Switcher: Android joins the ‘attack-the-router’ club

securelist.com/blog/mobile/76969/switcher-android-joins-the-attack-the-router-club/

Authors

Nikita Buchka

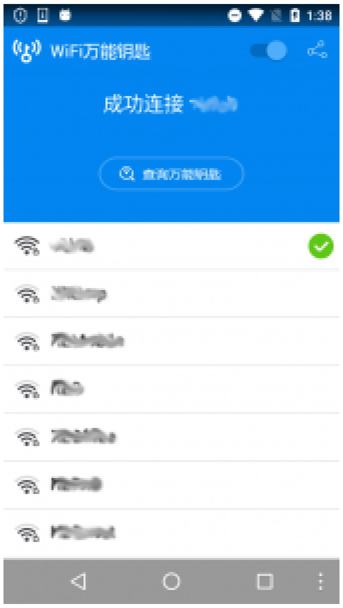
Recently, in our never-ending quest to protect the world from malware, we found a misbehaving Android trojan. Although malware targeting the Android OS stopped being a novelty quite some time ago, this trojan is quite unique. Instead of attacking a user, it attacks the Wi-Fi network the user is connected to, or, to be precise, the wireless router that serves the network. The trojan, dubbed Trojan.AndroidOS.Switcher, performs a brute-force password guessing attack on the router’s admin web interface. If the attack succeeds, the malware changes the addresses of the DNS servers in the router’s settings, thereby rerouting all DNS queries from devices in the attacked Wi-Fi network to the servers of the cybercriminals (such an attack is also known as DNS-hijacking). So, let us explain in detail how Switcher performs its brute-force attacks, gets into the routers and undertakes its DNS-hijack.

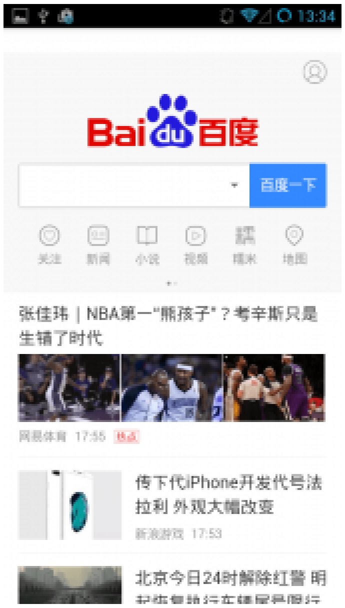
Clever little fakes

To date, we have seen two versions of the trojan:

