

DNS cache poisoning attack

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-04/0011.html>

From: Paul A. Wylie (pwylic_at_THEHUNTCORP.COM)

Date: 04/01/05

Date: Fri, 1 Apr 2005 10:33:01 -0700

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Yesterday, I discovered that my clients were being redirected from some of their normally-visited sites to a malware server that purports to be in Laos (in the domain web-search.la). My DNS servers are running on Win2k Server with full patches (according to HFNETCHK). At the time, they were not configured as recommended in MS KB article 241352. I reconfigured the servers, restarted the DNS services and did not see any further DNS poisoning yesterday, so I assumed I had bitten by a problem of my own making.

Today, however, I've discovered that the DNS cache poisoning continues, and a quick search for the domain web-search.la through Google reveals that the Internet Storm Center at SANS has been tracking this problem and recommends blocking all traffic to 216.127.88.131 and 218.38.13.108.

You can read more at:

<http://isc.sans.org/diary.php?date=2005-03-30>

<http://isc.sans.org/diary.php?date=2005-03-31>

Paul Wylie
Network Systems Manager
The Hunt Corporation

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--