看黑客如何轻易入侵大型企业

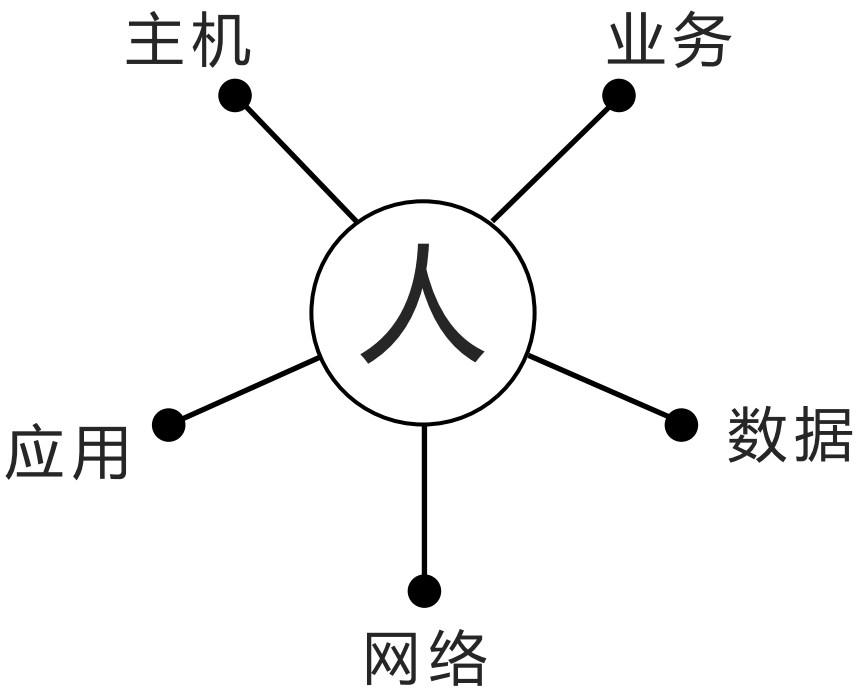
- - SOBUG合伙人　Seay（法师）- -

SOBUG

关于我

- SOBUG技术合伙人
- 《代码审计：企业级web代码安全架构》 作者
- 《Seay源代码安全审计系统》 作者
- 安全博客 cnseay.com 站长

六个安全维度



入侵目标转变为人

- 安全公司越来越多，应用和主机漏洞越来越少
- 大规模数据泄露，对员工发起入侵变得更容易
- 没有专注提供人员安全解决方案的公司

黑客，如何下手？

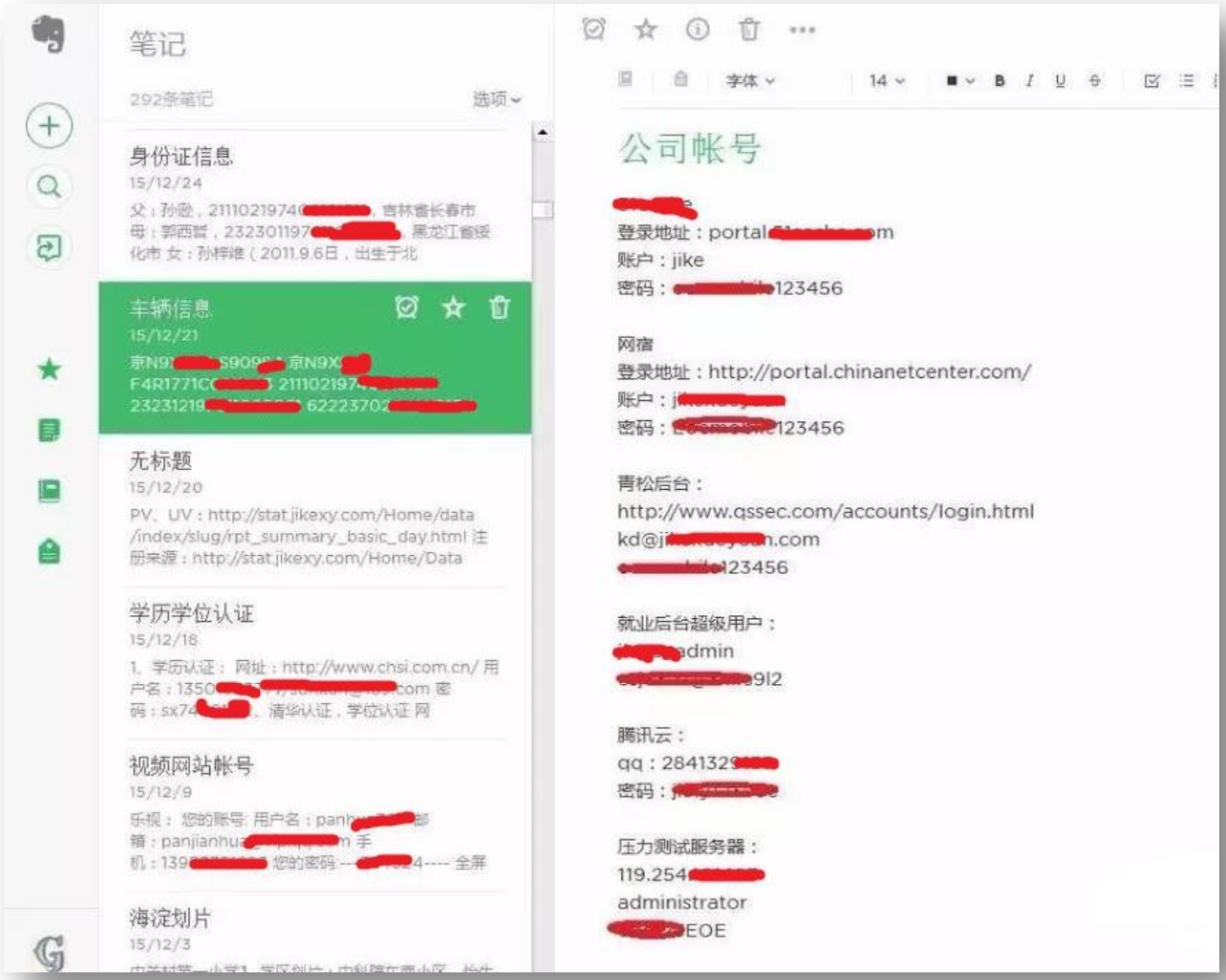
一个视频

BADUSB

云笔记、网盘、代码托管


印象笔记
EVERNOTE
市场部指标
银行会议
明年预算
定Q1目标
企划书


360云盘
PC云盘 新版
扫描并备份照片
帮你保存一生的记忆


笔记
292条笔记
选项
身份证信息
15/12/24
父：孙欲，211102197[redacted]，吉林省长春市
母：郭西贤，232301197[redacted]，黑龙江省绥
化市 女：孙梓维（2011.9.6日，出生于北
车辆信息
15/12/21
京N9[redacted]S909[redacted]京N9X[redacted]
F4R1771C[redacted]3 211102197[redacted]
23231219[redacted]62223702[redacted]
无标题
15/12/20
PV、UV：http://stat.jikexy.com/Home/data
/index/slug/rpt_summary_basic_day.html 注
册来源：http://stat.jikexy.com/Home/Data
学历学位认证
15/12/18
1、学历认证： 网址：http://www.chsi.com.cn/ 用
户名：1350[redacted]com 密
码：sx74[redacted]、清华认证，学位认证 网
视频网站帐号
15/12/9
乐视： 您的账号: 用户名：pan[redacted]邮
箱：panjianhu[redacted]m 手
机：139[redacted] 您的密码：---[redacted]4---- 全屏
海淀划片
15/12/3
字体
14
公司帐号
[redacted]
登录地址：portal[redacted]m
账户：jike
密码：[redacted]123456
网宿
登录地址：http://portal.chinanetcenter.com/
账户：j[redacted]
密码：[redacted]123456
青松后台：
http://www.qssec.com/accounts/login.html
kd@j[redacted].com
[redacted]123456
就业后台超级用户：
j[redacted]admin
[redacted]9l2
腾讯云：
qq：284132[redacted]
密码：j[redacted]
压力测试服务器：
119.254[redacted]
administrator
[redacted]EOE

