对于普通的互联网用户来说，无线路由器是大多数用户在第一次配置后就弃之角落的设备，最多在WiFi卡的时候重启一下。如此一来，无线路由器成为了家中的网络安全隐患。多年没有固件升级导致其存在一堆安全漏洞，容易受到黑客或恶意软件的攻击。路由器对于黑客来说是金矿（图片来源：wired）根据美国消费者协会去年的研究发现，83%的家庭和办公室路由器存在可被攻击者利用的漏洞，甚至包括许多知名品牌的设备。无线路由器一旦受到攻击，路由器可用于执行直接拒绝服务攻击（DDoS），或者黑客可以窃取用户的个人隐私。随着光纤宽带速度的增加，一些用户可能甚至没有注意到他们的路由器被黑客用来访问互联网，甚至用于挖掘虚拟货币。对于家庭用户来说，最大的风险是个人数据被盗。随着我们将越来越多的物联网（IoT）设备连接到我们的路由器，语音助理，智能摄像机等，而风险也随之增加。您连接的安全摄像头可能具有强大的保护功能，但如果您的路由器没有，这样一来导致家中全部的智能家居设备都容易受到攻击。目前最大的问题是，大多数家庭用户并不精通技术。很多人仍然使用默认密码，无论是WiFi网络本身，还是与之相关的管理员帐户。Banco de Brasil骗局是依赖此漏洞的众多攻击之一。在路由器的易用性和安全方面很难进行取舍，设置复杂了用户不会用，设置太简单路由器又不安全。厂商亟需设计一套既安全又简单的设置流程。