

社工 Demo

仅已知：QQ号为 7*****0

目的：挖掘目标的**隐私四大件**，『手机号』、
『身份证号』、『银行卡号』、『常用密码』

Google

全部 图片 地图 视频 新闻 更多

设置 工具

找到约 124 条结果 (用时 0.21 秒)

767788690 的贴吧 - 百度贴吧
dq.tieba.com/home/main?un=767788690&ie=utf-8&fr=pb
这两天吧里好多人说要放假回来当家教.....感觉好厉害的样子。我为啥一年学下来，发现高中... 2015-06-10. 学弟学妹们，学长来帮忙参报志愿哦~ 中学吧.

简单Google QQ号发现目标贴吧号

通过贴吧信息发现目标姓名，
高中某中学某班，大学某电，爱好
足球、编程、三体...

关注 私信

767788690

用户名: 767788690 | 吧龄: 8年 | 发贴: 2196

他的主页 他的成就

| 贴子

【我为球狂】 ◊真tm郁闷 | 足球社吧 2016-10-08
在我们2:0领先的情况下，我凭一人之力连扳两球2:2平

有人要来西电吗 | 中学吧 2016-06-03
我们叫西非电子科技大学简称西电。我们位于西罗安达市，是第三世界知名大学。特色是...

767788690: 回复 @2015届、晓曦 :啥时把你球拿到我班, 11班, 找罗

2012-9-2 22:56 回复

Google 71...90@qq.com

全部 图片 地图 视频 新闻 更多 设置 工具

找到约 4 条结果 (用时 0.25 秒)

新校区求租一卧室- 房屋租赁区- 西电睿思BBS - 手机版- Powered by Discuz!

rsbbs.xidian.edu.cn/forum.php?mod=viewthread&tid=950073&extra...2

2018年6月26日 - ... 附近卧...。安静无不良嗜好。有床和空调就行。沙发...; 2018-6-26 18:55:39. 联系方式: qq:7...0

新校区求租房- 房屋租赁- 好网|校园互动生活第一门户|西电考研|西电工 ...

club.xdnice.com 版块: 『二手 | 租房』, 房屋租赁 ▾

2018年6月26日 - 1 个帖子

出租方式: 床位-非中介. 所在地区: 西电新校...。联系 QQ: QQ 7...0. 电话: 15...30 ...

新校区求租房 [复制链接]

发表在 2018-6-26 18:02:49 只看楼主 阅读模式 ↗ ← →

租金: 650 元/月

配置: 床 空调

出租方式: 床位 -**非中介**

所在地区: 西电新校区及周边

联系人: 罗

具体地址: 西电新校区家属区

联系QQ: 

电话: 15...0

[新校区求租] 新校区求租一卧室 只看楼主

 ID: 14*****21

2018-6-26 18:54:28

男生, 求租新校区附近卧室一间, 7、8两个月, 800元左右。安静无不良嗜好。有床和空调就行

 ID: 14*****21

2018-6-26 18:55:39

联系方式: qq:70...0

电话: 15...30

通过 Google QQ邮箱发现泄露目标手机号, 睿思ID (某电站内BBS) ,
某 IDb*****w, 所在某电新校区, 姓氏罗, 姓名简写, 未知号码14*****21



根据泄露的手机号，利用**支付宝**转账功能发现目标姓名，支付宝ID与睿思ID前半部分吻合，确定此人。



2018西安电子科技大学网络与信息安全学院硕士研究生拟录取名单

school.freekaoyan.com，陕西，西安电子科技大学，西安电子科技大学复试录取 ▾

2018年6月23日 - 2018西安电子科技大学网络与信息安全学院硕士研究生拟录取名单. 本站小编

107018161132899, 罗力, 085211, 计算机技术, 全日制, 非定向.

107018161132899	罗力	083900	网络空间安全	全日制	非定向
107018161132901	罗力	085211	计算机技术	全日制	非定向
107018161132918	杜新月	085211	计算机技术	全日制	非定向

2014陕西省普通高校招生单设本科录取考生名单 - 陕西招生考试信息网

www.sneac.com/htm/2014/pkzx/A10.html ▾

44, 商州区, 1001150425, 罗力, 男, 理工, 611, 西安电子科技大学, 贫困A|电子科学与技术. 45, 商州区, 1001151676, 李玉成, 男, 理工, 507, 西安工程大学, 贫困A| ...

