How can you detect if your computer has been violated and infected with DNS Changer?

An industry wide team has developed easy "are you infected" web sites. They are a quick way to determine if you are infected with DNS Changer. Each site is designed for any normal computer user to browse to a link, follow the instructions, and see if they might be infected. Each site has instructions in their local languages on the next steps to clean up possible infections.

For example, the http://www.dns-ok.us/ will state if you are or are not infected (see below).

- **No Software is Downloaded!** The tools do not need to to load any software on your computer to perform the check.
- **No changes are performed on your computer!** Nothing is changed on your computer when you use sites like http://www.dns-ok.us/.
- **No scanning!** The "are you infected with DNS Changer" tool does not need to scan your computer.

If you think your computer is infected with DNS Changer or any other malware, please refer to the security guides from your operating system or the self -help references from our fix page (http://www.dcwg.org/fix).

The following table is a list of all easy "are you infected" sites. It includes the links to the security organizations who are maintaining the sites. Each site has instructions in their local languages on the next steps to clean up possible infections.

URL	Language	Maintainer
www.dns-ok.us	English	DNS Changer Working Group (DCWG)
www.dns-ok.de	German	Bundeskriminalamt (BKA) & Bundesamt für Sicherheit in der Informationstechnik (BSI)
www.dns-ok.fi	Finnish, Swedish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the national information security situation awareness system.
www.dns-ok.ax	Swedish, Finnish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the national information security situation awareness system.
www.dns-ok.be	Dutch/French	CERT-BE is the primary Belgian contact point for dealing with Internet security threats and vulnerabilities affecting Belgian interests.
www.dns-ok.fr	French	Le CERT-LEXSI est la division de veille et d'enquête sur

		Internet, dédiée à la protection du patrimoine en ligne des organisations.
www.dns-ok.ca	English/French	Canadian Internet Registration Authority (CIRA) and Canadian Cyber Incident Response Centre (CCIRC)
www.dns-ok.lu	English	CIRCL (Computer Incident Response Center Luxembourg) is the national Computer Security Incident Response Team (CSIRT - CERT) coordination center for the Grand-Duchy of Luxembourg
www.dns-ok.nl	Dutch	SIDN (the Foundation for Internet Domain Registration in the Netherlands)
dns-ok.gov.au	English	CERT Australia, Stay Smart Online, and Australian Communications and Media Authority joint page on DNSChanger Information
dns-changer.eu	German, Spanish, English	ECO (Association of the German Internet Industry)
dnschanger.detect.my	Malaysian, English	Hosted by CyberSecurity Malaysia and MYCERT
dns-ok.jpcert.or.jp	Japanese	JPCERT/CC - Japan Computer Emergency Response Team Coordination Center
www.dns-ok.it	Italiano	Telecom Italia Security Operation Center - IT.TS.SOC

If you are not affected by DNS Changer then do nothing.

If the Check-Up Site indicates that you are affected then either follow the instructions on that site or go to the "FIX" page.

Manually Checking if your DNS server have been Changed

The following pages would help check to manually see if you have DNS Changer DNS servers configured on your computer. Use of the "check up" pages are more effective, but some would want to check manually.

- **Checking for DNS Changer on Windows XP**
- Checking for DNS Changer on Windows Vista (pending)
- **Checking Windows 7 for Infections**
- **Checking OSX for Infections**

Would my Service Provider Help Me?

Many service providers are notifying their customers. They are creating help pages that will help you detect and clean up DNS Changer from your system. Here is a partial list. Please contact your SP if you do not see them on the list.

