网络信息与安全技术报告

> *学号：1120180207*
>
> *姓名：唐小娟*
>
> *班级：07111801*

一、背景

社会工程学攻击，是一种利用“社会工程学”来实施的网络攻击行为。它利用人的弱点，以顺从你的意愿、满足你的欲望的方式，让你上当的一些方法。它主要有一些经典技术：直接索取、个人冒充、反向社会工程以及邮件利用；还有一些新技术：钓鱼技术、域欺骗技术、非交互技术以及多学科交叉技术。下一部分我将详细介绍一些技术手段，让大家有所防范。

二、技术手段

1. 反社会工程：它迫使目标人员反过来向攻击者求助的手段。采用破坏（对目标系统获取简单权限后，留下错误信息，使用户注意到信息，并尝试获得帮助）——推销（利用推销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）——支持（攻击者帮助用户解决系统问题，在用户不察觉的情况下，并进一步获得所需信息）**【*os：被人卖了还要帮人数钱~~~*】**
2. 邮件利用：采用木马植入在欺骗性信件里加入木马或者病毒；或者群发诱导欺骗接收者将邮件群发给所有朋友和同事。
3. 钓鱼技术：模仿合法站点的非法站点，诱导用户前往伪装站点之后截获受害者输入的个人信息（比如密码之类的）**【*os：好奇害死猫系列~~*】**
4. 域欺骗技术：这是钓鱼技术加DNS缓冲区毒害技术，首先攻击DNS服务器，将合法url解析成攻击者伪造的ip地址；之后在伪造ip地址上利用伪造站点获得用户输入信息。
5. 非交互技术：利用合法手段获得目标人员信息或者利用非法手段在薄弱站点获得安全站点的人员信息。**【*os：这大概就是攻击团伙了吧*】**
6. 多学科交叉技术：利用受害人的心理（比如忽视本地安全、密码设计过于简单）进行攻击。

这里为了让大家社会工程学攻击有所防范并且吸取教训，我开发了一个小游戏，它模拟了当下钓鱼软件的套路：利用人们的好奇或者贪心思想来获得他们想得到的利益。用这样的一个小软件，一方面是体验网络安全攻防过程的快乐，另一方面也是希望提醒大家不要被“天下免费的午餐”所欺骗。

三、开发环境

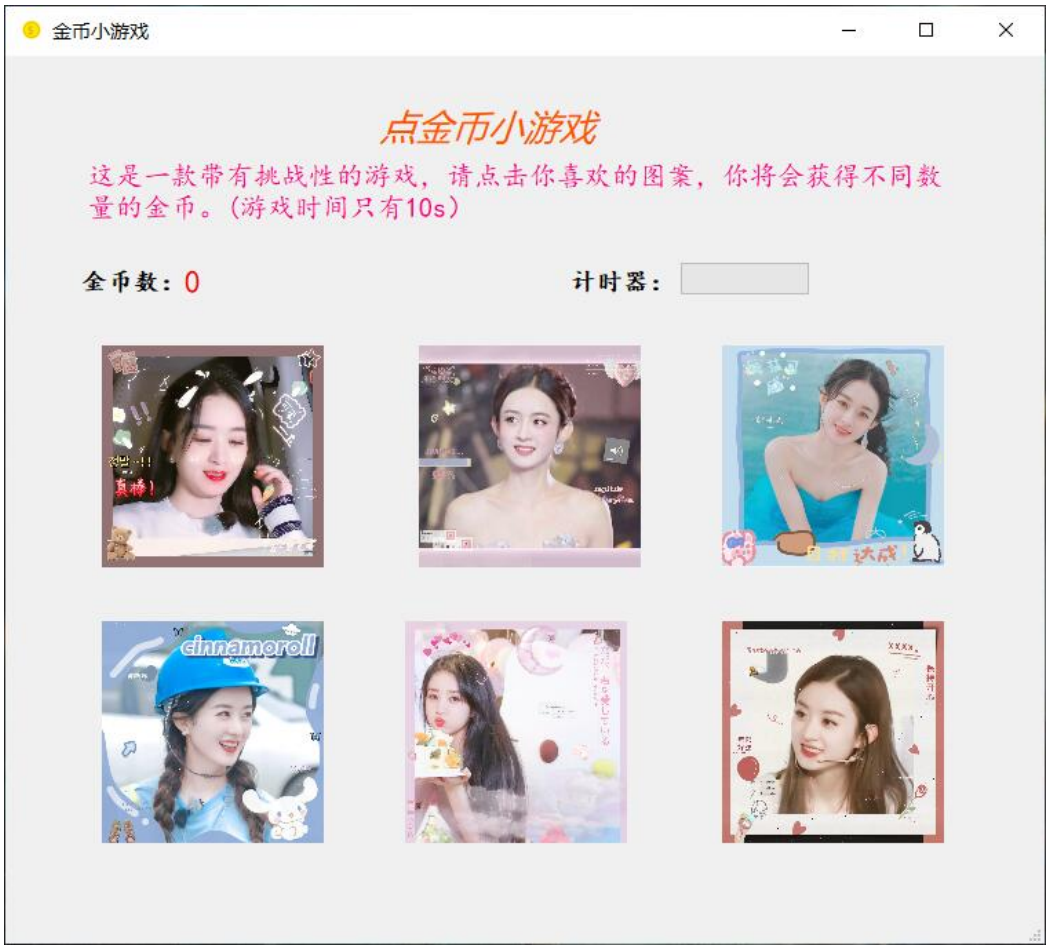
名称	信息
操作系统	Windows 10家庭中文版
界面应用程序开发框架	Qt 4.10
编程语言	Python、C++