搞定某云笔记，中国互联网公司指哪打哪

SOBUG

内部OA、邮箱等


登录企业邮箱
邮箱帐号/管理员帐号
请填写企业邮箱的完整帐号，或管理员帐号。
密码
5天内自动登录
登 录
正在使用https方式登录
忘记密码？

怎么搞定密码？

- 全网通用
- 常年不修改
- 个人信息组成

精确查询 ▾ User and Email ▾

seay 查询

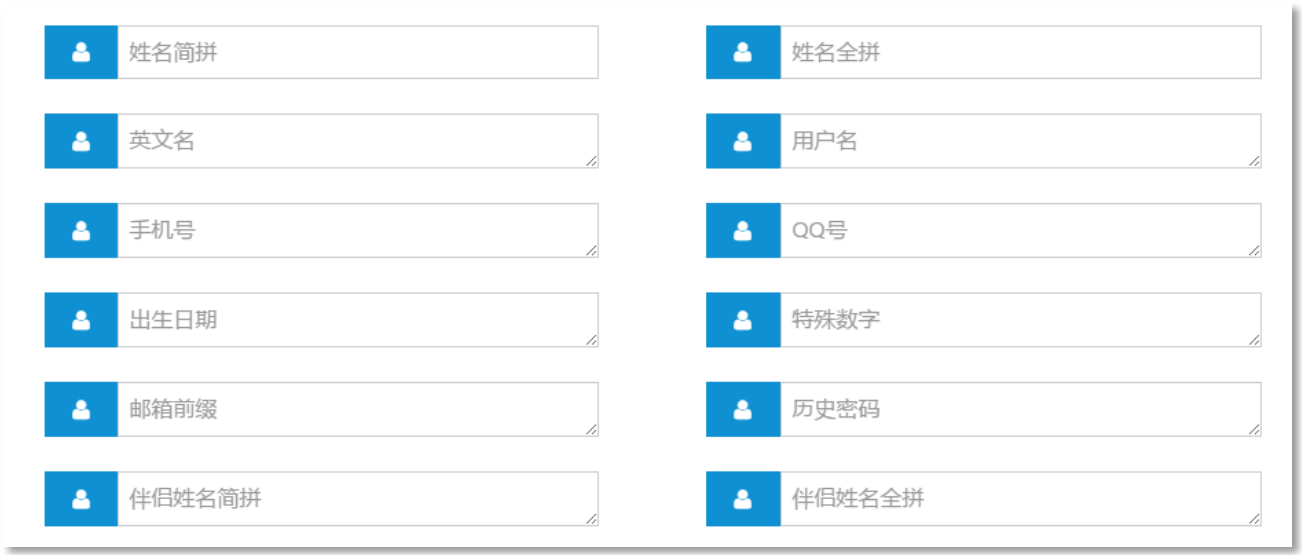
社工库申明：本站不收集任何信息,数据来自互联网,本站旨找回遗忘密码对已泄露密码进行修改,请勿非法使用否则一切后果自负。

查询完毕! 数据量:12条 耗时:10599毫秒

User/Account	mail	password	Source
seay1983	seay	26********(密码泄露)尽快修改密码	undefined
seay	muyi2003cn@yahoo.com.cn	16********(密码泄露)尽快修改密码	undefined
SEAY	1271916490@qq.com	d8********(密码泄露)尽快修改密码	undefined
seay	ls09@263.net	84********(密码泄露)尽快修改密码	undefined
seay		55********(密码泄露)尽快修改密码	undefined
seay	seay@x263.net	32********(密码泄露)尽快修改密码	undefined
seay	seayj@163.com	6e********(密码泄露)尽快修改密码	undefined
seay	miss.gabbana@qq.com	75********(密码泄露)尽快修改密码	undefined
seay	baoleiw@yahoo.com	42********(密码泄露)尽快修改密码	undefined

