

Readme

功能总体实现图

大概功能

微信

ak特性

使用方法

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

4、邀请加入企业

钉钉

ak特性

使用方法

1、一键获取企业通讯录

2、获取企业邀请链接(需要审批)

3、添加企业用户(高管模式)

4、删除已创建的企业账号

飞书

ak特性

使用方法

1、通讯录导出

2、创建删除用户

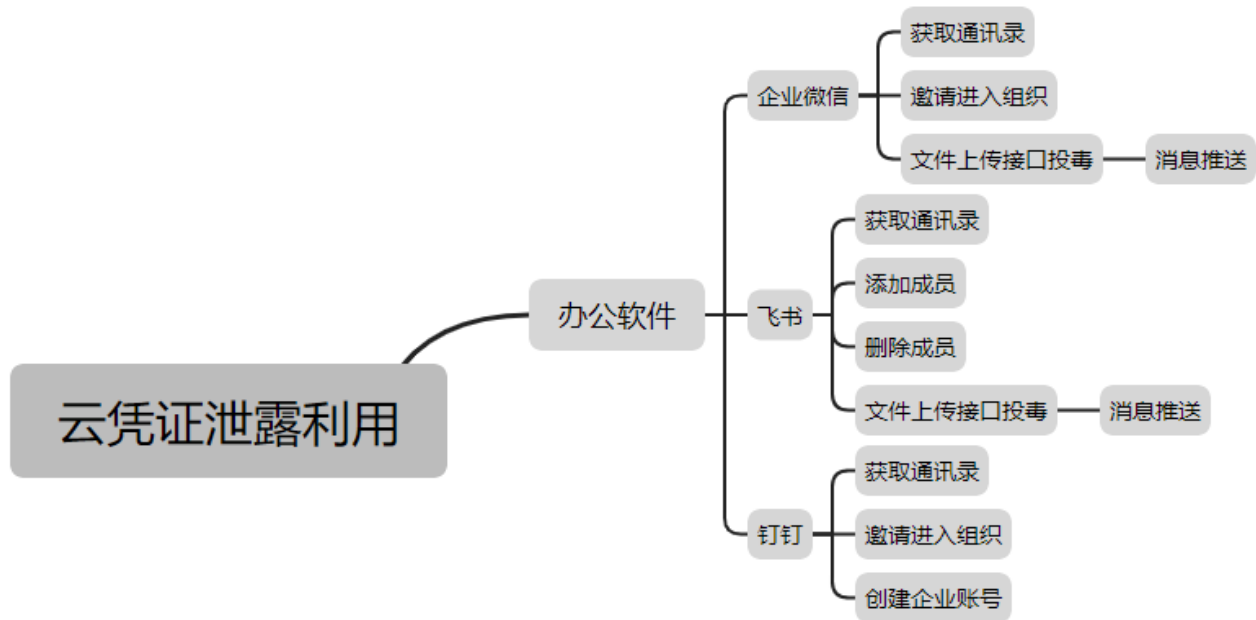
创建用户

删除用户

3、消息操作

上传文件

功能总体实现图



大概功能

微信

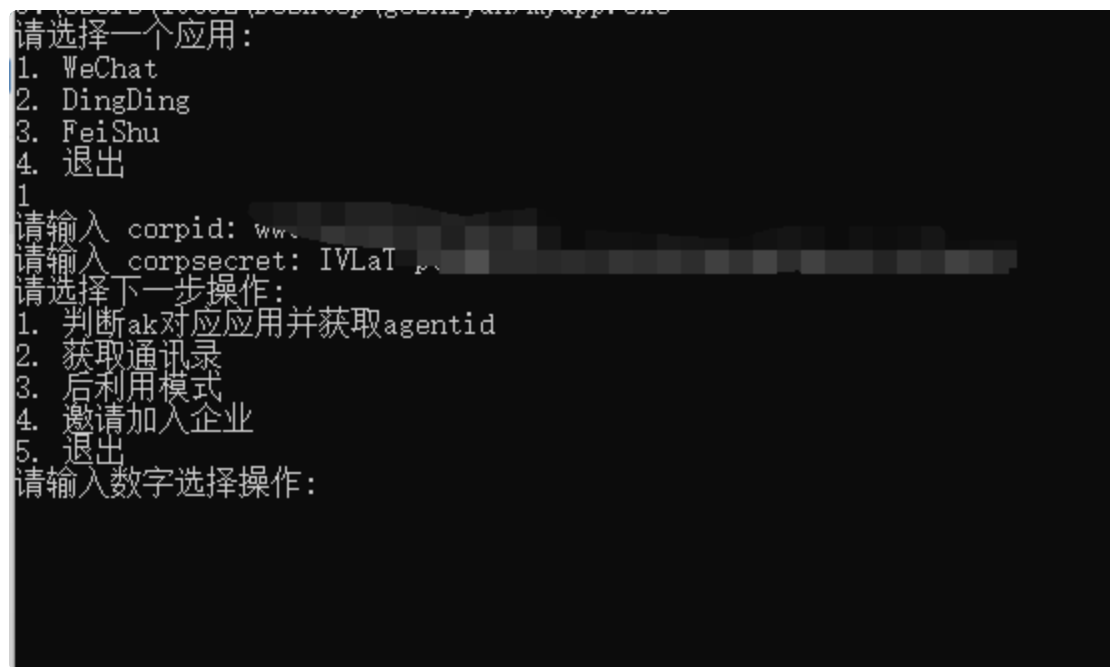
ak特性

开头为ww

使用方法

运行exe 逐步操作

