安卓木马 Switcher 加入“攻击路由器”的队伍

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Switcher: Android joins the ‘attack-the-router’ club		
原文作者	Nikita Buchka	**原文发布日期**	2016 年 12 月 28 日
作者简介	卡巴斯基移动恶意软件分析师，主要对安卓以及针对安卓平台威胁攻击感兴趣。		
原文发布单位	卡巴斯基实验室		
原文出处	https://securelist.com/blog/mobile/76969/switcher-android-joins-the-attack-the-router-club/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

安卓木马 Switcher 加入“攻击路由器”的队伍

尼基塔·布奇卡

2016 年 12 月 28 日

最近，在不断探索防范恶意软件侵扰网络世界之时 ,我们发现一款安卓木马行为不当。虽然攻击安卓操作系统的恶意软件在很久之前就已受挫 ,有点不可思议 ,但该木马有点特别。它不攻击用户转而攻击用户连接的无线网络 ,或者更准确的说,攻击提供网络的无线路由器。该木马被命名为 Trojan.AndroidOS.Switcher ,它针对路由器网络管理界面进行暴力破解攻击，猜测密码。倘若攻击成功，恶意软件会更该路由器设置中的 DNS 服务器地址，将被攻击的无线网络中所有设备的所有 DNS 请求重新路由到网络罪犯的服务器上（这样的攻击也被称为 DNS 劫持）。本文将详细介绍 Switcher 如何实施暴力破解攻击，入侵路由器并执行 DNS 劫持。

狡猾的骗术

到目前为止，我们已发现该木马的两个版本：

- acdb7bfebf04affd227c93c97df536cf; package name – com.baidu.com
- 64490fbecefa3fcdacd41995887fe510; package name – com.snda.wifi

只需打开应用内部的 URL 地址 http://m.baidu.com，就可以看到第一个版本把自己伪装成中国搜索引擎百度的移动客户端。第二个版本制作精良 ,伪装为一款非常流行的中国应用程序，用户之间共享无线网络的信息（包括安全密码）。例如，出差的旅客经常用这些信息连接不知道密码的公共无线网络。对于隐藏起来攻击路由器的恶意软件来说 ,这的确是一个好方法，因为此类应用的用户经常连接很多无线网络，容易造成感染扩散。

网络罪犯甚至创建网站（虽然设计拙劣）用于宣传和传播上述提到的假冒版本的 com.snda.wifilocating。且该网络服务器贮存的网站也被恶意软件的作者用作 C&C 服务器。

感染过程

木马实施以下行动：

1. 获取网络的 BSSID（基本服务集标识符）并通知 C&C 服务器木马已在该网络中激活。

2. 试图获取 ISP（互联网服务提供商）的名称并利用该名称确定对哪个异常 DNS 服务器进行 DNS 劫持。有三种 DNS 服务器可被利用：101.200.147.153, 112.33.13.11 和 120.76.249.59。其中，101.200.147.153 是默认选项，而其它两个只针对特定的互联网服务提供商。

3. 利用下述预定义的登录名和密码字典发动暴力破解攻击：

- admin:00000000
- admin:admin
- admin:123456
- admin:12345678
- admin:123456789
- admin:1234567890
- admin:66668888
- admin:1111111
- admin:88888888
- admin:666666
- admin:87654321
- admin:147258369
- admin:987654321
- admin:66666666
- admin:112233
- admin:888888
- admin:000000
- admin:5201314
- admin:789456123
- admin:123123
- admin:789456123
- admin:0123456789

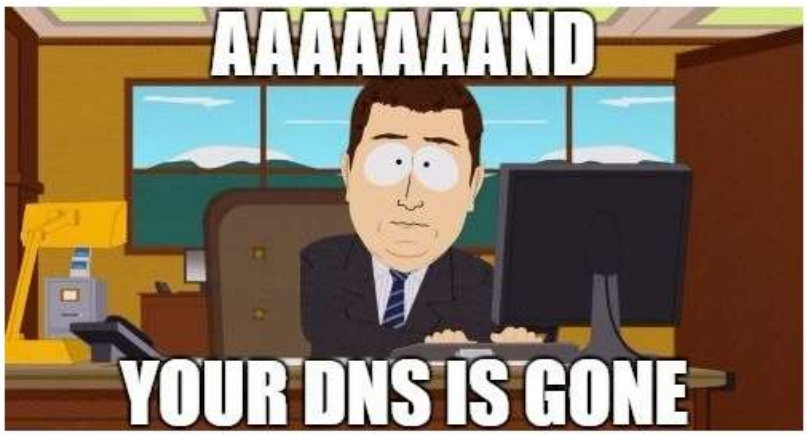
- admin:123456789a
- admin:11223344
- admin:123123123

木马获取默认网关地址之后，然后试图在嵌入式浏览器中访问该地址。借助 JavaScript，木马试图利用不同的登录名和密码组合登录。根据输入字段的硬解码名称和木马试图访问的 HTML 文档的结构， JavaScript 代码只在 TP-LINK 无线路由器的网络界面运行。

4. 如果访问管理界面成功，木马导航到 WAN（广域网）设置，用网络罪犯控制的流氓 DNS 服务器替换主要的 DNS 服务器，并用 8.8.8.8（即谷歌 DNS，如果流氓 DNS 服务器出现故障，它会确保稳定运行）替换备用 DNS 服务器。实施这些行动的代码一团糟，因为它在各种路由器上以异步模式运行。不过，我将展示网络界面截图，并重新排列代码的各部分，从而显示其运作方式。

