# Der aktuelle Fall „DNSChanger“ – was Computernutzer jetzt tun können

## Inhalt

## Was bisher geschah

Der Fahndungserfolg von FBI und anderen internationalen Behörden wurde in den Medien als Durchbruch gemeldet: die Drahtzieher hinter der Aktion seien festgenommen und die DNS-Server aus der Kontrolle der Täter schließlich in die Hände des FBI gelangt. Das FBI kann zwar diese DNS-Server unter Kontrolle haben, jedoch können sie nicht die mit „DNSChanger" infizierten Computer säubern. Nun gilt es also, alle betroffenen Computerbenutzer von unfreiwillig veränderten DNS-Einstellungen zu befreien, und ihnen dadurch auch nach dem 8. März 2012 eine reibungslose Kommunikation mit dem WWW zu ermöglichen.

Zum Verständnis sollten zwei unterschiedliche Ausprägungen der Schädlinge „DNSChanger" dargestellt werden:

**Ausprägung 1:** Der Schädling modifiziert die DNS-Einstellungen unter Windows auf dem befallenen Computer. Zu diesen Einstellungen zählen: die „hosts"-Datei und die DHCP-Einstellungen.
Werden die DNS-Einstellungen verändert, bedeutet das, dass der Computernutzer nicht mehr auf die Webseite gelangt, die er in der Browser-Adresszeile einträgt, sondern immer an ein vom Angreifer definiertes Ziel umgeleitet wird.

**Ausprägung 2:** Der Schädling verändert Nameserver-Einträge im Router.
Das bedeutet, dass die oben genannten Veränderungen nicht direkt auf einem PC stattfinden, sondern auf dem Router, der z.B. das Heimnetzwerk mit dem Internet verbindet.

Der Trojaner bringt Passwortlisten mit, die Standard-Logins für die gängigsten Router enthalten und ermöglicht so den Zugriff auf das Webinterface des Routers. Ist der Zugriff mittels der Passwortlisten möglich, weil unter Umständen das Standard-Passwort durch den Benutzer nicht verändert wurde, verändert der Schädling die Nameserver Eintragungen des Providers mit den IP-Adressen, die die Bösewichte für ihre Zwecke benötigen. Folglich ist dann jeder Webseitenaufruf des Benutzers seitens der Angreifer kontrollierbar.

## Was passiert am 8. März 2012?

An diesem Tag wird das FBI die DNS-Server abschalten, die sie aus der Kontrolle der Kriminellen übernommen haben. Das bedeutet, dass alle Computer, die

a) mit der von den Bösewichten verbreiteten „DNSChanger" Malware infiziert wurden und
b) bis zu diesem Datum ihre DNS-Einstellungen nicht auf „normal" gesetzt haben,

werden nach dem Abschalten der vom FBI kontrollierten DNS-Server mit Problemen bei der Verbindung zum Internet rechnen müssen.

# Wie teste ich meine Interneteinstellungen?

Wir stellen an dieser Stelle Maßnahmen vor, die Benutzer von Computern mit Windows Betriebssystemen (XP, Vista, 7) selbst durchführen können, um ihren PC auf unmittelbare Schäden durch „DNSChanger" Malware zu überprüfen.
Sollte es sich bei dem zu überprüfenden Gerät um einen Rechner in einem Firmennetzwerk handeln, kontaktieren Sie zunächst Ihren Systemadministrator.

Bevor Sie mit der unten beschriebenen manuellen Prüfung der Interneteinstellungen beginnen, führen Sie einen kompletten Antivirus-Scan auf ihrem gesamten Rechner durch. Anschließend besuchen Sie die Webseite: www.dns-ok.de. Erhalten Sie auf dieser Webseite eine Warnanzeige (siehe Screenshot 1), sind die nachfolgend genannten Schritte unerlässlich.


**Screenshot 1:** Die Warnanzeige auf der Webseite dns-ok.de. Sie weist darauf hin, dass die DNS-Einstellungen des besuchenden Computers nicht korrekt sind!