ISP	Page
AT&T	AT&T DNS Changer information page for Home and Business Customers and 8 Suggestions for Mitigating and Preventing DNSChanger Malware in your Enterprise - What Can Help You Avoid Being a Victim
Bell Canada	Important information about DNS Changer malware
CenturyLink	CenturyLink DNSChanger Customer Notice
Comcast	DNS Changer Bot FAQ
COX	COX DnsChanger Malware Information
Shaw Communications	Shaw Virus Protection
Telecom Italia	Assistenza Tecnica per DNS Changer Malware
Time Warner Cable & RoadRunner	Time Warner Cable & Roadrunner Website for DNS Changer Malware
Verizon	Verizon's Virus Help Website for DNS Changer Malware

Goto this site to check your PC (only) > http://www.dns-ok.us/

DNS Changer Check-Up

DNS Resolution = GREEN

Your computer appears to be looking up IP addresses correctly!

Had your computer been infected with DNS changer malware you would have seen a red background. Please note, however, that if your ISP is redirecting DNS traffic for its customers you would have reached this site even though you are infected. For additional information regarding the DNS changer malware, please visit the FBI's website at:
http://www.fbi.gov/news/stories/2011/november/malware_110911

Checking for DNS Changer on Windows XP

The easiest way to check if your system is violated with DNS Changer malware is to go to one of the "are you infected sites" (see below). These sites only require someone to visit. The "are you infected site" will inform you if you are infected.

Note: These sites only detect for DNS Changer. You might be infected with other malware. Please take appropriate precautions to protect your computer.

URL	Language	Maintainer
www.dns-ok.us	English	DNS Changer Working Group (DCWG)
www.dns-ok.de	German	Bundeskriminalamt (BKA) & Bundesamt für Sicherheit in der Informationstechnik (BSI)
www.dns-ok.fi	Finnish, Swedish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the national information security situation awareness system.

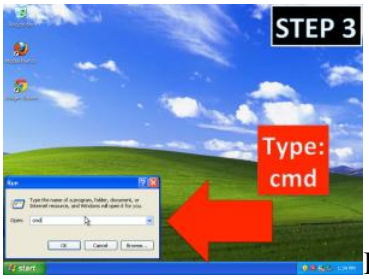
www.dns-ok.ax	Swedish, Finnish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the national information security situation awareness system.
www.dns-ok.be	Dutch/French	CERT-BE is the primary Belgian contact point for dealing with Internet security threats and vulnerabilities affecting Belgian interests.
www.dns-ok.fr	French	Le CERT-LEXSI est la division de veille et d'enquête sur Internet, dédiée à la protection du patrimoine en ligne des organisations.
www.dns-ok.ca	English/French	Canadian Internet Registration Authority (CIRA) and Canadian Cyber Incident Response Centre (CCIRC)
www.dns-ok.lu	English	CIRCL (Computer Incident Response Center Luxembourg) is the national Computer Security Incident Response Team (CSIRT - CERT) coordination center for the Grand-Duchy of Luxembourg
www.dns-ok.nl	Dutch	SIDN (the Foundation for Internet Domain Registration in the Netherlands)
dns-ok.gov.au	English	CERT Australia, Stay Smart Online, and Australian Communications and Media Authority joint page on DNSChanger Information
dns-changer.eu	German, Spanish, English	ECO (Association of the German Internet Industry)
dnschanger.detect.my	Malaysian, English	Hosted by CyberSecurity Malaysia and MYCERT
dns-ok.jpcert.or.jp	Japanese	JPCERT/CC - Japan Computer Emergency Response Team Coordination Center
www.dns-ok.it	Italiano	Telecom Italia Security Operation Center - IT.TS.SOC

Manually Checking for DNS Changer Infections

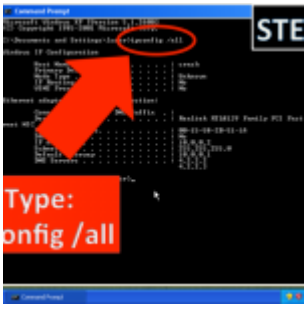
The following are the original manual checks to see if you computer is infected with any of the DNS Changer malware.

To check if your Windows XP machine is infected, first click the "Start" button.

Clicking the start button opens the Windows menu. Locate the "Run" option in the menu and
select it.



