

Re: WinDefend

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-09/msg00629.html

- *From:* Gruselle <Gruselle@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 26 Sep 2006 11:25:02 -0700
-

Thanks MowGreen: I see someone else had same problem.
Did what you said. Found Application Extension "winio.dll" which had following Properties:
General – Created 18 Nov 2002; Modified 18 Mar 2002; Accessed 26 Sept 2006
Version – 2.0.0.0
Description: WinIo
Copyright: Copyright@1998–2002, Yariv Kaplan
Item Info: Company: <http://www.internals.com>
This website describes Winio as "This library allows direct I/O port and physical memory access under Windows 9x/NT/2000 and XP. Version 2.0 provides faster I/O port access, better memory mapping support and can be used from non-administrative accounts under Windows NT/2000 and XP."
Looks kosher but is it?

"MowGreen [MVP]" wrote:

Gruselle,

Here's a thread from April concerning winios.sys :
<http://www.windowusbbs.com/showthread.php?t=53271>

Locate the file in C:\WINDOWS, right click it and choose Properties.
Click the Version tab.
Check for information next to Description and Copyright.
Also, check the info under Item name.

It may be a legit file that hasn't been classified by SpyNet; it may be a malicious file suspected, but not yet detected as a specific malware.

You can try scanning the file here:
http://www.virustotal.com/flash/index_en.html

Unfortunately, that site has been seeing very heavy traffic lately and you may be asked to submit the file via email. The scan results will be emailed back to you.

Please us posted on just what this copy of winio.sys *is*.

Re: WinDefend

MowGreen [MVP 2003–2006]

=====
-343- FDNY
Never Forgotten
=====

Gruselle wrote:

I frequently get this Warning in Event Viwer immediately after connecting to BT Broadband: Event 3004
"Windows Defender Real–Time Protection agent has detected spyware or other potentially unwanted software.
For more information please see the following:
<http://www.microsoft.com>
Scan ID: {ECDF5B2E–5D1A–41F7–B7A0–0887FBE0907C}
User: MARTIN\Martin G
Name: Unknown
ID:
Severity ID:
Category ID:
Path Found: driver:WINIO;file:C:\WINDOWS\winio.sys
Alert Type: Unknown
Detection Type:
The Microsoft link says:
We're sorry
There is no additional information about this issue in the Error and Event Log Messages or Knowledge Base databases at this time. You can use the links
in the Support area to determine whether any additional information might be available elsewhere.
Does anyone know the answer!