```
▼ Plain Text |
1  请选择一个应用:
2  1. WeChat
3  2. DingDing
4  3. FeiShu
5  4. 退出
6  1
7  请输入 corpid: xxx
8  请输入 corpsecret: xx
9  请选择下一步操作:
10 1. 判断ak对应应用并获取agentid
11 2. 获取通讯录
12 3. 后利用模式
13 4. 邀请加入企业
14 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。

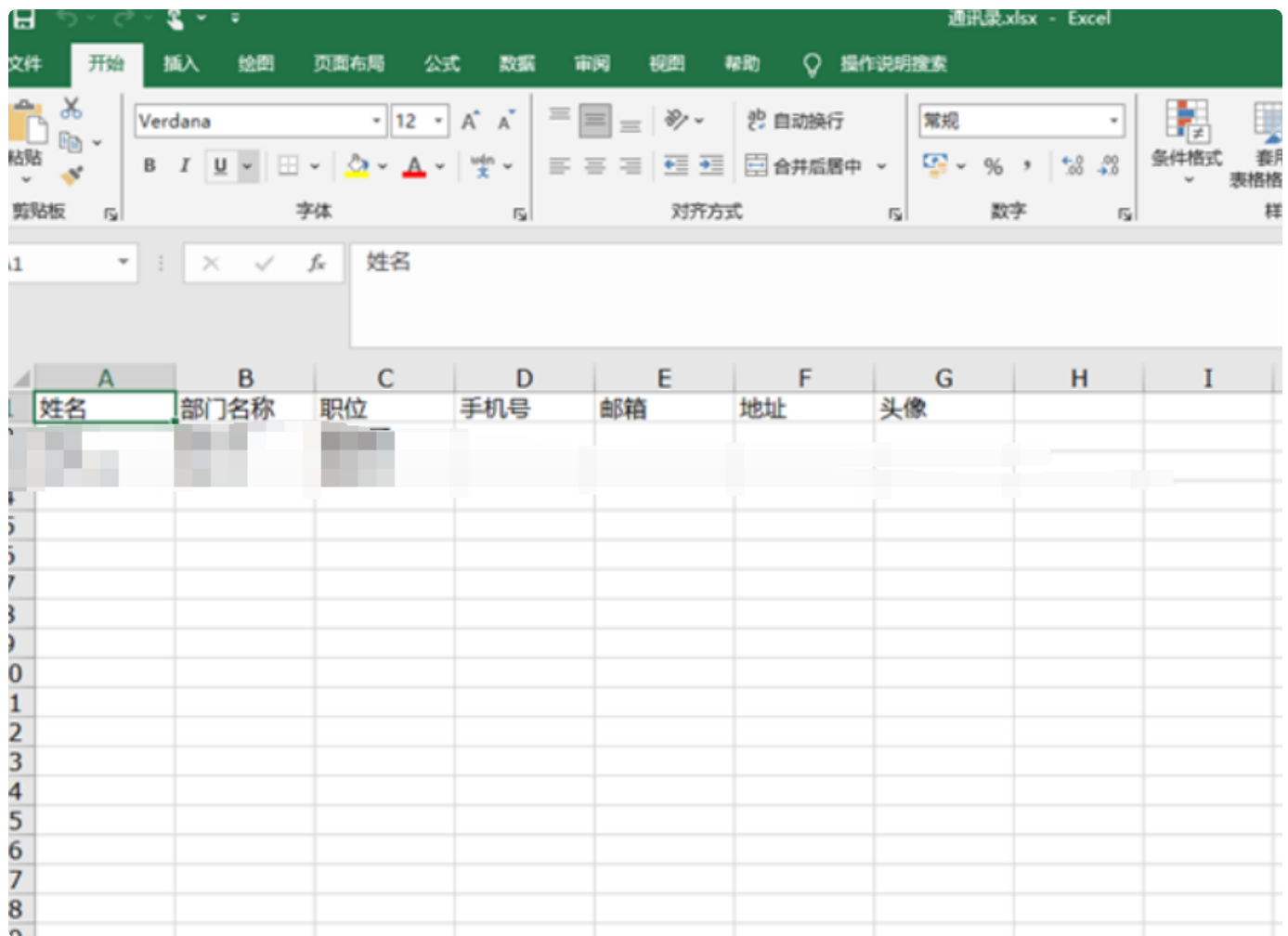
4、邀请加入企业模块，需要比较高权限的ak，拥有高权限ak后可自动生成二维码，扫描填写信息即可加入企业。

1、判断ak对应的应用

