DNSChanger Malware

DNS (Domain Name System) is an Internet service that converts user-friendly domain names into the numerical Internet protocol (IP) addresses that computers use to talk to each other. When you enter a domain name, such as www.fbi.gov, in your web browser address bar, your computer contacts DNS servers to determine the IP address for the website. Your computer then uses this IP address to locate and connect to the website. DNS servers are operated by your Internet service provider (ISP) and are included in your computer's network configuration. DNS and DNS Servers are a critical component of your computer's operating environment—without them, you would not be able to access websites, send e-mail, or use any other Internet services.

Criminals have learned that if they can control a user's DNS servers, they can control what sites the user connects to on the Internet. By controlling DNS, a criminal can get an unsuspecting user to connect to a fraudulent website or to interfere with that user's online web browsing. One way criminals do this is by infecting computers with a class of malicious software (malware) called DNSChanger. In this scenario, the criminal uses the malware to change the user's DNS server settings to replace the ISP's good DNS servers with bad DNS servers operated by the criminal. A bad DNS server operated by a criminal is referred to as a rogue DNS server.

The FBI has uncovered a network of rogue DNS servers and has taken steps to disable it. The FBI is also undertaking an effort to identify and notify victims who have been impacted by the DNSChanger malware. One consequence of disabling the rogue DNS network is that victims who rely on the rogue DNS network for DNS service could lose access to DNS services. To address this, the FBI has worked with private sector technical experts to develop a plan for a private-sector, non-government entity to operate and maintain clean DNS servers for the infected victims. The FBI has also provided information to ISPs that can be used to redirect their users from the rogue DNS servers to the ISPs' own legitimate servers. The FBI will support the operation of the clean DNS servers for four months, allowing time for users, businesses, and other entities to identify and fix infected computers. At no time will the FBI have access to any data concerning the Internet activity of the victims.

It is quite possible that computers infected with this malware may also be infected with other malware. The establishment of these clean DNS servers does not guarantee that the computers are safe from other malware. The main intent is to ensure users do not lose DNS services.

What Does DNSChanger Do to My Computer?

DNSChanger malware causes a computer to use rogue DNS servers in one of two ways. First, it changes the computer's DNS server settings to replace the ISP's good DNS servers with rogue DNS servers operated by the criminal. Second, it attempts to access devices on the victim's small office/home office (SOHO) network that run a dynamic host configuration protocol (DHCP) server (eg. a router or home gateway). The malware attempts to access these devices using common default usernames and passwords and, if successful, changes the DNS servers these devices use from the ISP's good DNS servers to rogue DNS servers operated by the criminals. This is a change that may impact all computers on the SOHO network, even if those computers are not infected with the malware.

