

Re: strange startup files and win32cfg

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-10/3251.html>

From: Sir_George (Sir_George_at_mailinator.com)

Date: 10/25/03

Date: Fri, 24 Oct 2003 16:21:33 -0600

yankele,

Visit the following Symantec site for some useful info;

<http://securityresponse.symantec.com/avcenter/venc/data/false.nimda.aris.email.message.html>

--

Sir_George

For better access to newsgroups;

<http://www.microsoft.com/windowsxp/pro/using/newsgroups/setup.asp>

"yankele" <yankelecakker@hotmail.com> wrote in message
news:02a301c39a6a\$92155bb0\$a401280a@phx.gbl...

> I recently noticed in my RunOnce value in the Win2k
> registry an entry called MS38495 for which the value was
> win32cfg.exe. That file exists in my WINNT\System32
> directory but is not identifiable. If I try to remove the
> entry from the RunOnce listing, it reinstalls itself. I
> have been unable to identify the MS38495 name either in
> the MS Knowledge Base or in the Newsgroups, nor have I
> been able to come up with much for win32cfg.exe. I think I
> remember seeing somewhere that it was a "nasty" file but I
> can't seem to track it down. A search in the registry led
> me to discover that the entry for win32cfg.exe was in the
> following key
> [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
> NT\CurrentVersion\Winlogon] where Shell was given the
> value explorer.exe Win32cfg.exe.
> When I deleted that value, I was able to stop the file
> from loading and so far everything seems to be running
> correctly. Am I correct in assuming that such an entry
> should not appear in the Shell value which should be only
> explorer.exe?
> Can anyone tell me what win32cfg.exe is and whether or not
> it is useful to let it run?
> Thanks.