43	商州区	1001150425	姚奕琳	男	理工	563	武汉理工大学	贫困A 矿业类
44	商州区	1001150428	罗力	男	理工	611	西安电子科技大学	贫困A 电子科学与技术
45	商州区	1001151676	李玉成	男	理工	507	西安工程大学	贫困A 电气工程及其自动化

通过 Google 关键字发现目标本科及研究生阶段所在的学院, 专业, 高考所在地, 户籍, 准考证号, 成绩。

A screenshot of a Google search results page. The search bar at the top contains the query "1405010021". Below the search bar, there are several tabs: 全部 (selected), 图片, 地图, 视频, 新闻, and 更多. On the right side of the header are the settings and tools icons. A message below the tabs says "获得 7 条结果 (用时 0.22 秒)".

[XLS] 2017年物理与光电工程学院国家助学金初审名单

spoe.xidian.edu.cn/_.../01AF0CBC8A9732A1F54FE57CF1A_81DEBA7D_91C0.xls... ▾
150, 147, 1405010021, 罗方亮, 6222620810009266194, 二等. 151, 148, 14050180029, 张祎帆,
6222620810009266194, 二等. 152, 149, 14050180030, 王道 ...

[XLS] 物理与光电工程学院2016年度助学金初审公示名单

stp.xidian.edu.cn/upothers/2016-11/20161107/20161107171409_53860.xlsx ▾
2016年11月7日 - 97, 96, 16050310047, 任晋钰, 一等, 357, 1405010021, 罗方亮, 二等. 98, 97,
16050310030, 沈科委, 一等, 358, 14050180029, 张祎帆, 二等.

1	2017年物理与光电工程学院国家助学金推荐名单				
2	序号	学号	姓名	交通银行卡号	等级
3	147	1405010021	罗方亮	6222620810009266190	二等
4					

通过 Google 未知号码发现本科奖学金情况，银行卡号，并确定之前的未知号码为学号。

性别: 男
年龄: 20-29
生日: 1984-08-15
星座: 处女座
现居地: 中国 陕西 西安
婚姻状况: 恋爱中
血型: AB
故乡: 中国 陕西 西安



由于 **QQ空间** 设置为所有人可见，通过QQ号进入，发现目标年龄，生日，血型，有对象，与留言中为ID为婳的人互动频繁，怀疑是其对象【后续发现错误】，本科宿舍靠近操场6xx左室，说说泄露手机号，高中真人照片等。



QQ 资料里泄露163邮箱，学校，所在地。

昵称:罗 

群号:48387643

群名:J 厉鬼...彝族 |



昵称:罗 

群号:56025220

群名:久。9。

介绍:永久。9班。



昵称:风骑士

群号:66301059

群名:永不言败的六班

介绍:2008年11月23号建立此群。大家要共同团结哦!



昵称:罗 

群号:71417456

群名:初三九班

介绍:。。



昵称:罗 

群号:86975998

群名:□.

介绍:只有城中现初三9班进，其他人进死定了



昵称:罗 

群号:94858710

群名:豆子三号



21:56

通过 **QQ群** 历史关系，可查询
到目标小学、初中同学的联系方式。

小声bb: TG @shegongkubot



通过手机号或者QQ号可添加目标微信号，以某电某院直系学弟有事情请教为由通过好友，通过朋友圈可挖掘目标生活画像。

超过4000万人正在使用

Fox76***90 ♂

他还没有填写个人简介

+关注 私信

他的主页 他的相册

43 关注 1 粉丝 1 微博

★ Lv1

⑨ 陕西

⌚ 标签 体育

查看更多 >

微关系

他的关注(43)

河北华... 木热合... 张呈栋 郑大世

查看更多 >

通过微博搜索QQ发现可疑用户，关注了众多国足球员，但并未泄露敏感信息，后来证实是目标小号。

微博高级搜索

关键词: 西安电子科技大学 足球

类型: 全部 热门 原创 关注人 认证用户 媒体 观点

包含: 全部 含图片 含视频 含音乐 含短链

时间: 请选择日期 选择时间 至 请选择日期 选择时间

地点: 陕西 西安

搜索微博 取消

bay show
8月4日 12:21 来自 荣耀V10 我AI的快
#西安电 #电子科技大学 #足球 #国足 #国足去哪了，那人和人思想分离是假的明明白白的我
9

