

17 June 2009

By: Lucian Constantin, Web News Editor

[The Cligs URL Shortening Service Hacked](#)

Almost 2.2 million URLs hijacked as a result



Cligs hacked and 2.2 million short URLs hijacked
Cligs

A popular URL shortening system called Cligs was [compromised](#) Monday morning. The unknown hacker has pointed some 2.2 million short URLs to a legit blog post about Twitter hashtags.

URL shortening services allow users to create shorter and more convenient aliases for long URL. These are particularly useful on Twitter or other environments that enforce character limits on messages. According to recent stats, along with tinyurl.com, bit.ly, ustre.am and is.gd, cli.gs is one of the most widely used URL shorteners on the web and the fourth most popular on Twitter.

The Monday attack doesn't seem to have had any particular malicious intention behind it, since the page the hijacked URL pointed to was harmless. It is more likely that whoever is responsible tried to make a point.

"It's clear, though, that this hack could have been much worse. It's not yet apparent what the intentions were of the hackers, but they could have just as easily redirected millions of shortened urls to a website hosting malware," Graham Cluley, senior technology consultant at Sophos, [commented](#). "That's one of the reasons why it can be helpful to run a plug-in that will expand shortened urls before you click on them," he added.

Pierre Far, the creator of the Cligs service, [announced](#) that the vulnerability had been identified and patched and that 93% of the hijacked URLs were restored from backups. Out of the remaining 161,232 unrecovered URLs, 95,123 were not associated with any account and will be redirected to the Cligs home page. It is now up to the users themselves to change the remaining ones.

Roel Schouwenberg, senior antivirus researcher at Kaspersky, [pointed out](#) that, "Having control to so many URLs makes these services a very attractive target." Gunter Ollmann, VP of research at Damballa, and formerly chief security strategist at IBM Internet Security Systems, feels the same. "I suspect that this won't be the last time a shortened URL service provider will be compromised. There's [sic.] good money to be made by the bad guys if they exploit these kinds of services - so there's motivation and skills in abundance [sic.] to do so," he [said](#).