

Exploitation of routers using alternate DNS servers

This project will use an already discovered flaw in Eircom's Netopia routers to prove that using just free and readily available tools these boxes could be exploited and steal credit card information, passwords and other sensitive information from unsuspecting broadband users. And it can all be done from a remote location and give the perpetrator almost complete anonymity. I got this idea after watching a TV show called "The Real Hustle" on the BBC where they setup a wireless access point that captured credit card details, but I thought I could expand on that and cause it to happen to an unsuspecting home broadband user whether they are using a wireless or wired connection.

To do this I shall use 3 computers running linux or mac to experiment with the software required. I will test several different configurations of each of the pieces of software to see what works the best and how effective each are at capturing data. I will also experiment with an Eircom router to see how efficiently one could change the DNS servers on the box. I would configure a DNS server on a 'server' machine that redirected all internet traffic to itself, it would then use a web server with a proxy server which would make everything appear as if it was functioning correctly. This proxy server would be setup to redirect users when they browse to a payment page, the server would then capture the details when they were entered and the user would not suspect that their credit card details had been captured until money disappeared from their account. The level of data capture could be increased by adding low-level packet sniffing using DHCP spoofing or ARP poisoning, and TCP packet capture program. This could be used to capture a large array of details such as mail login details (POP3/SMTP), MSN "Windows Live" Messenger/other IM based conversations and VOIP calls. This could be used by an attacker to attain even more sensitive information through social engineering, by getting the names of things important to them like service providers they use and who they work for. Such information could also be used for identity theft.

This issue potentially affects up to 43% of all households and businesses within Ireland with broadband, which is 560,000 people. All of whom are Eircom customers. And more broadly it affects a number of businesses in Ireland who use IP based VPNs, as all information being passed through the servers can be logged allowing the possible capture of login information and allowing an attacker to steal data from that network. All of the software used is free and most of it is also open source.