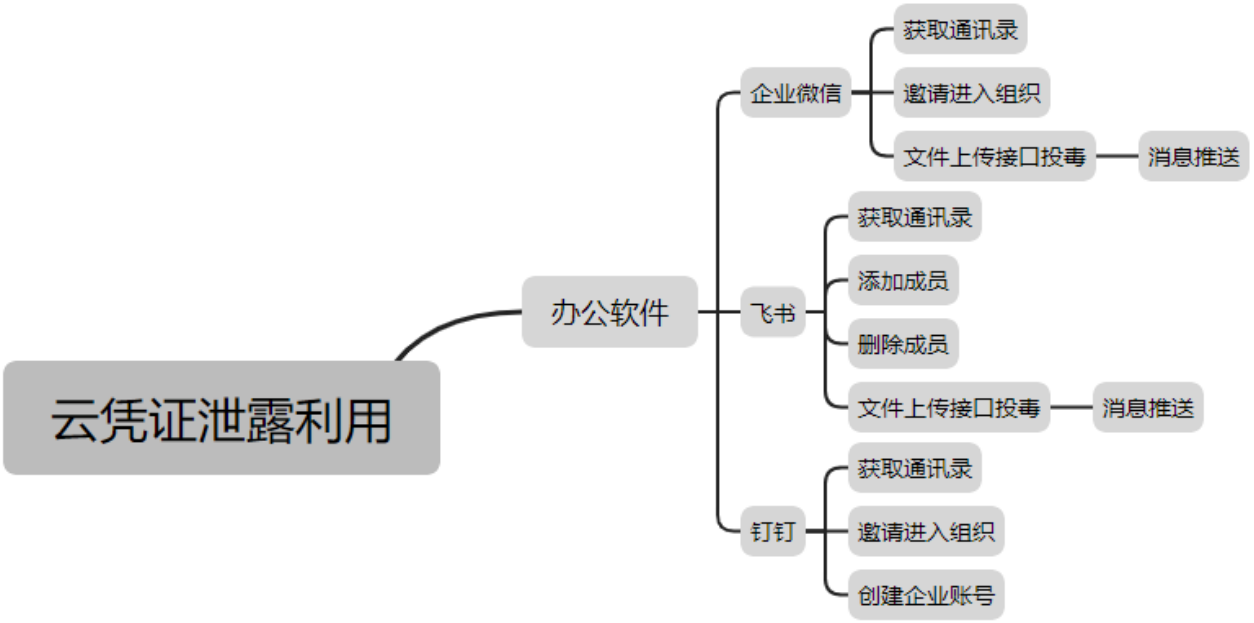
Readme

发送消息

功能总体实现图



大概功能

微信

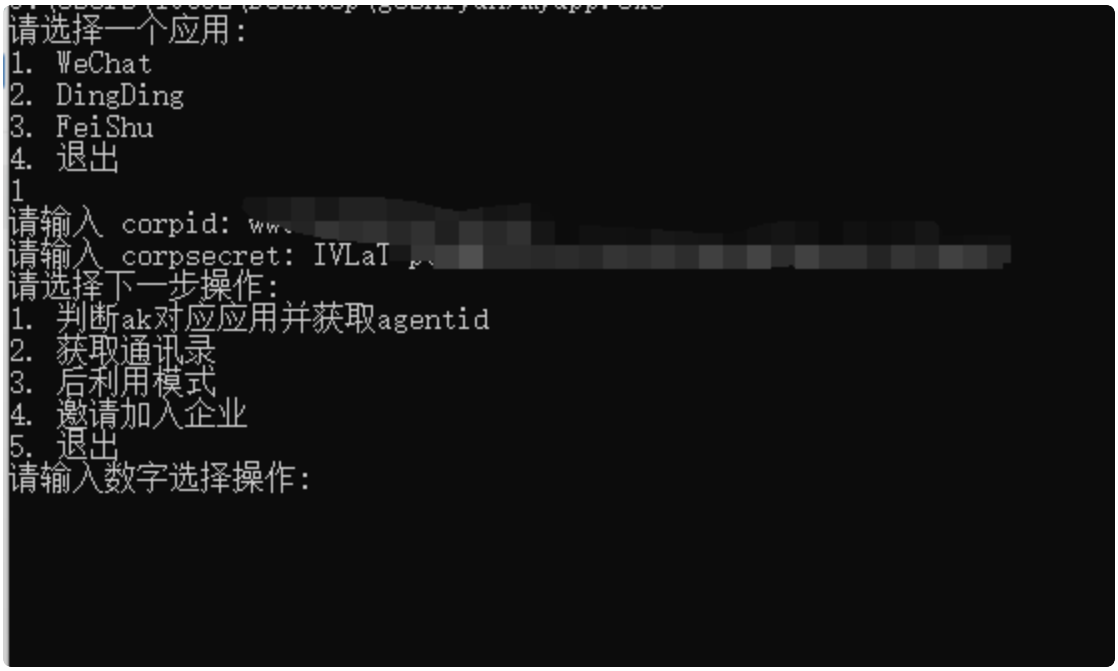
ak特性

开头为ww

使用方法

运行exe 逐步操作

```
请选择一个应用:
1. WeChat
2. DingDing
3. FeiShu
4. 退出
1
请输入 corpid: xxx
请输入 corpsecret: xx
请选择下一步操作:
1. 判断ak对应应用并获取agentid
2. 获取通讯录
3. 后利用模式
4. 邀请加入企业
5. 退出
```



