世相扫描

七个儿女难养一个娘

本报记者 **吕文杰** 通讯员 **常丽**

90岁的张老太太怎么也没想到自己含辛茹苦把两个儿子和5个闺女养大，自己老后,儿女们却不赡养她。

无奈之下，张老太太将儿女们告上法庭。而法庭上儿女们的表现更让老人心酸，甚至庭审结束后儿女们连个招呼都不跟老人打，就各顾各地离开了法庭，只留下了老人孤零零的身影。

面对法律，儿女们仍在观望，老人每个月只有110元的生活费，应该如何应对今后的生活？

无奈之举——雇外孙女有偿服务外婆

张老太太祖籍唐河县，早年随丈夫来到南阳市定居，育有5个女儿和两个儿子。其中年龄最大的已经70多岁，最小的也快50岁。

事情要从11年前的一次家庭会议说起。2003年，大儿子和全家人一起开了个会，表示他会赡养父亲，而母亲则由二弟赡养，随后全家人签订了协议，5个女儿也在协议书上签了字，表示同意不继承父母的财产，同时也不承担赡养父母的义务。

就这样风平浪静度过了4年，张老太太的丈夫去世后，大儿子负责给老父亲送了终。这时候二儿子开始不平衡了：凭什么大哥只照顾父亲4年，而母亲身体到现在依然很好，看样子活到90多岁也很轻松。

2013年，二儿子照顾母亲10年后，开始不再照顾老太太，老太太靠着每个月110多元的补贴款艰难度日。最后小女儿看不过去，帮助老太太找了一间出租屋，并每个月出1500元雇佣老太太的外孙女照顾老太太。其间，小女儿不停和几个哥哥、姐姐交涉，但是惹来的却是更深的矛盾，兄弟姐妹之间见面就吵，甚至动手打架。

老太太的小女儿这时候也骑虎难下：照顾老太太，每个月就得承担巨大开支，不照顾的话心里不是滋味。无奈之下,小女儿动员老太太把连同她在内的兄弟姐妹7人全部当做被告告上法庭。

庭审当天——儿女们把老人弃在法庭

4月15日，这起案件在卧龙区法院梅溪法庭开庭。

刚一宣布开庭,老太太的情绪就激动起来，指着对面的儿女们泣不成声，讲述自己早年一个人养活儿女是多么不易,现在儿女们都生活得很好,却对她不管不问。

被告席上的儿女们,在听了老母亲的控诉后,却毫无羞愧之色,个个振振有词。

大儿子说:“我已经按赡养协议给父亲养老送终了,我可以拍着良心说我没有不孝。”

二儿子说：“虽然按照协议母亲归我养，但我已经养了她10年，仁至义尽了，大哥养父亲才养4年，比起来我亏多了，养活母亲大家人人应有份。”

而女儿们也表示：“出嫁女不继承财产也不养父母，当初立有赡养协议，协议上也没要求我们赡养父母。”

其中有一个儿媳妇还指责老太太偏心：“当初照顾长女的小孩好几年，都不去照顾我们的孩子，而且长女承诺要赡养你，现在她怎么不管了?”

当天的庭审现场，几个儿女们又一次吵成一片,最终不欢而散。

离开法庭时，儿女们没有给老太太打声招呼，把老母亲丢在法庭就各自回家了。到了中午12点多，承办法官看实在没有人来接老人回家，便找出案卷材料，按上面的电话一个一个给7个被告打过去，结果不是关机，就是挂断了电话。最终还是跟老太太的外孙女联系后，才把老太太从法庭接走。

判决结果——七个儿女必须尽孝

这起案件的争议焦点回归到了这一纸赡养协议上,已经承担赡养父亲义务的大儿子是否可以不再赡养母亲,女儿们是否可以以放弃继承权为由拒绝赡养母亲。

根据《老年人权益保障法》第17条的规定,家庭中有多个子女的,赡养人对于赡养义务的具体承担方式,可以签订分工协议的方法进行。协议时,应根据“条件好的多负担,条件差的少负担”的原则,共同履行这一义务,但无论条件多差,子女赡养父母的义务是不得免除的。同时法律还规定,协议的内容应当以不损害老人的合法利益为前提,而且所定协议只能在子女间发生效力,签订协议的子女也不得以此对抗对父母的赡养义务。

就本案而言,大儿子虽然已经给父亲养老送终,但是他不得以此为理由拒绝赡养母亲。

另一方面,民间“嫁出去的女儿,泼出去的水”的说法导致许多出嫁女产生了出嫁后便不再承担赡养老人的义务。这种做法与国家法律相违背,出嫁女仍应对年老父母有赡养扶助的法定义务。同时，出嫁女也有继承父母财产的权利,权利和义务不能抵消,不能以未分得娘家财产为由拒绝赡养父母。