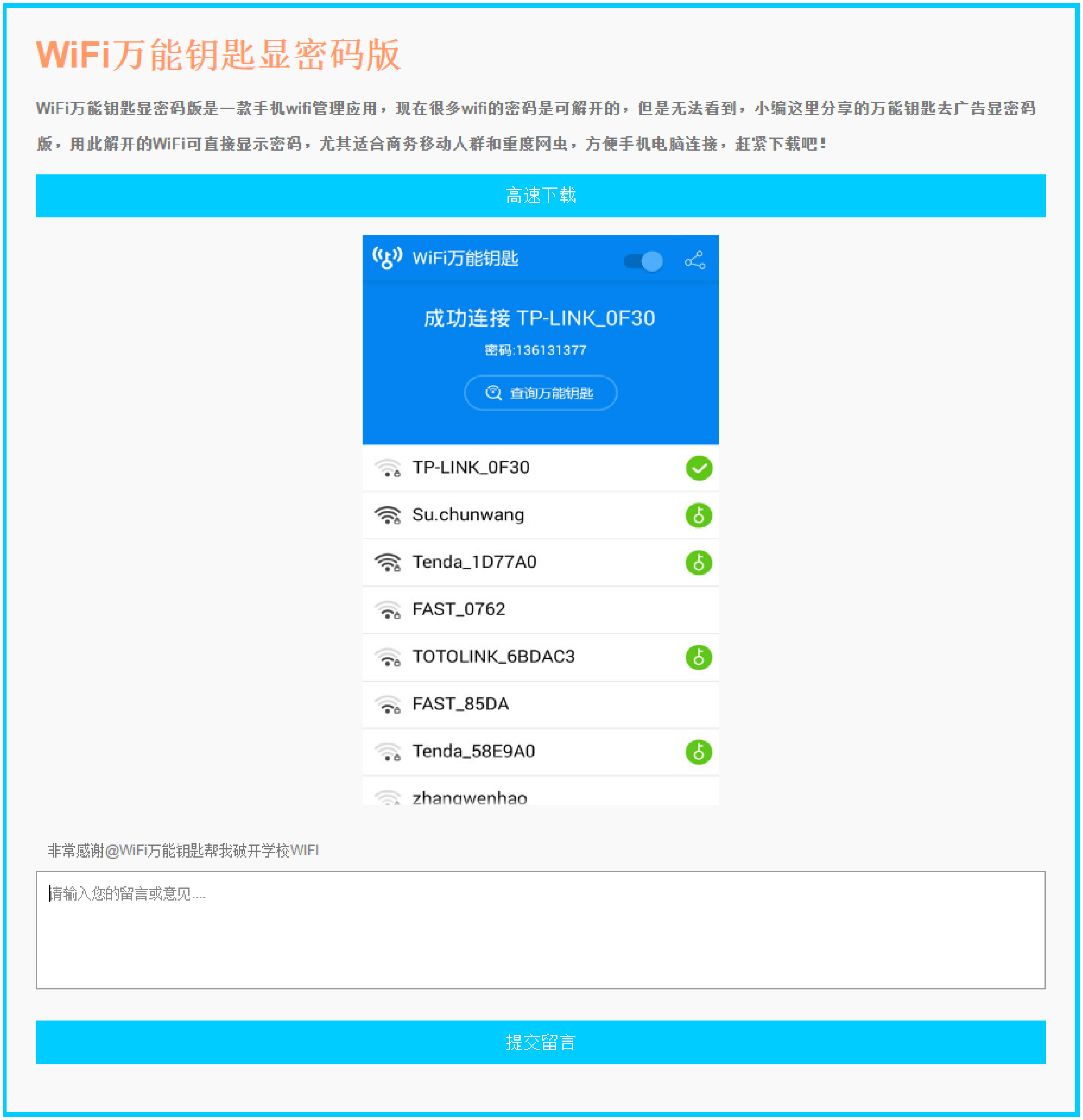
- acdb7bfebf04affd227c93c97df536cf; package name – com.baidu.com
- 64490fbecefa3fcdacd41995887fe510; package name – com.snda.wifi

The first version (com.baidu.com), disguises itself as a mobile client for the Chinese search engine Baidu, simply opening a URL http://m.baidu.com inside the application. The second version is a well-made fake version of a popular Chinese app (http://www.coolapk.com/apk/com.snda.wifilocating) for sharing information about Wi-Fi networks (including the security password) between users of the app. Such information is used, for example, by business travelers to connect to a public Wi-Fi network for which they don’t know the password. It is a good place to hide malware targeting routers, because users of such apps usually connect with many Wi-Fi networks, thus spreading the infection.





The cybercriminals even created a website (though badly made) to advertise and distribute the aforementioned fake version of com.snda.wifilocating. The web server that hosts the site is also used by the malware authors as the command-and-control (C&C) server.



WiFi万能钥匙显密码版

WiFi万能钥匙显密码版是一款手机wifi管理应用，现在很多wifi的密码是可解开的，但是无法看到，小编这里分享的万能钥匙去广告显密码版，用此解开的WiFi可直接显示密码，尤其适合商务移动人群和重度网虫，方便手机电脑连接，赶紧下载吧！

成功连接 TP-LINK_0F30

密码:136131377

非常感谢@WiFi万能钥匙帮我破开学校WIFI

请输入您的留言或意见....

