

Hard Drive keeps filling up

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-09/0891.html>

From: Harris Samuel W PORT (*HarrisSW_at_mail.ports.navy.mil*)

Date: 09/22/03

To: security-basics@securityfocus.com

Date: Mon, 22 Sep 2003 14:08:40 -0400

I have been having a problem for a week now and can't seem to detect the culprit. This is on my home network. On my wife's machine, the OS is Windows XP, 2.8G, Broadband connected, with 802.11g Linksys wireless router. I have 3 firewalls running on it, zonelabs, tiny and the firewall included with XP. I have an online subscription to McAfee virus software, and it is kept up to date as new updates are issued. I have checked Task Manager and shut down the processes that I knew wouldn't cause me a problem, the rest seem innocent enough, (to my knowledge). I've done netstat several times and haven't discovered any obvious unknown connections. I have even locked the firewall down (Zonelabs) on several occasions, to eliminate the possibility that it was being accessed by an unknown process or program. I have Ad-Aware and Spy-Bot on the computer. I have all the updates to XP installed. I have used the Shavlik software and have updated everything it comes up with, I have used the Microsoft Security Analyzer to check for any security problems and have installed all that was called for.

Now for the problem. 2 weeks ago my daughter called me up and was frantic, because she had been instant messaging and some putz came on and told her to invite him in or she would be sorry. She didn't and she was. He infected her with some worm that proceeded to fill up her hard drive. I had given her an old computer that I had and it only had a 12G hard drive. I used VNC to check her computer out and tried to stop the bleeding, but it was too much for me. Well, a few days later I get a message that my computer is almost out of space. I have an 80G hard drive. I looked at the file system but couldn't find the files that were big enough to fill it up like that. I was performing a scan with McAfee (which detected nothing by the way) and noticed that the computer was spending an inordinate amount of time on a .tmp file. I looked at the folder that was in question, and bingo I found all the used space. There were several files in the folder that all ended in .tmp. One I remember was McV90.tmp. There were others, but that is the one I remember. It was 48G all by itself. I tried to open it to view it, but couldn't find a program that I had that could open it up. I deleted the file and regained my space back. A couple of days later the space was being eaten up again. I deleted it again and began monitoring it every few hours to see if there was any more action. I couldn't detect much for a few hours, then it started up again.

I shut the firewall, so if it was external to the computer, then I

SecurityFocus BASICS: Hard Drive keeps filling up

would stop any outgoing action. The firewall came up with a few complaints, but nothing out of the ordinary (I think it wasn't out of the ordinary) This didn't seem to stop the process, so I am assuming the problem is in the computer. I have a Windows 2000, Redhat, 9.0, Redhat 8.0 on the rest of my network. No problems with any of them. I have googled, I have McAfee'd, I have done a few other search engines, but I come up empty as to what this is. Spybot and Ad-Aware found nothing, as I run them daily. Any ideas where to go next? I am fresh out of ideas at the moment

Sam