目的:泄露企业微信key，获取后的后利用，包含获取组织架构，整体通讯录，后续钓鱼社工利用。

功能:分为四大模块，分别为判断ak对应应用、获取通讯录、后利用模式、邀请加入企业。

1、可以通过判断ak对应应用去定位我们获取了哪个应用的api权限。

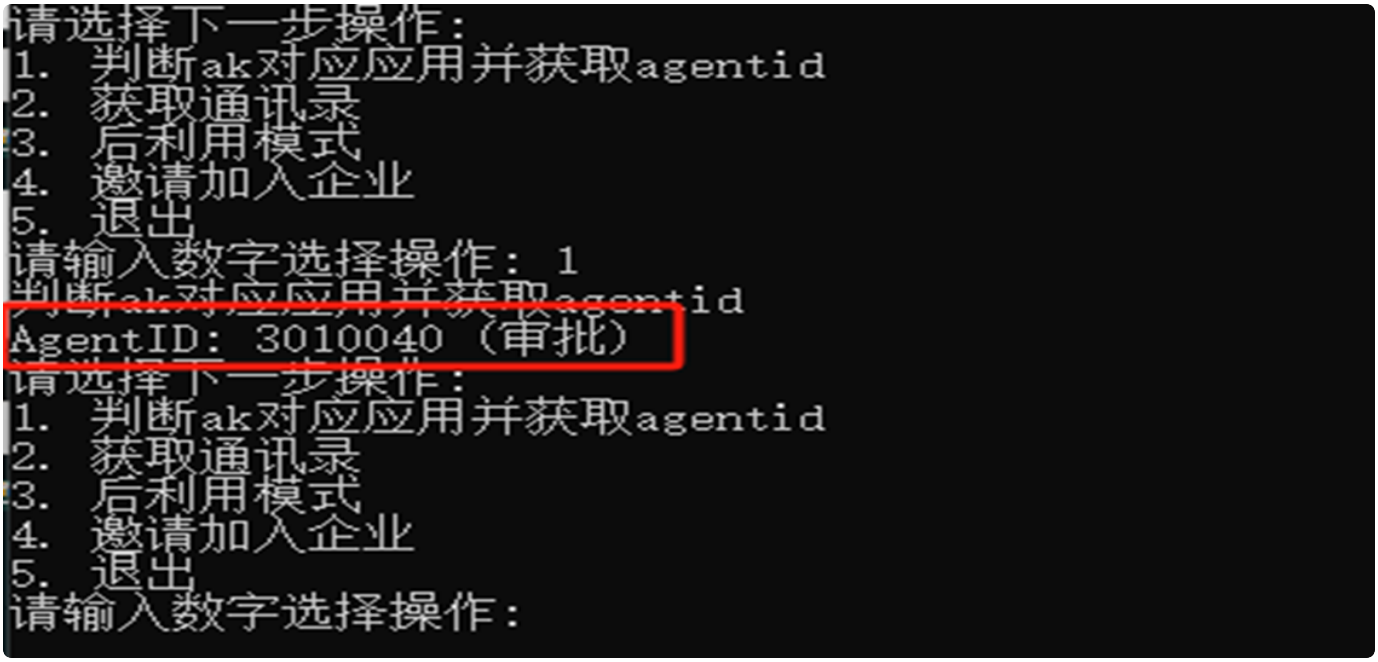
2、一般应用都有调用获取通讯录api的权限，获取通讯录可方便我们后续利用。

3、后利用模式分为上传文件、下载文件和下发消息功能，第一步上传我们的木马或者钓鱼话术文件至企业微信存储桶中，然后通过通讯录定位社工钓鱼的人，进行定点发送我们的木马或者是钓鱼话术，从而

