

Re: Large files being written to c:\winnt\temp

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-09/1776.html>

From: Jeff Cochran (jcochran.nospam_at_naplesgov.com)

Date: 09/18/03

Date: Thu, 18 Sep 2003 20:44:00 GMT

You could configure auditing on the systems to track the files, check the owner attribute to see if it's a particular account, and check what services may be running. These don't sound like normal hacker files, and resemble quite a few automatic backup types of file names. It's interesting to know the content, I'm assuming there's no extension on them (make sure that extensions of known file types is displayed on the system in question when you look at the names).

Jeff

On Thu, 18 Sep 2003 08:25:02 -0700, "Yoke" <dale_yocum@fws.gov> wrote:

>On both systems, no new program installations have been
>done near these time periods. I have my computers do
>automatic downloads of the windows updates but even then
>I don't see a windows update being 1.05GB. All of the
>files are eight-digit numerics (ex. 12018087, 46083071,
>etc.). I first discovered this when the C:\ drive ran
>out of space. Of 25 computers on a network, I only know
>of these 2 having this weird activity. I tried to look
>at the file content in Notepad but it is just computer
>gibberish. I have noticed that 1 of the PCs has had this
>activity 8 times since May 2002 but most in 2003. Thanks
>for the thoughts.

>

>

>>-----Original Message-----

>>Perhaps you can tell us what the file content is.

>>

>>Many programs can by default write to a file in the temp
>directory.

>>

>> Did this just start all of a sudden..

>>

>>Was a new install done around the time the files started
>to appear.

>>

>>
>> "Yoke" <dale_yocum@fws.gov> wrote in message
>> news:0fb201c37ded\$732a0280\$a301280a@phx.gbl...
>>> Not sure if this question is a security issue.....
>>>
>>> I have 2 computers on my network that occasionally get
>>> very large files written to the c:\winnt\temp folder.
>It
>>> doesn't appear to be an application writing these files
>>> b/c many times the modified time is during the early AM
>>> hours when the workstation is locked and no one is here
>>> to use them. My router is running NAT and I'm also
>using
>>> BlackICE. BlackICE does not show any traffic. Anyone
>>> have any idea how I can check to see where these files
>>> are coming from or what they are? These files do not
>>> seem to be written on any type of pattern. The file
>type
>>> reads FILE and often these files range from 20MB to
>1.1GB.
>>
>>
>>.
>>