

7 March 2009

By: Lucian Constantin, Web News Editor

Telegraph.co.uk

The Daily Telegraph's website leaks hundreds of thousands of subscriber e-mails
Telegraph Media Group

[Telegraph.co.uk Website Hacked](#)

SQL injection vulnerability compromises subscriber passwords and e-mails

HackersBlog, the Romanian whitehat hacking outfit, have disclosed an SQL vulnerability in a section of the telegraph.co.uk website. According to the group, the flaw gives attackers access to over 700,000 e-mail addresses and user passwords.

The Daily Telegraph, also referred to as The Telegraph, is one of the biggest daily newspapers in UK. It was founded in 1855 and currently has a daily circulation of almost 850,000. The telegraph.co.uk website is home to the online version of The Daily Telegraph and its sister paper The Sunday Telegraph and is one of the most popular consumer websites in Britain.

The SQL injection flaw affecting one of the website's sections was discovered by a Romanian self-confessed ethical hacker going by the online handle of "unu" (someone). "Unu" is a member of [HackersBlog](#) and has recently disclosed similar vulnerabilities in popular websites belonging to [The International Herald](#), [UK's National Lottery](#), [Kaspersky Labs](#), [Bitdefender Antivirus](#), or [Symantec](#).

According to the evidence published by the hacker, a poorly sanitized page of the Telegraph's website allows the execution of SQL queries through URL manipulation. These can be used to reveal all the databases and information about them.

[img=2][img=3][img=4]

Information such as the usernames and passwords of the site's members can also be extracted by exploiting the same vulnerability. Even more serious is the fact that the passwords are stored in plain text form instead of being hashed.

The severity of the security breach doesn't stop here. According to "unu," in one database table he discovered the e-mail addresses of the people subscribed to the website's newsletter. This is "A real treasure for spammers," the hacker claims, because "there [are] quite a bunch of them." One of the published screenshots shows how "unu" successfully extracted the 700,000th e-mail address.

Rik Ferguson, solution architect at antivirus vendor Trend Micro, [advises](#) that "if you are a Telegraph subscriber and are concerned about the safety of any other online accounts you may have I would encourage you to change your passwords on those other accounts, and of course on the Telegraph web site."

The date displayed by the affected web page, according to the screenshots, is February 17, 2009, but there is yet no indication whether the issue has been addressed or not. According to some accounts, the vulnerable section, which has intentionally been blotted in the images, has been taken offline. One of the HackersBlog admins resumed to saying that "we will do a full disclosure if the vulnerability isn't patched in usefull time or if it's been patched after the admin is contacted."

Note: We will return with more information as/if it becomes available.

Update: Telegraph.co.uk's Communities Editor, Shane Richmond, announced on his blog that "The main part[s] of our website are not affected, nor are the accounts of My Telegraph users or Telegraph blog commenters."

Mr. Richmond cites Paul Cheesbrough, chief information officer at Telegraph Media Group, who confirms that a partner site, more specifically search.property.telegraph.co.uk, has been affected. The CIO notes that the vulnerable code is two years old and that it's being rewritten. Furthermore, he thanks HackersBlog on behalf of the company for bringing the issue to its attention.

Read the complete statement [here](#)