SEO Poisoning - What are SEO Poisoning Attacks?

427 Administrator Mon, Apr 5, 2010 Web Development   0 5095

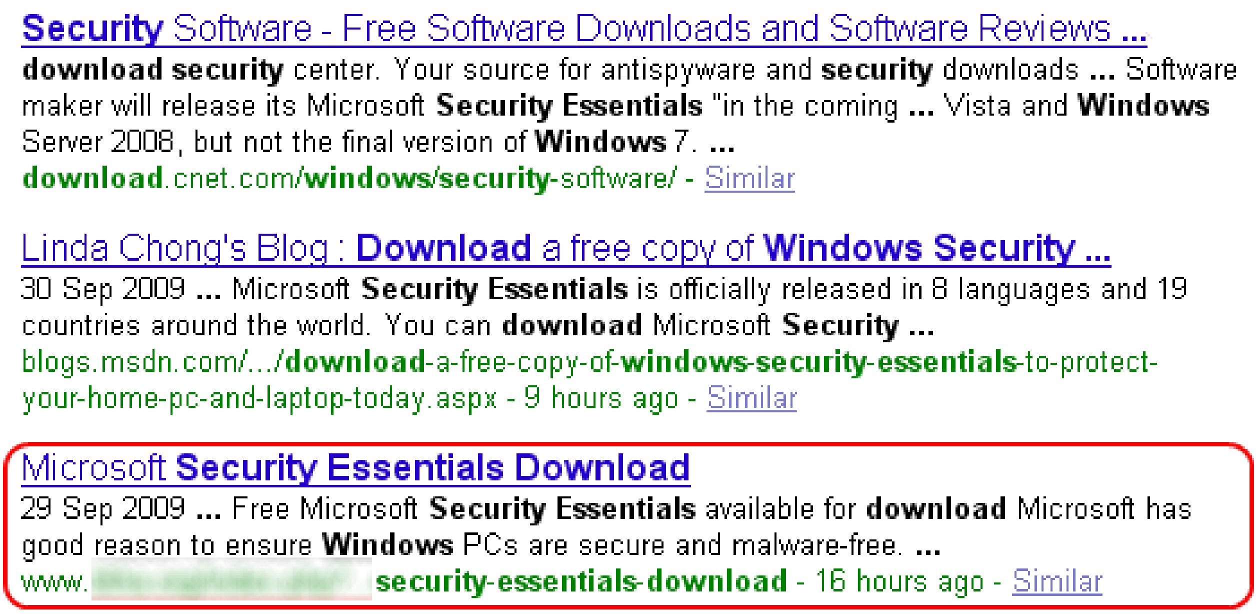
Search engine optimization (SEO) poisoning is an increasingly popular method of attack for cyber-criminals and one that shows they are using more sophisticated techniques. In the last year, attackers have poisoned search results on everything from celebrity news to Google Wave invitations. But what makes these attacks such a success?

Millions of searches are conducted each day on popular search engines by people all around the world. In order to share what are they looking for with the wider public - perhaps giving us an idea of what's hot and what's not - a number of major search engines provide a way to glimpse into the Web's query stream to discover the most popular search keywords or topics. True to form, wherever people are on the internet - the hackers are close to follow, and they are using this information to conduct attacks.

What are SEO Poisoning Attacks?

SEO poisoning attacks are primarily attacks on popular websites using XSS or cross server scripting. Most common SEO poisoning attack today is the the Iframe attack. This is the case when a very popular page with proper SEO is targeted by malicious hackers. What they do is exploit the input and display vulnerablity on these sites. I frames are then injected into such sites so when you search for some key word related to the popular site like say netgoons.com you may be redirected ater a while to some unknown site selling you viagra or free computer malware scanner.

A malicious SEO poisoning attack, also known as a Blackhat SEO attack, occurs when hackers manipulate search engine results to make their links appear higher than legitimate results. As a user searches for related terms, the infected links appear near the top of the search results, generating a greater number of clicks to malicious Web sites.



Security Software - Free Software Downloads and Software Reviews ...
download security center. Your source for antispyware and **security** downloads ... Software maker will release its Microsoft **Security Essentials** "in the coming ... Vista and **Windows** Server 2008, but not the final version of **Windows** 7. ...
download.cnet.com/**windows**/**security**-software/ - Similar

Linda Chong's Blog : **Download** a free copy of **Windows Security** ...
30 Sep 2009 ... Microsoft **Security Essentials** is officially released in 8 languages and 19 countries around the world. You can **download** Microsoft **Security** ...
blogs.msdn.com/.../**download**-a-free-copy-of-**windows**-**security**-**essentials**-to-protect-your-home-pc-and-laptop-today.aspx - 9 hours ago - Similar

Microsoft **Security Essentials Download**
29 Sep 2009 ... Free Microsoft **Security Essentials** available for **download** Microsoft has good reason to ensure **Windows** PCs are secure and malware-free. ...
www.[redacted] **security**-**essentials**-**download** - 16 hours ago - Similar

SEO poisoning can be used to drive traffic to an intentionally created malicious site, or it can take advantage of existing and popular Web properties by using cross site scripting (XSS) on a legitimate site. One common SEO poisoning method used today is to take already existing Web pages where a file has been uploaded to redirect the user to a malicious site. As the site is known and has often been around for years, it appears legitimate when it comes up at the top of the search results. The cybercriminals exploit the input and display vulnerability on these sites. This malicious site could be anything from advertising cut price Viagra or offering to ‘scan’ your computer for malware for example.

By targeting the top Google searches, hackers are able to drive traffic to sites using highly popular search terms. The average number of malicious sites in any Google search using hot/trending topics (as ranked by Google), by the end of last year (2009), stood at 13.7% for the top 100 results. This means that for every 100 results - around 14 of the links suggested to you may be to a malicious site and not what you were searching for at all.

An example of how closely the cybercriminals follow hot trending topics was recently seen when Websense Security Labs discovered that search terms relating to the new Apple iPad announcement had become the target for Blackhat SEO poisoning attacks before the product was even launched. In the lead up to Apple’s official announcement in January, there was a great deal of anticipation and speculation over the Internet. As people become interested in finding more information on the product, related search terms gained momentum, and as they did so Blackhat SEO attacks began to climb up the search result listings. Clicking on the rogue results lead to a fake anti-virus site which contained a file. If the file is installed it reports non-existent infections and disturbs the user with persistent pop-ups. In order to "clean" the system the rogue program is offered for a price. While we were able to provide protection to our customers immediately, at the time of our analysis the file on the rogue AV site had a characteristically low (30%) detection rate, as AV companies struggled to catch up with such attacks in real time.

SEO poisoning attacks are successful because they move in quickly and move on just a fast. As soon as a malicious campaign is recognized and removed from search results, the attackers can automatically redirect their botnets to a new, timely search term.

These ongoing campaigns have a proven formula and are likely to gain steam in 2010. This in turn may cause a trust issue in search results among consumers unless the search providers change the way they document and present links. But if you can't trust your search results then who can you trust? Unfortunately, without dynamic Web protection from high-risk threats through real-time security updates and increased visibility into modern Web security risks, the answer is likely to be unwelcome. A bit like SEO poisoning.

Online URL:
https://www.articlediary.com/article/seo-poisoning-what-are-seo-poisoning-attacks-427.html