

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



August 3, 2012 Release # 177

-- Begin Transmission --

## DNS Changer Malware – Part 1

# DNS Changer Malware

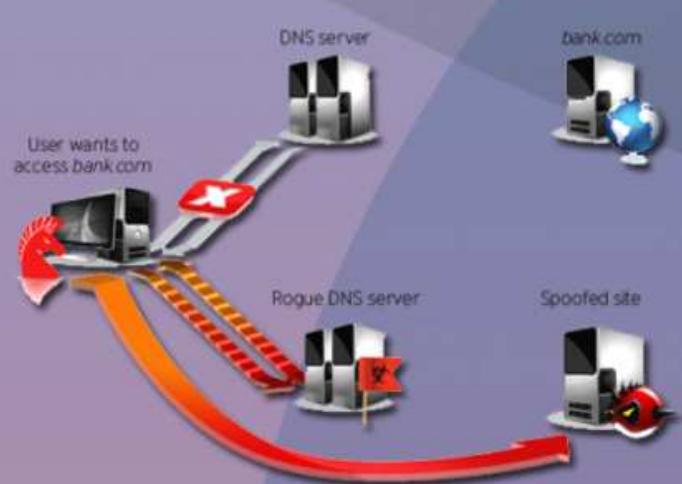


**What is DNS?**  
DNS stands for "Domain Name System." It is the Internet standard for assigning IP addresses (119.92.167.154) to domain names such as [pjlhuillier.com](http://pjlhuillier.com). A DNS acts like a phone book that translates human-friendly host names to PC-friendly IP addresses. Pjlhuillier.com is easier to remember than 119.92.167.154.



**What are DNS changer Trojans?**  
DNS changer Trojans are malware designed to modify infected systems' DNS settings without the users' knowledge or consent. Once modified, systems use foreign DNS servers, which are usually set up by cybercriminals. Users with infected systems who try to access certain sites are instead redirected to malicious sites.

**How a DNS Changer Trojan infects users' systems:**



**How do DNS changer Trojans work?**

DNS changer Trojans are dropped onto systems by other malwares. Once installed, DNS changer Trojans silently modify infected systems' DNS settings. Cybercriminals do this so victims would use foreign DNS servers instead of the ones provided by their Internet Service Providers. They set up DNS servers to resolve certain domains to malicious IP addresses.

Modifying systems' DNS settings allows cybercriminals to perform malicious activities like:

- Steering unknowing users to bad sites:** These sites can be phishing pages that spoof well-known sites in order to trick users into handing out sensitive information. A user who wants to visit his bank site, for instance, is instead unknowingly redirected to a rogue site.
- Replacing ads on legitimate sites:** Visiting certain sites can serve users with infected systems a different set of ads from those whose systems are not infected.
- Controlling and redirecting network traffic:** Users of infected systems may not be granted access to download important software updates from vendors like Microsoft and from their respective security vendors.
- Pushing additional malware:** Infected systems are more prone to other malware infections (e.g., FAKEAV infection).

To be continued...

-- End of Transmission --

**Information Security:** It's a Shared Responsibility  
REFERENCE(S): [When Stalking Goes Online](#)

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

Document Code: 2012ICT\_15SECAD030