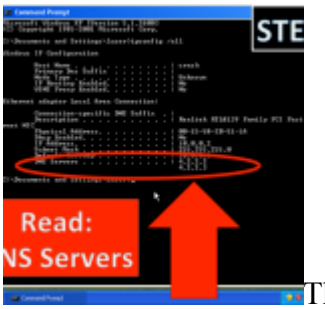
In the dialog, type in "cmd", as the name of the program to run. (This opens a DOS shell. This is also available under other parts of the Windows Menu.)



In DOS shell, type in the command:

```
ipconfig /all
```

and hit enter.



The command you entered displays information about your computer's network settings. Read the line starting with `"DNS Servers"`. There might be two or more IP addresses listed there. These are the DNS servers your computer uses. **Write down these numbers**

Are Your DNS Settings OK?

The malicious Rove viruses changed some peoples DNS settings to use computers they operated.

Compare your DNS settings with the known malicious Rove DNS settings listed below:

Starting IP	Ending IP	CIDR
85.255.112.0	85.255.127.255	85.255.112.0/20
67.210.0.0	67.210.15.255	67.210.0.0/20
93.188.160.0	93.188.167.255	93.188.160.0/21
77.67.83.0	77.67.83.255	77.67.83.0/24
213.109.64.0	213.109.79.255	213.109.64.0/20
64.28.176.0	64.28.191.255	64.28.176.0/20

What if I'm infected?

If you computer is infected, please refer to our page that list tools to clean DNS Changer and other self help guides to clean your computer – http://www.dcwg.org/fix/

Checking Windows 7 for Infections

The easiest way to check if your system is violated with DNS Changer malware is to go to one of the "are you infected sites" (see below). These sites only require someone to visit. The "are you infected site" will inform you if you are infected.

Note: These sites only detect for DNS Changer. You might be infected with other malware. Please take appropriate precautions to protect your computer.

URL	Language	Maintainer
www.dns-ok.us	English	DNS Changer Working Group (DCWG)
www.dns-ok.de	German	Bundeskriminalamt (BKA) & Bundesamt für Sicherheit in der Informationstechnik (BSI)
www.dns-ok.fi	Finnish, Swedish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the national information security situation awareness system.
www.dns-ok.ax	Swedish, Finnish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the national information security situation awareness system.
www.dns-ok.be	Dutch/French	CERT-BE is the primary Belgian contact point for dealing with Internet security threats and vulnerabilities affecting Belgian interests.
www.dns-ok.fr	French	Le CERT-LEXSI est la division de veille et d'enquête sur Internet, dédiée à la protection du patrimoine en ligne des organisations.
www.dns-ok.ca	English/French	Canadian Internet Registration Authority (CIRA) and Canadian Cyber Incident Response Centre (CCIRC)

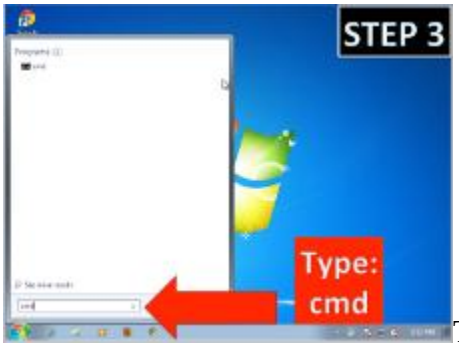
www.dns-ok.lu	English	CIRCL (Computer Incident Response Center Luxembourg) is the national Computer Security Incident Response Team (CSIRT - CERT) coordination center for the Grand-Duchy of Luxembourg
www.dns-ok.nl	Dutch	SIDN (the Foundation for Internet Domain Registration in the Netherlands)
dns-ok.gov.au	English	CERT Australia, Stay Smart Online, and Australian Communications and Media Authority joint page on DNSChanger Information
dns-changer.eu	German, Spanish, English	ECO (Association of the German Internet Industry)
dnschanger.detect.my	Malaysian, English	Hosted by CyberSecurity Malaysia and MYCERT
dns-ok.jpcert.or.jp	Japanese	JPCERT/CC - Japan Computer Emergency Response Team Coordination Center
www.dns-ok.it	Italiano	Telecom Italia Security Operation Center - IT.TS.SOC

