热线:96000 E-mail:xdkb@kuaibao.net 现代快报
责编:陈海飞 美编:时芸 组版:孙佩 2014.3.1 星期六

路由器漏洞

路由器也会被“劫持”?昨天,央视的一则报道引起了网友们的热转。报道称,家庭使用的路由器存在安全漏洞,容易被黑客“劫持”,而遭劫后,用户的银行卡号、密码等信息就有可能被黑客获取,进而导致经济损失。看到这里,小伙伴们都惊呆了,怎样避免路由器被劫持呢?专家提醒,勤换口令和密码,时常给路由器进行固件升级,并且注意上网安全,能尽量避免路由器被劫持。

现代快报记者 朱蓓 实习生 薛涵

电脑上弹窗不断蹦出
上网速度越来越慢
刷微博跳出一些游戏广告

你家的路由器可能被黑了

银行账号、支付密码等也会因此泄露;专家提醒:勤换口令和密码

路由器被“劫持” 银行账号、支付密码会被盗

上网时一直有广告弹出,杀毒也解决不了?那么,你家的路由器可能被黑客“劫持”了。昨天,央视的一则报道引起网友们一片惊呼,路由器作为电脑、手机和外界网络的“中间环节”,用户的淘宝账号、银行账号和密码等数据都会从这儿“经过”,一旦路由器被劫持,那岂不是所有信息都有泄露的危险?

电脑弹窗不断跳出、上网速度越来越慢、上微博却跳出一些游戏广告,遇到这种情况要小心了,有可能路由器已经被劫持。厦门的刘先生就遇到了这样的情况,他登录新闻网站,却跳出了非常多的广告窗口,而且关闭的速度都赶不上不断弹出的速度。不仅他自己电脑遭殃,就连家人的手机也出现了类似问题。经检测,原来刘先生家的路由器遭到了黑客的劫持。

路由器为啥会被劫持?央视报道称,一些厂商会给路由器“留后门”,而且一些路由器会存在弱口令漏洞等问题。

路由器销售商 没听过路由器被“劫持”

南京市场上的路由器情况如何?销售人员是否清楚路由器的这些漏洞?昨天,现代快报记者走访了南京珠江路电子市场。

恒基通讯市场的一个业主小付告诉记者,一般家用的无线宽带路由器,大部分会用来打网络游戏,经常出现的问题可能是信号比较弱,还有辐射问题。当被问及路由器被黑客“劫持”和路由器厂家“留后门”等问题时,他则表示并不清楚。

而赛格数码广场二楼的路由器专卖区,销售人员则表示路由器经常出现一个漏洞:路由器将网络分享以后,容易被蹭网,加大了IP地址被修改的可能性,从而导致信息泄露。但对于路由器本身,销售人员说:“没听说过路由器劫持这种事。”

专家释疑

不停跳广告就是路由器被“劫持”?

出现大量的弹窗广告是否就能确认路由器被劫持?南京邮电大学软件学院教授陈丹伟告诉记者,用这种办法来判断路由器是否被劫持并不靠谱。因为一些运营商也会“植入广告”,一些网站也会以合法的方式给用户推送广告。

陈丹伟说,如果连在同一个路由器上的几个电脑、手机设备都出现了类似的情况,应该就能判断为路由器被劫持了。

厂家给路由器“留后门”?

对于厂商主动“留后门”便宜了黑客的说法,陈丹伟认为,厂商应该不会主观上这样做,但是他们的一些接口会被黑客利用。“厂商在开发路由器的时候,会有一些调试接口或维修接口,这主要是为了维护方便,但却有可能被恶意利用。”

路由器为啥能被“劫持”?