名称	信息
软件运行环境	Windows环境

四、技术设计思路

该小程序是一个点击金币游戏，被攻击的后果是不断给你的QQ好友或者TIM好友发送消息。

4.1 界面设计

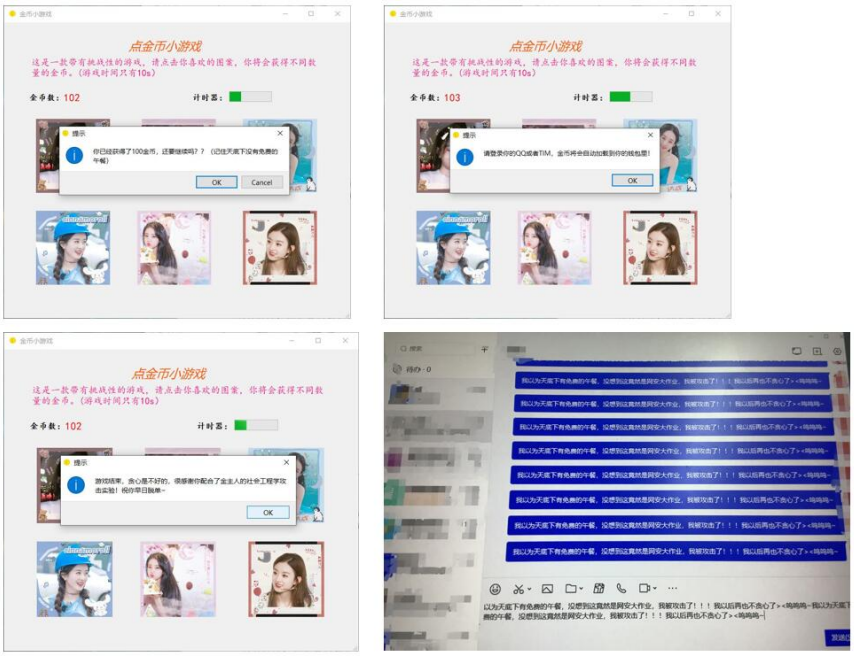


为了完美模拟当下钓鱼网站的逻辑，我采用了钱和美女的要素，使整个软件看起来极具有诱惑力，所以这就是第一关：你是否会对钱和美女太过好奇。如果你对这些不感兴趣，那么你就从苗头上扼杀了被攻击。

4.2 逻辑设计

4.2.1 游戏

简要介绍：打开程序，你会看到如上界面，接下来，你会不断点击图片，当点击数目达到100的时候，你会被弹出提示界面，问你要不要继续。如果点击取消，你就会躲避攻击，否则后台攻击脚本就会开始运行；为了让这个小游戏看起来比较真实，设定时间限制，如果达到时间还没有获得100金币，则不会进行攻击，游戏直接退出。具体见下图：



