



The current case „DNSChanger“ – what computer users can do now

Content

What happened so far?	2
What is going to happen on 8 March 2012?	2
How can I test my Internet settings?	2
On the PC	3
On the router	5
General advice	6



What happened so far?

The successful undertaking of the so called "Operation Ghost Click", carried out by the FBI and other international law enforcement entities, was celebrated in the media – the criminal masterminds were put behind bars and the rogue DNS servers were taken over by the FBI. The FBI is able to control these DNS servers but they cannot disinfect any computer affected by "DNSChanger" malware. Therefore, it is now essential to free all affected computer users from changed DNS settings they did not authorize and therefore ensure a smoothly functioning connection to the Internet after 8 March 2012.

There are two different characteristics of "DNSChanger" malware which should become clear with the following explanation:

Character 1: The malware modifies the DNS settings on an infected Windows PC. These settings include the "hosts" file and the DHCP settings. If the DNS settings are changed, a user does not reach the website he/she intended to reach when using the web browser. The attacker redirects the user to a predefined target.

Character 2: The malware modifies the name server settings within the router. This means, that the changes are not directly made on a PC but on the router, which, e.g. connects the home network with the Internet.

The Trojan is equipped with password lists which contain the standard log-ins for the most common routers on the market. The Trojan can easily gain access to the router's web interface in case the user never edited the standard factory-set password. This way, the bad guys can change telecommunication service provider's name server settings for their individual purposes and control each and every user attempt to open a website.

What is going to happen on 8 March 2012?

The FBI will shut down the formerly rogue DNS servers they now have under their control. This means that all users with computers which

- a) are infected with the "DNSChanger" malware spread by the bad guys and
- b) have not set their DNS settings to "normal" state

can expect to experience problems connecting to the WWW after the FBI took down the DNS servers.

How can I test my Internet settings?

At this point, we present measures computer users with Microsoft Windows operating systems (XP, Vista and 7) can perform themselves to check their PC for immediate damages caused by "DNSChanger" malware.

If the device to be tested is a computer in a company's network, please contact your system administrator first.



Before you manually start testing the settings described below, perform a complete antivirus scan on your entire PC. After that, visit the website <http://dns-ok.de>

If this website shows a red warning sign (see screenshot 1), you inevitably have to go through the steps described below.

If the website displays a green bar, the DNS settings of your system and router are ok and there has been no manipulation by the current "DNSChanger" malware. Please be aware that this online test can only be performed flawlessly without any proxy settings in the browser.

ACHTUNG: Ihre DNS Konfiguration ist manipuliert

Screenshot 1: Warning message displayed on dns-ok.de. It alerts that the visiting computer's DNS settings are not correct!

Attention: If the online test or the manual tests presented show your DNS settings are correct, this does not necessarily mean your computer is free from malware! In any case, please conduct regular computer scans with comprehensive and up-to-date antivirus software, e.g. G Data InternetSecurity 2012 with BootCD.

On the PC

Step 1: Check the "hosts" file

Open a text editor. When using [Windows Vista](#) or [Windows 7](#), run the text editor as administrator. To do so, right-click the text editor executable file and then left-click "Run as administrator".

Now, within this text editor, open the "hosts" file. You can find it under

C:\Windows\system32\drivers\etc

You might have to choose "All files (*.*)" at the bottom right corner of the file selector window to see and subsequently select the "hosts" file.

When using [Windows XP](#), the "hosts" file contains only one entry: localhost is connected to 127.0.0.1 The default "hosts" file under [Microsoft Windows Vista](#) and [Microsoft Windows 7](#) contains no entry at all. Note: All lines starting with a hash (#) character are comment lines and are therefore ignored by the system and can be ignored by you as well.

```

Datei Bearbeiten Format Ansicht ?
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10      x.acme.com     # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost

```

Screenshot 2: A „hosts“ file in Microsoft Windows 7 containing several comment lines

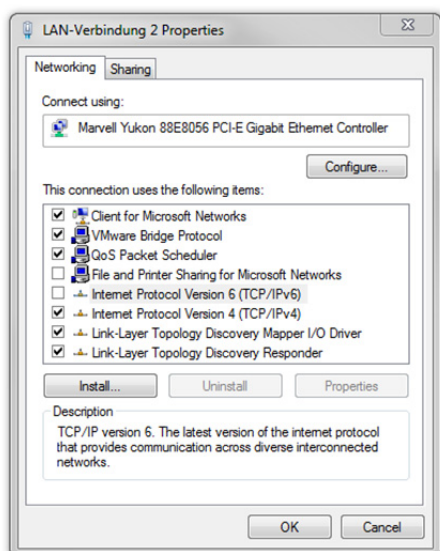
If you see additional entries in your "hosts" file, without a preceding hash character and regardless of the operating system, this can be an indication of a modification made by malware.