综上，卧龙区法院梅溪法庭参考2013年河南省城镇居民人均消费性支出14821.98元，判决每年七个子女各向老太太支付七分之一的赡养费2117.43元。

也许，最终法律能帮老太太讨回公道，可是老太太失去的亲情又在哪里找回？

社会关注

家用路由器拒绝“裸奔”

近日，被称为“网络核弹”的OpenSSL安全漏洞让网民忧心忡忡。人们发现,原来自己的个人网上信息安全如此弱不禁风。而不久之前,国家互联网应急中心公布出的路由器后门事件,也是个人网络安全的一大威胁。不过,与OpenSSL危机个人用户只能束手无策相比,在路由器安全上,用户可以更多地主动防范。

路由器后门引网友担忧

不久前,国家互联网应急中心发布的“2013年我国互联网网络安全态势综述”中,一段关于路由器安全的表述,引爆了关于路由器这个如今家庭中几乎不可或缺的产品的安全性话题。

该报告称,国家信息安全漏洞共享平台（CNVD）分析验证,D-LINK、Cisco、Linksys、Netgear、Tenda等多家厂商的路由器产品存在后门,黑客可由此直接控制路由器,进一步发起域名系统(DNS)劫持、窃取信息、网络钓鱼等攻击,直接威胁用户网上交易和数据存储安全,使得相关产品变成随时可被引爆的安全“地雷”。以D-LINK部分路由器产品为例,攻击者利用后门,可取得路由器的完全控制权,CNVD分析发现,受该后门影响的D-LINK路由器在互联网上对应的IP地址至少有1.2万个,影响大量用户。

厂商留后门为方便调试

软件中所说的“后门”,一般指开发软件的程序员为了某种目的,在软件中保留的不为外人所知的程序。通过后门,可以绕过软件的安全机制直接获得控制权限。一位软件行业人士如此通俗地解释“后门”:就像酒店中每位客人的钥匙打不开其他人的房间,但酒店服务员会有一把万能钥匙,能打开每一个房间以便进行打扫。平时万能钥匙掌握在酒店手中，住店客人的财物是安全的,可一旦万能钥匙被窃贼掌握,那每个住店客人的财物都可能被席卷一空。

“极路由”创始人王楚云表示,一些路由器厂商确实会在产品上留下后门,主要目的是为了更方便地对产品进行调试,并没有什么不良的用意。但他同时承认,“后门”的存在确实让路由器变得更不安全，一旦黑客发现路由器的“后门”所在,就可以实现对路由器的远程控制,用户的隐私也就难保了。

家用路由器有多重风险

有“后门”的路由器有隐患,没“后门”的路由器同样不安全。

王楚云介绍,除了厂家有意识留下的“后门”,还有一类是开发者在写代码时留下的bug,这和“后门”一样都属于系统漏洞，同样可能被黑客发现并利用。事实上,除了路由器之外,任何网络设备,都不可避免地存在或多或少的漏洞。用一句设备商人士的话说,“只有没被生产出来的设备不存在漏洞”。

对于这一类的系统漏洞,解决的方式就是定期进行系统升级,为已经发现的漏洞打上补丁。当然这不是一个一劳永逸的过程,“网络安全就是一个发现漏洞与打补丁交替进行的过程”,360公司副总裁曲晓东说。

没有“后门”,定期升级弥补漏洞的路由器是否就是安全的呢?答案同样遗憾。“黑客们可以通过诱骗用户登录挂木马网站以及直接破解密码等方式来实现对路由器的入侵。”王楚云说。

网络名人、邪红色信息安全组织创始人Evi1m0曾经在网上以讲故事的方式介绍了自己如何一步步破解了隔壁“女神”家的路由器,从而掌握了“女神”大量个人信息的过程。尽管这个过程听起来很有神秘感，但据王楚云介绍,破解路由器并不是一种非常高深的技术,甚至可以说得上是简单,国内能做到这一点的大有人在。Evi1m0本人也表示,他的做法主要是为了引起人们对路由器安全的重视,“真正的高手是不屑于攻击普通家用路由器的”。