The infection process

The trojan performs the following actions:

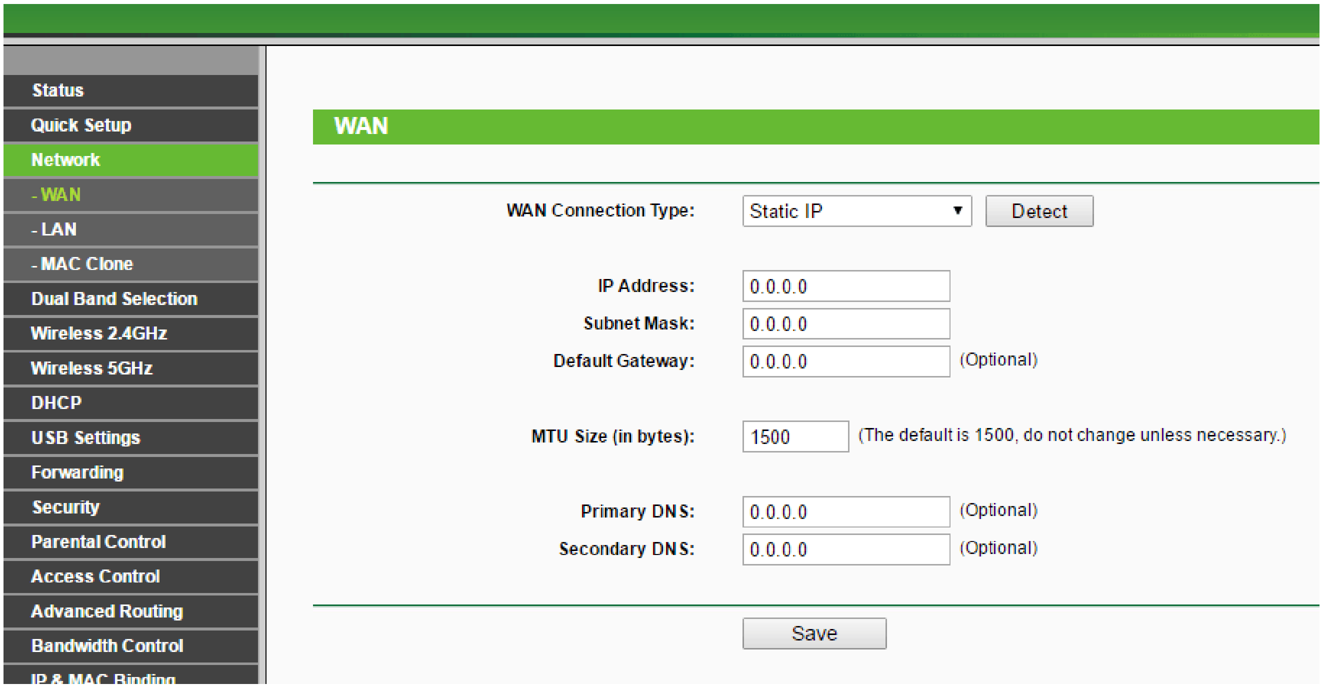
1. Gets the BSSID of the network and informs the C&C that the trojan is being activated in a network with this BSSID
2. Tries to get the name of the ISP (Internet Service Provider) and uses that to determine which rogue DNS server will be used for DNS-hijacking. There are three possible DNS servers – 101.200.147.153, 112.33.13.11 and 120.76.249.59; with 101.200.147.153 being the default choice, while the others will be chosen only for specific ISPs

3. Launches a brute-force attack with the following predefined dictionary of logins and passwords:

- 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

The trojan gets the default gateway address and then tries to access it in the embedded browser. With the help of JavaScript it tries to login using different combinations of logins and passwords. Judging by the hardcoded names of input fields and the structures of the HTML documents that the trojan tries to access, the JavaScript code used will work only on web interfaces of TP-LINK Wi-Fi routers

- If the attempt to get access to the admin interface is successful, the trojan navigates to the WAN settings and exchanges the primary DNS server for a rogue DNS controlled by the cybercriminals, and a secondary DNS with 8.8.8.8 (the Google DNS, to ensure ongoing stability if the rogue DNS goes down). The code that performs these actions is a complete mess, because it was designed to work on a wide range of routers and works in asynchronous mode. Nevertheless, I will show how it works, using a screenshot of the web interface and by placing the right parts of the code successively.