▲ 收起 | Q 查看大图 | C 向左旋转 | C 向右旋转

收藏 | 转发 | 11 | 5

bay show
是时候请我们西非电子科技大学的足球队去开黑了@西安电子科技大学

@新浪体育 V
【中国大学生队0-21不敌德国高中队】中国青少年国际足球锦标赛19岁组总决赛第二轮，四支中国球队均大比分告负，其中，人大九五0-21负于德国柏林网足球队，华中科大0-10负于韩国青丘高中，西南交大0-11负于韩国宝仁高中，华北电力1:10负于巴基斯坦伊斯兰堡足协队。详情：♂青年比赛-大学生遭高中队狂屠

青年比赛-大学生遭高中队狂屠
近日，兴业银行中国青少年国际足球锦标赛19岁组总决赛展开第二轮角逐，四支中国球队均大比分告负

12岁组总决赛

2016年10月28日 21:56 来自 微博 weibo.com 转发 5566 | 评论 6420 | 5928

2016年10月29日 20:27 来自 华为麦芒4

收藏 | 转发 | 评论 |

通过微博精准搜索“某电 足 球”关键字，结合某ID发现常用微博号，泄露教育信息，生日，研究生宿舍，女友ID及其众多舍友ID，华为Offer、某公司实习等。

他的粉丝 75



好涵

关注 102 | 粉丝 52 | 微博 8

地址 陕西 西安

简介 好涵的温柔小仙女

通过 [微博搜索](#) 关注

+ 关注



好涵

关注 102 | 粉丝 52 | 微博 8

地址 陕西 西安

简介 好涵的温柔小仙女

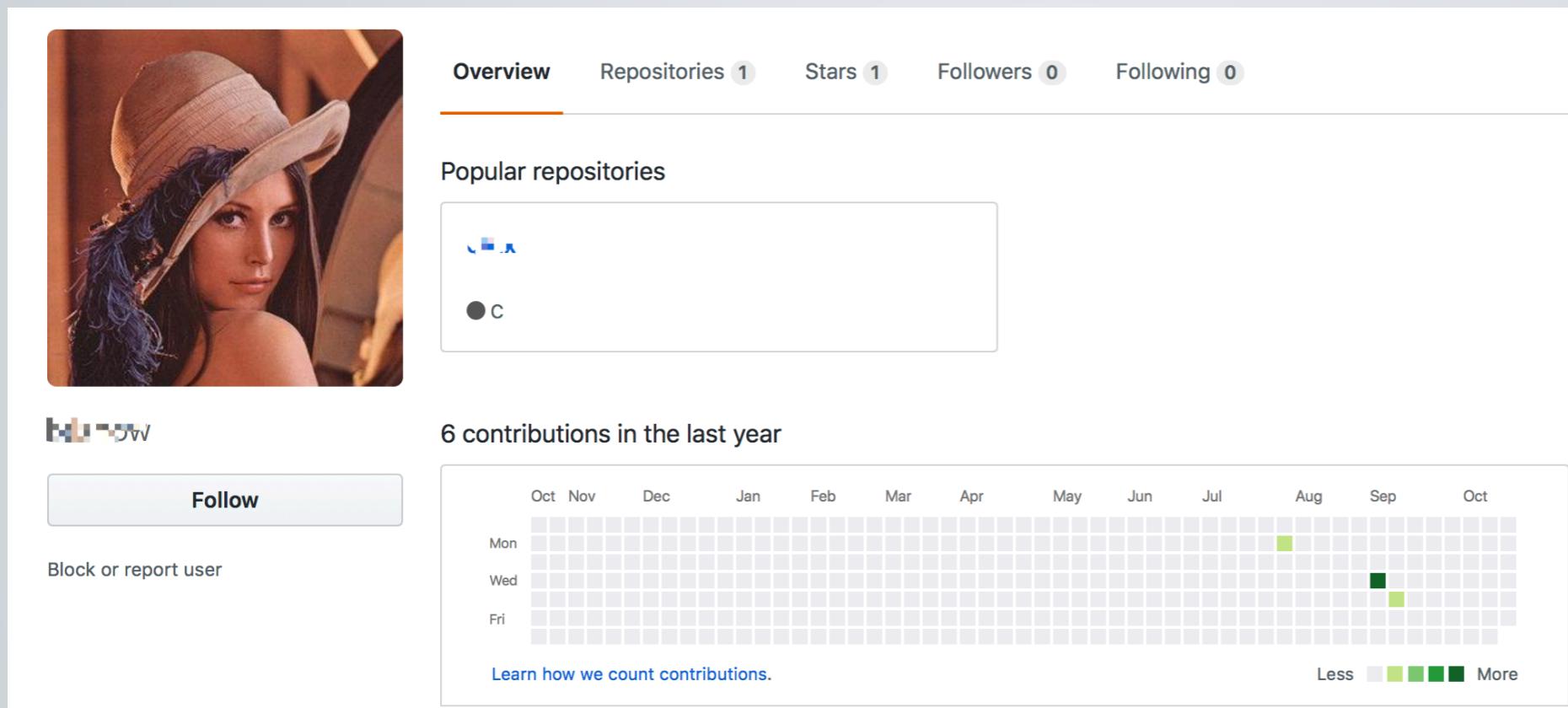
通过 [荣耀V10 我AI的快](#) 关注

+ 关注



通过微博发现既是粉丝又是关注的没有几人，同时粉丝多为僵尸粉，结合空间首条说说点赞中某人头像及QQ的ID，确定其女友微博ID，通过空间留言，得到女友真实姓名，屈某某。

**Github并未泄
露隐私，仅在项目
中提及研究生学校
及学院名。**



The screenshot shows a GitHub user profile for a user named 'h3nry'. The profile picture is a woman wearing a hat. The top navigation bar includes 'Overview' (which is underlined in orange), 'Repositories 1', 'Stars 1', 'Followers 0', and 'Following 0'. Below this, there's a section titled 'Popular repositories' which is currently empty. A 'Follow' button is visible. The main feature is a 'Contributions' heatmap for the last year, showing activity levels from 'Less' (light gray) to 'More' (dark green). The heatmap shows contributions in August and September.