弱密码容易成攻击对象

尽管攻击路由器的技术难度并不大,但现实生活中,我们似乎不常遇到路由器被他人控制的情况。

“一来这个过程很多用户自己根本不会察觉,二来这种对路由器的攻击需要和对方处在同一局域网下,很多人的邻居并不是懂这种技术的黑客。”Evi1m0解释道。

360安全专家石晓虹表示,与黑客通过路由器后门或漏洞攻击相比,通过对“弱密码”的攻击,才是路由器面临的最主要威胁。据他介绍,路由器有两个重要的密码,一个是WiFi密码,主要是为了防止他人蹭网,这个密码的重要性很多人都知道;另一个是路由器管理密码,主要是对路由器上网账号、WiFi密码、DNS、联网设备进行管理设置,很多厂商都选择“admin”这样简单的单词作为路由器管理的初始密码,而很多用户并不了解这个密码的重要性,往往对初始密码不做任何改动。

这种“弱密码”路由器连接的电脑,只要访问一个带有攻击代码的恶意网页，路由器DNS就会自动被篡改为黑客指定的DNS,(DNS相当于用户访问网址的“导航仪”),这种情况下,用户电脑会出现上网变慢、正常网站却弹出色情广告等情况,甚至访问网银官方地址也可能实际打开的却是钓鱼网站。

对于这一威胁,路由器大厂腾达就在其官网上发布公告提醒用户“我们强烈建议用户:不使用厂商出厂默认的管理员用户名和密码,一定要对原始用户名和密码进行修改”。

隐私与个人信息被窃取

再回到之前Evi1m0所讲述的案例中,他总结了自己在破解隔壁“女神”路由器之后的收获：获得了女神的照片,劫持了她的微博、微信、人人、QQ、淘宝等所有登录过的账号,通过淘宝又获取了她的手机号……

试想一下，如果用户的这些信息都被人一览无遗,那就意味着他的主要个人信息、与人交往的情况都被他人掌握,更有可能他的微博、微信上会突然出现了完全不是自己发送的内容。

这还不是最严重的。王楚云表示,路由器被非法掌握,最大的危害是访问网页可能被劫持到钓鱼网站上。“当你登录淘宝或者网银时,却被转到了一个虚假网页上，你所填写的个人信息、密码都会被人记录下来,这时可能带来的损失可就大了。”

360曾经发布过的一份报告显示,从黑客攻击者篡改DNS设置的目的上看,49.5%的篡改是为了向用户推送色情网页和游戏广告;28%的篡改是为了将淘宝等电商网站劫持到付费推广页面，从而骗取推广佣金;还有22.5%的其他各类劫持,如将正规网站的访问请求劫持到钓鱼网站或木马网站。

采取安全措施降低风险

再安全的路由器也难以挡住真正的黑客,对于用户来说,采取一些必要的安全措施,还是可以大大提高家用路由器的使用安全性,从而将自己面临的风险降至最低。综合安全专家们的建议,用户在使用路由器时应该注意以下几点：

1.家中WiFi的连接密码要尽可能复杂一些，尽量使用10位以上的密码,最好是大小写字母、数字、特殊符号的组合，这样可以让纯暴力破解变得很困难。

2.修改路由器默认的管理密码,不要再使用“admin”这样的弱密码,同时尽量设置得越复杂越好。

3.WiFi以WPA/WPA2加密认证方式设置密码,并关闭路由器的WPS/QSS功能，以免WiFi被他人蹭网后威胁整个家庭网络的安全。

4. 常登录路由器后台看看有没有接入不认识的设备,有的话过滤掉。

5.及时对路由器的固件进行升级,修复“后门”和漏洞。

6. 移动设备最好不要越狱不要ROOT。

7. 当电脑安装的杀毒软件提示面临攻击劫持时，不要掉以轻心直接忽略。 （据新华网）

大案直击

POS机上的“寄生虫”

本报记者 **张萌萌**

套现成功

2013年12月,周某在郑州市某条街上闲逛,路边不时有人递给他大大小小的广告单和名片。周某无聊地随手翻看着,目光停留在其中一张不显眼的名片上,名片上的内容很简单:能为信用卡提高信用额度并套现。世间竟有这样的“能人”,正急需用钱的周某眼睛一亮,决心去试试。

2014年1月5日，周某带着自己在工行办理的信用卡来到郑州市升龙国际广场，根据名片上的电话号码在广场的其中一个房间找到了“能人”。周某被要求脱掉上衣,并交出手机,两个小时的煎熬等待后,“能人”过来告诉他已经办好了,把周某的信用卡由5万元的信用额度提高到了20万元,并很快从该信用卡里刷出15万元现金,扣除事先说好的“手续费”,周某最后得到10.5万元。没想到这么容易就刷出一大笔钱,周某对“能人”无比佩服,虽然隐约觉得这种行为可能违法,但却顾不上深究,满心欢喜解了自己的燃眉之急。