Zeigt Ihnen die Webseite einen grünen Balken an, sind die DNS-Einstellungen in ihrem System und Router korrekt und eine Manipulation durch den aktuellen „DNSChanger" Schadcode liegt nicht vor. Bitte beachten Sie, dass für eine korrekte Durchführung dieses Tests auf der Webseite keine Proxy-Einstellungen im Browser aktiviert sein dürfen.

**Achtung:** Sollten Sie mit dem Online-Test und auch nach den unten aufgeführten manuellen Tests feststellen, dass all Ihre DNS-Einstellungen einwandfrei sind, bedeutet das nicht, dass ihr Computer generell frei von Schadcode ist! Bitte führen Sie in jedem Fall regelmäßige Überprüfungen ihres Rechners mit Hilfe einer umfassenden und aktuellen Antiviren-Lösung durch, z.B. der G Data InternetSecurity 2012 mit BootCD.

## Auf dem PC

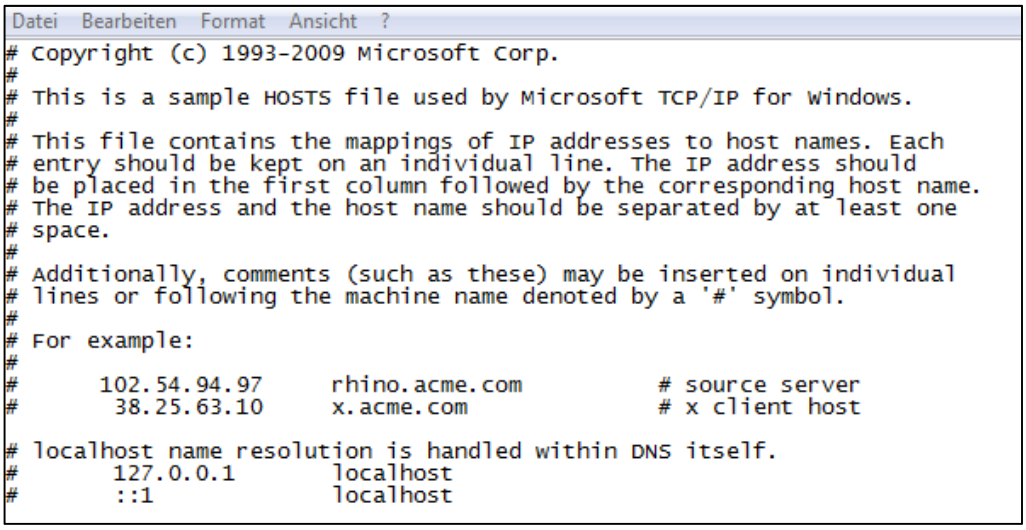
Schritt 1: Überprüfung der „hosts"-Datei

Öffnen Sie einen Texteditor. Führen Sie ihn in unter Windows Vista und Windows 7 als Administrator aus. Machen Sie dazu einen Rechtsklick auf die ausführbare Datei des Texteditors, und klicken dann mit links auf „Als Administrator ausführen".

Öffnen Sie nun in diesem Texteditor die „hosts"-Datei. Sie befindet sich unter Windows in **C:\Windows\system32\drivers\etc**.
Wenn Sie diesen Dateipfad erreicht haben, müssen Sie sehr wahrscheinlich in der Dateiauswahl-Maske (unten rechts) die Auswahl „Alle Dateien (*.*)" auswählen, um die „hosts"-Datei zu sehen.

Unter Microsoft Windows XP ist in dieser Datei standardmäßig nur ein Eintrag: localhost wird hierbei an die IP Adresse 127.0.0.1 gebunden.

Bei den Betriebssystemen Microsoft Windows Vista und Microsoft Windows 7 existieren standardmäßig keine Eintragungen in dieser Datei. Bei Zeilen, die mit einer Raute (#) beginnen, handelt es sich um einen Kommentar und diese Zeilen müssen nicht weiter beachtet werden.



