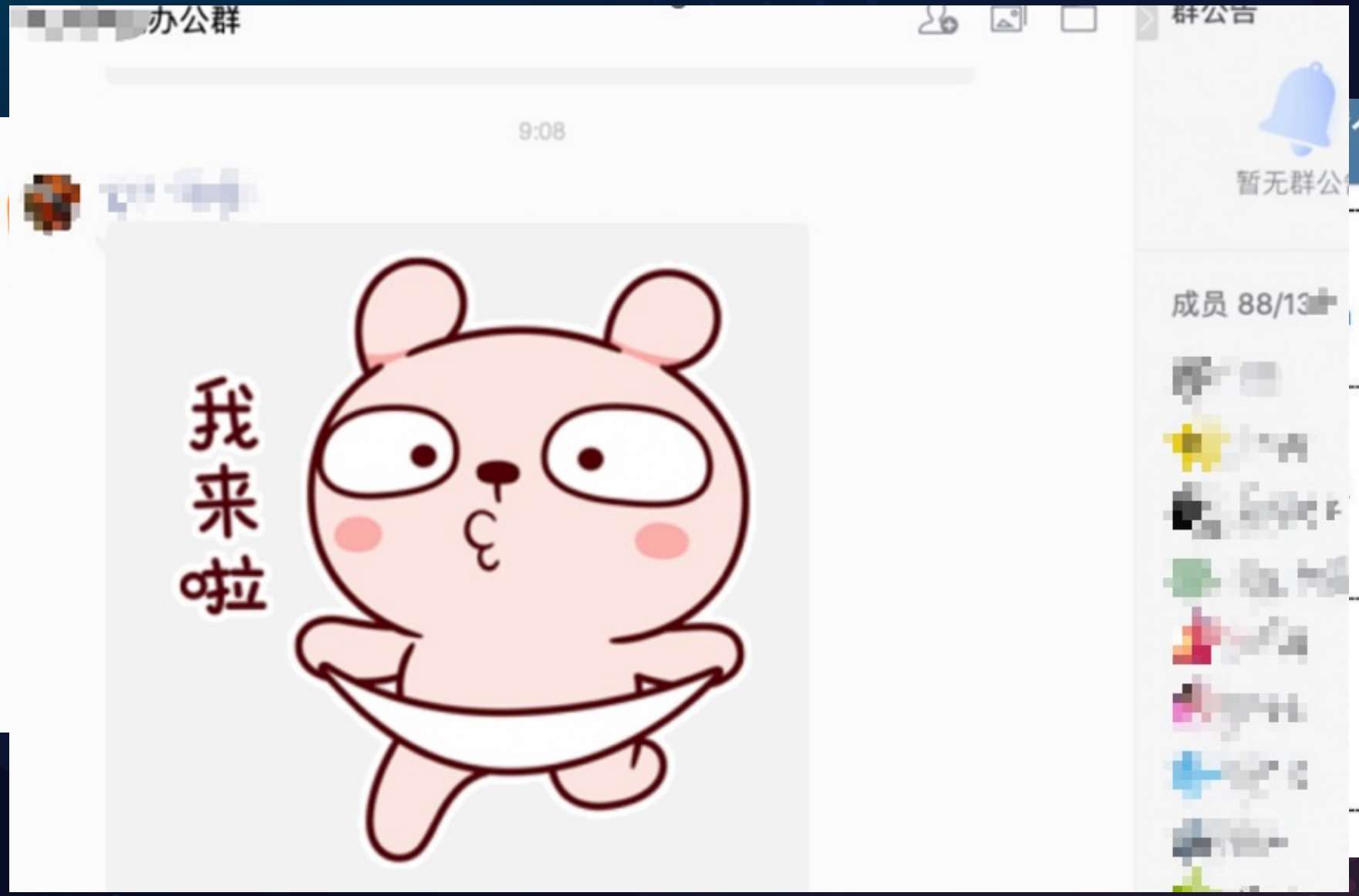
连wifi，badusb

二、攻击视角

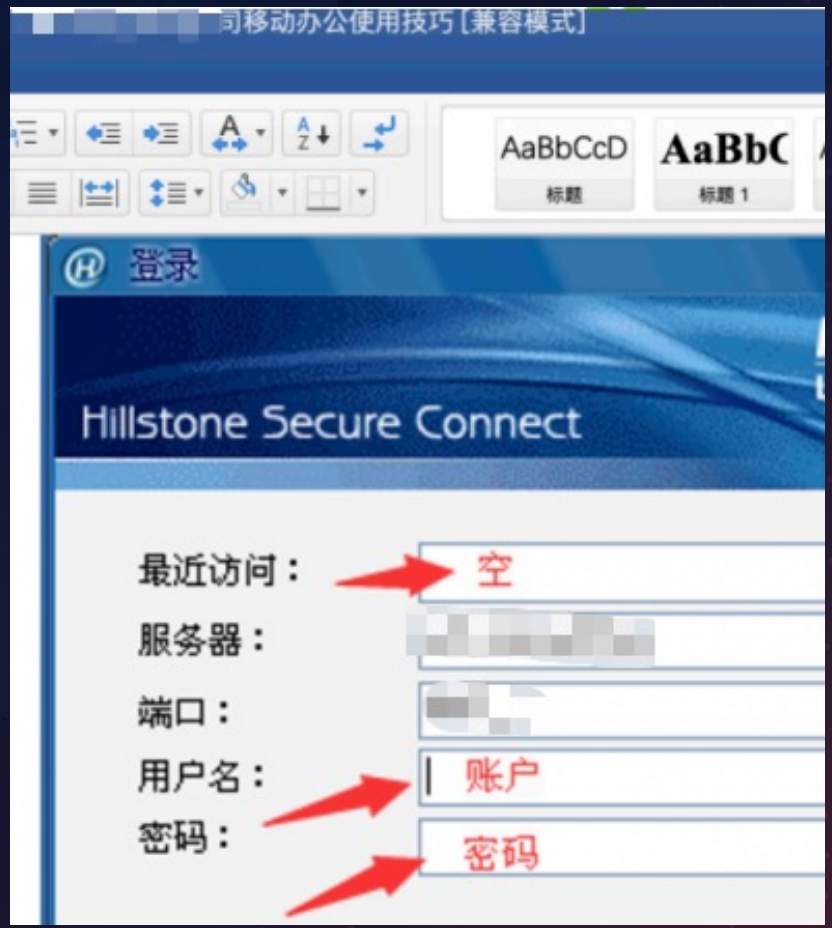
1. 个人信息泄露和企业安全的关联

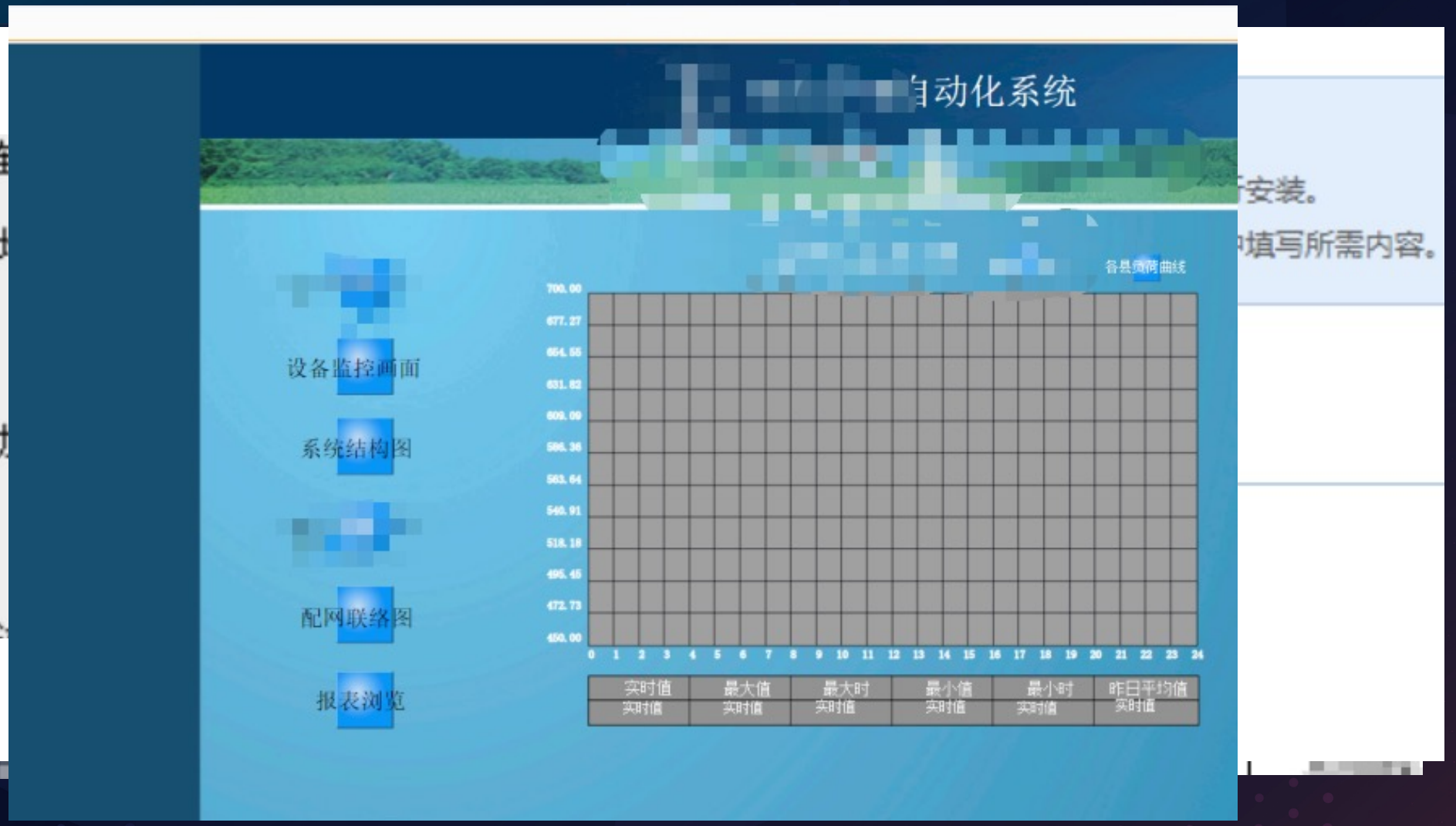
某初期信息收集后防守单位特点：

- 正面资产防护好，交互点较少
- 下属部门分布区域多
- 公司成立时间悠久


办公群
9:08
我来啦
群公告
暂无群公
成员 88/13


群在线文档
多人编辑、永久保存
90.7KB · 105次下载 今天
959KB · 99次下载 昨天
苹果IOS13以后协作平台安装说明 .rar
73.9MB · 10次下载 昨天
103KB · 49次下载 昨天
347KB · 62次下载 2020-12-13
835KB · 33次下载 2020-12-11
微信图片 .jpg
44.5KB · 11次下载 2020-12-10
61.2KB · 169次下载 2020-12-10
15KB · 142次下载 2020-12-7
140KB · 137次下载 2020-12-4
群文件存在大量文件，在文件中开始搜集情报


移动办公使用技巧[兼容模式]
登录
Hillstone Secure Connect
最近访问：
空
服务器：
端口：
用户名：
账户
密码：
密码


自动化系统
设备监控画面
系统结构图
配网联络图
报表浏览
各县负荷曲线
700.00
677.27
654.55
631.82
609.09
586.36
563.64
540.91
518.18
495.45
472.73
450.00
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
实时值
实时值
最大值
实时值
最大时
实时值
最小值
实时值
最小时
实时值
昨日平均值
实时值