“路由器被劫持和用户的上网情况关系不大,主要还是路由器自己存在一些漏洞。”陈丹伟介绍,路由器使用时,如果外网端口的一些应用有问题,黑客就很容易拥有对路由器的管理权限,就能更改路由器的设定。当路由器被劫持后,电脑上网时传出的“数据包”就能被黑客抓走,进而破解出用户的一些账号密码等信息。

怎样避免信息泄露?专家教你五招

1 勤换口令和密码

路由器最常见的一个漏洞是“弱口令”漏洞。路由器的初始口令和密码,大多是“admin”或“123456”等简单字母和数字,很容易被猜到。路由器买回安装设置后,要更换初始口令和密码,并经常更改。

2 上网用安全浏览器

路由器被劫持后,黑客可能会通过钓鱼网站、挂马网站来骗取消费者的银行账号等信息。陈丹伟建议,网友们最好使用一些安全厂商的浏览器,这些厂商一般会对网站、域名、IP地址等进行识别。

3 上网别乱点,特别是广告

“如果乱点链接打开网站,导致主机被劫持,那么黑客要想控制路由器就易如反掌。”陈丹伟说,上网时,一些广告网页和游戏网页不要乱点,特别是带有色情内容的网站,往往有恶意链接。

4 公共场所的WIFI别乱蹭

陈丹伟表示,在一些公共场所,你搜到的无线WIFI未必是真实的,比如一些人使用一台手机就能制作出一个“无线热点”,网友连上之后就有可能泄露个人信息。

5 经常进行固件升级

陈丹伟表示,目前路由器厂商对于路由器的漏洞“补丁”并不会像操作系统的补丁那样定期发布,所以使用者要经常关注所使用的路由器厂家的网站,看到升级公告后要及时升级。

漫画 雷小露

二维码藏毒

你“扫一扫”了吗?如今,黑白相间、形似迷宫的二维码已经深入人们的日常生活。随着智能手机的普及,二维码成为连接线上、线下的一个重要通道。然而,一些犯罪分子利用二维码传播手机病毒和不良信息,甚至是进行诈骗等犯罪活动,严重威胁消费者的财产安全。

据新华社

随手“扫一扫”,支付宝里18万存款没了

二维码使用很方便,但也容易被不法分子利用;专家提醒:扫描之前,请核实来源

“扫一扫”,存款瞬间被盗

近日,浙江嘉兴汪女士在扫二维码时遭遇了陷阱。在淘宝交易过程中,对方发来一个二维码,称必须扫描二维码才能显示商品信息。汪女士没多想,用手机扫了一下,点开链接,可网页一直没有显示出来,再登录支付宝账户时,发现密码已被修改,随后,支付宝、余额宝中的18万元被对方转走。

据办案民警介绍,汪女士扫二维码点开的链接被植入木马病毒,她的手机“中招”后,支付宝密码被对方获取,随后账户被盗刷。

类似的诈骗犯罪不时在各地上演。去年11月,福建一对母女在未核实来源的情况下扫描二维码,半小时内手机银行账户被盗刷200多万元;还有一位何先生也被以同样方法盗走152万元。

公安人员介绍,犯罪分子先将二维码植入病毒程序,编造理由或伪装成商家优惠券等,诱骗受害人扫描,从而获取受害人身份证号、银行账号、手机号码等重要信息,再以短信验证的方式篡改对方密码,将对方账户的资金转走。

二维码藏病毒,外观无法辨认

“只要手机上有微信或二维码识读软件,就能任意读取二维码。”灵动快拍董事长王鹏飞说,二维码在为用户带来便利的同时,也存在信息安全方面的漏洞。

据了解,不法分子在网上下载一款“二维码生成器”(工具软件),再将病毒程序的网址粘贴到二维码生成器上,就可以生成一个二维码,整个过程不超过1分钟。

业内人士指出,相关部门对二维码的监管也是“一片空白”,注册一家二维码企业并不需要专业资质,制作二维码也没有任何规定,发布二维码也没有任何限制,整个行业处在一种自由化状态。

国际关系学院信息科技系副主任王标说,二维码是否藏有病毒,从外观上无法辨别,用户一旦扫了“藏毒”二维码,就会导致隐私泄露、账户被盗刷等。

此外,二维码也成为一些不良信息传播渠道。记者在网上搜索到一条赢取优惠券的二维码,扫描后发现,这个二维码中并无优惠券信息,而是一家色情淫秽网站网址。

提醒

扫一扫前,请核实来源

国际关系学院信息科技系副主任王标建议,在“扫一扫”之前,广大用户应提高警惕,先核实二维码的来源,要选择正规企业、商家发布的二维码,不要扫描来源不明的二维码;同时,用户需要安装手机安全防护软件,及时更新,以降低信息安全风险。“当务之急是出台二维码的使用标准,完善针对移动互联网安全的法律法规。”王标说。