

# Re: Clarification–Win2k Netstat sockets interpretation

---

*Source:* <http://www.derkeiler.com/Newsgroups/alt.computer.security/2007-02/msg00022.html>

---

- *From:* warf <[warf@xxxxxxxxxxxx](mailto:warf@xxxxxxxxxxxx)>
  - *Date:* Mon, 05 Feb 2007 20:03:32 GMT
- 

Sebastian Gottschalk wrote:

warf wrote:

Hi Sebastian...through all the chatter I have lost the intent of your initial suggestion to use the De script to secure/disable my remote access. Are you definitively saying "it is safe and contains no uninvited actions?"

snip..

And I can't wait for an RFC for "remote–stabbing over TCP/IP" ...

I just realized; if we all had to sit on wet seats holding a wire connected to line voltage and an ethernet enabled switched so that any malicious code or commands sent from your computer would shock the shit out of the sender ... Remote Stabbing is pretty funny though...unless your loopback adapter misdirects the command–>home.

snip

So I take my saved SP4 upgrade I got before M\$ made us pull our pants down and take a shot of code to make sure we own the OS install.

Huh?

Metaphor for 'drop my protection'.

BTW...I drop the defenses reluctantly and incrementally to enable manual update [upgrade] from M\$ but still don't pass the 'wideopenvulnerable enough to allow your upgrade' test.

Are you talking about Windows Automatic Updates or the Windows Update

## Re: Clarification–Win2k Netstat sockets interpretation

website?

You make a good point...I was unaware that they are now different. Before [goodol'days] I could manually download every security update and servicepack from MS.com but now...they send you a bit of Cop–code that fails to run unless ALL defences are down [hence,the allusion to pants down]

snip...

I'm just making a point; I dislike all the tracking of everything I type,save,see,use,start,stop,plugin etc,

Even if this is just supposed to assist you?

I would have considered the original intent of cookies to be patently 'assistive'... but those days are long gone. I don't for a second consider datamining 'assistive'. They have evolved significantly.

Data is now so valuable companies are but a few steps behind the blackhats in implementing 'choice making software' that runs sans consent. Cookies are not software but the ability to trigger 'features' code is evolving rapidly....cookies are no longer benign. Supercookies ....well i am waiting to hear that justification. I don't need a law degree to know when I've been beaten up or robbed. I don't need a CompSci degree to know the Int–box is just the vehicle. Follow the money

Sebastien, motive and means almost certainly lead to the purps.

2points about "assistance in choice": I like to make choices and not have them made for me, it muddys the waters of 'what's good for me'. Secondly, see 1st point.

A the third of two points, trust has been broken so all websites are duly bound to establish trust...And since I decide when to trust, I need to be highly convinced.

Speaking of convincing, Are you sure the script from ntsvcfg is benign in addition to being useful?

snip...

Scripted cookies are certainly capable of doing malicious things,

So? What specifically?

reset browser features and security levels for one. Grab whatever data the browser is designed [or inadvertently designed to] hand over or allow.

I defer to your knowledge FTSoA. I am still suspicious of unstated assistance though.

as I read, AND, every problem [not of my own doing by disabling useful services] has occurred while temporarily enabling Java /Java–Scripting or 'mobile code' to accomplish a download or a device configuration.

## Re: Clarification–Win2k Netstat sockets interpretation

Interesting. Could it be that your Java VM and/or your webbrowser is totally outdated?

No. Latest Dec 19–06 download of firefox and t–bird. Windoz updates reluctantly on Auto[permision] to install required.

Speakingof...Windows claims to be unable to deliver me security updates from the website [~ms.com] and asks for full trusted status scripting,cookies,etc activated and sends me the 'validation' exe that fails to run [or did it,was it "assisting me" in some other unstatedway"??? BUT, auto updates bypass all security and permissions as long as the required services are running. So...who owns my computer?

I get security levels reset, host file manipulated etc...

WTF? A non–admin user doesn't even have write access to the HOSTS file.

vidasupra

I realize I am in gray water when trying to limit permissions and still allow software mods,registry cleaning etc..

I no doubt have vulnerabilities ..... i came here seeking help not claiming authority.

I do know something of human nature though and needn't be an expert in all fields to spot funkiness in areas of limited authority.

For all the banter,I am still at you mercy and seeking assitance.

The rest is entertainment and long distance connection...Or, am I responding to a BOT? Has AI finally made the leap?

You had me going HAL.

I doubt you are didactically 'out of date' on mal–techniques datamining and exploits, so what are you getting at?

You should learn to differ between non–identifying information, computer–identifying information and personal information, as well as who can read it under which circumstances.

You are absolutely correct there HAL, er ah, Sebastian. Unfortunately, the trust has been abused by so many marketers that until I learn enough about how to distinguish I will be handcapped.

## Re: Clarification–Win2k Netstat sockets interpretation

About exploits: The official statistics tell that Mozilla Firefox, if always kept up–to–date, was at best vulnerable for 34 days for a non–critical problem. Which could already have been worked around by pro–active configuration.

True...but I am talking about my INsecurity at an even more basic level; that of which options to disallow and which services to disable and ... I have come to accept that a determined and clever hacker will always have his/her way with my box....that didn't come out right!

....

A script is a script is a series of commands that you can read in cleartext. You can easily read how the script determines the Windows version, configures the services and adds registry entries.

ok, I'll give it a go.

....

I pity you. Mandrake is about the second–worst to start off.

You could probably pity me for more substantial reasons...like my need to inject humor to gain acceptance, and my unfortunate physical features, and...

ZA alerts me to ALLOW/DISALLOW every instance of a program, module or process before it makes a registry change.

If you're still running ZoneAlarm, you shouldn't wonder about anything going wrong in your system. The registry functions filter fucking it up a bit should be your least worries.

Can you give me a "F'r instance"?

Why are you so averse to ZA? of all the commercial FWs it at least allowed me a modicum of insight into what passes twixt my puty and the wire. Were it not for that I [most non–experts] would have no idea of how much undisclosed persons want our data and how much mischief is on the superhiway. This much I will admitt, now that I see figures like 605,000 instances reported of but a single mal–port seek in a month[day?] ...network admins must be sick of the "ZA just notified me of a blocked attack..." and i know from my ISP that even they don;t get any response from other ISPs to shutdown mal~ and attack sites. So, at least I have progressed to 'empathy' for you.

What about using Windows' security features? Now this allows you to define

Re: Clarification–Win2k Netstat sockets interpretation

security domains and, in contrast to the add-on nonsense, can actually enforce this policy.

BINGO! That is what I really really wanted to learn from you...how do I shut down non-essential services in W2k [or XP] and change permissions to harden and control what leaves and enters my computer?

The rest is entertaining and I hope you enjoy it as much as I and don't feel the need to light up after a reply...[that damned injection again!]

Seriously, my attempts have led to 'failure to connect', failure to launch', failure to fail... and even with all the reading I have been doing I suspect many admins seek the same thing ...else there would be no NG dedicated to this.

....

There an applet to ENABLE NETBIOS LOOKUP, DISABLE/BLOCK NETBIOS OVER TCP/IP

that still perplexes me...

Thanks for the assistance thus far Sebastian.

Warf.

.