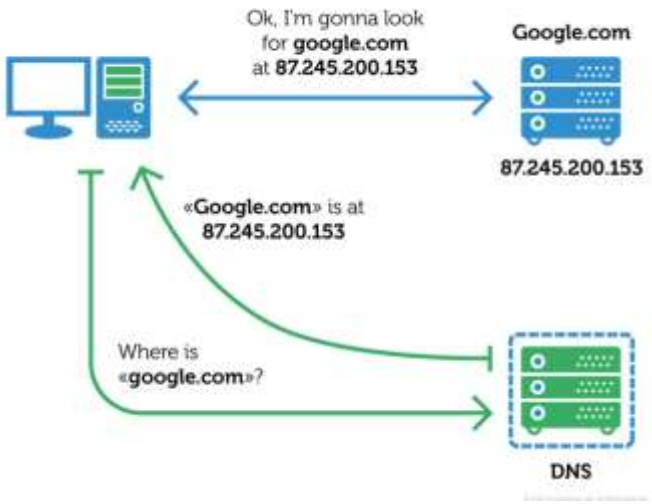

```
javascript:document.getElementsByName('bottomLeftFrame')[0]
    .contentWindow.document.getElementById('a3').click() // Select the 'Network' tab

javascript:document.getElementsByTagName('li')[1].click()// Select the 'WAN' menu item

javascript:document.getElementsByName('mainFrame')[0]
    .contentWindow.document.getElementsByName('dnsserver')[0]
    .value='' + this.myDns + ''                          // Set the Primary DNS input

javascript:document.getElementsByName('mainFrame')[0]
    .contentWindow.document.getElementsByName('dnsserver2')[0]
    .value='8.8.8.8'                                     // Set the Secondary DNS input

javascript:document.getElementsByName('mainFrame')[0]
    .contentWindow.document.getElementsByName('Save')[0].click() // Click the 'Save' button
```

5. 一旦 DNS 地址操作成功，木马就向 C&C 服务器报告成功的消息。

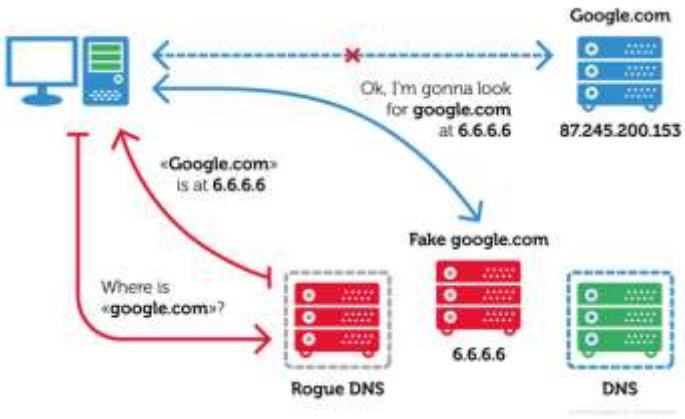


为什么影响恶劣？

要明白此类行为的影响，理解 DNS 工作的基本原理非常重要。该 DNS 将人类可读的网络资源（例如网站）解析为用于计算机网络实际通信的 IP 地址。例如，“google.com”将被解析为 IP 地址 87.245.200.153。一般而言，正常的 DNS 请求通过如下方式实现：



当使用 DNS 劫持时，网络罪犯会更改受害者（我们指的是路由器）的 TCP/IP 设置，迫使它向网络罪犯控制的路由器——流氓 DNS 服务器——发送 DNS 请求。因此，该方案变成这样：



正如你所看到的，受害者没有访问真正的 google.com，而是被骗进一个完全不相干的网站，访问网络资源。这可能是一个假冒的 google 网站，它会保存你的搜索请求，发送给网络罪犯，或者你访问的只是有大量弹窗广告和恶意软件的随机网站，抑或是其它的网站。攻击者利用名称解析系统（包括，例如所有的网络流量）几乎完全控制了所有的网络流量。

你可能会问——有什么影响呢？路由其无法浏览网站，风险何在呢？不幸的是，无线路由器最常见的配置是让连接设备的 DNS 设置相同，因此强迫所有网络设备使用相同的异常 DNS。因此，在获得路由器 DNS 设置访问权限之后，几乎可以控制该路由器提供的所有网络流量。

由于网络罪犯粗心，在 C&C 网站上留下了部分内部公开感染数据。

根据数据表明，他们已成功感染了 1280 个无线网络。如果情况属实，网络上所有用户流量都有可能受重定向的影响。

结论

Trojan.AndroidOS.Switcher 不会直接攻击用户。而是用网络钓鱼或二次感染等方式，攻击暴露在各种攻击之下的用户网络。对路由器设置进行篡改的主要威胁在于即使是重启路由器，新的设置也不会消失，而且我们很难发现 DNS 已被劫持了。即使异常 DNS 服务器关闭了一段时间，罪犯将设置 8.8.8.8 作为备用 DNS ,因此不会被用户或者 IT 人员发现。

我们建议所有的用户检查其 DNS 设置并搜索下列异常 DNS 服务器：

- 101.200.147.153
- 112.33.13.11
- 120.76.249.59

如果你的 DNS 设置中藏有一个此类服务器，请联系你的网络服务提供商寻求支持或向无线网络的主人警示。卡巴斯基实验室也强烈建议用户更改路由器网络管理界面的默认登录名和密码以便以后预防此类攻击。