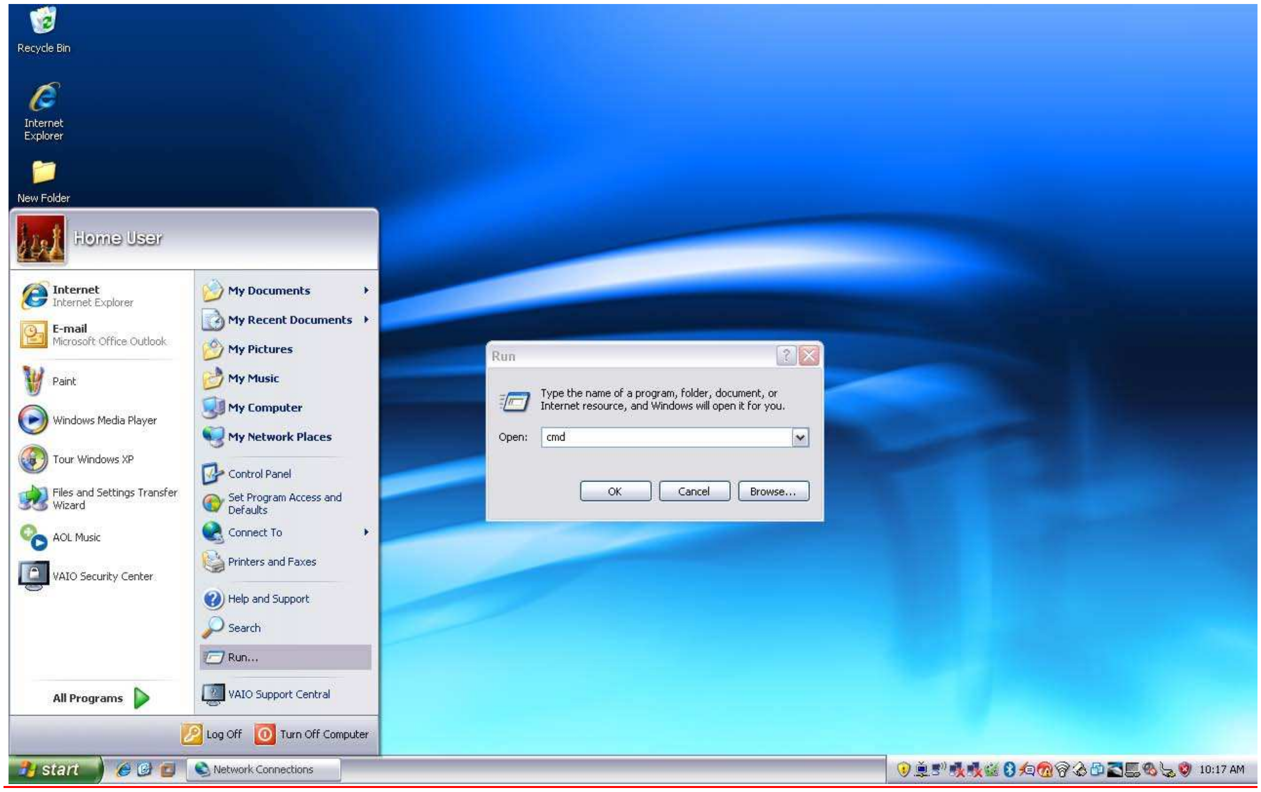
Am I Infected?

The best way to determine if your computer or SOHO router has been affected by DNSChanger is to have them evaluated by a computer professional. However, the following steps can help you gather information before consulting a computer professional.

To determine if a computer is using rogue DNS servers, it is necessary to check the DNS server settings on the computer. If the computer is connected to a wireless access point or router, the settings on those devices should be checked as well.

Checking the Computer:

If you are using a Windows computer, open a command prompt. This can be done by selecting Run from the Start Menu and entering cmd.exe or starting the command prompt application, typically located in the Accessories folder within Programs on your Start Menu, as shown below:



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

At the command prompt, enter:

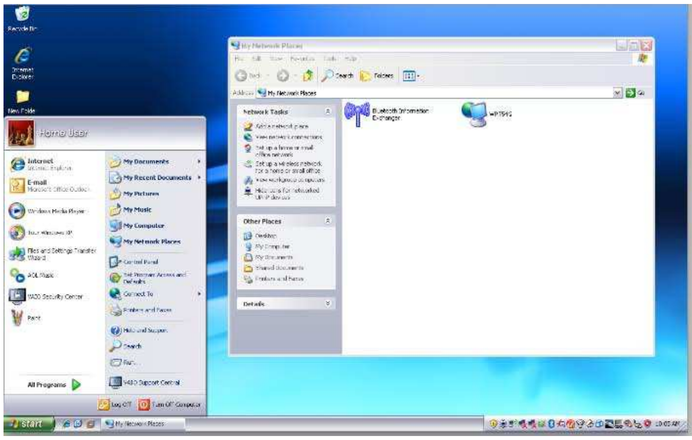
ipconfig / all

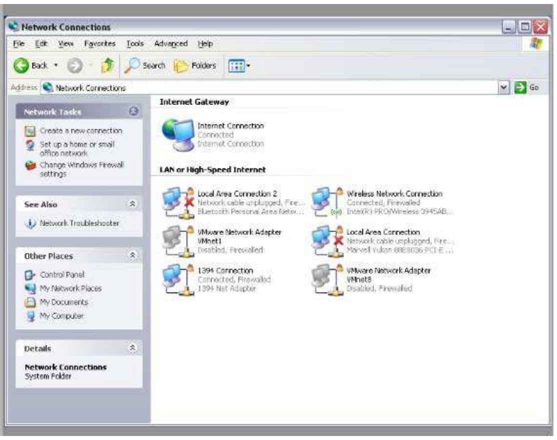
Look for the entry that reads "DNS Servers………"