寻求歪财

这个周某所佩服的“能人”名叫何方(化名),利用一台POS机钻政策和管理的漏洞，通过上街发名片和中间人介绍为持信用卡人套现,先后为13名持卡人刷卡13笔,资金流量1284.32万元,套现167.52万元,造成银行160余万元逾期未还和15余万元损失。他自己却按套现金额的25%~40%收取手续费非法获利,5月6日，宛城区检察院以非法经营罪批准逮捕了何方和另一犯罪嫌疑人李庭(化名)。

何方、李庭都是南阳人,经营着一家科技公司,24岁的李庭是法人代表;33岁的何方是合伙人,负责郑州的业务。年轻的两人一直梦想能不费吹灰之力发大财，但是始终没有得到命运之神的垂青。

2013年冬,何方开始谋划着“走偏门”赚钱,用POS机套现赚取“手续费”。他发现自己经营的POS机刷卡有限额,而且不能及时到账，便想到有业务往来的上海富友支付有限公司的POS机能及时到账,还很可能没有限额。于是他联系李庭,说明自己办理的POS机不能刷预授的信用卡,也就是不能多刷出资金,让李庭帮忙办一台富友公司的POS机。李庭碍于面子,又受到利益的驱使,决定违规为何方办理。

准备就绪

安装POS机,个人安装需要身份证、银行卡、租赁协议等;单位安装需要营业执照、税务登记证和对公银行账户等。李庭不愿以自己的名义办理,让女朋友周某去办。他伪造了一份房屋租赁协议交给周某,让周某以个人名义办理了一台POS机,署名时却按照何方的要求,署名为南阳市某宾馆。

李庭到案时供述,给何方办的这台POS机,他是有利益分成的,这台富友公司的POS机费率为1.25%,也就是说刷卡人刷卡会产生1.25%的手续费,这个手续费中银联拿走20%、发卡行拿走70%、富友拿6%、李庭拿4%。直到案发,李庭从这台POS机获利6000余元。

2013年12月，李庭把周某办好的POS机邮寄给在郑州的何方。何方盘算着如何赚钱,他知道,根据银联规定,信用卡有预授权,可以刷出现金超出卡内存款的15%。比如卡内有存款100万元,通过POS机可以刷出115万元现金。客户拿着信用卡来刷卡时,根据客户的要求,如果卡内存款不足,信用额度比较低,他就想办法通过网银转账往客户卡内注入大量资金，以提高信用卡的信用额度,如此便能刷出更多的现金,既满足了客户信用卡套现的要求,自己又能从中牟取利益。为了找来大量资金,何方还借了高利贷近百万元备用。

疯狂套现

一切工作就绪以后,何方大胆地开始疯狂套现。2013年底,他在郑州大街上大量发送可为信用卡提额和套现的名片，还联系了中介公司为自己“拉生意”,没想到消息一经发出,急着用钱找他的人还真不少。

赵某就是这样稀里糊涂地摊上了。2014年1月5日,赵某听信了在中介公司工作的老乡的传言，在郑州升龙国际广场找到何方，把自己仅有1000元信用额度的信用卡提高到12万元的额度，并当场刷出12万元，其中3.8万元为何方收取的“手续费”,中介公司老乡拿走1万元,赵某实际得到7.2万元。从1月底开始,信用卡所在行的工作人员便多次催促赵某还款,但直到案发,赵某才还了4000元,还有本金11.6万元和利息8000元未还。本文开头提到的周某刷了15万元,到手有10.5万元。但直到案发,周某仅还了银行2200元,至今还有本息20万余元未还。

就这样，仅在今年1月3日至5日三天，何方就先后为13名持卡人用POS机刷卡13笔,套现167万余元。他自己按刷卡金额的25%~40%收取巨额手续费。

案发被捕

就在何方幻想着客户将接踵而来，源源不断的现金将归他所有时,他不知道,如此大的资金流动和刷卡金额已经引起了银行和公安机关的注意。1月6日,富友公司接到公安机关的通知,将何方使用套现的POS机关闭。李庭听说后，马上将这台POS机收回南阳。何方也预感到事情不对,担心纸里包不住火,迅速把位于郑州升龙国际广场的公司搬迁。

然而，天网恢恢疏而不漏，违法的行径露出端倪岂能令其逃脱，2月14日，南阳市公安局经侦支队把此案件线索移交给南阳市公安局仲景派出所，仲景派出所民警通过从郑州、南阳多方调查取证，固定证据，寻找线索，于4月5日将何方在郑州抓获，4月15日李庭归案，这些利用POS机发歪财的“寄生虫”也必将得到法律的严惩。

（线索提供：朱振华 刘新娜）