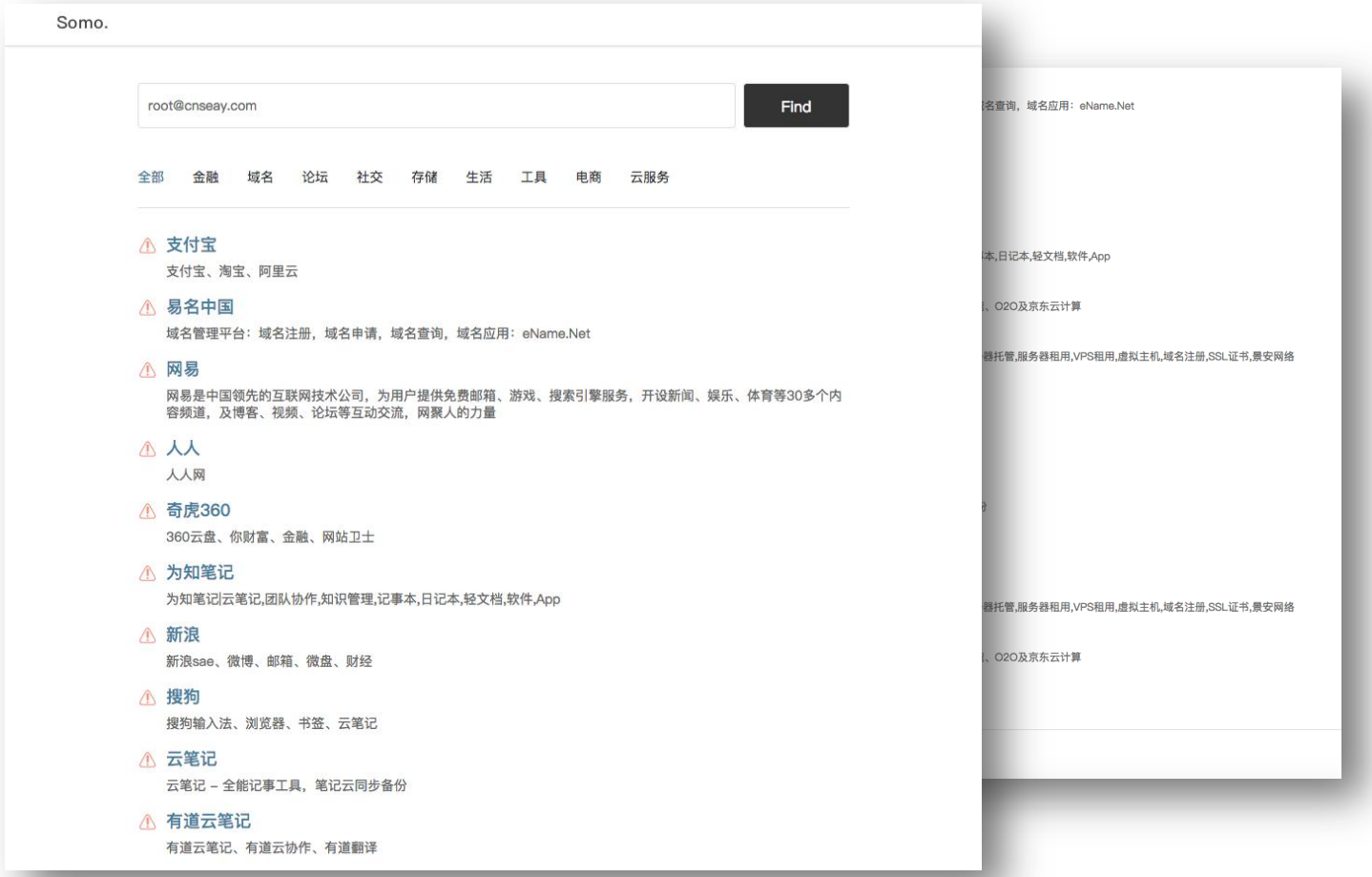
pass.cnseay.com

利用人性的弱点　精准的分析个人密码



SOBUG

Somo.sobug.com 查注册



SOBUG

真中有假 假中有真

- 申请权限
- 重置密码
- 发送木马

答复: 申请vpn
前天 17:58

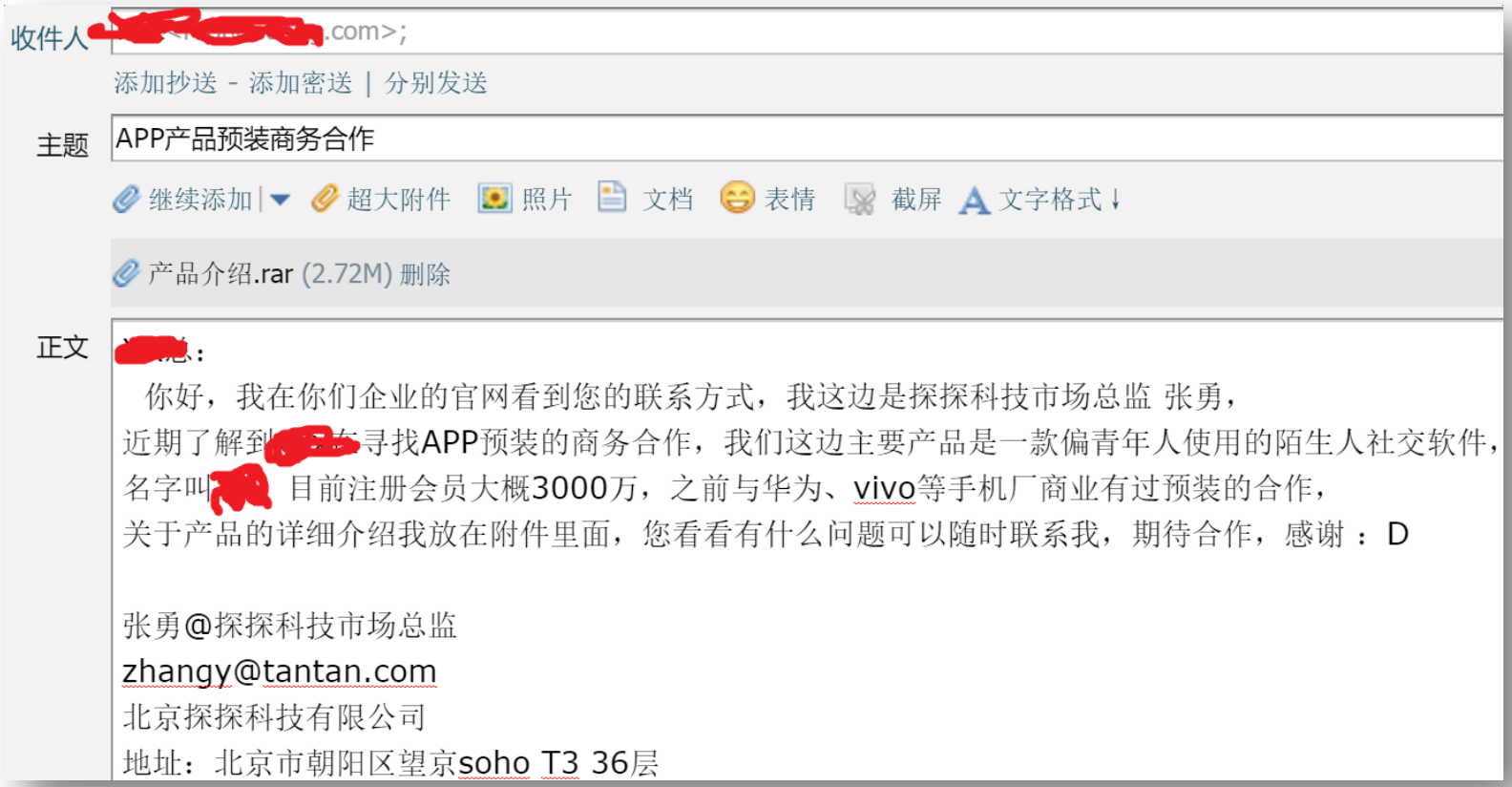
你的vpn已开通，用户名为邮箱前缀。
密码为:[redacted]svpn!@#

设置与登录方
法:http://wiki.[redacted].com/pages/viewpage.action?pageId=2982290
公司内网测试访问https://svpn[redacted].com
非办公网测试访问
https://svpn[redacted].com:4430