The numbers on this line and the line(s) below it are the IP addresses for your DNS servers. These numbers are in the format of nnn.nnn.nnn.nnn, where nnn is a number in the range of 0 to 255. Make note of the IP addresses for the DNS servers and compare them to the table of known rogue DNS servers listed later in this document. If the IP addresses of your DNS server appear in the table below, then the computer is using rogue DNS.

You can also look for your DNS servers without using the command prompt.

For windows XP machines, click on Start and select My Network Places. Then select Network Connections. In this example, the wireless connection is used.





Network Connections
System Folder

Internet Gateway

Internet Connection
Connected
Internet Connection

LAN or High-Speed Internet

Local Area Connection 2
Network cable unplugged, Fire...
Bluetooth Personal Area Netw...

Wireless Network Connection
Connected, Firewalled
Intel(R) PRO/Wireless 3945AB...

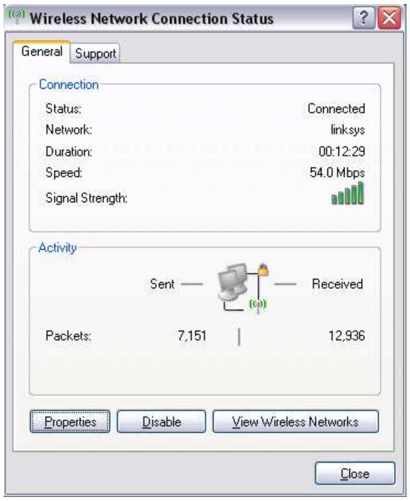
VMware Network Adapter VMnet1
Disabled, Firewalled

Local Area Connection
Network cable unplugged, Fire...
Marvell Yukon 88E8036 PCI-E ...

1394 Connection
Connected, Firewalled
1394 Net Adapter

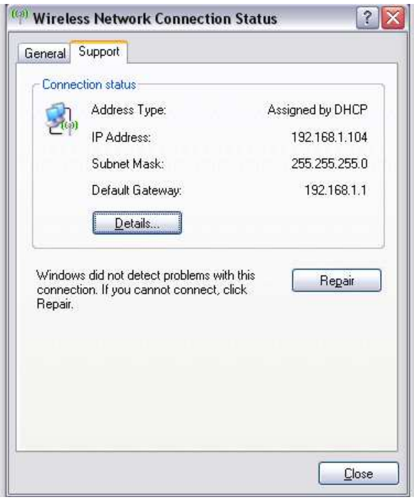
VMware Network Adapter VMnet8
Disabled, Firewalled

Click on the connection that is active. This will bring up the Network Connection Status screen. Click on Support and then Details. Check for the values that correspond to the DNS servers.



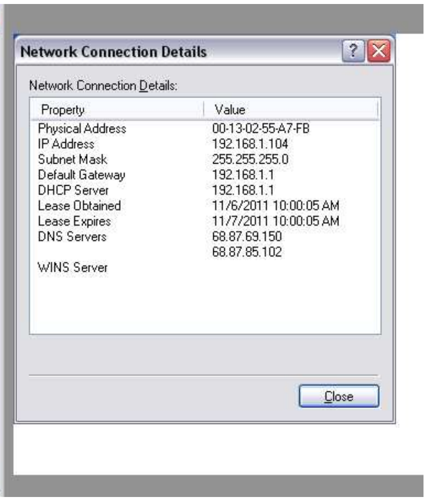
Status: Connected
Network: linksys
Duration: 00:12:29
Speed: 54.0 Mbps
Signal Strength:

Packets: 7,151 | 12,936



Address Type: Assigned by DHCP
IP Address: 192.168.1.104
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