Popular repositories

Follow

Block or report user

6 contributions in the last year

	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct
Mon											■		
Wed												■	■
Fri													

Learn how we count contributions.

Less ■ More ■

REG007

你注册过哪些网站？

地址：<https://www.reg007.com>

使用7*****0@qq.com注册过【中国知网】、【极客学院】

使用1*****0注册过【当当】、【CSDN】、【360】、【途牛】、【新浪微博】、
【新东方在线】、【学信网】、【3DMGAME】、【酷学网】、【智课】、【永乐票务】、
【布丁酒店】、【智联】、【千图网】、【中国人寿】、【极客学院】、【驾考宝典】、
【Mtime时光网】

通过搜集到的目标信息，利用密码生成器生成强针对性的密码字典，结合上述服务可继续深入。

以姓名、出生地为关键字搜索，发现其女友的相关信息。

大学2016年高校 候选考生名单

报名号	姓名	性别	生源省市	学籍所在中学名称	当前户籍	初审结论	入选专业范围及招生计划
1610561	王	男	陕西	宁	陕西省安	村委会	合格
1610566	屈	女	陕西	陕	陕西省商	村委会	合格
1610715	陈	男	陕西	汉滨	陕西省安	村委会	合格
1610828	张	男	陕西	宁	陕西省安康	平村委会	合格
1610848	王	女	陕西		陕西省宝	村委会	合格

到此为止吧...



等等，还有更骚的操作？！

《火绒溯源报告：“微信支付”勒索病毒》

病毒代码中的github链接 (https://raw.githubusercontent.com/qq*6/ja*et/master/upload/update_cfg.txt)

病毒作者的github主页 (https://github.com/qq*6/ja*et)

发现了病毒作者的提交记录

```
commit a62282ddde9fef7709ed2dfa2585a7d66d84bff4
Author: 罗 <16@qq.com>
Date: Tue Nov 27 03:02:06 2018 +0800

...
commit 1d1889a4a0ceb7554982d7a924ebe23200da94
Author: id19960417 <16@qq.com>
Date: Fri Mar 23 08:16:29 2018 +0800
```

在提交记录中，我们切换到“d1889a4a0ceb7554982d7a924ecebe23200da94”提交记录中，我们发现在本次提交中有一个名为“new 1 – 副本.txt”的BMP图片文件。

The screenshot shows the Microsoft Visual Studio interface with the following details:

- Title Bar:** cheat - Microsoft Visual Studio (管理员)
- Menu Bar:** 文件(F) 编辑(E) 视图(V) 项目(P) 生成(G) 调试(D) 工具(T) 测试(S) 分析(A) 窗口(W) 帮助(H)
- Toolbars:** Standard, Debugging
- Status Bar:** 行 8 列 17 字符 14 Ins
- Solution Explorer:** 显示了项目结构，包括 KeyboardJK, Server, Upload, 和 myLib。KeyboardJK 包含头文件 ClassKeyboardJK.h, ErrorCode.h, stdafx.h, targetver.h，源文件 dlmain.cpp, stdafx.cpp, 监听键盘.cpp，以及资源文件。Server 包含头文件，源文件源.cpp，以及资源文件。Upload 包含头文件，源文件。myLib 包含头文件。
- Task List:** 显示生成成功。
- Output Window:** 显示输出来源(S): 生成。
- Code Editor:** 正在编辑 Upload.cpp 文件，内容如下：

```
4 void start()
5 {
6     ClassEdll ce;
7     ce.screenCapture("C:\\\\Users\\\\newUser\\\\Desktop\\\\new 1 - 副本.txt");
8     sc("rtert");
9 }
10
11
12
13
14
15 int WINAPI WinMain( HINSTANCE hInstance,      HINSTANCE hPrevInstance,      PSTR
16 szCmdLine,int iCmdShow) {
17     start();
18     return 1;
19 }
```

The code in the editor highlights the line `ce.screenCapture("C:\\\\Users\\\\newUser\\\\Desktop\\\\new 1 - 副本.txt");` with a red box.

The screenshot shows a Baidu Zhihao profile page. At the top, there's a green header bar with the Baidu logo and navigation links. Below the header is a circular badge with the number '9' in the center, surrounded by metrics: '587 点赞数' (Likes), '影响力 9' (Influence 9), '回答数 461' (Answers 461), and '帮助的人 43.7万' (Helped people 43.7万). A cartoon character icon is in the center of the badge, labeled 'LV5'. To the right of the badge is a '私信' (Private Message) button. Below the badge, the user's name '罗' is displayed, followed by a blurred profile picture and a small 'f' icon. A tagline '生活不止有眼前的苟且，还有诗和远方' (Life is not just about眼前的苟且, there are poems and distant places) is shown. Below the tagline are three interest tags: '读书达人' (Reading Guru), '电视剧' (TV Drama), and '数码达人' (Digital Guru). The main content area has two tabs: 'TA的回答' (TA's Answers) and 'TA的文章' (TA's Articles). The 'TA的回答' tab is selected. It lists several recent answers with their details:

- 科技再发展几百年，啥病毒不小心走漏，别说中国祖宗也找不到
问：中华人民共和国会不会灭亡?
答：3 2013-07-04 译
会:不用多长时间；须:一定 田舍翁:种田的农民 翻译: 不用多长时间我一定杀死这个乡巴佬 ... 已采纳
- 问：会须杀此田舍翁的翻译
答：2 2006-12-16
油脸呗，99%都长
- 问：为什么会生米疮
答：1 2014-09-21
百度搜索 "lsy资源助手"
- 问：谁有九层妖塔下载地址嘛。谢谢
答：0 2015-11-11

