

## Re: reports of DCOM worm on the loose...#3

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-08/0025.html>

---

**From:** Nick FitzGerald (*nick\_at\_VIRUS-L.DEMON.CO.UK*)

**Date:** 08/12/03

Date: Tue, 12 Aug 2003 10:49:35 +1200  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Russ asked:

- > *The registry key which is modified in order to make the worm propagate is;*
- >
- > *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\*
- > *Value=Run*
- >
- > *Where the value is "windows auto update" = msblast.exe I just want to*
- > *say LOVE YOU SAN!! bill*
- >
- > *If anyone can explain why this would actually run the MSBLAST.EXE*
- > *please explain.*

It doesn't right away. That is done in the exploit payload.

This just makes sure that the code is run on successive restarts. CodeRed and Slammer were "pure" network worms and thus depended upon ongoing availability of non-patched machines and network saturation with their code to provide ongoing "re-infection" as infected machines were restarted. This beast is much more your traditional Win32 file-based malware which just happens to have a network spreading function. As such, there is a "permanent" copy of the code on the victim machine, so it sets itself to restart from that as the system comes up from restart.

BTW, the EXE has code that should create the mutex "BILLY", presumably as a self-infection marker. However, I cannot see the expected matching code to check for this mutex's existence, so multiple infection seems possible.

Also, the reports of code to DoS windowsupdate.com on 15 August may be misleading -- from a very quick look at the code, it seems the logic is "if it is after the 15th of the month then DoS" and if that condition fails the test "is it August or earlier then skip the DoS" is made. Thus, the DoS will start Saturday as that's the first date after the 15th since the worm's release and will continue until 1 Jan, when it will stop until 15 January, continue until 1 Feb, et seq.

NT-Bugtraq: Re: reports of DCOM worm on the loose...#3

--

Nick FitzGerald  
Computer Virus Consulting Ltd.  
Ph/FAX: +64 3 3529854

oo  
Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!  
With a growth rate exceeding 110%, the TICSA security practitioner  
certification is one of the hottest IT credentials available. And now, for  
a limited time, you can save 33% off of the TICSA certification exam! To  
learn more about the TICSA certification, and to register as a TICSA  
candidate online, just go to  
<http://www.trusecure.com/offer/s0100/>  
oo