WAN

WAN Connection Type: Static IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 (Optional)

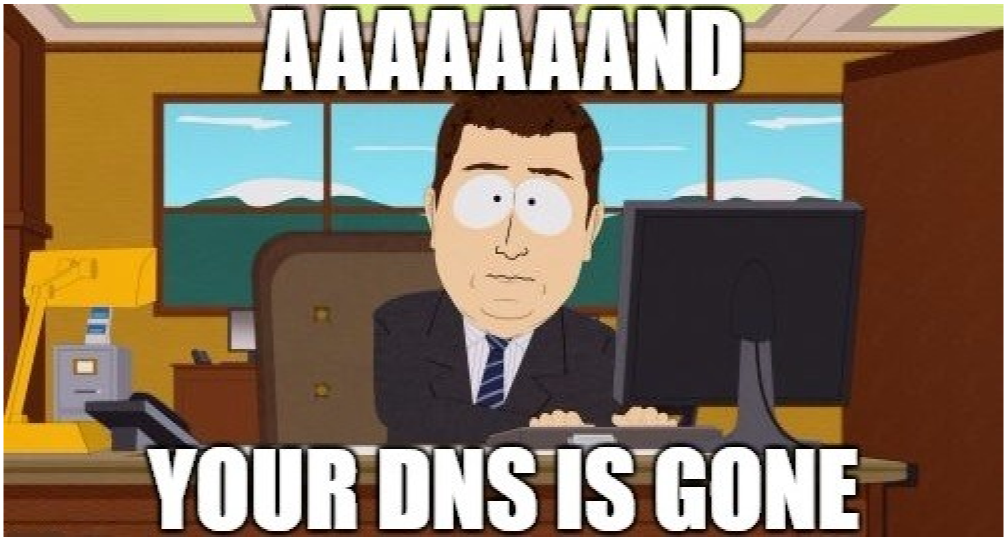
MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

Primary DNS: 0.0.0.0 (Optional)

Secondary DNS: 0.0.0.0 (Optional)

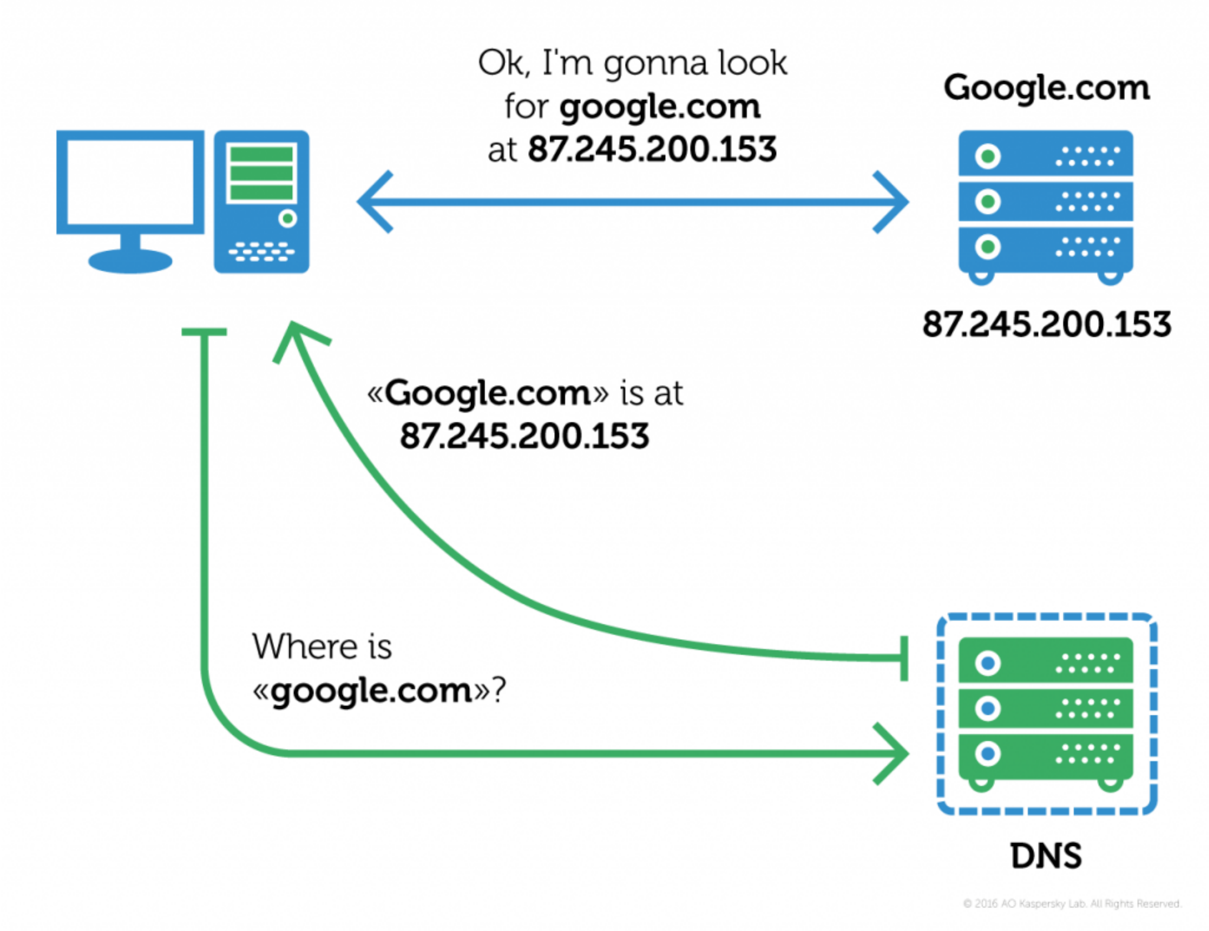
```
javascript:document.getElementsByName('bottomLeftFrame')[0]
    .contentWindow.document.getElementById('a3').click() // Select the 'Network' tab

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
```