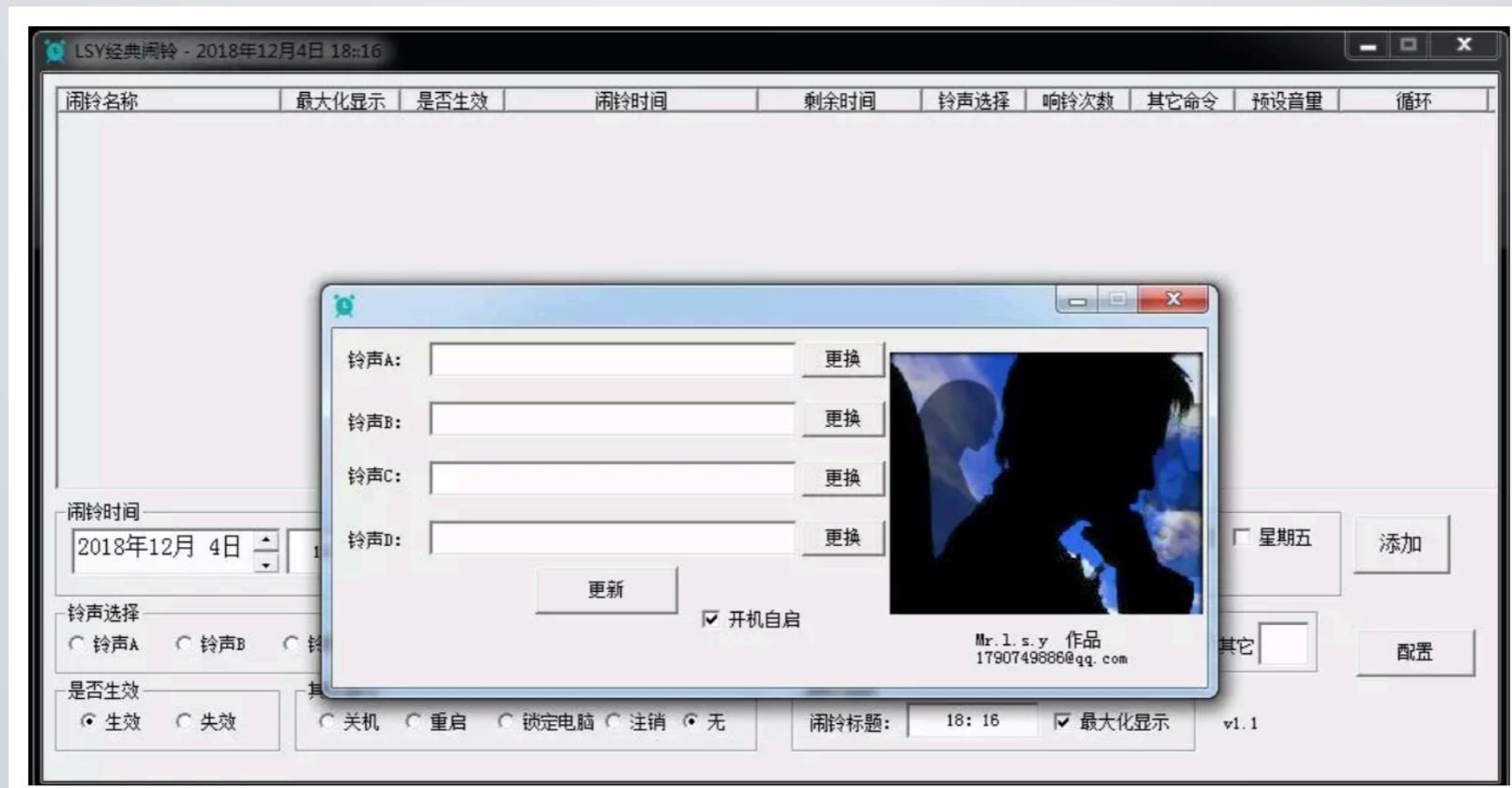
On the right side of the main content area, there are two sections: 'TA的关注(0)' (Followed by 0) which says '暂时没有关注' (Temporarily no follow) and 'TA的粉丝(1)' (Followers 1) which shows a small profile picture and a '更多' (More) link.

在任务栏中红框所示项目，可以看到病毒相关的一些工程正在被编辑，并得到一个疑似病毒作者的姓名，通过该姓名我们找到了相应的**百度知道首页** (http://zhidao.baidu.com/question/11*0859)

该百度知道页面中，找到了两款与该作者相关的软件：“lsy资源助手”和”LSY经典闹铃v1.1”，这两个软件包含有作者的QQ信息和作者姓名的缩写（Mr.l.s.y）。

“LSY经典闹铃v1.1”由于未知原因无法运行，“LSY经典闹铃v1.1”相关数据信息

[ANSI] 0x001912e0: 推广方式: 论坛, 天涯, 贴吧, 空间日志, 博客 (需要生效1天时间)
[ANSI] 0x00191341: 分组框2
[ANSI] 0x00191407: 编辑框7
[ANSI] 0x001914be: 1Fixedsys
[ANSI] 0x001914e3: 如: 宝贝链接失效你可以直接付款到270790749886@qq.com支付宝账号
[ANSI] 0x00191520: 请在付款说明填写: 资源助手购买: +你邮箱 (通过邮箱把账号发给你)
[ANSI] 0x00191561: 或其它联系也可以。6元一月, 12元两月以此类推10分钟内没收到账号
[ANSI] 0x001915a0: 请联系旺旺: lsy_1996或qq:1790749886请注上支付宝交易号



可以看到**阿里旺旺**账号名
I*****6，其中lsy刚好符合
“罗**“的汉语拼音缩写。通过我们搜索阿里旺旺用户名，我们找到相关用户信息，发现该账户确实与
2***@qq.com**相关QQ号存在联系。



通过病毒样本，可以发现其中一个恶意URL “http://www.my*****.top/adcheatReserved/gx.html”。

通过查询https://whois.icann.org/zh/lookup?name=www.my****.top进行域名反查

ICANN WHOIS

ABOUT WHOIS POLICIES GET INVOLVED WHOIS COMPLAINTS KNOWLEDGE CENTER

my [REDACTED].top Lookup

By submitting any personal data, I agree that any the personal data will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#).

