REMINDER: **Emailed to a group account. Do NOT reply using email group account.**
For comments or inquiries email infosec@pjlhuillier.com.

infosec@pjlhuillier.com ICT GROUP INFOSEC 101 CONFIDENTIALITY • INTEGRITY • AVAILABILITY

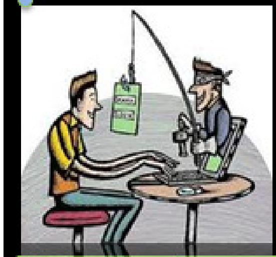
August 10, 2012 Release # 178

-- Begin Transmission --

DNS Changer Malware – Final Part

DNS Changer Malware

Why should users be concerned with this threat?
DNS changer Trojans may lead to a lot of problems for users, including:



No control over network traffic: DNS changer Trojans can lead victims to any site that cybercriminals choose. Such control makes DNS changer Trojans effective phishing or pharming tools. Users are still directed to a spoofed site even if they type in the correct URL.

Information theft: Cybercriminals can use DNS changer Trojans to steal victims' personal information.

Infection of connected systems: Some DNS changer Trojans can alter routers' DNS settings via brute-force attacks - a method used by application programs to crack encrypted data, such as passwords As a result, all systems connected to the "infected" router also become infected.

Disablement of security updates: Infected systems become more prone to even more infections since DNS changer Trojans often prevent access to security vendors' update download sites.

Exposure to rootkit infections: DNS changer Trojans are unobtrusive and may have rootkit capabilities. This makes detection and removal from systems even harder. Because of their stealthy nature, DNS changer Trojans will keep modifying an infected system's DNS settings to keep pointing to malicious DNS servers.

How can affected users get rid of DNS changer Trojans?

Affected users should reset the DNS settings of their systems after getting rid of DNS changer Trojans using their anti-malware solutions. To manually reset your DNS settings, follow these steps:

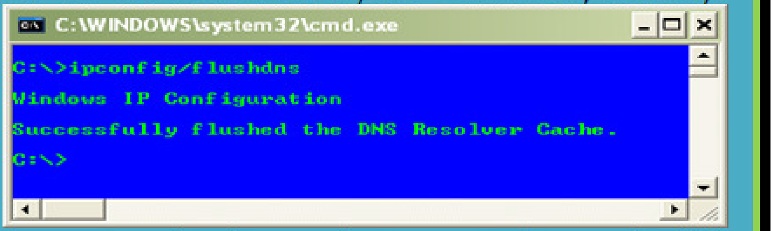
•Back up all of your important files onto a portable hard drive.

•Scan your system with updated Anti-virus and remove the DNS changer Trojans found in your computer.

•You can also do these manual steps to refresh your DNS settings. On your Microsoft Windows 7 operating system, reset your DNS settings by clicking the Start button or the Windows icon on the lower-left part of your screen. Type cmd in the Search box and hit the Enter key. For Windows XP, click Run, type cmd then hit the Enter key.

•In the Command Prompt window, type **ipconfig/flushdns** then hit the Enter key.

•A prompt saying, "Successfully flushed the DNS Resolver Cache" will appear.



```
C:\>ipconfig/flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\>
```

•After fixing your computer, look at your home router and make sure this automatically uses the DNS settings provided by your ISP. You'll need your ISP's help in resetting the DNS settings of your router.

•Changing your system's DNS settings is just one of the functions of DNS changer Trojans. It is a good idea to check your bank statements and credit reports, especially those saved in applications and web browsers, to make sure there are no unwanted charges or transactions. Change your online account passwords as well.

-- End of Transmission --

Information Security: It's a Shared Responsibility
REFERENCE(S): http://What-are-Phishing-and-Pharming? http://What-is-Rootkit? http://about-threats.trendmicro.com

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.

Document Code: 2012ICT_15SECAD031