（由于在实验的时候，我被攻击卡住了，所以只能借用其他设备进行拍照记录）

代码逻辑：

- 在程序开始时，我设置一个定时器，以此计时，并且当时间发生改变的时候，发送信号执行槽函数。槽函数主要是改变进度条的值和判断超时。
- 当点击图片的按钮时，发送点击消息，执行槽函数。槽函数根据随机生成的0-9的金币数加到总金币数上，并且判断总金币数有无达到100，若达到100则给出提示
- 给出提示的时候，如果点击确认，那么后台就会执行我写的exe程序，也就是攻击程序，如果点击取消，那么程序就会退出。
- 为了让用户获得金币数，我会引诱被攻击者登录QQ或者TIM，这样他就会不断发送消息，而难以发送自己想要发送的消息。某种意义上所造成的后果是受到DDos攻击了。

4.2.2 攻击脚本：

简要介绍：主要使用Python脚本写的并且打包成了exe文件。只要被攻击者打开TIM或者QQ，那么程序就会找到该窗口，不断发送消息。

代码逻辑：

- 首先设定发送消息内容，将测试消息复制到剪切板中。
- 不断循环：
    - 得到获得窗口句柄和窗口名称；
    - 根据得到的窗口句柄找到它的进程号
    - 根据进程号得到进程名称
    - 判断进程名称是否是“TIM.exe”或者“QQ.exe”，如果是的话，模拟发送键盘发送消息。

关键代码如下：

```
while True:
        hwnd_title = dict()
```

```
        win32gui.EnumWindows(get_all_hwnd, 0)
        for h, t in hwnd_title.items():
            # 获取窗口句柄
            name = t
            handle = win32gui.FindWindow(None, name)
            thread_id, process_id =
win32process.GetWindowThreadProcessId(h)
            process = psutil.Process(process_id)
            if(process.name()=="TIM.exe"or
process.name()=="QQ.exe"):
                # 填充消息
                win32gui.SendMessage(handle, 770, 0, 0)
                # 回车发送消息
                win32gui.SendMessage(handle,
win32con.WM_KEYDOWN, win32con.VK_RETURN, 0)
```

我的设计技巧：

（1）将程序改成了system名称，被攻击者不容易找到。（当然，如果我随机变换进程名称，那就难度更大）。【这个思路来源于，当时我把程序发给同学实验的时候，他找到了该进程，然后关闭了。那我为了加强我的攻击力度，一是循环的时候我没有设置睡眠，而是随机改变进程名，这样他的防范难度就增大了。】

（2）识别窗口放在循环体内，只要用户打开QQ界面或者TIM界面，那么他就会不断给当前界面的用户发送消息。

4.2.3 打包程序

将python程序用pyinstaller打包成exe程序，同样的用Qt自带的windepolyqt.exe打包Qt框架的程序，最后再用winrar将exe和dll打包成一个exe文件（金币小游戏），这个社会工程学软件就完成了，只要有一台电脑就可以运行，无需配置环境。

五、技术总结

社会工程学攻击的是人类薄弱的心理。在这个小程序中，首先是诱人的界面，再是获得金币后仍然想继续获得（天底下没有免费的午餐），当你以为一切可以毫不费力得到的东西，要么是没有价值的东西，要么是夺走你价值的东西。所以踏踏实实做好自己的事，得自己应该得的，才是为人处世之道（我的一点小见解）。最后我将给出一些防范方法和小tips来防范这些攻击。

六、防范方法

1. 注重保护人格隐私：现在很多社交网站都包含了大量的私人信息，其中邮件地址、手机号都是社工攻击有用的主要信息。因此注册的时候尽量不要使用个人真实信息。（小tips：可以在注册不同网站时候的姓名用该网站名字，比如唐淘宝、唐网易等等，这样如果联系你，你也知道哪个网站泄露了你的信息。）
2. 时刻保持警惕：电子邮件这些很容易被伪造，手机上收到不认识的人发来的短信，包括和自己很熟悉的朋友也要有所警惕，不要轻易相信自己所看到的。
3. 不要随意丢弃生活垃圾：像快递单号、账单这些丢弃的时候没有彻底销毁，如果被不怀好意的人捡到，就会造成个人信息的泄露。

4. 最最重要的一点就是不要过于好奇，不要过于贪心，多读书，多看新闻多看报。记住这两点，你就可以躲避大半的攻击。毕竟社工攻击利用的就是人的薄弱心理和短浅认识和经验。

【代码文件说明：game文件夹存放整个工程的代码；Python里面存放着攻击脚本文件】