Showing results for: myapplication.top

Original Query: myapplication.top

Contact Information

Registrant Contact Admin Contact Tech Contact

Name: Isy	Name: Isy	Name: Isy
Organization: 罗 [REDACTED]	Organization: Isy	Organization: Isy
Mailing Address: guangdong, maoming guangdong 525025 CN	Mailing Address: guangdong, maoming guangdong 525025 CN	Mailing Address: guangdong, maoming guangdong 525025 CN
Phone: +86.1 [REDACTED] 45	Phone: +86.1 [REDACTED] 45	Phone: +86.1 [REDACTED] 45
Ext:	Ext:	Ext:
Fax: +86.1 [REDACTED] 45	Fax: +86.1 [REDACTED] 45	Fax: +86.1 [REDACTED] 45
Fax Ext:	Fax Ext:	Fax Ext:
Email:1 [REDACTED] 86@qq.com	Email:1 [REDACTED] 86@qq.com	Email:1 [REDACTED] 86@qq.com

Submit a Complaint for WHOIS
[WHOIS Inaccuracy Complaint Form](#)
[WHOIS Service Complaint Form](#)

[WHOIS Compliance FAQs](#)

Registrar

WHOIS Server: Whois.55hl.com
URL: www.55hl.com
Registrar: JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD
IANA ID: 1469
Abuse Contact Email:abuse@55hl.com
Abuse Contact Phone: +86.2586883426x1009

Status

Domain Status:ok https://icann.org/epp#OK

Important Dates

Updated Date: 2018-07-11
Created Date: 2018-06-01
Registry Expiry Date: 2019-06-01

Name Servers

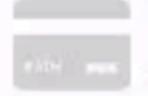
dns3.4cun.com
dns4.51dns.top
f1g1ns2.dnspod.net
f1g1ns1.dnspod.net

在前面溯源中找到的QQ邮箱（1*****86）和手机号（17*****45）同时在上述信息中出现。我们再以“LSY经典闹铃v1.1”软件中出现的另一个QQ邮箱号“29*****@qq.com”作为线索，在支付宝使用“忘记密码”方式获得相关手机号，对比前文中出现的手机号，也有极高的相似度。

支付宝 | 重置登录密码

你正在为账户 **290*@qq.com** 重置登录密码，请选择重置方式：

 经过检测，你在**不常用的环境下**操作，需要进行安全校验

 通过银行卡验证 **推荐**
可使用的任意一张银行卡进行验证 **立即重置**

 通过“验证短信+验证银行卡信息”
如果你的1*****45手机还在正常使用，且记得账户绑定的银行卡号，请选择此方式 **立即重置**

 通过人工服务
填写申请单，上传身份证件图片，我们会在48小时内受理，请耐心等待 **立即重置**

支付宝版权所有 2004-2016 ICP证：浙B2-20100257

综上所述，上述信息均指向
同一个主体，相关信息如
下：

姓名：罗**

QQ号：1*****86

手机号：1*****45

生日：19**年*月*7日



你好骚啊



you B me Greatly recruit
你逼我发大招

除此之外呢？！

';--have i been pwned?
<https://haveibeenpwned.com>

14亿
<http://dumpedlqezarfife.onion>

开房记录等老库
<http://site2.sjk.space>

查看贴吧用户动态与资料
<http://tools.vlan6.com/plugin/tb>

等等...

百度知道隐藏话题查看API
<https://zhidao.baidu.com/mucenter/homepage?entrytime={UID}&un=>

密码生成器
<https://www.itxueke.com/tools/pass>

firefox查询API，据说调用的也是have i been pwned的接口
<https://monitor.firefox.com>

备案信息
<https://www.tianyancha.com>
<http://www.beianbeian.com>

社工中最害怕碰到线索页面404或者500，这时有两种方法：

- 1、利用**搜索引擎**，找到线索页面并查看快照；
- 2、利用**互联网档案** (<https://web.archive.org>)，查看指定网页的历史页面；

聊天结束