攻击路径复盘

重点文件未加密处理

内部敏感文件应该进行加密处理后传递

个人身份信息数据泄露

员工在使用内部软件、应用时不关联个人信息。可以结合多因子和增加随机字符后使用

不安全的办公通讯方式

QQ、微信等社交软件工具

办公软件≠社交软件

个人隐私数据泄露面特点：

攻击成本低、损失大，风险高，难以发现和预警，难管控

内网横纵向渗透

历史漏洞，弱口令

2. 口令安全

在蜀国集团公司上班的安全保卫部部长赵云（假设：公元157年6月12）设置了如下的口令是否安全？

123456 → Top100弱口令

a123456 → Top100弱口令

ZhaoYun@1570612. → 社工字典

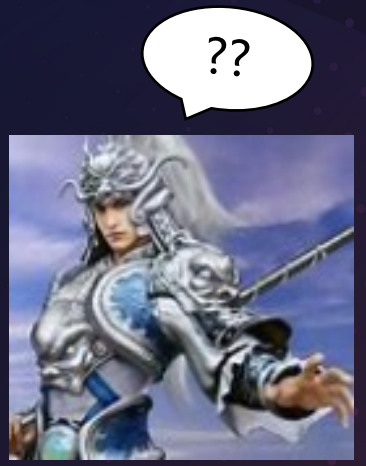
Sgjt@123. → 社工字典

Zy@1570612!@#123 → 键盘密码

1qazXSW@3edc → 键盘密码

1234$Qwertyui → 键盘密码

Qzygonec3! → 诗词密码



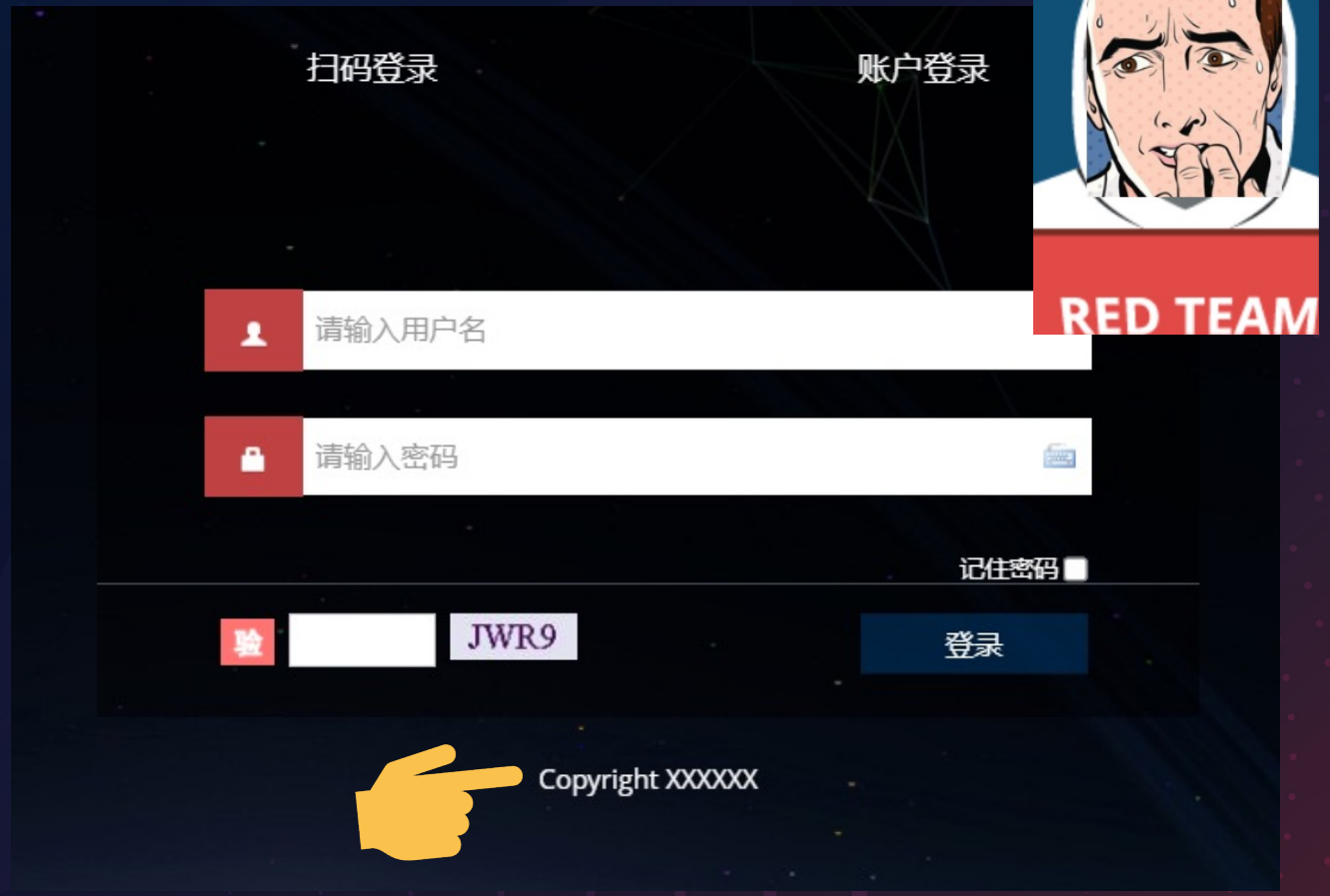
2. 口令安全

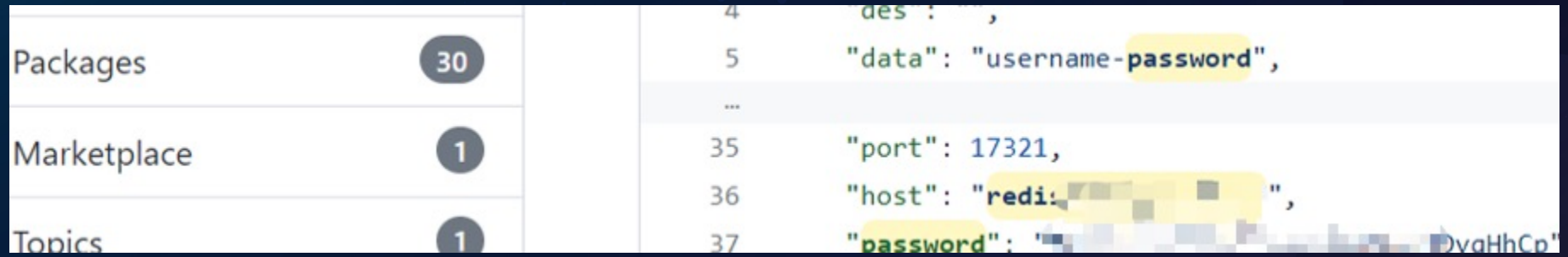
- 不使用弱口令作为密码