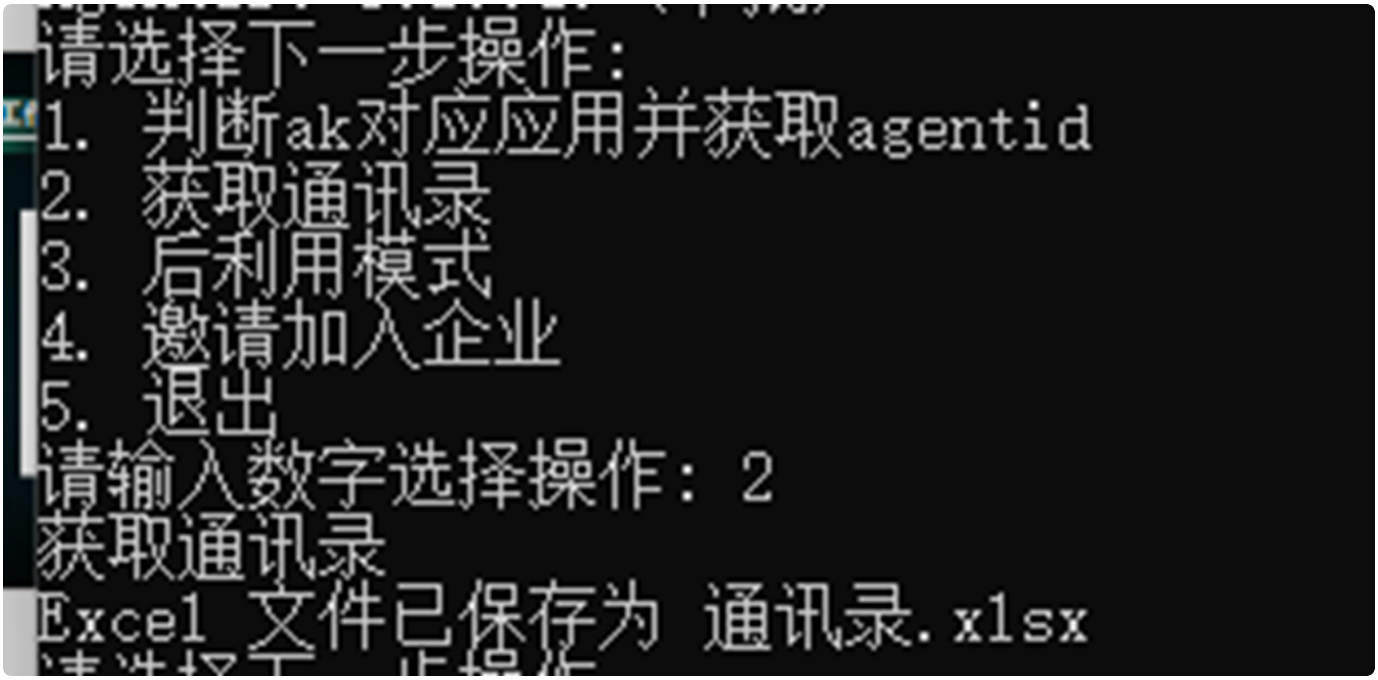
达到钓鱼的作用。

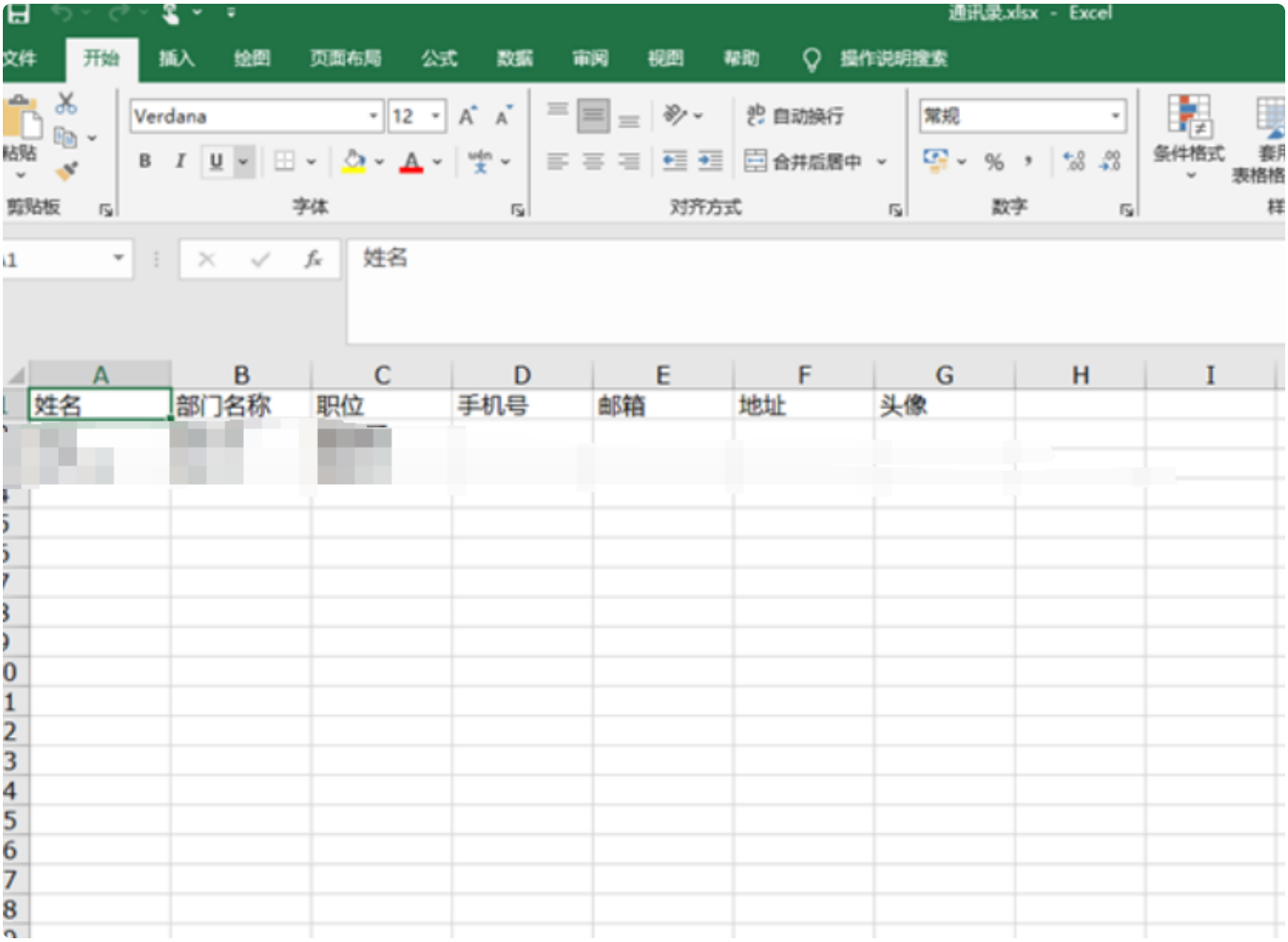
4、邀请加入企业模块，需要比较高权限的ak，拥有高权限ak后可自动生成二维码，扫描填写信息即可加入企业。