- If the manipulation with DNS addresses was successful, the trojan report its success to the C&C

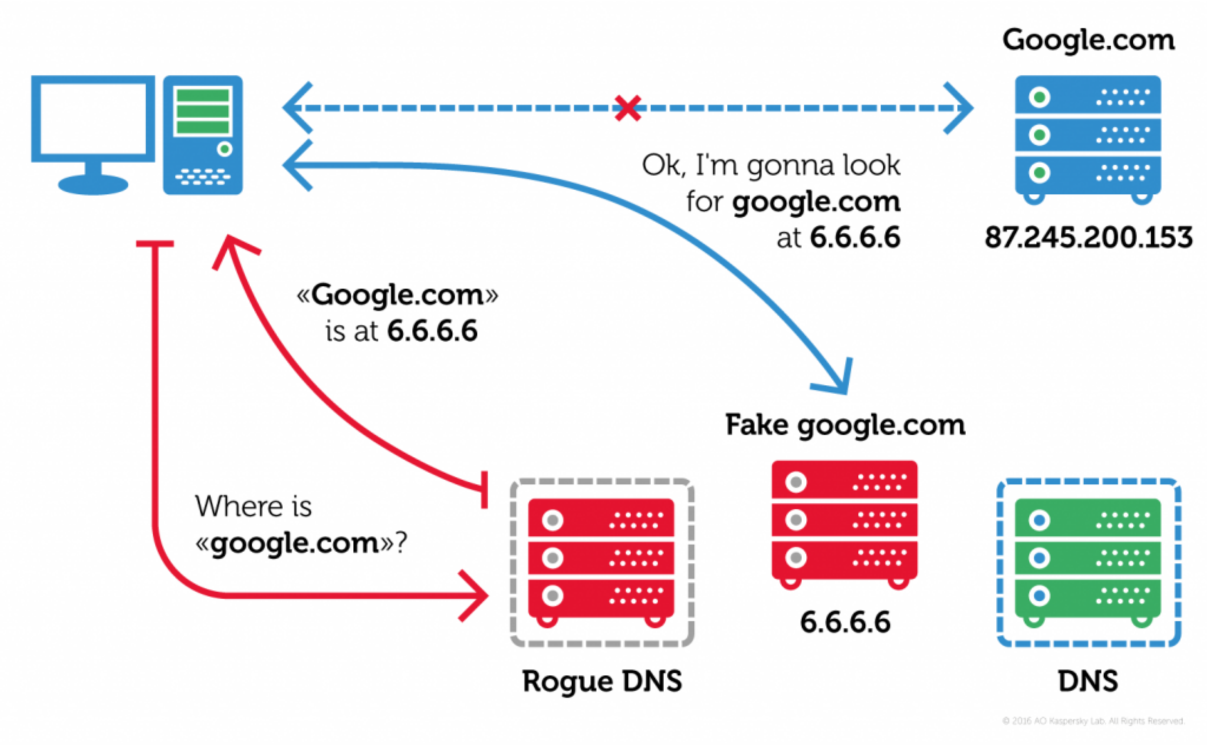


So, why it is bad?

