866-536-8614 | Contact Us
www.peakpositions.com

.ASPX .PHP URLs Struggle To Rank in Search Engines SQL Databases Tied To Third Party Injections Hackers.

as posted by Dancho Danchev @ 1:19 pm

Thousands of .ASPX .PHP URLs and SQL Database Site Injected To Serve IE Exploit

Once again confirming the trend of having more legitimate sites serving exploits and malware than purely malicious ones, Chinese hackers have been keeping themselves busy during the last couple of days, launching massive SQL injection attacks affecting over 100,000 web sites.

The SQL injection attacks serving the just patched Internet Explorer XML parsing exploit, are launched by several different Chinese hacking groups, and with several exceptions, are primarily targeting Asian countries which is a pretty logical move given the fact that it's a password stealing malware for online games that is served at the bottom line.

SQL stands for Structured Query Language that allows webmasters and web editors to communicate with their database. SQL is very complex and the potential for open doors and compromising paths is expansive. Incorrect authoring and implementation along with infrequent code updates can create a vast array of security lapses.

Hackers tend to target SQL databases and simple search boxes and email contact forms looking for server application error messages that contain valuable information that aid hackers in developing a successful hack attack that compromises websites.

Yahoo, Google, and MSN Live can and are used by hackers to as a source to gather key information about a website that often helps hackers find unlocked backdoors, SQL weaknesses, unsecured information and more.

It pays to hire an outside consultant that can identify SQL security holes and flaws and work to build security patches that help seal up vulnerable areas. It also pays huge dividends to outsource with a proven SEO firm that can help update code and provide SQL database security guidance in terms of best practices with IT Security. Page Code is critical to SEO success and also critical in terms of compliance with server side scripting and SQL database integrity.

More than 100,000 web sites have recently been cited as infected by Symantec and thousands more domains are being injected as previous campaigns and the number of affected sites typically accelerates very fast. Consider for a while the big picture. With or without a patch for the IE SQL exploit, committing cybercrimes through the exploitation of already patched client-side vulnerabilities would continue growing - it has been throughout all of 2008. Despite being old-fashioned compared to Russian cybercriminals that would have included the exploit within their web malware exploitation kits and started serving banker malware instead of password stealing malware, the Chinese attackers appear to be well aware of this trend, and therefore all of the IE exploit serving SQL sites are also serving several other exploits targeting Adobe's Flash, Acrobat Reader and RealPlayer for starters.

Recent studies continue emphasizing on the fact that millions of users not only continue browsing the web using insecure browsers, but also, are so browser vulnerabilities centered and they ignore the rest of the software running on their PCs as a potential infection vector given they're running an insecure versions of it - and yes they are. Cybercriminals are aware of this insecure Internet browsing, and are therefore including sets of exploits targeting each and every version known to be vulnerable of a particular software in order to increase the chances for a successful infection. This particular SQL injection attack is the most recent example of this mentality.

In 2008, cybercriminals continue infecting thousands of new hosts on daily basis using 2007's critical vulnerabilities, because instead

of patching vulnerable software, the majority of end users remain comfortable with their false feeling of security. Also the major search engines are responding by restricting .php, .asp, and .aspx urls pushing these urls far down in their organic search results in an effort to maintain the integrity of the organic search results and prevent further malware distribution.

Websites using SQL databases must take additional "white Hat SEO" steps to secure and maintain premium keyword rankings and top search listings in the major search engines, especially Google.

The author Dancho Danchev is an independent security consultant and cyber threats analyst, with extensive experience in open source intelligence gathering, malware and E-crime incident response. Dancho is also involved in business development, marketing research and competitive intelligence as an independent contractor. He's been an active security blogger since 2007, and maintains a popular security blog sharing real-time threats intelligence data with the rest of the community on a daily basis.

---

118 A Cass Street | Mailing Address: P.O. Box 2438 | Traverse City, Michigan (MI) USA 49685-2438
Tel: 231-922-9460 | Toll: 866-536-8614 | Fax: 231-929-3398
Office Hours: M-F 8AM-9PM EST* | Email: Info@peakpositions.com