1、判断ak对应的应用



2、获取全员通讯录





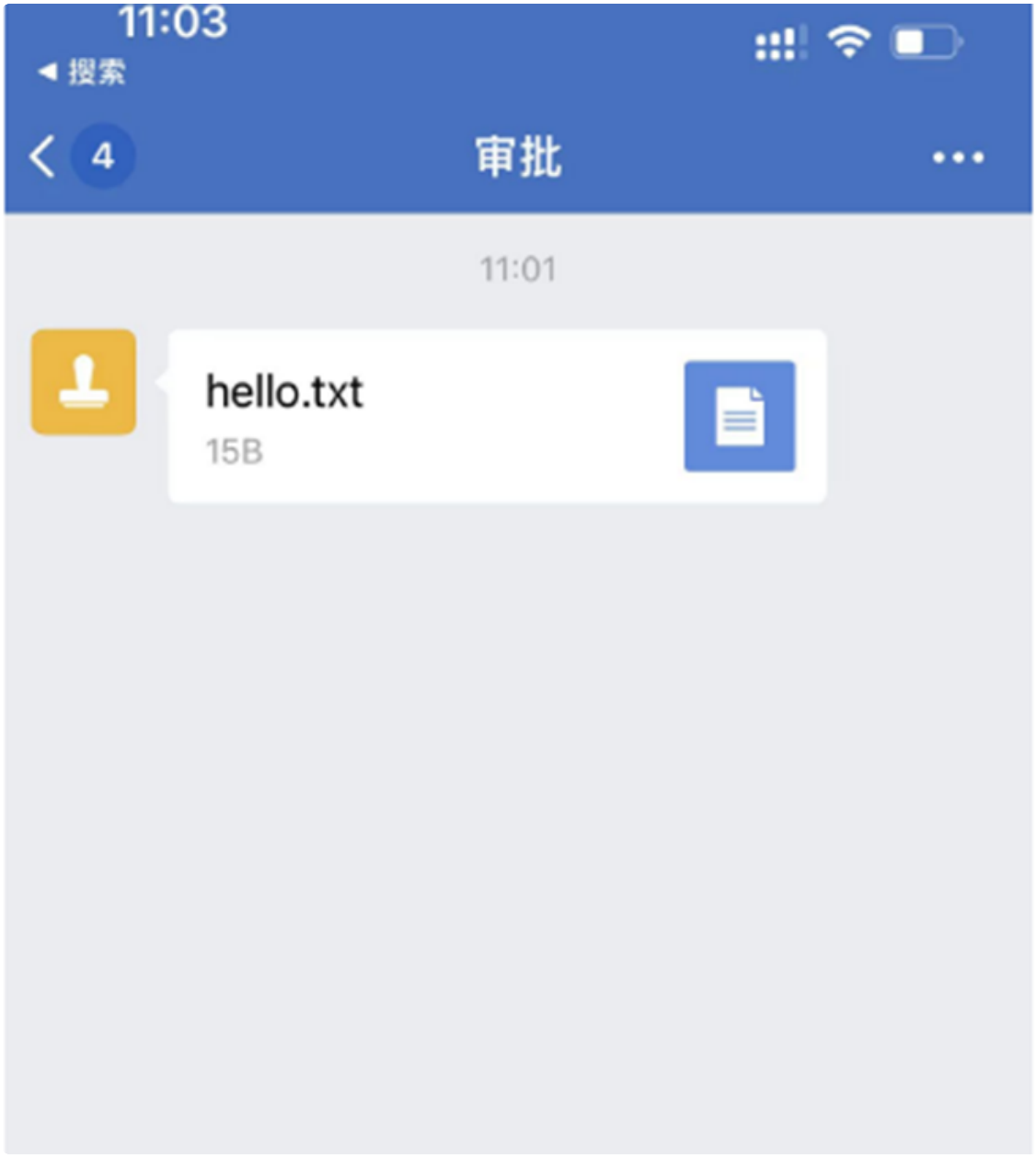
3、后利用模式

上传文件

下载文件

发送消息

传入用户id(由通讯录获取) mediaid(上传文件后回显的id) agentid(刚开始获取的应用Id)


11:03
搜索
4
审批
11:01
hello.txt
15B

4、邀请加入企业


请选择下一步操作:
1. 判断ak对应应用并获取agentid
2. 获取通讯录
3. 后利用模式
4. 邀请加入企业
5. 退出
请输入数字选择操作: 4
获取邀请加入企业二维码
二维码内容: https://work.weixin.qq.com/wework_admin/genqrcode?action=join&vcode=a
hare_api_mjoin&qr_size=3
请选择下一步操作:
1. 判断ak对应应用并获取agentid
2. 获取通讯录