- 避免口令中关联自身、企业信息
- 建议通过随机生成多位的口令做密码使用，并尽可能使用二次验证策略
- 不同的应用系统尽量不使用同一个密码，避免口令复用问题
- 不使用常见信息作为密码的组成元素

3. 人VS人

某攻击演练，目标是检测合算系统服务器的安全性

- 服务单一，互联网侧暴漏面少
- 服务上云
- 统一运维





Github泄露了其他公司测试系统的redis口令，考虑开发针对这套系统的密码设置习惯

8007e585ace58fb8e5908d57O757uf5ZCN

端口hex(公司名)Base64(系统名)

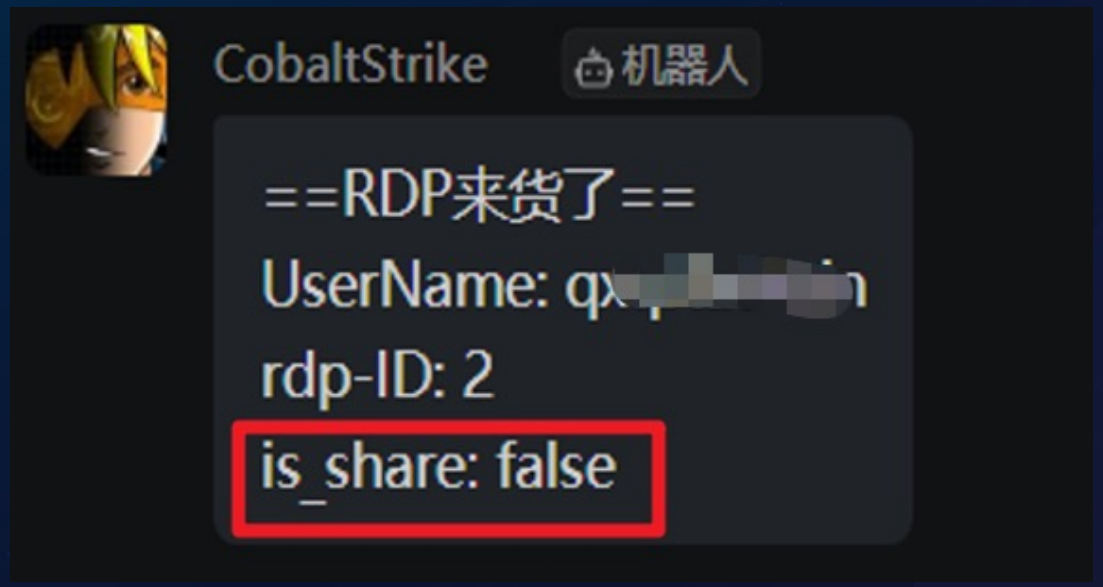
```
$ redis-cli.exe  -h 192.168.117.176 -p 6377
192.168.117.176:6377> auth 123456
OK
192.168.117.176:6377> info
# Server
redis_version:3.2.100
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:dd26f1f93c5130ee
redis_mode:standalone
os:Windows
arch_bits:64
```