```
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：1
判断ak对应应用并获取agentid
AgentID: 3010040 (审批)
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：
```

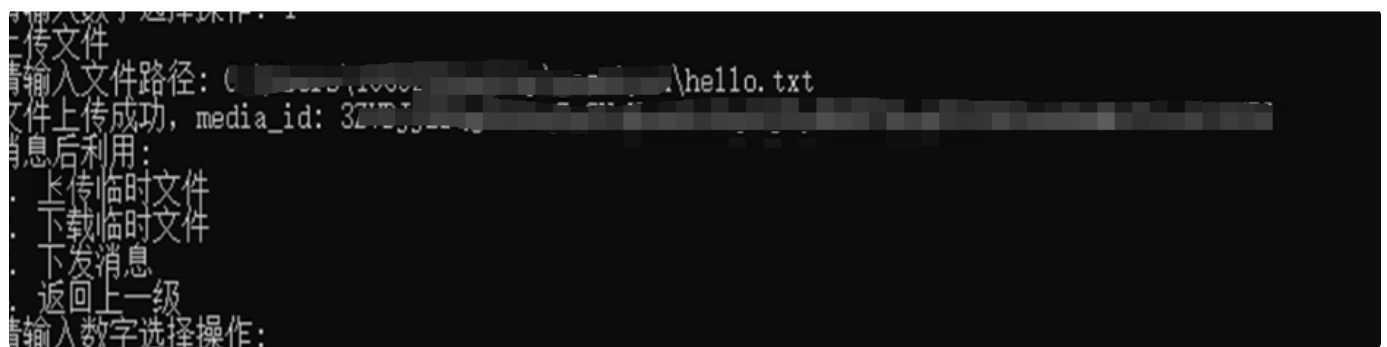
2、获取全员通讯录

