

# Alert: New version of Code Red, XXXX

*Source:* <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2001-08/0001.html>

---

*From:* Russ ([Russ.Cooper@RC.ON.CA](mailto:Russ.Cooper@RC.ON.CA))

*Date:* 08/05/01

Message-ID: <E9A01F52DC939448BBDE44ED2E1C468F167BDA@muskie.rc.on.ca>  
Date: Sat, 4 Aug 2001 23:48:17 -0400  
From: Russ <[Russ.Cooper@RC.ON.CA](mailto:Russ.Cooper@RC.ON.CA)>  
Subject: Alert: New version of Code Red, XXXX  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

-----BEGIN PGP SIGNED MESSAGE-----

Just a quick FYI, there is a new version of Code Red which appears to be spreading rather rapidly.

- Appears to be a new re-write.
- Drops some sort of remote access trojan.
- Turns off System File Checker (Windows File Protection.)
- Moves CMD.EXE to the scripts directory in IIS
- Looks like the way they make the entry into code very differently than before.
- If your IDS is looking for "NNNN", forget it (but then you should have been shot if you used this string anyway)

Cheers,

Russ - Surgeon General of TruSecure Corporation/NTBugtraq Editor

p.s. if we don't respond right away its because we're now going to go and light the fireworks here at my retreat. Might as well have lots of fireworks tonight!

-----BEGIN PGP SIGNATURE-----

Version: PGP Personal Privacy 6.5.2

iQCVAwUBO2zCARBh2Kw/17p5AQH95wQAqjGp7vRYK8SYky/ydyU1wxBmCe2c8Mpd  
DBdxrv+TY9112ZuH663ZspUOXThS9oeEyT4sdbVYNv8Z28nMipbioyTXYa5dw8po  
21tkilo6ZoGX+AmKJ6Kz7WDvMpHpEfzDr3JHGtxuev0/rcIXeRSN4urypMR3YnRz  
uw5ZW/F3U/I=

NT-Bugtraq: Alert: New version of Code Red, XXXX

=OhCV

-----END PGP SIGNATURE-----

---

Delivery co-sponsored by Trend Micro

---

**TREND MICRO REAL-TIME VIRUS ALERTS**

If you would like to know about a virus outbreak before CNN and ZDNet get Trend Micro Virus Info Feed FREE. Simply copy and paste a small piece of code to give your visitors a real-time top 10 list and the latest virus advisories. Setup takes just 10 minutes and requires no server-side code on your Web site. All content is updated automatically from Trend Micro's Web site.

<http://www.antivirus.com/banners/tracking.asp?si=8cation/vinfo/>

---

- **Previous message:** [Marc DeBonis: "Identix BioLogon Client security bug"](#)
- **Next in thread:** [Russ: "Re: Alert: New version of Code Red, XXXX"](#)
- **Reply:** [Russ: "Re: Alert: New version of Code Red, XXXX"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)