REMINDER: Emailed to a group account. Do NOT reply using email group account.
For comments or inquiries email infosec@pjlhuillier.com.

infosec@pjlhuillier.com
ICT GROUP
INFOSEC 101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

April 15, 2011 Release # 111

-- Begin Transmission --

Malicious JavaScript Attacks: What Can You Do? - Part 2

In part 1, we talked about why hackers use malicious JavaScript program attacks and why we should be concerned about it. Part 2 will now talk about its business impact and the threat of Search Engine Optimization (SEO) attacks.

How These Attacks Impact Your Business

Malicious JavaScript can impact business in many ways. Two primary issues are:

- ***Compromised websites*** – company sites can get compromised, and as a result may unintentionally expose visitors to malware. If your website is compromised, you will be perceived as being responsible for infecting anyone who visits it. This can cause damage to your corporate reputation and may result in negative publicity and lack of confidence from your customers or business partners.
- ***Users becoming malware victims*** – on the other hand, internal users can be exposed to malware if they visit sites injected with malicious JavaScript programs. These programs can silently redirect the victim's browser to load content and malware from a remote server or carry out Search Engine Optimization (SEO) poisoning attacks.

Search Engine Optimization Attacks

Search Engine Optimization (SEO) is an accepted practice of improving the visibility or ranking of a website or page in search engines. For example, if one types in 'Cebuana Lhuillier' in the Google, we would like to see our corporate website to be among the first sites to be recommended by Google. In a nutshell, SEO aims to come up with 'search engine friendly' sites.

Search engines publish guidelines for acceptable methods to improve a site's ranking. Using methods that fall outside those guidelines is considered unscrupulous. Attempting to fool search engine algorithms is sometimes called "**Black hat SEO**" when such unsavory tactics are used to drive more traffic to a site. It becomes **SEO poisoning** when that site becomes a malicious site. Here are some techniques considered unacceptable:

- **Keyword stuffing** (which means repeating popular key words in the page tags or in the content itself, often in a form that's hidden from the site visitors by coloring it to blend with the background or by placing it behind images). Web pages that have been "stuffed" are sometimes referred to as "poisoned pages."
- **Comment spam" or "spamdexing**---which consists of posting links to a site in the comments of many web blogs.
- **Link farming** coming up with a group of websites that all link to every other site in the group.

How do attackers compromise the legitimate web sites to insert their redirection tools? In some cases, they exploit vulnerabilities in the content management system or vulnerabilities in the hosting web server. Once compromised, the attacker uploads and installs the malicious SEO application.

This application generates SEO pages dynamically and extracts text from the search results, using any major search engine. The latest "hot" keywords can be found in such resources as Google Trends. The SEO page then links to other SEO pages so they'll be indexed, and/or links to the SEO pages are posted on other legitimate web sites in forums, blog comments sections, guest books, social networking status updates, etc. This gets the pages indexed by the search engine crawlers. When a user clicks on the poisoned search results, the request is redirected to the malicious site.

To be continued…what are the solutions to keep you safe from these attacks?

-- End of Transmission --

Information Security: It's a Shared Responsibility

References: https://secure.sophos.com/security/whitepapers/index.html

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.

Document Code: 2011ICT_15SECAD016