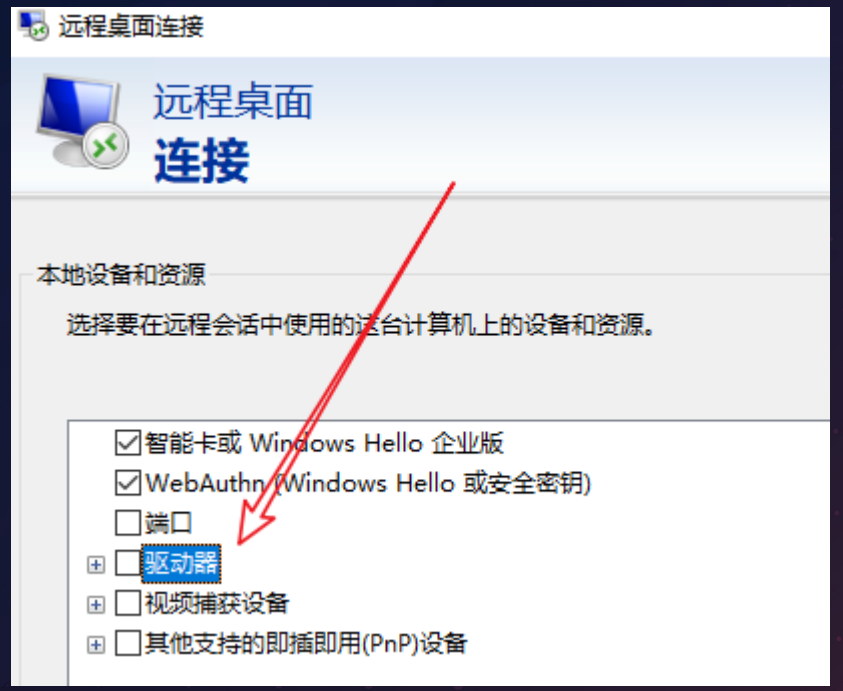
redis-server.exe	2588	IRP_MJ_CREATE	C:\redis\Redis-x64-3.2.100\dbghelp.dll	SUCCESS
redis-server.exe	2588	FASTIO_QUERY_INFORMATION	C:\redis\Redis-x64-3.2.100\dbghelp.dll	SUCCESS

1[redacted]7	http	SYSTEM *	[redacted]	redis-server.exe

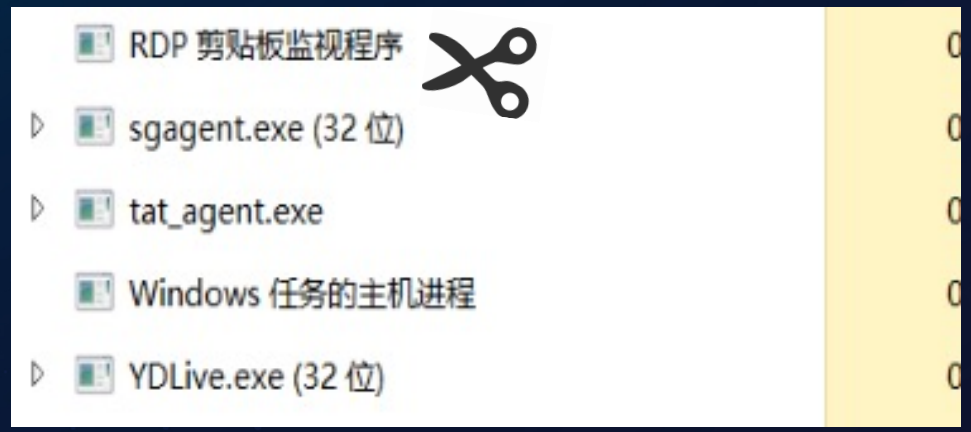
云主机IP

运维RDP登入查看信息，未打开驱动器





持续kill掉剪贴板进程，影响操作，运维为了同步数据开启了驱动器



```
用户名                 会话名                ID  状态      空闲时间    登录时间
[redacted]             rdp-tcp[redacted]      2  运行中          10  [redacted] 10:38
```

```
    12,269 弹性云服务器-（维护人员使用）.xlsx
<DIR>      数据库备份
     1,406 数据库查询.txt
         0 新建文本文档 (2).txt
       842 新建文本文档 (7).txt
       243 新建文本文档 (8).txt
     1,745 新建文本文档 (9).txt
     1,179 新建文本文档.txt
<DIR>      日志
     1,058 桌面助手.lnk
<DIR>      现网
    35,840 账号密码.docx
```