You can add a hash character to the beginning of each line with an additional entry to verify the situation. Restart your browser if necessary and visit the website <http://dns-ok.de>

Step 2: Check the DHCP settings

Users with a **Windows XP** computer need to click Start > Control panel > Network and Internet Connections > Network Connections and choose the active connection they are using to access the Internet. Right-click the connection and choose "Properties".

Windows Vista and **Windows 7** users click Start > Control panel > Network and Sharing Center and choose the active connection you are using to access the Internet as well, click and choose "Properties".



Screenshot 3: Properties of the active LAN connection

The option "Properties" will open up a new window (see screenshot 3).

Choose Internet Protocol (TCP/IP) under **Windows XP** and Internet Protocol Version 4 (TCP/IPv4) under **Windows Vista** and **Windows 7**. In any case, the options "Obtain an IP address automatically" and "Obtain DNS server address automatically" should be activated. If you can find any unknown DNS server address at this point, delete the IP and activate "Obtain DNS server address automatically".

Following this, open the Windows command-line shell (Start > All Programs > Accessories > Command Prompt). **Windows Vista** users have to run this command prompt as administrator to make the following instruction work. In the command prompt, type `ipconfig /flushdns` and execute it by pressing the enter key. This short command empties the system's DNS cache. Restart your browser if necessary and visit the website <http://dns-ok.de>

Step 3: Check the browser settings

Microsoft Internet Explorer (Version 9)

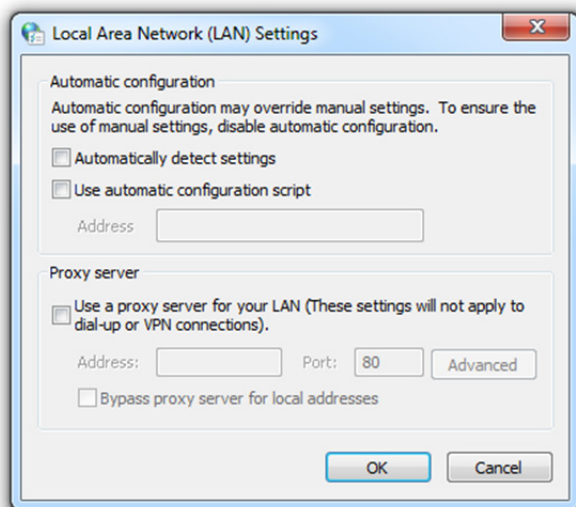
Click "Tools" > "Internet options". Then choose "Connections". Click "LAN settings" and check whether one of the three possible boxes is ticked. None of them should be ticked by default.

Mozilla Firefox (Version 9)

Click "Tools" > "Options" > and choose the "Advanced" tab. Then, choose the "Network" tab and "Settings" in the "Connection" section. Now check whether you see any entry in "Manual Proxy settings". By default, "No Proxy" should be activated.

Google Chrome (Version 16)

Click "Customize and control Google Chrome" and choose "Options" and then "Under the Hood". In the "Network" section, click "Change proxy settings". As Google Chrome uses the computer system's proxy settings, the Google Chrome settings are equivalent to the ones the Internet Explorer has.



Screenshot 4: The system's proxy settings, available in IE and Google Chrome

In the newly opened window, click "LAN settings" and check whether one of the three possible boxes is ticked. None of them should be ticked by default.

After checking your browser settings, restart the browser if necessary and visit the website <http://dns-ok.de>

On the router

Step 4: Check the router's network settings

If several computers in one local network are experiencing the potential "DNSChanger" problems, access your router via web interface. Please refer to the manual of your specific device to see how this access works.

By default, the setting "Obtain an IP address automatically" should be activated. If you can see DNS server addresses at this point, delete those. Restart your router.

Subsequently, open the Windows command-line shell (Start > All Programs > Accessories > Command Prompt) on any PC of the local network. [Windows Vista](#) users have to run this command prompt as administrator to make the following instruction work. In the command prompt, type `ipconfig /flushdns` and execute it by pressing the enter key. This short command empties the system's DNS cache. Restart your browser if necessary and visit the website <http://dns-ok.de>

For security reasons, you should furthermore change your router password immediately. This password change is especially important if you have never changed the factory-set password and also in case you now found settings on your router, which have been made by any unauthorized third party.

Attention: If the online test or the manual tests presented show your DNS settings are correct, this does not necessarily mean your computer is free from malware! In any case, please conduct regular computer scans with comprehensive and up-to-date antivirus software, e.g. G Data InternetSecurity 2012 with BootCD.



General advice

- Use an up-to-date, comprehensive security solution with a virus scanner, firewall, spam filter, http scan and real-time protection. A spam filter, to get rid of unwanted spam, is a must-have, too.
- Always keep your software, browser and operating system up-to-date and regularly install updates to close existing security vulnerabilities.
- Change the factory-set passwords on devices right after configuring those devices.
- If you realize your computer has been infected, change all passwords in use, e.g. for (online) email accounts, online-banking accounts, shopping websites, social networks, instant messengers and many more.