钉钉

ak特性

开头为ding

使用方法

运行exe 逐步操作

```
请选择一个应用:
1. WeChat
2. DingDing
3. FeiShu
4. 退出
2
请输入appKey: xxxx
请输入appSecret: xxx
Access Token: xxxx
请选择一个操作:
1. 获取通讯录
2. 邀请进入组织
3. 创建企业账号
4. 删除企业账号
```

目的:泄露钉钉应用key的后利用，包括获取token，获取通讯录，获取企业邀请链接，添加删除企业高管用户。

功能:分为三大模块，分别为获取通讯录、获取企业邀请链接、添加删除企业高管用户。

1、通过泄露的ak获取token，在具有通讯录的权限以及白名单的情况下获取通讯录

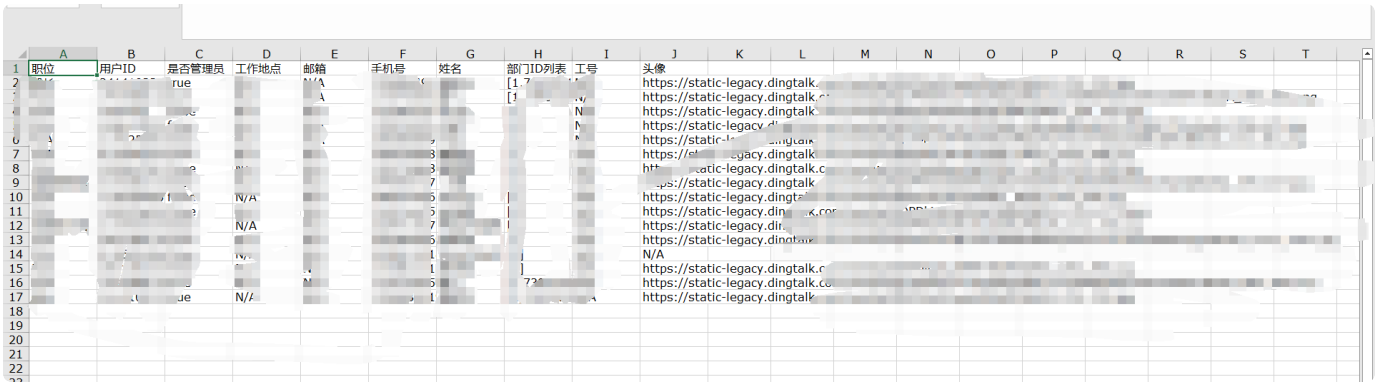
2、通过接口调用获取企业邀请链接，可填写内容进入企业。

3、调用接口自定义请求包，创建高管用户，高管用户(隐藏手机号、DING等消息)

4、可以删除创建的企业账号

1、一键获取企业通讯录

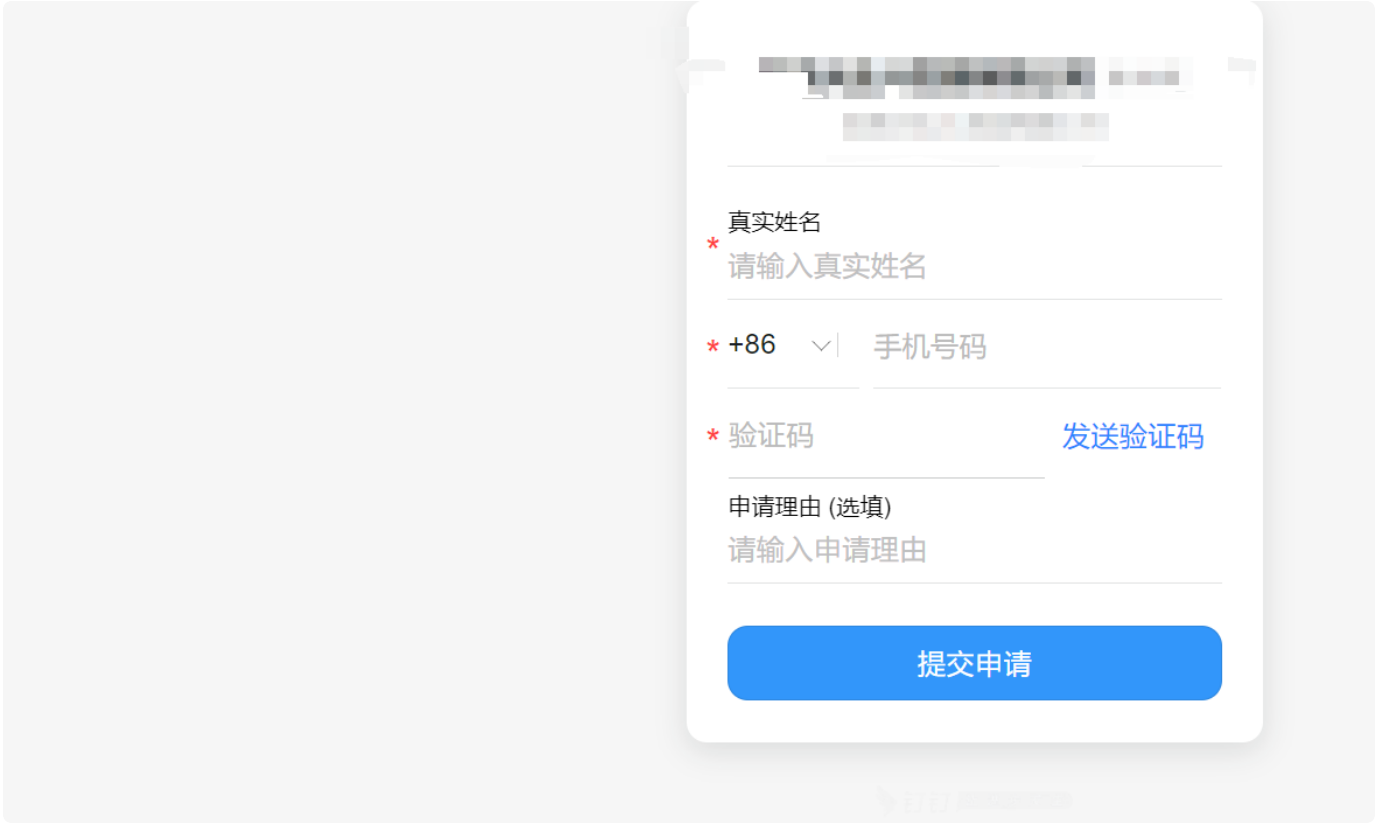
```
请输入appKey: din
请输入appSecret: rywI
Access Token: 27e0
请选择一个操作:
1. 获取通讯录
2. 邀请进入组织
3. 创建企业账号
4. 删除企业账号
5. 退出
请输入数字选择操作: 1
员工信息已保存到钉钉通讯录.xlsx文件.
```



