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

April 29, 2011 Release # 112

-- Begin Transmission --

Malicious JavaScript Attacks: What Can You Do? – Final Part

With the popularity of SEO poisoning attacks growing, the search results of today's most popular search terms are littered with malicious links that could lead to plenty of trouble and lost productivity. Awareness and doing the best security practices will help us mitigate the damage from an attack and not being attacked at all. Getting into these tools and practices will reduce the risk of SEO poisoning attacks.

10 Ways to Protect against SEO poisoning attacks:

1. Enable Secure browsing functionality within the browser – whether you use the Internet Explorer or Mozilla Firefox, you need to enable secure browsing features in order to block malicious content that you may encounter while searching.

2. Utilize free safe search and safe browsing utilities – there are number of free utilities out there today from security vendors that can augment what the browser has to offer, providing risk scoring to links directly within search results before one even clicks the link.

3. Make sure AV is installed and updated – Yes, this is a no-brainer, but it bears repeating. Hackers will take advantage of an unprotected machine.

4. Ensure machines are patched – similarly, hackers will use your computer's operating system and application vulnerabilities against you when you start using un-patched machines to visit poisoned pages.

5. Initiate searches for news directly in news sites – consider looking for topical news directly within their favorite news outlet sites to bypass search results that may be likely to be poisoned.

6. Search for video directly to YouTube – one popular way of hackers taking advantage of your curiosity is by making poisoned pages that look like you are home. When you click the link, you will be asked to download Flash, but is directed to malware instead.

7. Remember that most sites stream without need for extra software – be reminded that you have your own video players installed. Some sites might ask you to install Flash but make sure you download it from legitimate sites like adobe.com.

8. Don't auto-click Yes when pop ups come from strange sites – remember to be skeptical when clicking yes to any pop up that materializes from strange sites found through search engines, even if they were high ranking or legit.

9. Utilize encrypted search – some researchers believe that SEO poisoning techniques to cloak malicious content from security vendors and search engine crawlers can be used against the hackers. Poisoned sites refer to non-malicious content when traffic doesn't come from a search engine. Use Google's beta encrypted search to trick poisoned sites into not knowing where your traffic comes from.

10. Remind users that you've got their AV needs covered – A large majority of hackers use SEO poisoning to trick you into downloading fake Antivirus software. Don't forget that you already have AV installed and understand what a fake anti virus scan page looks like to avoid future problems.

-- 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.