7	WEB服务器 服务器 数据库服务器	[redacted]	不通
8	WEB服务器 服务器 数据库服务器		不通
9	WEB服务器 服务器 数据库服务器		不通
备注	密码：[redacted] 设备密码三个分别是：[redacted]		

攻击路径复盘

ByteDance 字节跳动 | Security 安全与风控 × 安全范化 BYTEDANCE SECURITY

Step One

DLL劫持上线云主机

Step Two

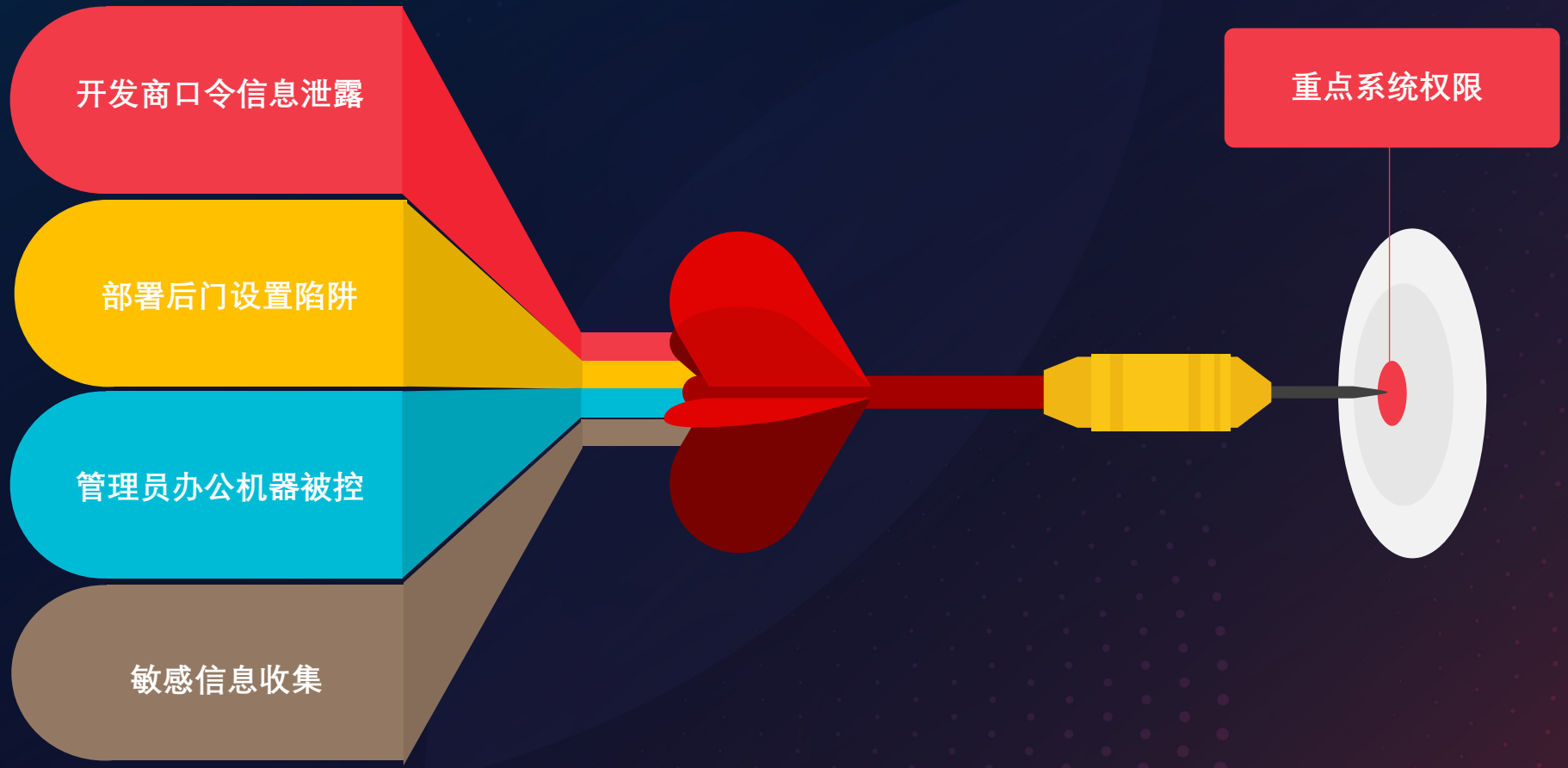
在运维管理员交互过程中设置陷阱

Step Three

运维人员开启驱动器连接RDP，通过共享访问运维办公机器文件

Step Four

搜集口令、服务器信息的敏感文件



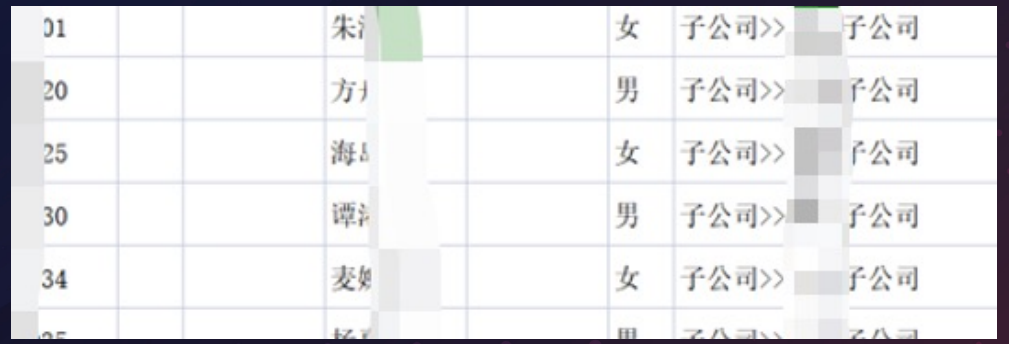
4. 人员安全意识切入点

进行邮箱探活 → 社工字典爆破邮箱 → 来往信件定位敏感信息和关键人员

```
Testing: chenh
Testing: chenh
Testing: duanyu
Testing: duanyu                    -->  [+] user exits!!!!!
Testing: chenmi
Testing: chenmin                   -->  [+] user exits!!!!!
Testing: chengar                                              -->  [+] user exits!!!!!
Testing: chengu
Testing: chengu
Testing: zhangw
Testing: zhangw
Testing: zhangm
```

```
Testing: fa                    @2019  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: fa                    @2018  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: f                     @2017  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: g                     @2021  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: g                     @2020  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: g                     @2019  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: g                     @2018  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: g                     @2017  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: h                     gh@2021  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing:                       1  -->  ('OK', [b'LOGIN completed'])  -->  [+] success!!!!!!!
Testing: h                     @2020  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: ha                    @2018  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: ha                    @2019  -->  ['ERROR', "b'LOGIN Login error password error'"]
Testing: ha                    @2017  -->  ['ERROR', "b'LOGIN Login error password error'"]
```

