

19 June 2009

By: Lucian Constantin, Web News Editor



Nine-Ball attack infects over 40,000 websites  
Nineball

## [Nine-Ball Mass Injection Attack Makes over 40,000 Victims](#)

*Obfuscated rogue code serves flurry of exploits to unsuspecting visitors*

Security researchers from Websense [warn](#) that a new wave of web injection attacks is rapidly making thousands of victims. The new complex threat, dubbed Nine-Ball, features obfuscated code, multi-level redirection, visitor filtering and attempts to exploit multiple vulnerabilities found in popular applications.

This new mass injection follows the similar [Gumblar](#) / [Martuz](#) and [Beladen](#) / Shkarkimi attacks, which already infected tens of thousands of websites since the middle of May. Compromised websites will have a malicious hidden IFrame injected into their pages and IFrame code will be obfuscated through a JavaScript function called String.fromCharCode.

"We are calling this mass compromise Nine-Ball because of the final landing site," the Websense researchers, who have been tracking the threat since the beginning of June, note. "If a user visits one of the infected sites, they are redirected through a series of different sites owned by the attacker and brought to the final landing page containing the exploit code."

If exploits have the purpose of dropping a trojan downloader on the computers of unsuspecting visitors, "The malicious code attempts to exploit MS06-014 (targeting MDAC) and CVE-2006-5820 (targeting AOL SuperBuddy), as well as employing exploits targeting Acrobat Reader and QuickTime," the analysts warn.

Attackers have come to rely heavily on drive-by exploits in recent times, because users have repeatedly demonstrated a failure to keep the software installed on their computer updated. The multitude of widely deployed applications such as Flash Player, Quicktime, Java, and Adobe Reader has also increased the available attack surface, adding to the reliability of such a technique, from an attacker's perspective.

The Websense researchers note that a trojan downloader and a PDF exploit associated with this threat have a very low detection rate on VirusTotal, an online service employing 40 of the best known antivirus scanning engines. However, David Harley, director of malware intelligence at ESET, [points out](#) that this "may mean that the malware is, because of obfuscation and other factors, only detected using some form of behavioural [sic.] analysis that may not be deployed (or deployable) in on-demand scanning mode [used on VirusTotal]."