

Re: SYMANTEC doesn't detect TROJAN, !!WARNING TROJAN ATTACHED!! – first_3sum.wri (0/1)

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-12/2385.html>

From: NormanM (my.aren't@we.nosy.invalid)

Date: 12/27/02

From: NormanM <my.aren't@we.nosy.invalid>

Date: Fri, 27 Dec 2002 06:00:27 GMT

On Thu, 26 Dec 2002 22:01:23 -0800, Hunter Watson <djgka876@keocm.net>

wrote:

*>I am concerned because after the restore operation
>"ms spool32.exe" is no longer in the Windows folder but
>the 2 .DAT files are. Is there another file on my HD that puts
>"ms spool32.exe" in the windows folder? And why does
>"ms spool32k.dat" contain the info that was there before I deleted it?
>The info seems to be stored somewhere else. Is there a key logger
>program lurking on my HD or is it contained in "ms spool32.exe".*

AFAIK, Windows Restore only changes system files to an earlier restore point without altering user data files. Since any file with the .dat extension is a user file, it should not be either changed, or deleted by running System Restore.