

Re: Unknown startup items

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-12/0511.html>

From: Steven L Umbach (n9rou_at_n0-spam-for-me-comcast.net)

Date: 12/24/04

Date: Fri, 24 Dec 2004 19:54:13 GMT

Use the Autoruns free utility from SysInternals. It will tell you who claims to be the publisher of the file and the path to the folder which may give you a hint. I think the new version will also tell if the file is signed, though not being signed does not mean it is bogus. Process Explorer could also help you. The links below will take you to those programs. --- Steve

<http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml>

<http://www.sysinternals.com/ntw2k/freeware/procexp.shtml>

"Dan" <po98ujh9@hotmail.com> wrote in message

news:OR7VvmG6EHA.3756@TK2MSFTNGP14.phx.gbl...

>I have 2 startup entries in msconfig for which there is nothing listed

>under "command", making it impossible for me to tell what they are starting

>(at least using msconfig). Registry locations are

>HKLM\software\microsoft\windows\current version\run &

>HKCU\software\microsoft\windows\current version\run. How can I determine

>what these items are? I'm fairly certain they have to do with a recently

>installed ATI TV tuner card, but I want to be sure. I'm pretty familiar

>with what runs on the machine; the hijack this log seems to show nothing

>out of the ordinary, but I'd still like to know what this is. Looking at

>these location in the registry turns up nothing unexpected or unknown to

>me, except under the above HKLM entry where NWEReboot REG_SZ with

>nothing under data appears. What might this be?

>

> TIA

>

> Dan