Manually Checking for DNS Changer Infections

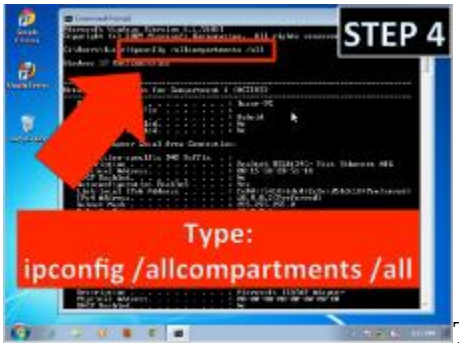
The following are the original manual checks to see if you computer is infected with any of the DNS Changer malware.

To check if your Windows 7 machine is infected, first click the "Start" icon.

This opens the Windows Menu. Click on the “Search” field at the bottom.



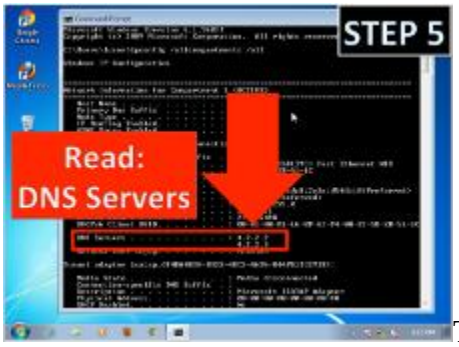
Type in **cmd**, and hit enter.



This opens a DOS shell. In the DOS shell, type in the command:

```
ipconfig /allcompartments /all
```

and hit enter. (Windows users might be used to just typing "`ipconfig /all`". This also works, but might not list all the routing compartments if you have a VPN setup in Windows7.)



The output will be very long, since Windows7 by default has support for IPv6. Most likely, you want to look for the IPv4 information under the section entitled "Ethernet adapter…". Look for the "DNS Servers" line, and write down these numbers. There may be two IP addresses listed there.

Are Your DNS Settings OK?

The malicious Rove viruses changed some peoples DNS settings to use computers they operated. Compare your DNS settings with the known malicious Rove DNS settings listed below:

Starting IP	Ending IP	CIDR
85.255.112.0	85.255.127.255	85.255.112.0/20
67.210.0.0	67.210.15.255	67.210.0.0/20
93.188.160.0	93.188.167.255	93.188.160.0/21
77.67.83.0	77.67.83.255	77.67.83.0/24
213.109.64.0	213.109.79.255	213.109.64.0/20
64.28.176.0	64.28.191.255	64.28.176.0/20

What if I'm infected?

If you computer is infected, please refer to our page that list tools to clean DNS Changer and other self help guides to clean your computer – http://www.dcwg.org/fix/

Checking OSX (MAC) for Infections

The easiest way to check if your system is violated with DNS Changer malware is to go to one of the "are you infected sites" (see below). These sites only require someone to visit. The "are you infected site" will inform you if you are infected.

Note: These sites only detect for DNS Changer. You might be infected with other malware. Please take appropriate precautions to protect your computer.