职位	用户ID	是否管理员	工作地点	邮箱	手机号	姓名	部门ID列表	工号	头像
		rue							https://static-legacy.dingtalk.
									https://static-legacy.dingtalk.
									https://static-legacy.dingtalk
									https://static-legacy.dingtalk
									https://static-legacy.dingtalk
									https://static-legacy.dingtalk
									https://static-legacy.dingtalk.c
									https://static-legacy.dingtalk
			N/A						https://static-legacy.dingta
									https://static-legacy.din k.cor
			N/A						https://static-legacy.dir
									https://static-legacy.dingtalk
									N/A
									https://static-legacy.dingtalk.c
									https://static-legacy.dingtalk.co
		ue	N/A						https://static-legacy.dingtalk

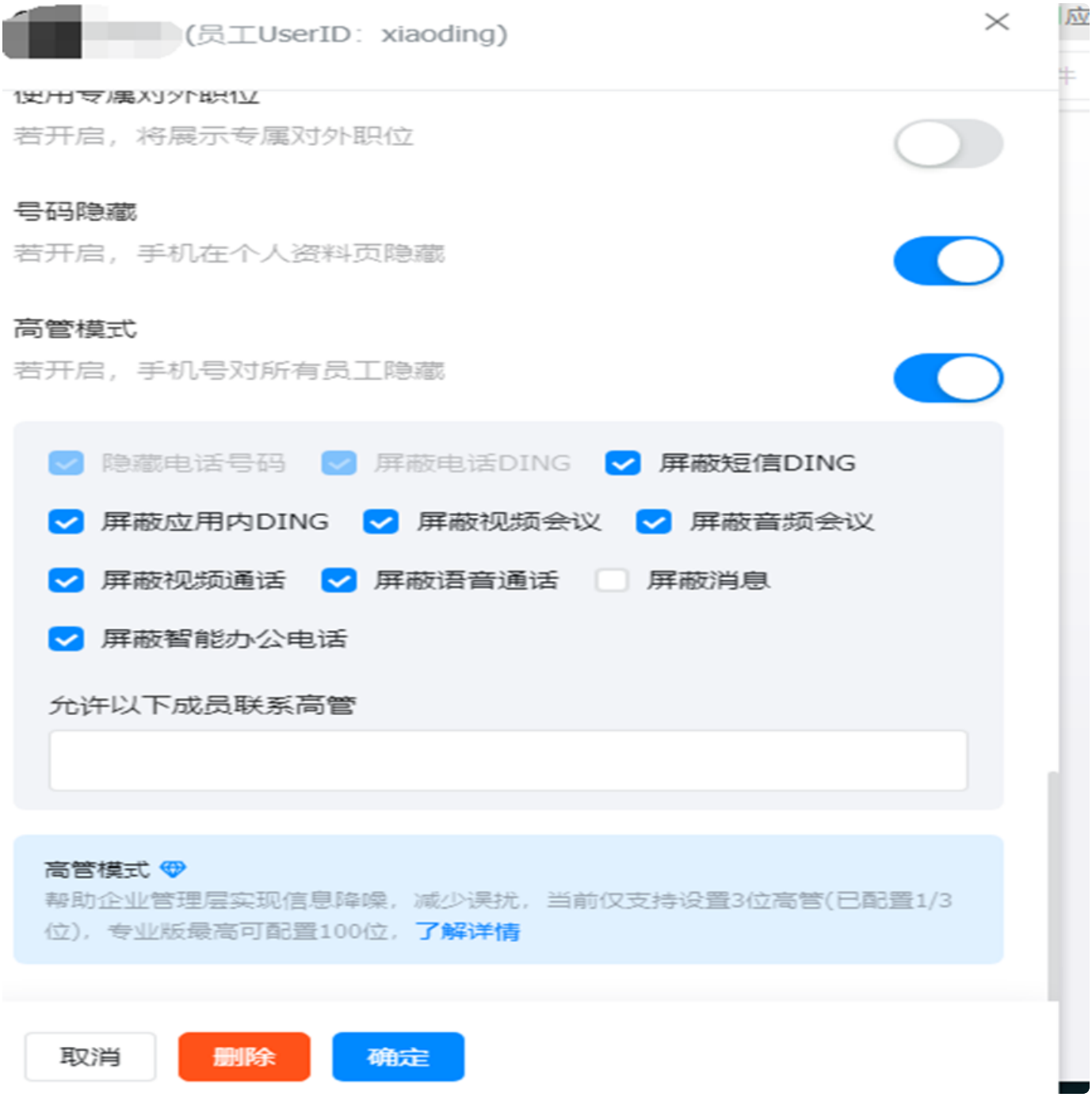
2、获取企业邀请链接(需要审批)

```
请输入appKey: ding
请输入appSecret:
Access Token: 27e0
请选择一个操作:
1. 获取通讯录
2. 邀请进入组织
3. 创建企业账号
4. 删除企业账号
5. 退出
请输入数字选择操作: 2
邀请链接: https://wx-in-i.dingtalk.com/invite-page/weixin.html?bizSource=____source____&corpId=d
```



