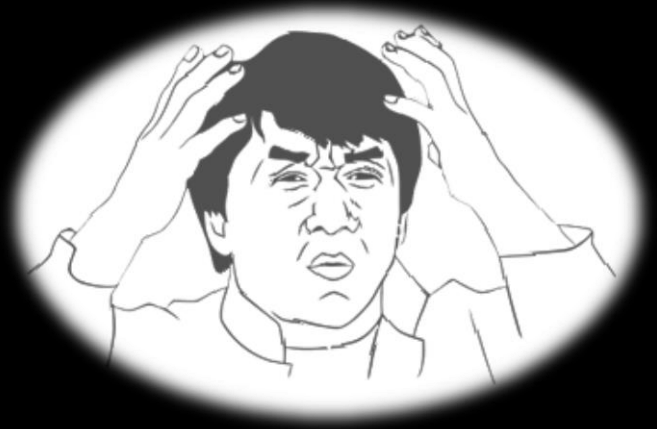

在玩什么呐？
我在烧水。
烧什么水？
智能物联网，用手机APP控制家里的水壶烧水。


哦？你这个水壶里面有没有无线地理记录引擎(wigle.net)方面的配置？
那是什么？没注意过。怎么了？
如果有这个wigle，那么你家的wifi可能存在安全风险。
什么意思？没听明白

简单来说就是你家wifi有漏洞，黑客有办法窃取你的wifi密码。

从电水壶里偷Wifi密码？



那么这窃取密码是怎么做到的呢？
首先我们先要做几个名词解释

WIGLE.NET
All the networks. Found by Everyone.

Wigle.net叫做无线地理记录引擎，它是一个收集全球无线热点信息的网站。可以注册服务，并提交相关的信息热点，如**GPS**坐标、名称、**MAC**地址、加密类型。

1 9wxyz 2abc .com
People, Businesses & Places

192.Com 你可以把它当作英国黄页，他可以列出个人和企业的姓名、地址、年龄、房价，航拍实景照片、公司总监报告、家庭记录等等！

twitter

美国公司推出的国际微博

用户购买产品后在Twitter上谈论他们的智能水壶

用户使用内置WIGLE但配置存在问题。

黑客从推特上找到电水壶主人的帐号

到192.com上通过TW帐号查询用户的位置和IP信息

到wigle.net上获取用户的wifi详细信息

最后一步：设置一个与水壶最先连的网络名称相同且信号更强的热点，让智能水壶强行切换到黑客的热点上来。

然后黑客就可以在你家外面坐着晒太阳，用定向天线指着你的房子，通过你的智能水壶切入内网，发送几个命令让智能水壶向自己泄露明文的WIFI key。

有个问题，这个黑科技貌似现在在中国无法实现吧？况且不远万里来偷我wifi成本也太大了，感觉没什么可担心的。

The Pen Test Partners的研究员Ken Munro，在伦敦某场节目中轻松黑掉这个智能水壶。实验证明了在物联网中配置不当的设备，将对我们造成严重的安全威胁。

当前物联网的安全和隐私问题值得注意，物联网安全是一块很大的蛋糕，你不知道什么时候会有中国wigle.net和192.com，或许你个人的wifi不值一提，那如果遭殃的是企业呢？漏洞还没有被利用并不代表它不是威胁。