URL	Language	Maintainer
www.dns-ok.us	English	DNS Changer Working Group (DCWG)
www.dns-ok.de	German	Bundeskriminalamt (BKA) & Bundesamt für Sicherheit in der Informationstechnik (BSI)
www.dns-ok.fi	Finnish, Swedish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the

		national information security situation awareness system.
www.dns-ok.ax	Swedish, Finnish, English	CERT-FI is the Finnish national reporting point for computer security incidents and information security threats. CERT-FI is also responsible of maintaining the national information security situation awareness system.
www.dns-ok.be	Dutch/French	CERT-BE is the primary Belgian contact point for dealing with Internet security threats and vulnerabilities affecting Belgian interests.
www.dns-ok.fr	French	Le CERT-LEXSI est la division de veille et d'enquête sur Internet, dédiée à la protection du patrimoine en ligne des organisations.
www.dns-ok.ca	English/French	Canadian Internet Registration Authority (CIRA) and Canadian Cyber Incident Response Centre (CCIRC)
www.dns-ok.lu	English	CIRCL (Computer Incident Response Center Luxembourg) is the national Computer Security Incident Response Team (CSIRT - CERT) coordination center for the Grand-Duchy of Luxembourg
www.dns-ok.nl	Dutch	SIDN (the Foundation for Internet Domain Registration in the Netherlands)
dns-ok.gov.au	English	CERT Australia, Stay Smart Online, and Australian Communications and Media Authority joint page on DNSChanger Information
dns-changer.eu	German, Spanish, English	ECO (Association of the German Internet Industry)
dnschanger.detect.my	Malaysian, English	Hosted by CyberSecurity Malaysia and MYCERT
dns-ok.jpcert.or.jp	Japanese	JPCERT/CC - Japan Computer Emergency Response Team Coordination Center
www.dns-ok.it	Italiano	Telecom Italia Security Operation Center - IT.TS.SOC

Manually Checking for DNS Changer Infections

The following are the original manual checks to see if you computer is infected with any of the DNS Changer malware.

To check if your OSX computer is infected, first click the Apple icon in the top left.

Then, select “System Preferences…”

This opens the System Preferences dialog box. Locate the "network" icon. **HINT:** Type "network" in the top right corner search field.

This opens the Network settings dialog box. Read the "DNS Server" line. Write down these IP addresses.

Are Your DNS Settings Ok?

The malicious Rove viruses changed some peoples DNS settings to use computers they operated. Compare your DNS settings with the known malicious Rove DNS settings listed below:

Starting IP	Ending IP	CIDR
85.255.112.0	85.255.127.255	85.255.112.0/20

67.210.0.0	67.210.15.255	67.210.0.0/20
93.188.160.0	93.188.167.255	93.188.160.0/21
77.67.83.0	77.67.83.255	77.67.83.0/24
213.109.64.0	213.109.79.255	213.109.64.0/20
64.28.176.0	64.28.191.255	64.28.176.0/20

What if I'm infected?

If you computer is infected, please refer to our page that list tools to clean DNS Changer and other self help guides to clean your computer – http://www.dcwg.org/fix/

Why am I visiting this page?

You're looking for information on how to clean up or fix malicious software ("malware") associated with DNS Changer. It's possible that either your computer or your home router has been modified to use resources once controlled by criminals to redirect your traffic. You can find more information about this malware on our main page:

- http://www.dcwg.org

or visiting the FBI page about DNS Changer:

- http://www.fbi.gov/news/stories/2011/november/malware_110911

If you think you have been affected by this malware, you do need to fix your computer. The malware tool kits used that change your computer's DNS settings are very pervasive. Initially, the only way researchers could ensure that a machine was fixed was to reformat the hard drive and reinstall the operating system from scratch. The malware affected the boot blocks on the

hard disk of the computer, so even if people just reverted their operating system to a prior backup, the malware could reclaim the PC. Later on, several anti-malware software companies came up with fixes that removed software correctly. Some of them are listed below.

In addition to modifying your computer's DNS settings, the malware also looked for home routers to which the computer was attached and modified their DNS settings as well. Not only were the infected computers using rogue DNS services, but other devices in the household or office as well, including wifi-enabled mobile phones, tablets, smart HDTVs, digital video recorders, and game consoles. The criminals would change the web content that users downloaded to suit their needs and make money.