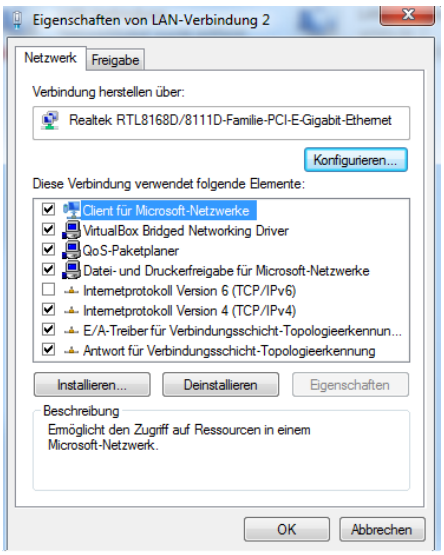

**Screenshot 2:** Eine „hosts"-Datei in Windows 7 mit auskommentierten IP-Adressen.

Sollten sich, egal in welchem Betriebssystem, in der „hosts"-Datei weitere Eintragungen befinden, ohne eine Raute am Anfang der Zeile, kann dies ein Indiz für eine Modifikation durch Schadsoftware sein.

Zur Überprüfung können Sie folgendes tun: Schreiben Sie vor die weiteren Einträge in der Liste jeweils eine Raute (#).
Starten Sie dann ggf. Ihren Browser neu und machen Sie den Test auf http://dns-ok.de.

## Schritt 2: Überprüfung der DHCP Einstellungen

Für Windows XP klicken Sie auf Start > Systemsteuerung > Netzwerkumgebung. Wählen Sie dort die Netzwerkverbindung aus, über die Sie die Internetverbindung herstellen.
Bei Windows Vista und Windows 7 klicken Sie Start > Systemsteuerung > Netzwerk und Internet > Netzwerk und Freigabecenter und wählen dort ebenfalls die Netzwerkverbindung aus, mit der die Internetverbindung hergestellt wird.




**Screenshot 3:** Optionen der aktiven Lan-Verbindung

Über den Menüpunkt „Eigenschaften" öffnet sich ein Fenster (siehe Screenshot 3). Dort wählen Sie Internetprotokoll (TCP/IP) für Windows XP und Internetprotokoll Version 4 (TCP/IPv4) für Windows Vista und Windows 7 aus. In allen Fällen sollte „IP Adresse automatisch beziehen" und „DNS-Serveradresse automatisch beziehen" aktiviert sein. Sollte ein unbekannter DNS-Server angegeben sein, löschen Sie den Eintrag und aktivieren „DNS-Serveradresse automatisch beziehen".

Abschließend starten Sie die Eingabeforderung (Start > Ausführen > *cmd*). Windows Vista Benutzer müssen die Eingabeforderung als Administrator starten, damit dieser

Vorgang funktioniert. Geben Sie nun *ipconfig /flushdns* ein und bestätigen die Eingabe mit der Return-Taste. Dadurch wird der DNS-Speicher geleert. Starten Sie ggf. Ihren Browser neu und machen Sie den Test auf http://dns-ok.de.

Schritt 3: Überprüfung der Browsereinstellungen

### Microsoft Internet Explorer (Version 9)

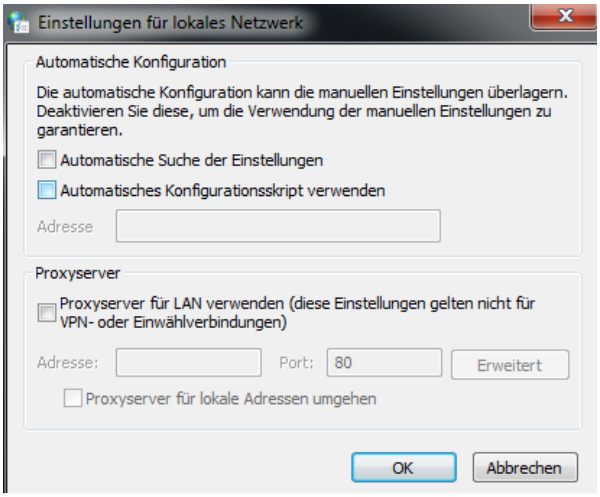
Klicken Sie im Internet Explorer auf Extras > Internetoptionen und wählen Sie die Registerkarte Verbindungen aus. Klicken Sie auf „LAN-Einstellungen" und überprüfen, ob einer der drei möglichen Haken gesetzt ist. Hier sollte standardmäßig keine der Optionen ausgewählt sein.