```
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：2
获取通讯录
Excel 文件已保存为 通讯录.xlsx
请选择下一步操作：
```



3、后利用模式

上传文件



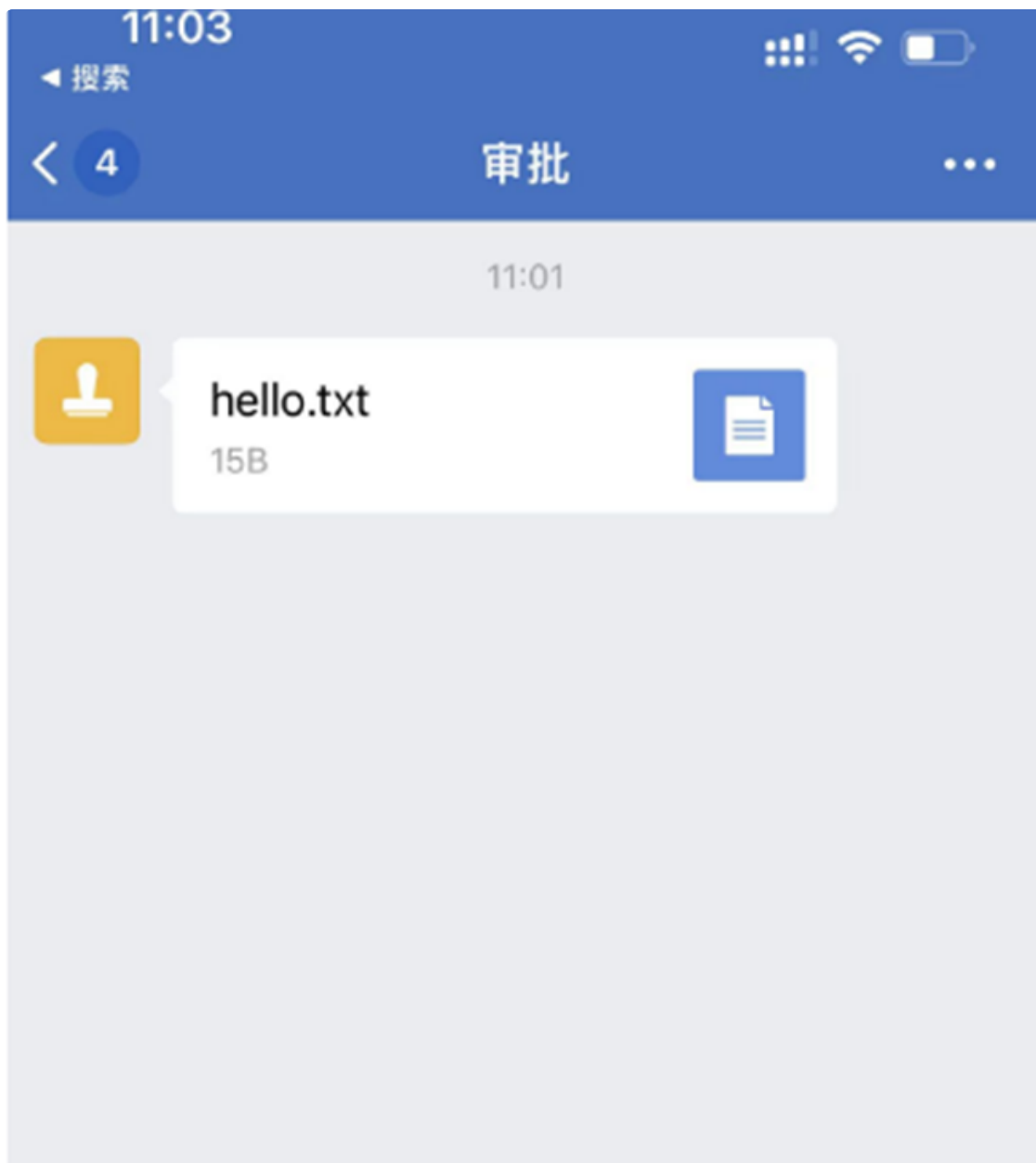
下载文件



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)



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[REDACTED]
hare_api_mjoin&qsize=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
3. 后利用模式
```



钉钉

ak特性

开头为ding

使用方法

运行exe 逐步操作


```
1  请选择一个应用：
2  1. WeChat
3  2. DingDing
4  3. FeiShu
5  4. 退出
6  2
7  请输入appKey: xxxx
8  请输入appSecret: xxx
9  Access Token: xxxx
10 请选择一个操作：
11 1. 获取通讯录
12 2. 邀请进入组织
13 3. 创建企业账号
14 4. 删除企业账号
```