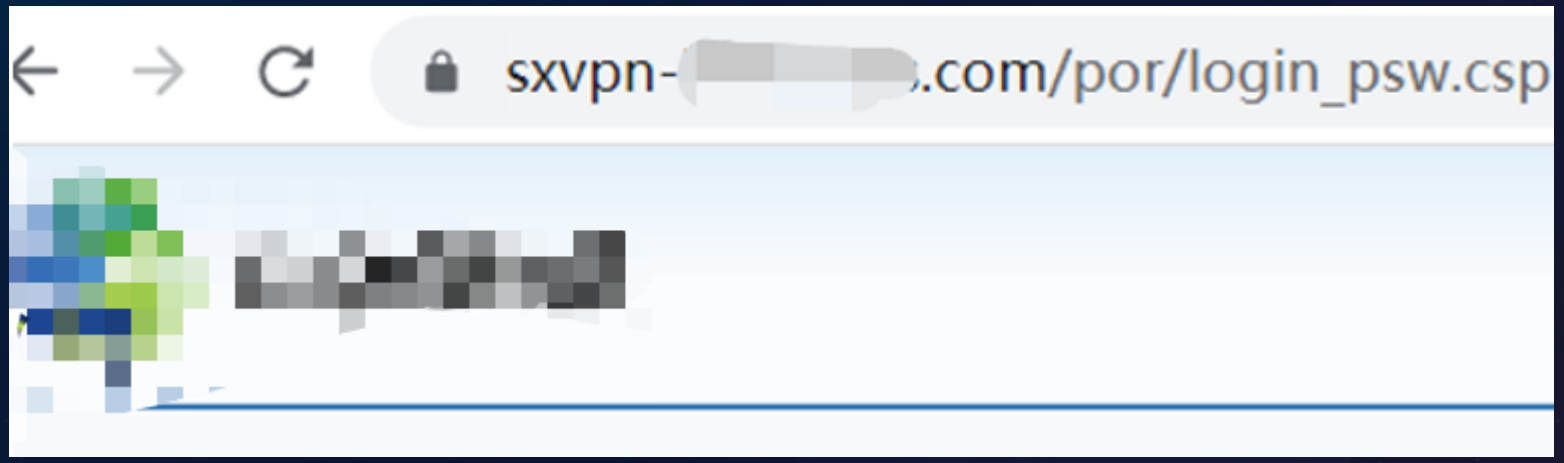
敏感信息未分离发送，未设置异常设备登入后提醒

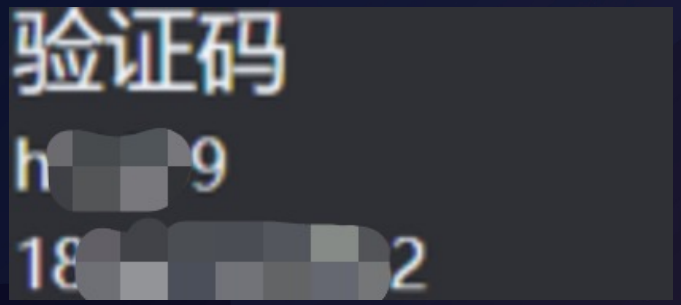


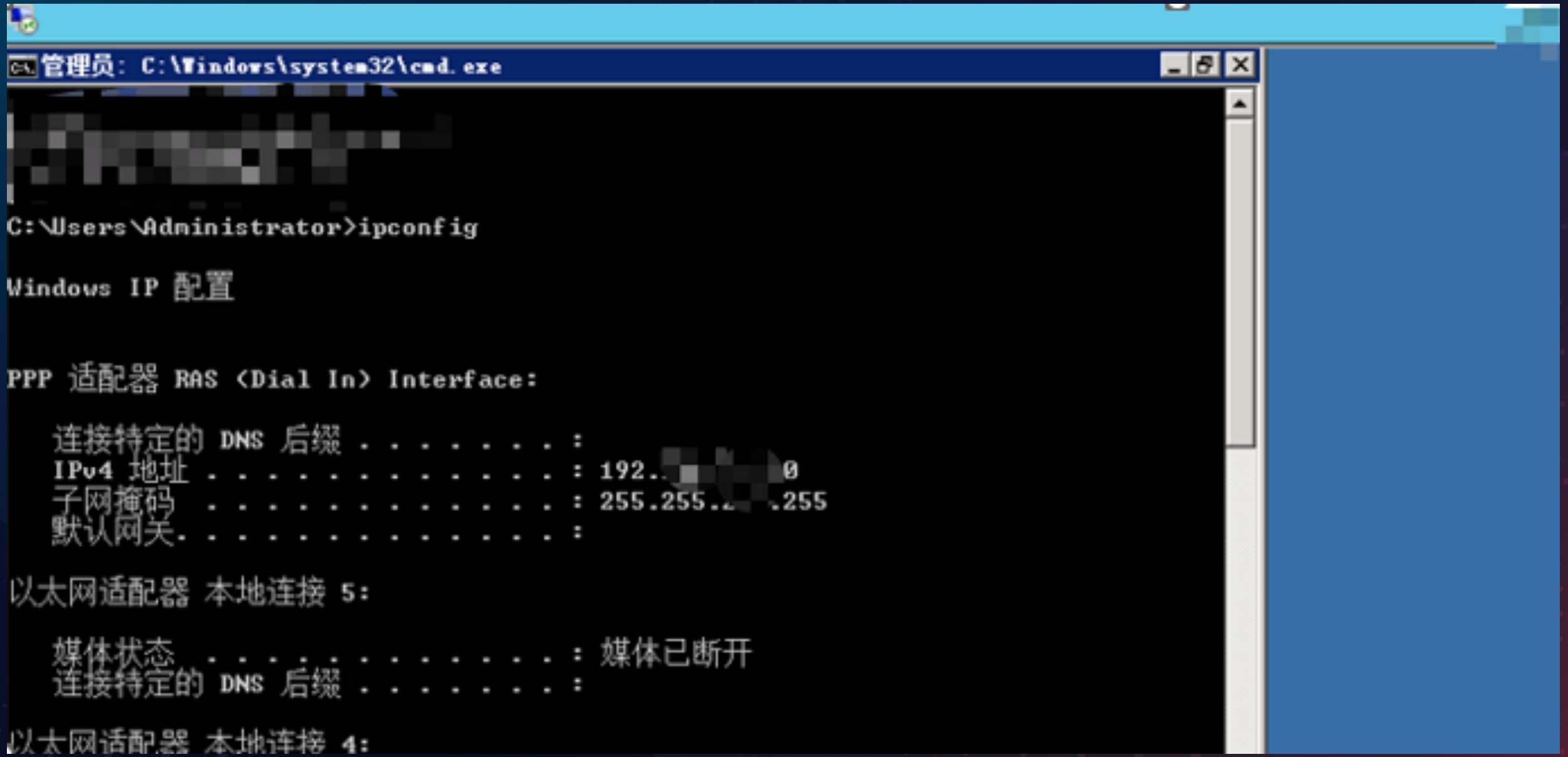
VPN存在短信验证码

定位新入职信息部门员工 → 结合内部人员信息搜集表 → 获得信息部门员工邮箱权限 → 准备钓鱼

通过信息部门员工邮箱权限进行VPN账号钓鱼 → 通过交互的方式获得短信验证码






管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig
Windows IP 配置
PPP 适配器 RAS (Dial In) Interface:
连接特定的 DNS 后缀 . . . . . :
IPv4 地址 . . . . . : 192.
子网掩码 . . . . . : 255.255.
.255
默认网关. . . . . :
以太网适配器 本地连接 5:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
以太网适配器 本地连接 4:

抵御钓鱼攻击

监控和审计

组织应该对系统和网络进行监控和审计，及时发现和响应任何异常活动和事件

安全培训

加强安全意识，提高员工对钓鱼攻击的识别能力和警惕性，定期进行安全意识培训

内部模拟

先一步攻击者模拟钓鱼，常态化对抗钓鱼攻击，洞见未来

强制身份验证

对于敏感操作和访问，应该强制要求用户进行身份验证，可以通过多因素身份验证来实现

制度建立

奖惩机制，规范相关需求的申请流程，对涉密邮件发信设定要求等

三、总结

- 安全建设不应该是简单的设备的堆叠和单纯的模板套用，需要结合自身的特点针对性进行防护加强
- 网络安全是动态的过程，安全事件和安全技术的出现都能影响对抗的天平，需要进行紧密关注和实时响应
- 重视攻击面管理，监控攻击者可能的入侵路径（与自身网络或业务存在关联的节点，也是入侵路径中难以管理的一环）eg：开发商项目完成后敏感信息清除方式和管控

THANK YOU FOR READING

 zhengyang@seclover.com