

Re: Strange Client Behavior: Port 8002 Looking for Other Ports

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2005-01/0473.html>

From: Shalom B. (*Anonymous_at_inter.net*)

Date: 01/11/05

Date: Tue, 11 Jan 2005 19:49:36 +0000 (UTC)

I would first try and use the following command to list all network connections and the PID of each process involved in the connections listed and then use the Windows Task Manager to find the Image Name of the Process with the corresponding PID.

```
% Netstat.exe -ano
```

Below is a utility I wrote, a simple batch file that enhances Netstat.exe and includes the Process's Image Name in the output, It however requires Tasklist.exe which unfortunately is not found on Windows 2000 but if you manage to get your hands on Tasklist.exe from an XP installation, it should work fine.

```
:: BEGIN Netstate.cmd

@echo off
setlocal

if "%1"==" " set param=-an

set sys32=%windir%\system32
%sys32%\ipconfig.exe | find /i "ip address" > %temp%\IPCFG && for /f
"tokens=15 delims= " %%g in (%temp%\IPCFG) do (
    set IP_ADD=%%g
)

for /f %%g in ('%sys32%\hostname.exe') do set Hostname=%%g

%sys32%\netstat.exe -p TCP -o %param% | find /i /v "Foreign Address" |
find /i /v "Active Connections" >> %temp%\TCPS
%sys32%\netstat.exe -p UDP -o %param% | find /i /v "Foreign Address" |
find /i /v "Active Connections" >> %temp%\UDPS

for /f "tokens=1,2,3,4,5,6,7 delims=: " %%g in (%temp%\TCPS) do (
```

microsoft.public.win2000.networking: Re: Strange Client Behavior: Port 8002 Looking for Other Ports

```
for /f "tokens=1,2 delims= " %%y in (
    '%sys32%\tasklist.exe /NH /FI "PID eq %%m"'
    ) do (
        echo. %%g, %%h%IADDR_LOCAL%, %%i, %%j%IADDR_REMOTE%, %%k, %%l,
%%y, %%z
    )
)

for /f "tokens=1,2,3,4,5,6 delims=: " %%g in (
    %temp%\UDPS
    ) do (
        for /f "tokens=1,2 delims= " %%y in ('%sys32%\tasklist.exe /NH /FI
"PID eq %%l"') do (
            echo. %%g, %%h, %%i, %%j, %%k, , %%y, %%z
        )
    )
)

endlocal

del /f %temp%\TCPS
del /f %temp%\UDPS
del /f %temp%\IPCFG

:: END Netstate.cmd
```

Will wrote:

> *I have strange symptoms on a Windows 2000 client. For long
> periods each day, this client, which is behind Microsoft Proxy
> 2.0, stops access to the Internet. In the sniffer trace, what
> I see is repetitive behavior where the client will send out TCP
> connections from source port 8002 to successive ports on our DNS
> server. It appears to attempt connection to each port three
> times, and then it goes on to the next one. 1937, 1938, 1939,
> etc.*
>
> *This sure looks like some kind of port sniffing activity, maybe a
> virus, but does anyone recognize the source port number and
> behavior as belonging to some legitimate Windows 2000 client
> behavior?*
>

```
@echo off
setlocal
```

Re: Strange Client Behavior: Port 8002 Looking for Other Ports

```
if "%1"==" " set param=-an
```

```
:: Variable Initalisations
```

```
set sys32=%windir%\system32
```

```
%sys32%\ipconfig.exe | find /i "ip address" > %temp%\IPCFG && for /f "tokens=15 delims= " %%g in
```

```
(%temp%\IPCFG) do (
```

```
    set IP_ADD=%%g
```

```
)
```

```
for /f %%g in ('%sys32%\hostname.exe') do set Hostname=%%g
```

```
%sys32%\netstat.exe -p TCP -o %param% | find /i /v "Foreign Address" | find /i /v "Active Connections" >>
```

```
%temp%\TCPS
```

```
%sys32%\netstat.exe -p UDP -o %param% | find /i /v "Foreign Address" | find /i /v "Active Connections" >>
```

```
%temp%\UDPS
```

```
for /f "tokens=1,2,3,4,5,6,7 delims=: " %%g in (%temp%\TCPS) do (
```

```
    for /f "tokens=1,2 delims= " %%y in (
```

```
        '%sys32%\tasklist.exe /NH /FI "PID eq %%m"'
```

```
    ) do (
```

```
        echo. %%g, %%h%IADDR_LOCAL%, %%i, %%j%IADDR_REMOTE%, %%k, %%l,
```

```
%%y, %%z
```

```
    )
```

```
)
```

```
for /f "tokens=1,2,3,4,5,6 delims=: " %%g in (
```

```
    %temp%\UDPS
```

```
) do (
```

```
    for /f "tokens=1,2 delims= " %%y in ('%sys32%\tasklist.exe /NH /FI "PID eq %%l"') do (
```

```
        echo. %%g, %%h, %%i, %%j, %%k, , %%y, %%z
```

```
    )
```

```
)
```

```
endlocal
```

```
del /f %temp%\TCPS
```

```
del /f %temp%\UDPS
```

```
del /f %temp%\IPCFG
```