请选择一个应用：

```
1. WeChat
2. DingDing
3. FeiShu
4. 退出
```

2

请输入appKey: ding

请输入appSecret: 4egpr

Access Token: b4d72e4f

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

The image shows a registration form with the following fields and elements:

- Two blurred input fields at the top.
- A label "真实姓名" (Real Name) with a red asterisk and the placeholder text "请输入真实姓名" (Please enter real name).
- A label "+86" with a dropdown arrow and the label "手机号码" (Mobile Number).
- A label "验证码" (Verification Code) with a red asterisk and a blue link "发送验证码" (Send Verification Code).
- A label "申请理由 (选填)" (Application Reason (Optional)) with the placeholder text "请输入申请理由" (Please enter application reason).
- A blue button labeled "提交申请" (Submit Application).

3、添加企业用户(高管模式)

```
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. 文件操作
请输入数字选择操作：3
请输入用户姓名：ccc
请输入手机号码：v
```

(员工UserID: xiaoding)

×

使用专属对外职位

若开启, 将展示专属对外职位

号码隐藏

若开启, 手机在个人资料页隐藏

高管模式

若开启, 手机号对所有员工隐藏

☒ 隐藏电话号码

☒ 屏蔽电话DING

☒ 屏蔽短信DING

☒ 屏蔽应用内DING

☒ 屏蔽视频会议

☒ 屏蔽音频会议

☒ 屏蔽视频通话

☒ 屏蔽语音通话

☐ 屏蔽消息

☒ 屏蔽智能办公电话

允许以下成员联系高管

高管模式

帮助企业管理层实现信息降噪, 减少误扰, 当前仅支持设置3位高管(已配置1/3位), 专业版最高可配置100位, [了解详情](#)

