Poisoning your own DNS for fun and profit

devblogs.microsoft.com/oldnewthing/20130129-00

January 29, 2013

Raymond Chen

When you type a phrase into the Windows Vista Start menu's search box and click *Search the Internet*, then the Start menu hands the query off to your default Internet search provider.

Or at least that's what the Illuminati would have you believe.

A customer reported that when they typed a phrase into the Search box and clicked *Search the Internet*, they got a screenful of advertisements disguised to look like search results.

What kind of evil Microsoft shenanigans is this?

If you looked carefully at the URL for the bogus search "results", the results were not coming from Windows Live Search. They were coming from a server controlled by the customer's ISP.

That was the key to the rest of the investigation. Here's what's going on:

The ISP configured all its customers to use the ISP's custom DNS servers by default. That custom DNS server, when asked for the location of `search.live.com`, returned not the actual IP address of Windows Live Search but rather the IP address of a machine hosted by the ISP. (This was confirmed by manually running `nslookup` on the customer machine and seeing that the wrong IP addresses were being returned.) The ISP was *stealing traffic from Windows Live Search*. It then studied the URL you requested, and if it is the URL used by the Start menu Search feature, then it sent you to the page of fake search results. Otherwise, it redirected you to the real Windows Live Search, and you're none the wiser, aside from your Web search taking a fraction of a second longer than usual. (Okay, snarky commenters, and aside from the fact that it was Windows Live Search.)

The fake results page does have an *About This Page* link, but that page only talks about how the ISP intercepts failed DNS queries (which has by now become common practice). It doesn't talk about redirecting *successful* DNS queries.

I remember when people noticed widespread hijacking of search traffic, and my response to myself was, "Well, duh. I've know about this for years."

Bonus chatter: It so happens that the offending ISP's Acceptable Use Policy explicitly lists as a forbidden activity "to spoof the URL, DNS, or IP addresses of «ISP» or any other entity." In other words, they were *violating their own AUP*.

Related

Raymond Chen

Follow