Poisoned Search Results: More of a Malware Threat Than You Probably Think

By Tim Sprinkle | The Exchange – Tue, Jun 19, 2012 11:06 AM EDT

http://finance.yahoo.com/blogs/the-exchange/poisoned-search-results-more-malware-threat-probably-think-150643365.html

Be careful what you click on when searching the Web; the international cybercrime community is coming for you.

That's the message from Internet security firm Blue Coat, which earlier this year found that poisoned search engine results remain the number one malware threat on the Web, accounting for a full 40 percent of all cyberattacks in 2011. The popular bait-and-switch tactic is nearly four times more likely to snag unsuspecting users than the once common email-based approach, which now only accounts for 11 percent of attacks. Social networking rounds out the top three threats with 6.5 percent.

The Blue Coat report was based on an analysis of the Web traffic of more than 75 million users. "Searching is at least as dangerous as going into your email in-box and clicking on things," Chris Larsen, Blue Coat's chief malware expert, recently told USA Today.

The scam works like this: The bad guys set up themed "bait sites" using terms that are likely to show up in search engine results, as a way to trick users into visiting their sites. When the unsuspecting user clicks on a poisoned result in their search engine, thinking they are going to a legitimate site related to their search, they are served a site designed by the phishers to gather their financial information or get them to download a piece of malware or otherwise fall victim to whatever scam they are running. In many cases, users don't even know they have been victimized until it's too late.

A Numbers Game

It's the sheer scale of search engine traffic that attracts the scammers. With millions of users clicking on Google and Bing search results every hour of every day, sooner or later someone is going to slip up and visit a malware site.

Still, the study revealed some interesting trends in search poisoning strategy. The conventional wisdom is that cyber criminals are more likely to focus on major news events or celebrity stories that would generate lots of traffic for their sites, but in fact they seem to prefer to target searches to terms that only a few people will be searching for to give themselves a better chance of showing up at the top of the search results page. People don't expect poisoned search results when looking for obscure

refrigerator parts or Christmas decorating ideas, Larsen said, so their guard is down and they are more likely to click.

And, unfortunately for everyday users, poisoned search results are far from rare. There were 26 million new malware samples reported in 2011, according to the Anti-Phishing Working Group, and nearly 40 percent of the world's computers are thought to be infected. According to Blue Coat, 1 in every 142 searches last year led to a malicious link, while research by Web security firm Symantec has found that as many as one in three search results in its studies are poisoned. Either way, the odds heavily favor the bad guys.

Case in point: Earlier this year, search results related to the popular Hunger Games series of books and movies were poisoned on a large scale by cyber criminals, setting off international warnings from Web security firms.

Stay Safe Out There

So what can average users do to protect themselves from the risks of poisoned search results? Awareness is the key, as is a basic understanding of what legitimate Web addresses look like. Here are a few suggestions from Blue Coat.

Scan the site description — Google and Bing display two lines of "flavor text" alongside their text search results, which can provide clues to the site's provenance. "Look for disjointed, random text, like it was mashed up by a computer (because it was)."

Check out the domain name — "Is it one you've heard of? Does it seem to have something to do with the topic you were searching for?"

Preview before clicking — "Google now has a 'preview' feature, where text-search results have a little button to the right. If you hover your mouse on it, it will display an image of the page. This lets you see if the page 'looks legit.'"

Know your top level domains (TLDs) — "There are a lot of two-letter TLDs assigned to specific countries: .RU = Russia, .IN = India, etc. If you're searching for a U.S. culture topic, like Halloween costume ideas, or Thanksgiving recipes, or Christmas decorations and your search returns results on .RU or .IN, etc, ask yourself if it's likely that a site hosted there would really have good content about your search topic."

Use protection — It's always important to protect your computer with antivirus and antimalware software, which will block many of the malicious infrastructures that run search engine poisoning attacks.