

15 July 2009

By: Lucian Constantin, Web News Editor



Eircom DNS servers
redirect users to
advertising pages
instead of legit
websites
Eircom Group

[Possible DNS Hack at Ireland's Largest ISP \[UPDATED\]](#)

Legit links redirected to ad-sponsored search engines

Customers of Eircom, the largest Internet service provider in Ireland, experienced serious DNS slowdowns and weirdness over the weekend. Users from different parts of the country reported that trying to open legit URLs in browsers redirected them to advertising pages.

Some of them suggested on forums that there were two separate incidents related to Eircom's DNSs. The first reports appeared around July 1st, when multiple customers complained about significant DNS slowdowns and timeouts.

"I'm having terrible issues this evening performing DNS lookups. Takes about 10 to 20 seconds to do the lookup but once done the page loads in normal time," [wrote](#) a user on boards.ie, a popular Irish community boards website. "Same problem here in Mayo and it won't let me log onto my ps3," another one [confirmed](#) several minutes later.

The unresponsiveness of Eircom DNS servers seemed to still be an issue at the time of writing this article. However, over the weekend, users started experiencing other DNS-related problems as well. Legit URLs like facebook.com or twitter.com began displaying advertising pages instead of the popular social networking websites.

"Anyone else getting this when going on to rte [Ireland's national television website] via eircom BB [broadband]?", a user [asked](#) on July 3rd, while posting a screenshot of a search engine accompanied by the picture of a scantily dressed woman. "Ye Seems their DNS was hacked again.. Apparently it hapened recently with eBay.ie same picture and everything," he later [added](#).

Rik Ferguson, solutions architect at antivirus vendor Trend Micro, also reported about the issues. "So far there are very few details on the nature of the problem over at Eircom, but it is certainly clear that many Eircom subscribers are being redirected to bogus websites and rumours abound that Eircom's DNS has been compromised," the researcher [wrote](#) on his blog. He suggests that affected users switch to using OpenDNS.

[OpenDNS](#) is a free DNS service used by millions of home users as well as organizations worldwide. In addition to increased stability, reliability and very fast response times, the service offers features such as parental control, phishing protection, URL typo correction, personal URL shortcuts and many more.

Fortunately, this attack, if it indeed is an attack, does not seem to be malicious in nature and at best is focused around generating income. Nevertheless, it is rather invasive and annoying for the affected parties, preventing them from accessing legit resources over the Internet.

Back in August 2008, we [reported](#) a similar incident affecting customers of a large Chinese ISP, China Netcom (CNC). At the time, hackers poisoned the DNS server with a fake entry that directed users trying to access an inexistent domain to a page loading exploits. The ISP normally loaded an advertising page for such mistyped or bogus URLs.

That attack was a lot more subtle than the problems Eircom is having right now, because

the hackers wanted to go undetected for as long as possible. However, this is not applicable for an income-generating scheme, whose success is directly tied to the traffic on the rogue page.

Update: Eircom has released an official [announcement](#) confirming the DNS problems. "Customers may have recently experienced delays in web browsing and may have been unable to access the Internet. In some cases, customers may have been redirected to incorrect websites," it reads.

As far as details go, they remain scarce, the ISP only noting that, "This issue has been caused by an unusual and irregular volume of internet traffic being directed onto our network, and this impacted the systems and servers that provide access to the Internet for our customers." It is yet unclear if this refers to a distributed denial of service (DDoS) attack, or something else.

The company stressed that it "is working continuously to minimise the impact for customers and has taken a number of steps, including software updates and hardware interventions, to fully restore internet service."

Update 2: Eircom subscribers reported a new wave of service problems on July 14. The company has released a new official [statement](#), confirming the problems. "Last night eircom.net customers experienced significant congestion while browsing the web," the ISP announces.

A new denial of service attack is again named as a possible source for the recent troubles. "While it is too early to confirm, eircom believes that it is related to an unprecedented volume of traffic deliberately directed at our network which has caused difficulties for customers over recent days," the company says.

Clearly, the issue must be pretty serious for it to last so long. Eircom notes that it "has been in contact with other operators in the Irish market to collaborate and pool technical expertise in this area."

Correction: The article was modified to reflect that the second statement quoted in the fifth paragraph belongs to the same person as the first. A reported spelling error has also been corrected in the 9th paragraph.