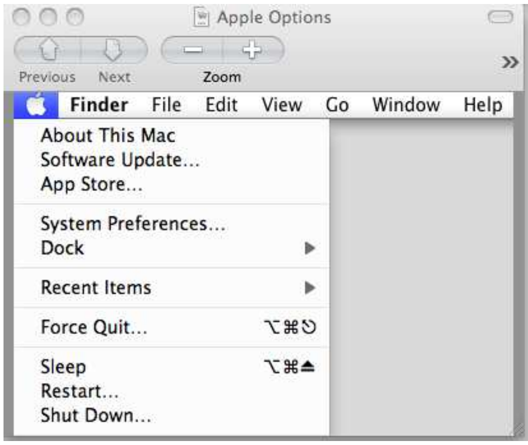
Windows did not detect problems with this connection. If you cannot connect, click Repair.

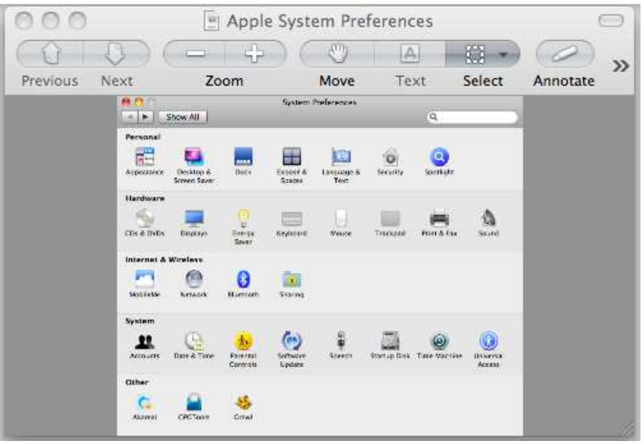


Network Connection Details:

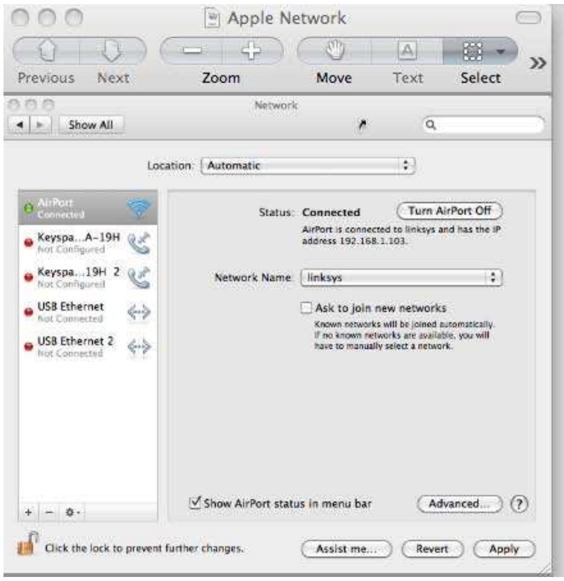
Property	Value
Physical Address	00-13-02-55-A7-FB
IP Address	192.168.1.104
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	192.168.1.1
Lease Obtained	11/6/2011 10:00:05 AM
Lease Expires	11/7/2011 10:00:05 AM
DNS Servers	68.87.69.150 68.87.85.102
WINS Server	

If you are using an Apple computer, click on the Apple in the top left corner and choose System Preferences. Then, from the Apple System Preferences window, choose Network.





The Apple Network pane will show a number of possible connections on the left side. Choose the one that is active for you and click on the Advanced button in the right lower corner. Then choose DNS from the options to show the DNS servers you are using.



Location: Automatic

Status: Connected

AirPort is connected to linksys and has the IP address 192.168.1.103.

