

## 第十二章 社会工程学



### 内容提纲

- 1 概述
- 2 社会工程学常用技术
- 3 社工库与社会工程学工具
- 4 防范社会工程学


## 社会工程学

- 人是核心要素
  - IATF核心要素：人、技术和操作，其中人是所有者、核心、安全最危险的



## 社会工程学

- 定义
  - 维基百科：社会工程是操纵他人采取特定行动或者泄露机密信息的行为。它与骗局或欺骗类似，故该词常用于指代欺诈或诈骗，以达到收集信息、欺诈或访问计算机系统的目的。大多数情况下，攻击者与受害者不会面对面接触




## 社会工程学

---

- 定义

- 韦氏词典：“社会(Social)”是指“社区中属于或与生活、福利以及人际关系有关的”，“工程(Engineering)”是指“对物理、化学等纯科学进行实际应用的艺术或科学”，组合起来的意思就是：社会工程学是一门艺术或者科学，它有技巧地诱导人们在生活中的某些方面采取某种行动。




## 社会工程学

---

- 定义

- Hadnagy：社会工程是一种操纵他人采取特定行为的行为，该行为不一定符合“目标人”的最佳利益，其结果包括获取信息、取得访问权或让目标采取特定的行动。




## 社会工程学

---

- 定义

- 更一般的定义：社会工程是一种利用人的弱点（例如人的本能反应、好奇心、信任、贪婪等）进行诸如欺骗、伤害来获取利益的方法，简单地说就是“诱骗”。



## 社会工程学

---

- 定义

- 从网络攻防的角度看：社会工程是操纵他人采取特定行动或者泄露机密信息的行为，该行动不一定符合“目标人”的最佳利益，其结果包括获取信息、取得访问权或让目标采取特定的行动。

# 社会工程学

## ■ 意义

- 在当前网络安全防护技术越来越强，单位或组织越来越重视网络安全防护系统建设的今天，纯技术的网络攻击的难度越来越大，借助社会工程学实施网络渗透攻击成为了一种主流的网络攻击形态。APT攻击过程中，就常常采用社会工程学的方法来实现攻击目的。

# 内容提纲

- 1 概述
- 2 社会工程学常用技术
- 3 社工库与社会工程学工具
- 4 防范社会工程学

## 常用技术

- 社会工程主要是针对人的攻击，因此，攻击者或社会工程师（社会工程学的实施者）必须掌握心理学、人际关系学和行为学等知识和技能，以便收集和掌握实施入侵所需要的相关资料与信息、开展具体的攻击行动，常见形式有伪装、引诱、恐吓、说服、反向社会工程等。

### 一、伪装

- 伪装成管理员或熟悉的人向用户发送信息、打电话，或伪造知名Web站点（钓鱼网站），如银行、政府网站，让用户误以为是真的网站而去访问等，进而达到攻击的目的

## 一、伪装

### ■ 伪装的原则或技巧

- 尽可能了解要伪装的目标
- 加入个人爱好会提高成功率
- 练习方言或表达方式；不要低估打电话的作用
- 伪装越简单，成功率越高
- 伪装必须自然
- 为目标提供合理的结论或下一步工作安排等

## 一、伪装

- 网页仿冒俗称网络钓鱼（Phishing），是社会工程学欺骗原理与网络技术相结合的典型应用。

2018年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面53049个。2014~2018年仿冒我国境内网站的钓鱼页面数量统计情况如图5-12所示，2018年仿冒我国境内网站的钓鱼页面数量月度统计情况如图5-13所示。