Below are some steps to follow:

1. The first thing you want to do is make a backup of all of your important files. You might go to a computer store or shop online for a portable hard drive and copy all of your files onto that drive.
2. Either you or a computer professional that you rely upon and trust should follow the "self help" malware clean up guides listed below. The goal is to remove the malware and recover your PC from the control of the criminals that distributed it. If you were already thinking of upgrading to a new computer, now may be a good time to make the switch.
3. Once you have a clean PC, follow instructions for ensuring that your DNS settings are correct. If you're not using a new PC, you'll want to check that your computer's DNS settings are not still using the DNS Changer DNS servers. We hope to have some of our own instructions soon. Until then, the instructions and screen shots found in step 2 at http://opendns.com/dns-changer are quite good if you want to manually set your DNS settings. You also have the option to return to using your ISP-provided automatic settings by choosing the "automatically" option (Windows) or deleting any DNS servers listed (MacOS).
4. After you have fixed your computer, you will want to look at any home router you're using and make sure they automatically use DNS settings provided by the ISP. We'll have a document for this soon.
5. Changing DNS is only one of the functions of the malware kits. The malware could have been used for capturing keystrokes or acting as a proxy for traffic to sensitive sites like bank accounts or social media. It would be a good idea to check your bank statements and credit reports as well as change passwords on any online accounts especially saved passwords from your applications or web browsers.

How can you fix, remove, and recover from a DNS Changer Violation?

Please take immediate steps to safe guard your computer and data if any of the test indicate that you might be violated with DNS Changer. If the Check-Up Site indicates that you are affected then either follow the instructions on that site ***or*** run one of the following free tools listed below to remove DNSChanger and related threats:

Name of the Tool	URL
Hitman Pro (32bit and 64bit versions)	http://www.surfright.nl/en/products/
Kaspersky Labs TDSSKiller	http://support.kaspersky.com/faq/?qid=208283363
McAfee Stinger	http://www.mcafee.com/us/downloads/free-tools/stinger.aspx
Microsoft Windows Defender Offline	http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline
Microsoft Safety Scanner	http://www.microsoft.com/security/scanner/en-us/default.aspx
Norton Power Eraser	http://security.symantec.com/nbrt/npe.aspx
Trend Micro Housecall	http://housecall.trendmicro.com
MacScan	http://macscan.securemac.com/
Avira	http://www.avira.com/en/support-for-home-knowledgebase-detail/kbid/1199 Avira's DNS Repair-Tool

How can I use these tools to clean my computer?

Each of these tools has instructions for their use. BUT, the best recommendation is to use one of the proven "self help" malware clean up guides – using several tools to insure you clean all the infections from your computer. Most malware will disable your software and anti-virus updates. The procedures below address that problem, using several tools to remove the blocks, remove the malware, and then update your computer.

Guide	How to Use	Language
Microsoft's Safety and Security Center	Microsoft's authoritative portal for all their security guidance, tools, and capabilities.	English
Apple's Security Page with pointers to keep your MAC safe	Scroll down to the section on "Checking Security in your System." This has the pointers to insure your MAC is as secure as possible.	English
DSL Report's Security Cleanup FAQ	A community driven self help guide to fix malware problems on your systems.	English
Andrew K's Malware Removal Guide	Andrew K is an individual who share's his experience on-line. This guide is an often referenced guide to remediate malware problems on a computer.	English
Public Safety Canada'a Malware Infection Recovery	The Canadian Public Safety office (publicsafety.gc.ca) has a malware removal guide updated and focused to help the	English

Guide	general population.	
Australia's Stay Smart Online Factsheet to help Remove Malware	Stay Smart Online Factsheet 11, Part 1 - You suspect your computer is infected with malicious software - what should I do?	English

References to Sites on DNSChanger

The following are validated site with accurate information about DNSChanger and what you can do to check to see if you are violated with the malware and what you can do to remediate the problem.

- INTECO-CERT's DNSChanger Information page. (Spanish) DNSChanger Information