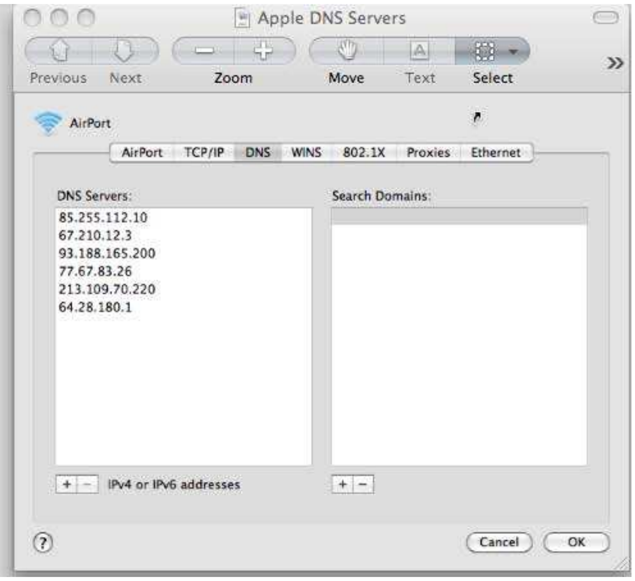
Network Name: linksys

□ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

☑ Show AirPort status in menu bar

Click the lock to prevent further changes.



DNS Servers:

85.255.112.10
67.210.12.3
93.188.165.200
77.67.83.26
213.109.70.220
64.28.180.1

IPv4 or IPv6 addresses

Search Domains:

Compare whether your computer has DNS servers listed in the number ranges listed below.

Rogue DNS Servers

85.255.112.0 through 85.255.127.255	To make the comparison between the computer's DNS servers and this table easier, start by comparing the first number before the first dot. For example, if your DNS servers do not start with 85, 67, 93, 77, 213, or 64, you can move on to the next step. If your servers start with any of those numbers, continue the comparison.
67.210.0.0 through 67.210.15.255	
93.188.160.0 through 93.188.167.255	
77.67.83.0 through 77.67.83.255	
213.109.64.0 through 213.109.79.255	
64.28.176.0 through 64.28.191.255	

If your computer is configured to use one or more of the rogue DNS servers, it may be infected with DNSChanger malware.

Home computers with high-speed Internet connections and office computers typically obtain their IP settings via DHCP from a device on the network. In these cases, the computers are provided with an IP address, default gateway, and DNS server settings. The IP addresses usually fall into one of three ranges of private addresses—192.168.0.0 to 192.168.255.255; 172.16.0.0 to 172.31.255.255; and 10.0.0.0 to 10.255.255.255. In most homes, computers are assigned an IP address in the range 192.168.1.2 to 192.168.1.254, and the default gateway and DNS servers are set to 192.168.1.1. To determine if your computer is utilizing the rogue DNS servers, read the next section, *Checking the Router.*

If you are unable to locate your DNS server settings, obtain assistance from the Help program bundled with your operating system, reputable online sources, or a trusted professional.

Checking the Router

Small office/home office routers connect your network of computers and devices to your Internet service provider. The SOHO router may have been purchased and installed by you or installed by your ISP. Linksys, D-Link, Netgear, and Cisco are common SOHO router brands, but there are many others.

The DNSChanger malware is capable of changing the DNS server settings within SOHO routers that have the default username and password provided by the manufacturer. If you did not change the default password at the time the SOHO router was installed, you must check the SOHO router settings.

The procedure to access your SOHO router setting varies by manufacturer, so consult your product documentation. Once you have access to the SOHO router configuration, compare the DNS servers listed to those in the rogue DNS servers table above. If your SOHO router is configured to use one or more of the rogue DNS servers, a computer on your network may be infected with DNSChanger malware.

What Should I Do?

In addition to directing your computer to utilize rogue DNS servers, the DNSChanger malware may have prevented your computer from obtaining operating system and anti-malware updates, both critical to protecting your computer from online threats. This behavior increases the likelihood of your computer being infected by additional malware. The criminals who conspired to infect computers with this malware utilized various methods to spread the infections. At this time, there is no single patch or fix that can be downloaded and installed to remove this malware. Individuals who believe their computer may be infected should consult a computer professional.

Individuals who do not have a recent back-up of their important documents, photos, music, and other files should complete a back-up before attempting to clean the malware or utilize the restore procedures that may have been packaged with your computer.

Information regarding malicious software removal can be found at the website of the United States Computer Emergency Readiness Team: https://www.us-cert.gov/reading_room/trojan-recovery.pdf.