

Possible worm infection or something else?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-11/0711.html>

From: Giancarlo Ballestracci – IT & Technical Support (giancarlo.ballestracci_at_progenit.it)

Date: 11/28/03

To: <security-basics@securityfocus.com>, <focus-virus@securityfocus.com>

Date: Fri, 28 Nov 2003 09:41:21 +0100

Hi The Group,

I hope someone get me a good advice about this problem. I have a notebook with multiboot startup (2 Win2k, 1 WinXP). On the first partition Win2k, svchost.exe take the 100% of CPU's resources. The system is regularly patched (SP4 and all the latest Hot Fixes), personal firewall and Antivirus clients updated. Scans with Symantec and Trend Micro have nothing found. I've tried to shut down all the services possible, without good result. I've also removed the last six applications installed on: nothing happen. Only in safe mode (clear...), the CPU work fine.

It's possible that a (new) worm sleep inside the client? Initially, I have thought about a Blaster Worm... I've checked also the system registry, but nothing strange in on RUN key of LOCAL MACHINE.

Anybody can light me?

Thanks in advance

Giancarlo
IT Manager