取消

删除

确定

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"}
```

飞书

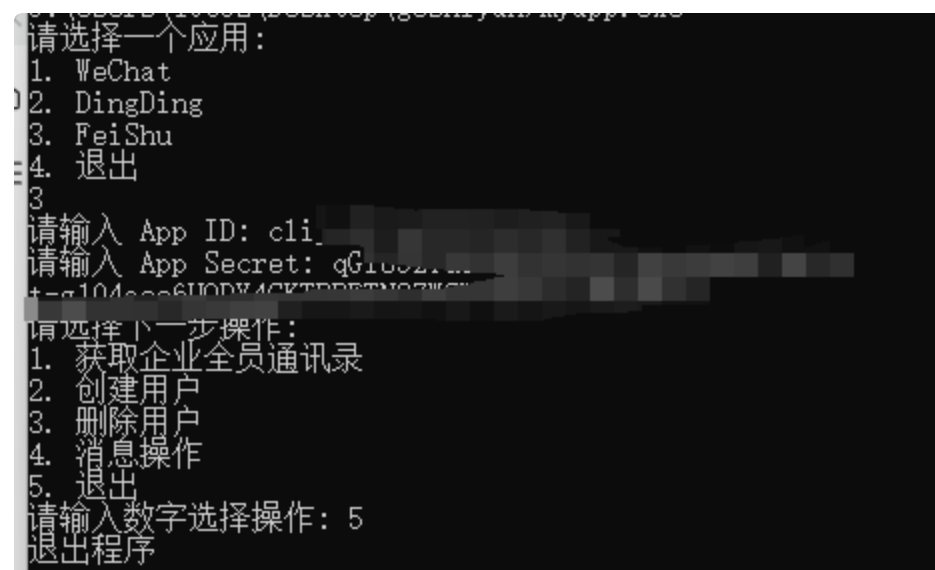
ak特性

开头为cli_

使用方法

▼ Plain Text |

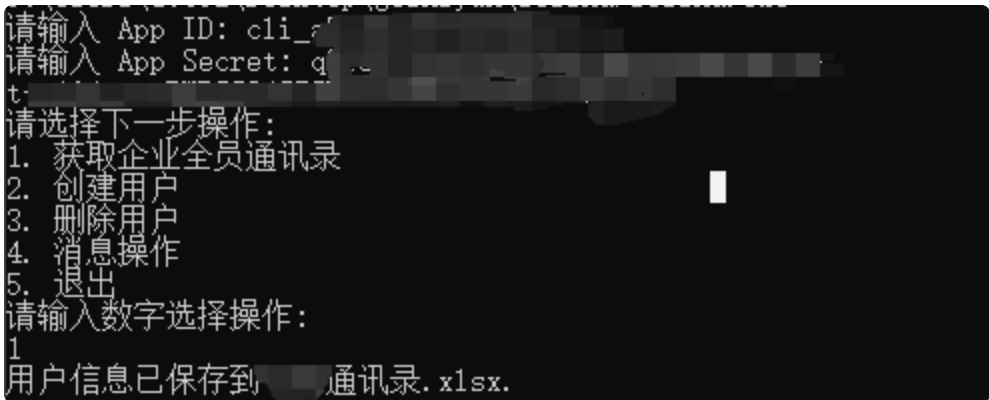
```
1  请选择一个应用：
2  1. WeChat
3  2. DingDing
4  3. FeiShu
5  4. 退出
6  3
7  请输入 App ID: xxxx
8  请输入 App Secret: xxxx
9  请选择下一步操作：
10 1. 获取企业全员通讯录
11 2. 创建用户
12 3. 删除用户
13 4. 消息操作
14 5. 退出
```



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。

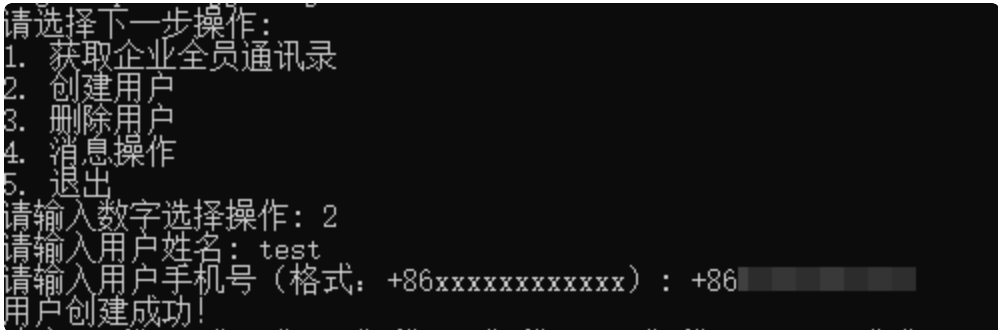
1、通讯录导出



	A	B	C	D	E	F	G	H	I	J	K	L
1	Avatar Origin	City	Departmen	Email	Employee	Mobile	Job Title	Is Tenant	MName	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												
12												

2、创建删除用户

创建用户



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?](https://yqeqcevudux.feishu.cn/invite/choose?token=)
[token=](#)回 TD
退订

点击链接则可加入企业

安

🎉你好, t***

你收到了来自 [REDACTED] 的邀请。加入该企业, [REDACTED] 后高效协作

同意加入

拒绝邀请



2 位同事已加入

删除用户

```
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
请输入数字选择操作: 3
请输入要删除用户的user_id: cc9343cb
用户删除成功.
```

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

```
消息操作相关功能:
1. 上传文件
2. 下载文件
3. 发送消息
4. 退出
请输入数字选择操作:
```

上传文件

```
请输入数字选择操作: 1
执行上传文件操作
请输入文件路径: C:\Users\top\hello.txt
文件上传成功, File Key: file_v2_b50041a9-015ebg
消息操作相关功能:
1. 上传文件
2. 下载文件
3. 发送消息
4. 退出
请输入数字选择操作:
```

给出file key

发送消息

通过file key和user id去发送给指定人员

```
执行发送消息操作
请输入接收消息的用户ID (receive_id): 34k
请输入文件的key (file_key): file_v2_b50041a9-015ebg
消息发送成功!
```



hello.txt

15 Byte