3、添加企业用户(高管模式)

v



4、删除已创建的企业账号

```
请选择一个操作:
1. 获取通讯录
2. 邀请进入组织
3. 创建企业账号
4. 删除企业账号
5. 退出
请输入数字选择操作: 4
删除账号响应: {"errcode":0,"errmsg":"ok","request_id":"15[redacted]"}
```

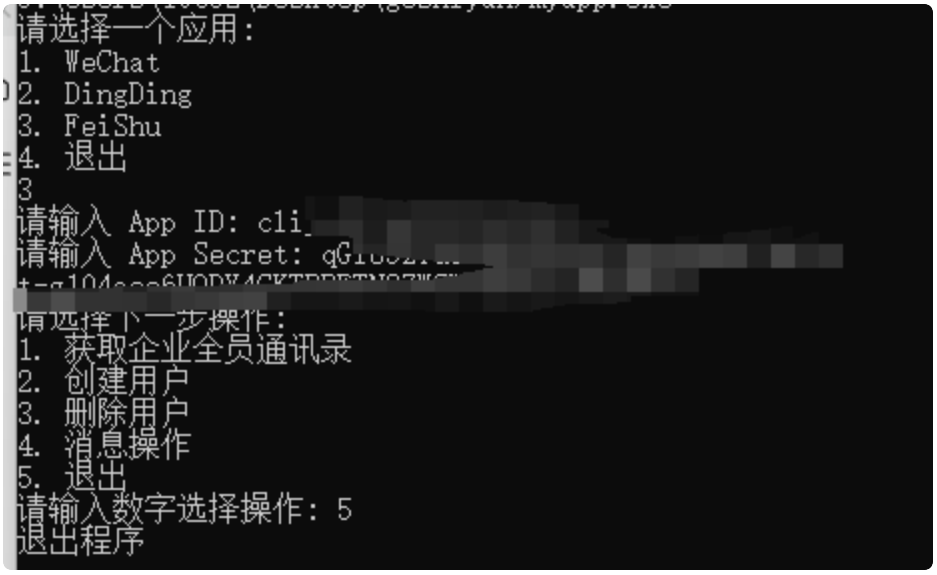
飞书

ak特性

开头为cli_

使用方法

```
请选择一个应用:
1. WeChat
2. DingDing
3. FeiShu
4. 退出
3
请输入 App ID: xxxx
请输入 App Secret: xxxx
请选择下一步操作:
1. 获取企业全员通讯录
2. 创建用户
3. 删除用户
4. 消息操作
5. 退出
```



