

## is win32cfg.exe nasty?

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-10/2364.html>

---

**From:** Yankele Cakker ([yankelecakker\\_at\\_hotmail.com](mailto:yankelecakker_at_hotmail.com))

**Date:** 10/24/03

Date: Fri, 24 Oct 2003 20:35:58 GMT

I noticed that my win2k system began to run agonizingly slowly. Found that it was winlogon which was hogging most of my resources. In the registry key [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] found an entry for Shell for which the value was "explorer.exe win32cfg.exe". This didn't look too good to me because it corresponded with a "strange" entry in my RunOnce registry key named MS38495 for which the value was "win32cfg.exe". If I tried to delete this it would reload by itself. Which is where the winlogon came in. So I removed the win32cfg part of the Shel entry and just left the explorer.exe. When I eliminated all of this stuff, my pc ran fine again. I was unable to find anything useful regarding either MS38495 or win32cfg.exe in the Knowledge Base or in a search of the Newsgroups. Google also had almost nothing. Does anyone have any information about this? What does win32cfg.exe do and was I correct in removing it? I seem to remember reading somewhere that it was put in by a virus, a worm or spyware but I am not quite sure. Any help would be greatly appreciated.

Thanks.

--

Yankele Cakker

My reply e-mail address is correct as is. The courtesy of providing a correct reply address is more important to me than time spent deleting spam.

Celeron 500, 256RAM, 20G HD, Cable

Gigabyte GA-GF 1280, SB PCI128

Win2k, IE6, OE6, AVG, Kerio