# ASP and ASP.NET Websites Targeted in Mass SQL Injection Attack

Written by ph0bYx
Monday, 05 July 2010 13:33 - Last Updated Monday, 05 July 2010 13:35

By Lucian Constantin, Softpedia.com

A known gang of hackers active on the Asian underground online gaming market is behind a new mass SQL injection attack that has infected thousands of pages. Attackers are targeting ASP and ASP.NET websites and exploit two critical Internet Explorer vulnerabilities to infect their visitors with a gaming trojan.

According to researchers from Santa Clara-based Web application security vendor Armorize, who analyzed the attack in detail, these are the same hackers who managed to inject malware into the Wall Street Journal and Jerusalem Post websites last month. The Armorize experts refer to the gang as the "DNF666" group, after the dnf666.net domain used in their first attack back in March.

The ultimate goal of this hackers is apparently to steal login credentials for several online games popular in Asia, like aion.plaync.co.kr, aion.plaync.jp or df.nexon.com. “[The] Attacker group runs businesses selling (illegal) plugins for online games,” the researchers explain .

The gang's favorite method of attack is SQL injection and so far only ASP and ASP.NET websites using SQL Server as database engine were targeted. Successful compromise results in a rogue  element loading malicious content from external URLs being inserted into the page. The third-party domains used in this attack are 4589.in and 22dnf.com [don't visit].

It seems that attackers rotate the vulnerabilities they target with each attack. Early last month in the robint.us and 2677.in attacks, the CVE-2010-1297 zero-day Adobe Flash Player and Reader vulnerability was exploited. However, in these latest compromises, the exploits used target two critical Internet Explorer vulnerabilities (CVE-2010-0806 and CVE-2010-0249) disclosed earlier this year, including the one used to **attack Google** and thirty other Fortune 500 companies (Operation Aurora).

Online games can have huge user bases, especially the ones tailored for Asia, the largest and most active online gaming market. Unfortunately, this immense popularity of online games has also led to the rise of an underground economy based solely on selling virtual goods like stolen game characters or illegal plug-ins. As an example of just how big this is, in May security researchers from Symantec **found** a single cache containing over 44 million stolen online gaming logins.