

By: Nando2008pa, Security and Search Engines Editor

[Thousands of Clean and Pirate Websites Affected by Massive Web Attack](#)

The IFrame attack continues

A few days ago, security researchers around the world spotted a new avalanche of IFrame attacks that revealed a pretty new hack technique: the users are redirected to several pages until they reach a 'deadly' final one which attempts to deploy the infection. Today, security researcher Dancho Danchev has [published](#) a blog post in order to disclose a couple of new websites affected by the threats. "These are the high profile sites targeted by the same group within the past 48 hours, with number of locally cached and IFRAME injected pages within their search engines," Dancho Danchev mentioned in the blog post. The IFrame injection affected both clean and malicious websites, so extra-care is obviously recommended when browsing suspicious pages. For instance, the US Administration of Aging, the University of Vermont and some BitTorrent websites are all targeted by the web attacks. The exploit is started through newly-introduced domains, most of them hosted on .info domains, which attempt to redirect the users to infected pages. Just like past attempts, once the visitor reaches the final website, he is recommended to download an ActiveX control, actually a new variant of the Zlob Trojan horse. Downloading the malicious files obviously brings the infection in your computer, making it entirely vulnerable to other future attacks. However, there are even more changes, according to the folks at Computer Associates. "This fake codec is actually a hijacker that will change your DNS settings whether you are acquire your IP settings through DHCP or set your IP information manually. This hijacker will attempt to re-route all your DNS queries through 85.255.x.29 or 85.255.x.121," it is mentioned on the CA [page](#). "If you use a static IP address, CA AntiSpyware will set your DNS server to 198.6.1.1 to prevent your DNS queries from continuing to go through the rogue DNS servers. Please change your DNS server to the DNS server provided by your IP or Network Administrator." However, refusing the download and avoiding getting the files is probably the best solution that would keep your computer clean and unaffected by the threat.