To appreciate the impact of such actions it is crucial to understand the basic principles of how DNS works. The DNS is used for resolving a human-readable name of the network resource (e.g. website) into an IP address that is used for actual communications in the computer network. For example, the name “google.com” will be resolved into IP address 87.245.200.153. In general, a normal DNS query is performed in the following way:



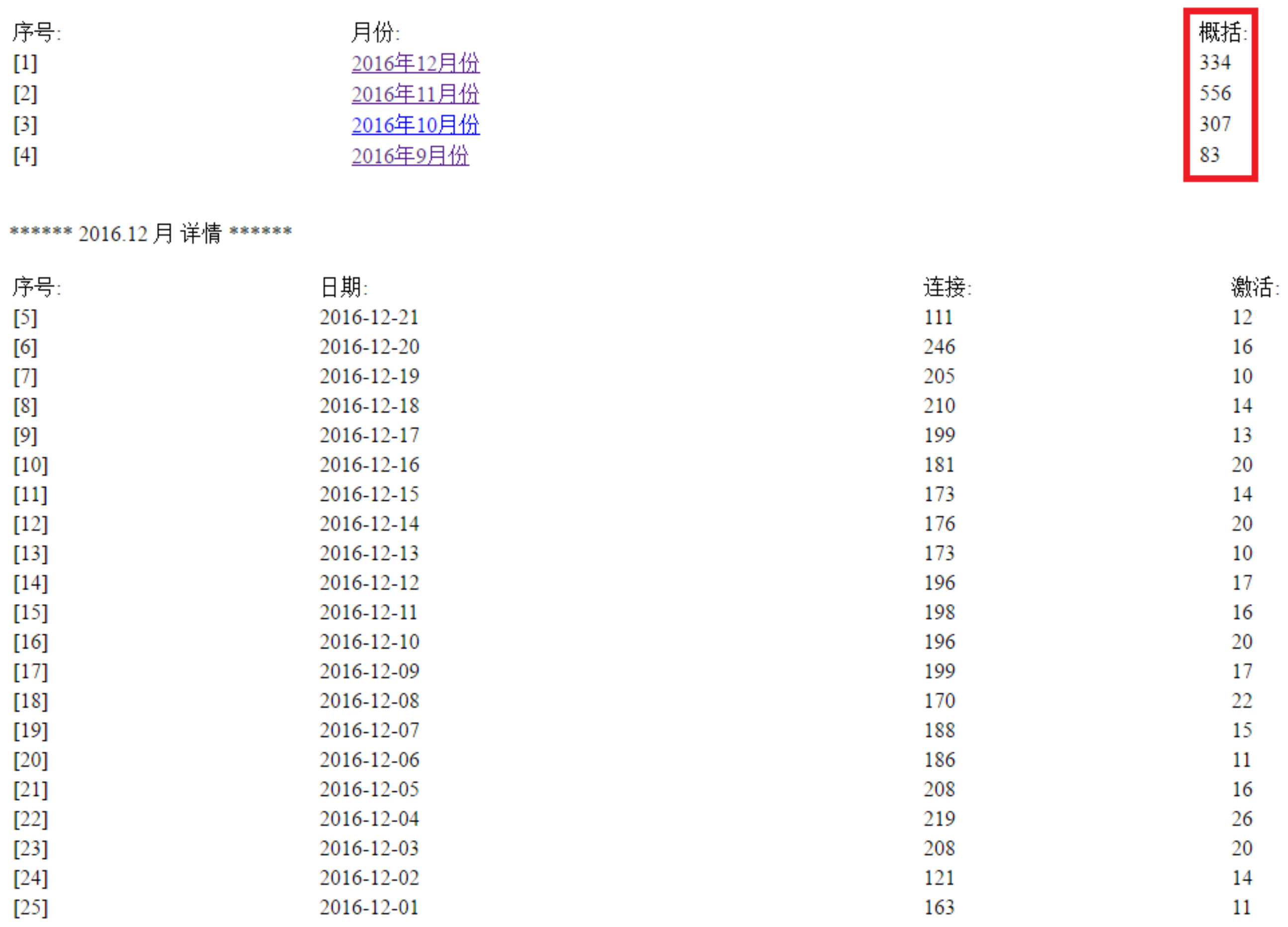
When using DNS-hijacking, the cybercriminals change the victim's (which in our case is the router) TCP/IP settings to force it to make DNS queries to a DNS server controlled by them – a rogue DNS server. So, the scheme will change into this:


Google.com
Ok, I'm gonna look for google.com at 6.6.6.6
87.245.200.153
«Google.com» is at 6.6.6.6
Fake google.com
Where is «google.com»?
6.6.6.6
Rogue DNS
DNS
© 2016 AO Kaspersky Lab. All Rights Reserved.

As you can see, instead of communicating with the real google.com, the victim will be fooled into communicating with a completely different network resource. This could be a fake google.com, saving all your search requests and sending them to the cybercriminals, or it could just be a random website with a bunch of pop-up ads or malware. Or anything else. The attackers gain almost full control over the network traffic that uses the name-resolving system (which includes, for example, all web traffic).

You may ask – why does it matter: routers don't browse websites, so where's the risk? Unfortunately, the most common configuration for Wi-Fi routers involves making the DNS settings of the devices connected to it the same as its own, thus forcing all devices in the network use the same rogue DNS. So, after gaining access to a router's DNS settings one can control almost all the traffic in the network served by this router.

The cybercriminals were not cautious enough and left their internal infection statistics in the open part of the C&C website.



序号:	月份:	概括:
[1]	2016年12月份	334
[2]	2016年11月份	556
[3]	2016年10月份	307
[4]	2016年9月份	83

****** 2016.12 月 详情 ******

序号:	日期:	连接:	激活:
[5]	2016-12-21	111	12
[6]	2016-12-20	246	16
[7]	2016-12-19	205	10
[8]	2016-12-18	210	14
[9]	2016-12-17	199	13
[10]	2016-12-16	181	20
[11]	2016-12-15	173	14
[12]	2016-12-14	176	20
[13]	2016-12-13	173	10
[14]	2016-12-12	196	17
[15]	2016-12-11	198	16
[16]	2016-12-10	196	20
[17]	2016-12-09	199	17
[18]	2016-12-08	170	22
[19]	2016-12-07	188	15
[20]	2016-12-06	186	11
[21]	2016-12-05	208	16
[22]	2016-12-04	219	26
[23]	2016-12-03	208	20
[24]	2016-12-02	121	14
[25]	2016-12-01	163	11

According to them, they successfully infiltrated 1,280 Wi-Fi networks. If this is true, traffic of all the users of these networks is susceptible to redirection.

Conclusion

The Trojan.AndroidOS.Switcher does not attack users directly. Instead, it targets the entire network, exposing all its users to a wide range of attacks – from phishing to secondary infection. The main danger of such tampering with routers' setting is that the new settings will survive even a reboot of the router, and it is very difficult to find out that the DNS has been hijacked. Even if the rogue DNS servers are disabled for some time, the secondary DNS which was set to 8.8.8.8 will be used, so users and/or IT will not be alerted.

We recommend that all users check their DNS settings and search for the following rogue DNS servers:

- 101.200.147.153
- 112.33.13.11
- 120.76.249.59

If you have one of these servers in your DNS settings, contact your ISP support or alert the owner of the Wi-Fi network. Kaspersky Lab also strongly advises users to change the default login and password to the admin web interface of your router to prevent such attacks in the future.

- DNS
- Google Android
- Mobile Malware
- Router

Authors

Nikita Buchka

Switcher: Android joins the ‘attack-the-router’ club

Your email address will not be published. Required fields are marked *