-----邮件原件-----
发件人:[redacted]
发送时间: 2016年3月27日 18:58
收件人: g-ops <g-ops@[redacted]>
主题: 申请vpn

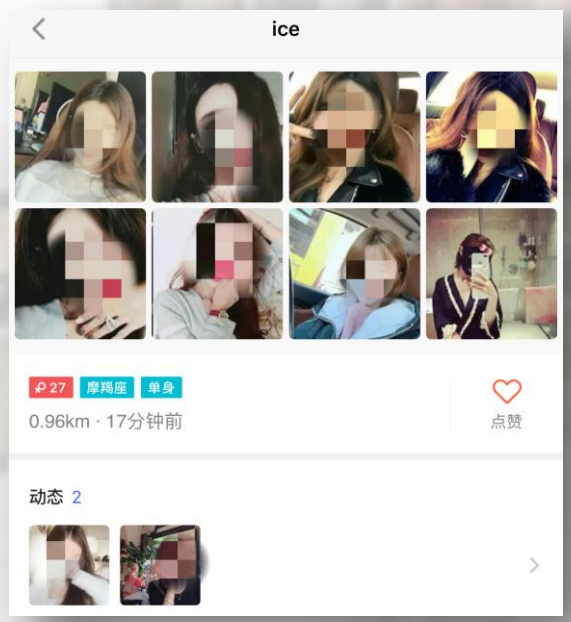
因明天出差去拜访合作伙伴，在合作伙伴面谈的时候需要用到一些数据，同时在外边需要处理公司事

真实案例 入侵某大型企业



附近人也有黑客

入侵某大型企业



上图只是个做“O2O”业务的

Wi-Fi之窃听风云

- 员工私建Wi-Fi
- Wi-Fi 密码特征
- Wi-Fi 钓鱼

More

...

- 手机信号屏蔽+GSM短信嗅探
- 新入职的XX之混入企业内部群
- 朋友圈照片之廉价仿造的工牌
- 开源代码中插入的木马
- ... ...

勾搭专线