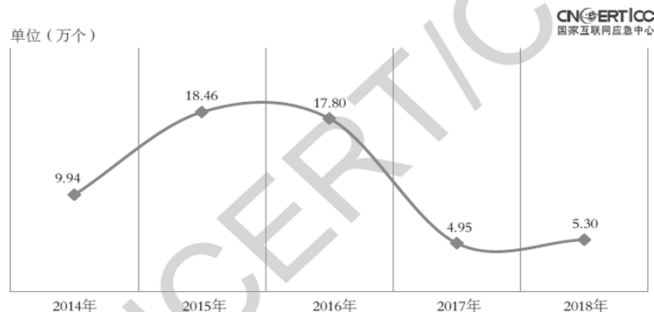


图 5-12 2014~2018 年仿冒我国境内网站的钓鱼页面数量统计（来源：CNCERT/CC）

## 一、伪装

- 伪装网站URL中常见字符伪装字符
  - 字母o与数字0



## 一、伪装

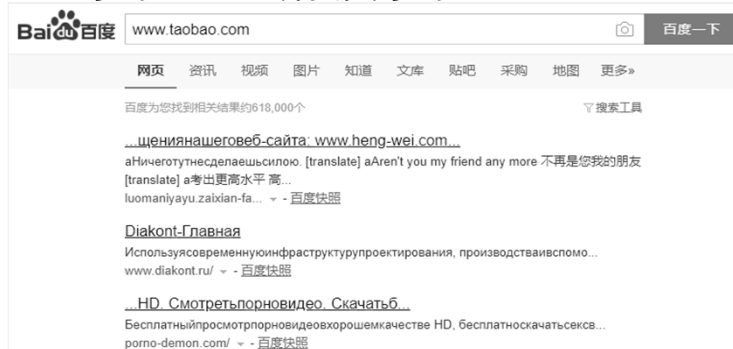
- 伪装网站URL中常见字符伪装字符
  - 将英文字母a (o) 替换为西里尔文 (Cyrillic) 字母a (o) 或俄文字母a (o)





## 一、伪装

- 伪装网站URL中常见字符伪装字符
  - 将英文字母a（o）替换为西里尔文（Cyrillic）字母a（o）或俄文字母a（o）



## 一、伪装

- 伪装网站URL中常见字符伪装字符
  - 将大写英文字母I替换为数字1
  - 将大写Y替换成大写字母V或反过来

## 一、伪装

- 伪装网站URL中常见字符伪装字符
  - 将大写英文字母I替换为数字1
  - 将大写Y替换成大写字母V或反过来
  - 2020非冠疫情期间出现的：用cclc来伪装（美国）疾控中心（center for disease control）的简称cdc，主要用于伪装域名，如用cclc.gov伪装成cdc.gov

## 一、伪装

- 利用同一单词不同形式来迷惑受害者。
  - 2018年，安全研究人员在Python软件库中发现了一个名为“Colourama”的盗窃加密货币的恶意Python软件包，它仿冒的是Python软件库中下载排名前20的软件包“Colorama”。恶意包名称中的“Colour”与被仿冒的Python包名称中的“Color”的意思是一样的，只差一个字母，很具有迷惑性。尽管该恶意Python包上线不久就被发现，但在被发现之前还是有151个用户已经下载了该软件包

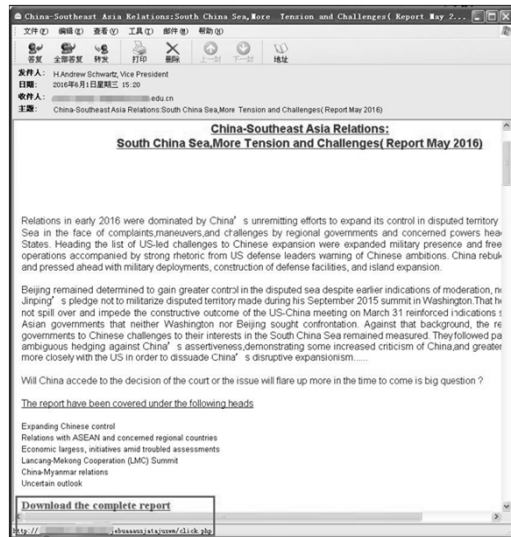
## 二、引诱

- 通过中奖、免费赠送礼品、有诱惑力的资料等内容，引诱用户打开网页、邮件及附件、短信里的网络链接等手段，实现木马的传播，进而控制用户的计算机；通过有奖调查、比赛投票、赠送礼品等手段，要求填写账号、密码、联系方式等信息，来收集用户的个人信息等

## 二、引诱

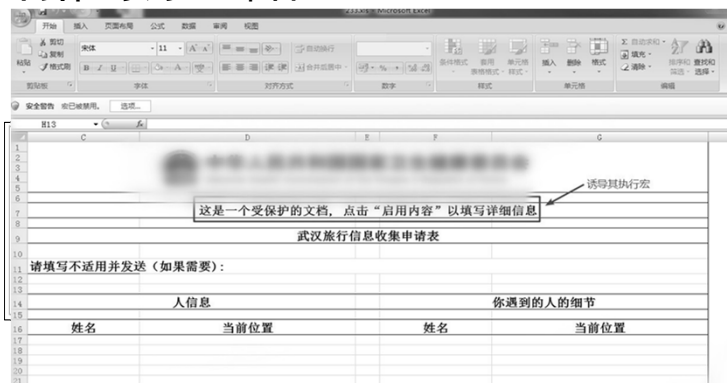
- 大到APT组织，小到社会上一些小黑客、不法分子，大量利用热点事件作为诱饵文档来实施社会工程攻击，如南海问题、中美贸易战、重大流行疾病、重大选举、战争等