目的:泄露飞书应用key的后利用，包括获取token,获取通讯录,创建删除用户，消息推送功能

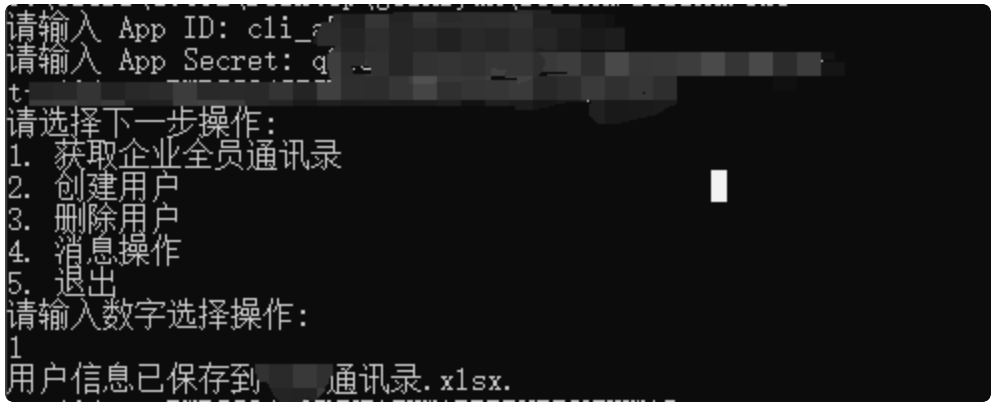
1、首先通过获取的token遍历所有组织号，然后通过组织号获取所有人员通讯录

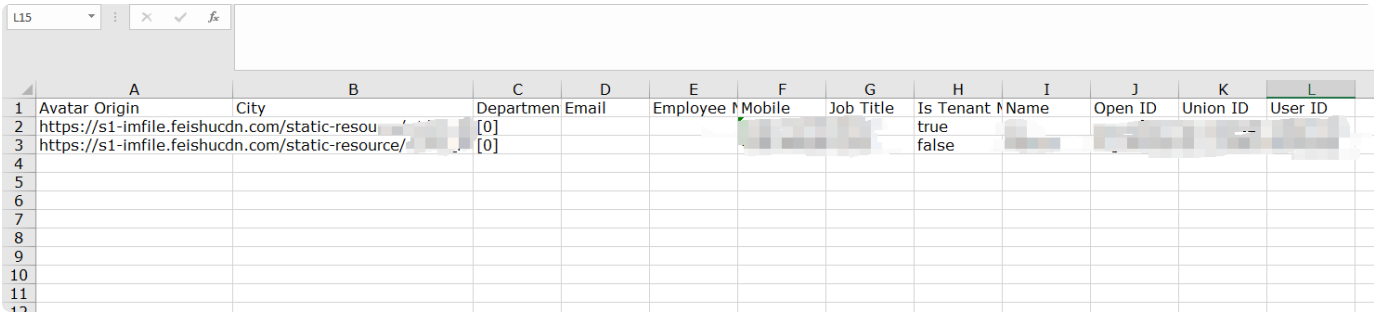
2、通过接口创建别人看不到手机号的用户

3、删除创建的用户，通过userid

4、消息操作分为上传文件、下载文件和下发消息功能，第一步上传我们的木马或者钓鱼话术文件至存储桶中，然后通过通讯录定位社工钓鱼的人，进行定点发送我们的木马或者是钓鱼话术，从而达到钓鱼的作用。

1、通讯录导出

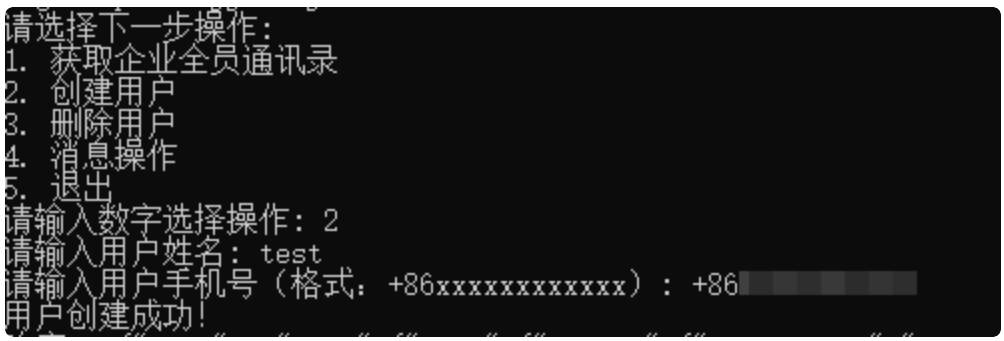




	A	B	C	D	E	F	G	H	I	J	K	L
1	Avatar Origin	City	Departmen	Email	Employee N	Mobile	Job Title	Is Tenant M	Name	Open ID	Union ID	User ID
2	https://s1-imfile.feishucdn.com/static-resou		[0]					true				
3	https://s1-imfile.feishucdn.com/static-resource/		[0]					false				
4												
5												
6												
7												
8												
9												
10												
11												

2、创建删除用户

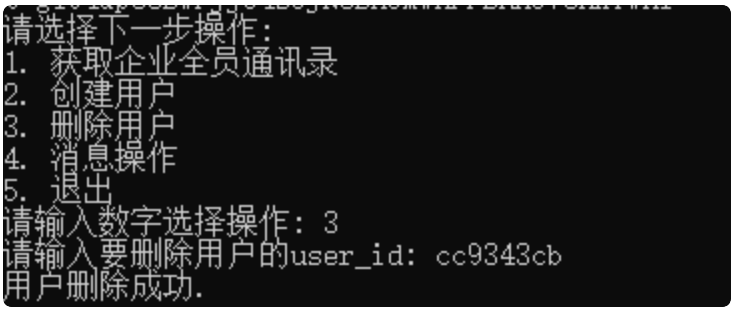
创建用户




106912660376
短信
【飞书】你好
****管理员邀请你加入企业，点击链接确认是否加入该企业。
yqeqcevudux.feishu.cn/invite/choose?
回 TD 退订

点击链接则可加入企业

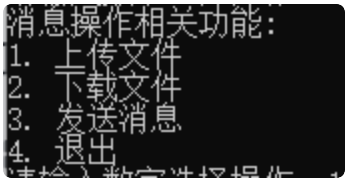
删除用户



通过提供八位user_id删除用户

3、消息操作

分为上传文件、下载文件、发送消息



上传文件

给出file key

发送消息

通过file key和user id去发送给指定人员