第三章

常见漏洞与风险

——移动智能终端的风险

2016-12-22

3.2 移动智能终端的风险

伪基站攻击

WWW欺骗

手机木马攻击

无密码wifi攻击

•2016-12-22

什么是伪基站？

伪基站设备一般由笔记本电脑、主机、发射器和天线等组成，通过短信群发器、短信发信机等相关设备能够搜取以其为中心、一定半径范围内的**手机卡信息**。

伪基站的工作原理是什么？

信号干扰

干扰和屏蔽一定范围内运营商的手机信号,一般可维持10秒左右

发送诈骗信息

用户手机信号被强制连接到伪基站设备上，伪基站乘机发送诈骗信息

改变号码

发送诈骗信息时，能把发送号码显示为任意号码

伪基站的危害？

01 大量的垃圾短信，传播商业广告、不实信息或违法信息

02 使所在区域的无线网络资源紧张并出现网络拥塞现象，影响用户的正常通信

03 诈骗短信诱导用户给出隐私信息，或点击危险链接，造成财产或其他损失

伪基站攻击

WWW欺骗

手机木马攻击

无密码wifi攻击

•2016-12-22

什么是WWW欺骗？

WWW欺骗，又称中间人攻击，其中包括DNS欺骗、HOSTS欺骗等。比如你正在访问的网页，它可能已被黑客篡改过，网页上的信息是虚假的。

案　例

虚假网页

8月12日，家住郑州的张先生发现一封新邮件，来源与淘宝网网址类似，为“ｗｗｗ．ｔａｏｂａｏ-0ｔ．ｃｎ”。新邮件说，张先生中了大奖。张先生打开链接，随即进入一个类似于淘宝网的网站。

他按照网上的“领奖步骤”填写了姓名、银行账号等个人资料，并按照领奖规则，向指定账户汇入1900元税金，“客服人员”又提醒说还需汇入5800元保证金、6800元解冻金……这时，他才发现被骗了。

如何防止WWW欺骗？

01 对于经营性网页，要检查该网站首页有没有红盾工商标志或ICP经营标志。

02 注意网页地址栏的地址信息。如显示有绿色小锁头、有https字样，则相对安全。

03 在域名注册网站上查阅该网站的域名，如果注册人是个人而不是企业则需小心。

……

伪基站攻击

WWW欺骗

手机木马攻击

无密码wifi攻击

•2016-12-22

什么是手机木马？

木马（Trojan），也称木马病毒，是指通过特定的程序（木马程序）来控制另一台移动设备。手机木马即是手机中的木马病毒，它能够**窃取**客户输入的用户名、密码以及手机交易码等信息，并发送远程服务器。

手机木马的危害？

- 访问特定网站，增加流量或通话费用
- 窃取用户通话及短信信息
- 窃取用户键盘输入的敏感信息

此外，它还可以导致用户手机自动关机、死机，手机个人资料被删、自动拨打电话、自动发送短信邮件等。

手机木马传播的途径？

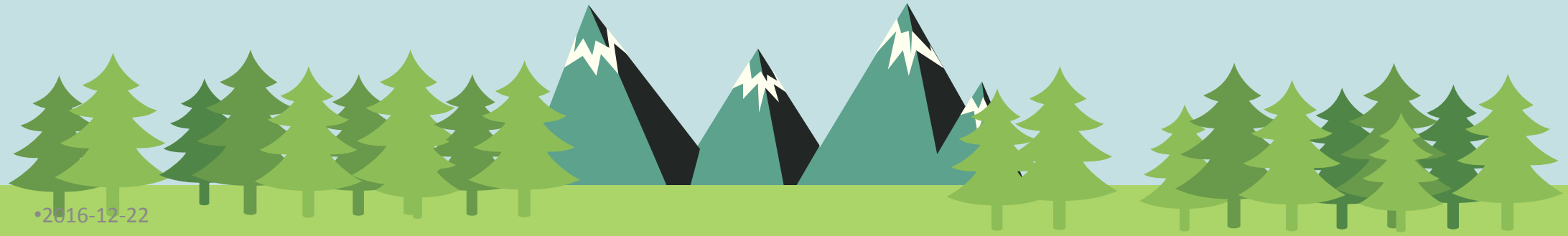
- 通过手机短信等即时通讯工具消息植入
- 山寨App应用捆绑木马植入
- 通过浏览网站、下载铃声等方式进行传播

伪基站攻击

WWW欺骗

手机木马攻击

无密码wifi攻击



什么是无密码WIFI攻击？

手机连接过某些无密码的公共 WiFi 后，攻击者可以通过**监听或截获**信息的方式损害用户的利益。

无密码WIFI攻击的手段有什么？

01 截获各种手机用户名、密码、上网记录、设备信息、聊天记录及邮件内容

02 利用手机的自动连接功能，攻击者伪造比较常见的公共WiFi，欺骗用户登录伪造的同名 WiFi

使用公共WIFI该注意什么？

01 关掉手机、平板电脑等设备无线网络自动连接功能

02 尽量不进行与资金有关的银行转账和支付行为

03 除非情况特殊，谨慎连接无密码WIFI

谢谢观看