## 二、引诱



## 二、引诱

- 2020.2: APT组织利用肺炎疫情相关题材制作的钓鱼邮件



## 二、引诱

- 2020.2：APT组织利用肺炎疫情相关题材制作的钓鱼邮件



## 三、恐吓

- 利用人们对安全、漏洞、病毒、木马、黑客等内容的敏感性，以权威机构或系统管理员的面目出现，散布诸如安全警告、系统风险之类的信息，使用危言耸听的伎俩恐吓欺骗计算机用户，下载安全防护软件、漏洞补丁，或执行系统升级、更改口令等，进而控制用户的计算机或网络应用账户等

### 三、恐吓

- 2016.3.19：希拉里竞选团队主席John Podesta收到的钓鱼邮件



### 三、恐吓

- 假冒网易邮箱管理员的身份给用户发送的安全告警邮件



### 三、恐吓

- 假冒网易邮箱管理员的身份给用户发送的安全告警邮件



### 三、恐吓

- 假冒网易邮箱管理员的身份给用户发送的安全告警邮件



## 四、说服

- 让他人以你所期望的方式去行动、反应、思考或建立信仰的过程，其中包含了情感和信仰等因素，同时需要熟悉心理学知识。要想成功地实现说服的目标，应遵循5项基本原则：目标明确；构建共识；洞悉并融入环境；灵活应变；内省并保持理性，不受自己的情感的影响

## 四、说服

- 安全专家Hadrnagy在《社会工程》一书中给出的“主题乐园”案例

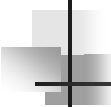


## 五、反向社会工程

- 反向社会工程（Reverse Social Engineering）：攻击者通过技术或者非技术的手段给网络或者计算机应用制造“问题”，使其目标人员深信不疑。然后，诱使工作人员或者网络管理人员透露或者泄漏攻击者需要的信息，甚至执行攻击者希望的攻击操作，如下载带有病毒的文件，重启服务等

## 五、反向社会工程


- 反向社会工程步骤：
  - 破坏 (Sabotage)。对目标系统实施初步攻击并获得基本权限后，留下错误信息，使用户注意到信息，并尝试获得帮助。
  - 推销 (Marketing)。利用推销术，确保用户能够向攻击者求助，比如冒充是系统维护公司，或者在错误信息里留下求助电话号码等。
  - 支持 (Support)。攻击者帮助用户解决系统问题，在用户没有察觉的情况下，进一步获得所需信息或执行想要的操作等



## 案例分析

---

- 案例一：过于自信的CEO



## 案例分析

---

- 案例二：让用户安装木马



## 案例分析

- 案例三：已知某公司一高管的QQ号，要求获得其QQ密码和邮箱密码

## 案例三（续）

- 调研
  - 了解对方的企业文化 公司背景，又注册了一堆目标公司相关行业的一些论坛 调查这家公司
  - 目标公司大概运营了4年之久，有不小的行业知名度
  - 渗透了一家目标同类型公司。目的是挑个简单的先进去找些行业术语，规范文档
  - 试探攻击该公司网站，失败！

## 案例三（续）

### ■ 攻击步骤：

- A. 以投资关系接触目标用户
- B. 利用利益诱惑方式深入了解目标
- C. “竞争”心理社会工程学攻击实施
- D. 后续渗透及资料窃取

## 案例三（续）

- 周二上午10:00 加对方QQ为好友
- E:你好,在论坛看到你发布你们公司一些在做的项目,想了解下,你这会方便么?
- T:你是说哪个项目?你了解什么?
- E:<http://abbs/> 就是这个项目 我想了解下你们的进度,想知道什么时候可以测试产品。
- T:目前已经可以测试了,你是那里的? 做什么的?
- E:能先让我测试下么?
- T:可以测试,不过你要提供你的信息给我。
- E:你是员工? 还是PM? 还是???
- T:PM? 你到底是做什么的?