### Mozilla Firefox (Version 9)

Klicken Sie im Mozilla Firefox auf Extras > Einstellungen > Erweitert und wählen Sie dort den Menüpunkt „Netzwerk" aus. Klicken Sie auf „Einstellungen" und überprüfen, ob unter „Manuelle Proxy-Konfiguration" eine Eintragung stattgefunden hat. Standardmäßig sollte die Option „Kein Proxy" ausgewählt sein.

### Google Chrome (Version 16)

Klicken Sie auf „Google Chrome anpassen" und wählen den Menüpunkt „Details" aus. Im Abschnitt „Netzwerk" klicken Sie auf "Proxy-Einstellungen ändern". Da Google Chrome die Proxy-Einstellungen des Systems verwendet, sind die Einstellungen äquivalent zu denen des Internet Explorers.




**Screenshot 4:** Die Proxy-Einstellungen des Systems

Klicken Sie im sich öffnenden Fenster des Internet Explorers auf „LAN-Einstellungen" und überprüfen, ob einer der drei möglichen Haken gesetzt ist. Hier sollte standardmäßig keine der Optionen ausgewählt sein.

Nach der Überprüfung ihres Browsers starten Sie diesen ggf. neu und machen den Test auf http://dns-ok.de

## Auf dem Router

Schritt 4: Überprüfung der Netzwerkeinstellung des Routers

Sollten mehrere Computer in ihrem lokalen Netzwerk von der Problematik betroffen sein, rufen Sie das Webinterface Ihres Routers auf. Den konkreten Zugriff entnehmen Sie bitte der Gebrauchsanleitung Ihres Routers.

In den Standardeinstellungen sollte „IP-Adresse automatisch über DHCP beziehen" aktiviert sein. Sind an dieser Stelle jedoch DNS-Server eingetragen, entfernen Sie diese. Starten Sie den Router

neu.
Anschließend starten Sie die auf einem Computer des Netzwerks die Eingabeforderung (Start > Ausführen > *cmd*). Windows Vista Benutzer müssen die Eingabeforderung als Administrator starten, damit dieser Vorgang funktioniert. Geben Sie nun *ipconfig /flushdns* ein und bestätigen die Eingabe mit der Return-Taste. Dadurch wird der DNS-Speicher geleert. Starten Sie ggf. Ihren Browser neu und machen Sie den Test auf http://dns-ok.de.

Außerdem sollten Sie aus Sicherheitsgründen das Zugangspasswort zu Ihrem Router unverzüglich ändern. Ganz besonders dann, wenn Sie das ab Werk vergebene Standardpasswort noch nie geändert haben und auch, wenn an Ihrem Router Einstellungen vorgenommen wurden, die nicht von einem dazu Berechtigten durchgeführt wurden.

**Achtung:** Sollten Sie mit dem Online-Test und nach den beschriebenen manuellen Tests feststellen, dass all Ihre DNS-Einstellungen einwandfrei sind, bedeutet das nicht, dass ihr Computer generell frei von Schadcode ist! Bitte führen Sie in jedem Fall regelmäßige Überprüfungen ihres Rechners mit Hilfe einer umfassenden und aktuellen Antiviren-Lösung durch, z.B. der G Data InternetSecurity 2012 mit BootCD.

## Allgemeine Tipps

- G Data rät zudem zu einer umfassenden Sicherheitslösung, die den http-Traffic permanent auf Schadcode untersucht. PCs sind so vor Infektionen durch Drive-by-Downloads wirksam geschützt. Ein Spam-Filter zur Abwehr von unerwünschten E-Mails ist ebenfalls ein Muss.
- Halten Sie Ihr Betriebssystem, den oder die Browser und seine Komponenten sowie die installierte Sicherheitslösung immer auf dem aktuellen Stand. Installieren Sie Programm-Updates umgehend, um so bestehende Sicherheitslücken zu schließen.
- Ändern Sie die ab Werk eingestellten Passwörter bei Geräten umgehend nach der Einrichtung dieser Geräte.
- Sollten Sie auf Ihrem Computer eine Infektion mit Schadcode festgestellt haben, ändern Sie alle verwendeten Passwörter, z.B. für (online abgerufene) E-Mail Konten, Online-Banking, Shoppingportale, Soziale Netzwerke, Instant Messenger und vieles mehr.