

## Assembler snippet (Re: Suspicious WebDAV Traffic)

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-04/0020.html>

---

**From:** Tom Stewart (*tastewar\_at\_ALUM.MIT.EDU*)

**Date:** 04/14/04

Date: Wed, 14 Apr 2004 08:56:01 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

I don't consider myself an assembler hacker by any stretch, but I do read it doing every day debugging. Sorry, but this isn't code, it's data. Lots of spaces, periods, carriage return/linefeeds, numbers, letters.

The fact that something *\*can\** be disassembled doesn't mean it's code. CS stands for Code Segment, and it's supposed to be a prefix to a data reference to override the default segment (generally DS or SS). Alone, it doesn't mean anything, AFAIK. A 2E also happens to be a . character. Now, which interpretation is most likely?

BTW, even though it is data, that doesn't mean it isn't malicious.

-----

Earn up to 10 credit course hours toward the TruSecure ICSA Practitioner (TICSA) Credential and receive a TICSA exam coupon by attending the Infosecurity Canada 2004 conference. Featured speaker, Marcus J. Ranum, TruSecure inventor of the proxy firewall will present on June 3 at 11:30 AM. Visit <https://ticsa.trusecure.com> for certification details and <http://www.infosecuritycanada.com> for conference information. Become TICSA certified and see what happens!

-----