### 案例三（续）

- E:呵呵, 不好意思 还没自报家门 我的电子名片:  
张\*\* (总经理助理) tel:150XXX333  
河南省\*\*\*\*\*房地产开发集团 email:E@91ri.org
- T:房地产?和我们没什么关系。你怎么对我们项目有兴趣?
- E:集团预计在年底前要扩展三个新的子公司 其中包含\*\*\*\*\*的业务 但是因为一时间无法迅速构建团队, 所以董事会想要以投资方式收购成熟的团队和技术。
- T:大概明白了,不过我这会儿忙,你有什么事跟我助理谈吧.
- E:没关系 等你有空了我再找你详细聊吧 你的名片?
- T: 宋\*\*\*\*\* (PM) tel:13323XX4  
上海\*\*\*\*\*信息科技有限公司email:T@91ri.org

### 案例三（续）

- E:不好意思,我还需要问一个问题,你们公司股份制你是技术入股?
- T:嗯!有问题?
- E:只是先打听下,我们本来是预计以不超过300万收购一个团队,如果你有信心带出你现在的团队并能做好管理 那么你可以脱离你的公司,这样岂不是更好?
- T:这个问题我没考虑过 你还是先测试下产品
- E:怎么测试?
- T:目前只能我们内部测试,你想看看的话我为你演示吧(有钱就能有好的服务,没有白眼,没有我在忙的推延)
- E:现在吗?我这会儿不是很方便,等下有个会,晚上可以吗?(换我摆谱)

### 案例三（续）

- T:几点?
- E:9点可以么? (说晚上9点是想知道他们所谓内部测试是不是真实内部测试,呵呵)
- T:.....那时已经下班了
- E:那你说个时间吧
- T:好吧那就9点吧(看来晚上9点也能演示,那不像是纯内部的测试,或者...VPN?)
- E:嗯 好的 那我先出去了
- T:再见
- 晚上9点20我上网了... 让他等了一会儿 测试他的耐心和脾气呵呵
- T:你好! 来了请联系我
- T:你好! 来了么?
- E:不好意思! 堵车刚到家

### 案例三（续）

- E:怎么看到测试?
- 他发了个QQ远程协助... 简直...太幸运了 呵呵 这样我了解的就更多啦
- 只装了个咖啡防病毒 下面两个网卡3个网卡图标... 比较幸运 (因为很有可能有一个是VPN)
- 看了很多操作演示 然后我就开始...继续
- E:很不错的,这个是你主要开发?
- T:是的
- E:你们负责开发的一共多少人?
- T:大概30人做研发的
- E:你个人有没有考虑过独立出来呢?如果你能带团队一起这样 考虑下吧?
- T:没有考虑过

### 案例三（续）

- E:那如果我明天汇报后有关投资的问题应该联系谁?
- T:这个你要联系市场部的经理也就是我们副总\*\*\*\*
- E:哦 我知道了  
(看来这做技术的的确很专注...不吃荤腥...套不上他...套自己吧)
- E:如果是和你公司谈的话 有点...
- T:怎么?
- E:这笔投资并不小的 你是知道了 如果通过公司对你对我都没有利益嘛...
- T:这个我不懂,你跟他谈就好了.
- E:这样吧 你能不能先侧面帮我打听下看有没有这方面合作的意向 可以吗?
- T:这没问题 明天我问下给你答复 我要下了
- E:嗯 好 明天联系

### 案例三（续）

- 第二天 他告诉我他们那个副总包括老总也很感兴趣...而且他们老总给我来了一个电话 表示说我个人方面的利益可以放心 邀请我去上海.
- 我当然不能过去,不过我也跟他们老总谈了我很感兴趣 非常感兴趣 我们老板也说没问题 下周我们就去上海具体谈判
- 然后下周T就一直催我,我一直推说我这里有点小问题 后来在他们老总也跟我联系问我什么时间过去 我告诉他现在有另外一家和你们做同样产品的公司联系我们 到我们这里做了演示 不过不是我联系的是公司的一个市场部经理牵头的 所以投资的事情暂缓。我并在通话中透漏了我的私欲 “放心吧我不会让那经理得逞的!” 也给了对方老总充分的安慰” 如果有什么动态我会即时的通知你,希望\*总能配合我”

### 案例三（续）

- 两天后的早上，我拨了他老总的电话告诉他 对方公司的演示我已经看到了。告诉他们希望让T能配合一下找找那家公司产品上的不足...这样我有理由说服我的老板，T的老总说没问题，上班就让T联系我。（我绕过了T让他的老总告诉他这样就更可信了,借刀杀人说的就这招吧!）
- 这里我把之前渗透的那家公司的网站根目录放置了一个名为/pdemo.rar的文件包 里面塞了一些文档放了一个demo.exe文件

