

Re: What means 'CONNECT xyz.xyz.xyz.xyz:25 HTTP/1.1' in my apache protocol?

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2003-04/0281.html>

From: ynotssor ("ynotssor")

Date: 04/10/03

From: "ynotssor" <"ynotssor">
Date: Thu, 10 Apr 2003 09:53:44 -0700

"Stefan" <c-x-b@web.de> wrote in message
news:b7454c\$vdF\$06\$1@news.t-online.com

> What means 'CONNECT xyz.xyz.xyz.xyz:25 HTTP/1.1' in my apache protocol?
> And WHY didn't I have an ERROR in my error log???
>
> All entry (from one ip) in my access_log are:
>
> aaa.bbb.ccc.ddd -- [10/Apr/2003:15:35:58 +0200] "\x04\x01" --
> aaa.bbb.ccc.ddd -- [10/Apr/2003:15:36:19 +0200] "\x05\x01" --
> aaa.bbb.ccc.ddd -- [10/Apr/2003:15:36:20 +0200] "CONNECT
> xyz.xyz.xyz.xyz:25 HTTP/1.1"

Someone is attempting the HTTP CONNECT() METHOD exploit in order to pass spam email to port 25 of xyz.xyz.xyz.xyz, making it appear to the world that the spam originated from your server instead of from aaa.bbb.ccc.ddd.

<http://www.kb.cert.org/vuls/id/150227>

tony

--

use hotmail.com for any email replies

-----= Posted via Newsfeeds.Com, Uncensored Usenet News =-----

<http://www.newsfeeds.com> - The #1 Newsgroup Service in the World!

-----= Over 80,000 Newsgroups - 16 Different Servers! =-----