### 案例三（续）

- 下面的事情...就不用再说了 整个竞争心理社会工程学攻击实施完毕
- 后续的日子里，我告诉T让他给我做一个文档 详细关于两个产品的比较的文档 这样我有充足的时间看他机器上的文件...我截获了邮箱的密码，从邮箱找到了VPN帐户、办公系统帐户，并拿到了VPN后的两台服务器 并安装嗅探工具。到最后,就是几乎所有他们公司服务器。当然还有我想要的一些源代码...



## 案例分析

### ■ 经验教训

- 站在系统或安全管理员的立场上，不要让“人之间的关系”问题介入到你的信息安全链路之中，以至于让你的努力前功尽弃。
- 站在攻击者的立场上，当系统管理员的“工作链”上存放有你所需要的数据时，千万不要让他“摆脱”自身的脆弱环节，要想方设法地利用这个脆弱性环节

## 心理学的重要性

### ■ 杨义先《黑客心理学--社会工程学原理》

“所有信息安全问题，几乎都可以归因于人。具体地说，归因于三类人：破坏者（黑客）、保卫者（红客）和使用者（用户）。当然，这‘三类人’的角色相互交叉，甚至彼此重叠。不过，针对任何具体的网络空间安全事件，他们之间的界限还是非常清晰的！因此，如果把‘三类人’的安全行为搞清了，那么网络安全的威胁也就清楚明白了！而人的行为，包括安全行为，几乎都取决于其‘心理’。在心理学家眼里，‘人’就像一个木偶，而人的‘心理’才是拉动木偶的提线；或者说，‘人’只不过是‘魄’，而‘心理’才是‘魂’。所以，网络空间安全的根本，就隐藏在人的心里。”

## 内容提纲

- 1 概述
- 2 社会工程学常用技术
- 3 社工库与社会工程学工具
- 4 防范社会工程学

## 社工库

- 社会工程攻击所需要的信息称为“社工信息”，这些信息包罗万象，如个人的身份信息（姓名、身份证号、生日、住址、工作单位、联系电话、电子邮箱等），在各个网站上的账号、密码、分享的照片等，信用卡记录、住宿记录、订票记录、通信记录、短信内容、各种社交软件的聊天，网络地址信息、域名信息等。保存这些信息的结构化数据库称为“社会工程数据库（Social Engineering Database）”，简称为“社工库”。

## 社会工程学工具

- 在进行社会工程攻击时，经常需要制作钓鱼网站，制作并发送钓鱼邮件、诱饵文档，伪造短信等，这就需要借助社会工程攻击工具来完成

## 社会工程学工具

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Generator Attack Vector
- 10) Powershell Attack Vectors
- 11) Third Party Modules

99) Return back to the main menu.

set> 1

## 内容提纲

- 1 概述
- 2 社会工程学常用技术
- 3 社工库与社会工程学工具
- 4 防范社会工程学

## 防范社会工程学攻击

- 威瑞森的报告显示，94%的恶意软件通过电子邮件传播，排名第一的社会工程攻击是网络钓鱼

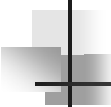
**2019 DBIR (PDF) verizon**

## 防范社会工程学攻击

- 既然社会工程攻击利用的是人的脆弱性，那么防范也要从人入手，主要有两方面工作：一量提高人的安全防范意识，二是加强网络安全管理，用规则来限制人的行为。

## 防范社会工程学攻击


- 防范方法
  - 一、学会识别社会工程攻击



## 防范社会工程学攻击

---

- 防范方法
  - 二、注意保护个人隐私信息

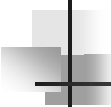


## 防范社会工程学攻击

---


- 防范方法
  - 三、充分认识社会工程人员意图获取的信息的价值





## 防范社会工程学攻击

- 防范方法
  - 四、及时更新、升级软件



## 防范社会工程学攻击

- 防范方法
  - 五、制定规范可行的安全管理规章制度

## 防范社会工程学攻击

- 总之，上述措施的最终目的都是提高人的安全意识，并自觉地、不折不扣地遵守各项网络安全规章制度，不为“情”所动，不为“利”所诱，不惧“恐吓”，只有这样才能有效抵御社会工程学攻击

## 本章小结



# 作业

0