

How did they get behind my NAT?

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2007-10/msg00006.html>

- *From:* Maniaque <maniaque27@xxxxxxxxx>
 - *Date:* Wed, 10 Oct 2007 10:38:41 -0000
-

Sorry I'm new here, not sure this is the right newsgroup to post to – I have a question that is about routers, security, and connectivity all rolled into one.

Yesterday while I was working on my desktop all of a sudden a session kicked in on my VNC server – my desktop background image disappeared and the RealVNC system tray icon turned black to indicate a session in progress. Within a couple of seconds, something hit my start menu, run dialog, "cmd", and typed "TFT" in the new command prompt window. At this point I panicked and shutdown the VNC service ASAP.

This post is not actually about the VNC problem, I found out today that the version I used had a known security flaw that allowed bypassing the password prompt. That is clearly what happened there, and could be easily fixed with upgrading to the newest version.

My question is how the attacker got to my VNC port!

Here's all the background I can muster:

- I am running an ADSL router, "Xavi" brand, "7028r" model, and it seems to run a "GlobespanVirata" chipset. This was provided to me by my previous ADSL provider, Telefonica Spain.
- I have a standard NAT lan, with a variety of devices connecting to the internet through the router.
- I have certain very specific ports forwarded to my desktop for remote access, peer-to-peer connectivity, etc. \
- I am NOT forwarding either of the VNC ports (standard ports 5900 and 5800), so to my limited knowledge the VNC service should not be accessible from the internet. I have of course tested this, and found that to be correct. The VNC service is not publically accessible.
- I do not have the firewall enabled on the router, because I assumed the NAT basically made it safe. I tried enabling the router firewall today but it also seems to block the services that I need to be able to access from the internet (eg HTTP, I run a small webserver), so that does not work for me.
- I WAS running uTorrent at the time of the attack (and had been for a few hours)
- I did get the IP address of the attacker from my VNC log, it was

How did they get behind my NAT?

"85.239.126.86", an address in germany. I have not looked for or found any further information. I guess I could try a port scan but I assume it's a zombie computer so what's the point.

Now my understanding is that "85.239.126.86" being an internet address, for the VNC session to work that address would need to be routable – the only way that that address could be routed on my network is through the ADLS router / gateway (I think). In theory I guess there could have been some sort of local tunnel set up, but I assume that would have required a virtual network adapter to have been set up on my computer? (I saw nothing like that, and virus and spyware scans have come up clean).

If it was routed through my router, how could the attacker have convinced the router to initiate the communication to my internal port 5900 on that particular machine??? The safety of a NAT, as I understand it, is that remote hosts cannot access an internal address unless there is explicit port forwarding enabled, or the session is initiated by a host behind the NAT, is that not correct?

I guess I'm only coming to the real point of my post now – assuming that I'm on the right track, and that this communication on port 5900 was happily handled by my router, could it have been initiated by another program on my desktop, specifically the uTorrent client? I've been logging sessions on my router since this morning, and I see that client connections are opened by the uTorrent client (very frequently, thousands per hour) with random local port numbers, that slowly seem to increase / cycle. It is possible that the uTorrent client made a client connection using local port number 5900 (which was also being used by the VNC server), and the computer/remote host that the uTorrent client was connecting to took advantage of this situation to test / probe / attack the VNC server on that port?

I guess the questions are:

- it it possible for a client TCP connection to be initiated by a local "client" program from a port that is already being used by a "server" program, like VNC server?
- what are the chances, statistically speaking, that this would happen? Would it be worth a hacker's time to set up servers as bittorrent participants / seeds in the hopes that some client computer makes a connection using a special port (eg VNC), which could then allow the computer's VNC server to be probed / tested for the known VNC vulnerability? It's the only explanation that I can think of, but I just can't see how it would be worth a hacker's time!

Final blurb: I set up a syslog server on my desktop and have been logging all incoming and outgoing sessions from my router (generating a nasty amount of log data, but I'll put up with it). This way I'll be able to see how the session gets set up, if I ever become aware of another similar situation. I will upgrade my VNC server of course, so the attack would need to use another vector. My concern of course is

How did they get behind my NAT?

How did they get behind my NAT?

that I may NOT be aware of it next time. My desktop is not hardened as a public server with all ports exposed – I'm very much counting on the fact that only specific selected ports should be accessible from outside. In theory, if any port on the desktop can be exposed, then my windows filesharing setup is just one of the things that would be vulnerable to brute-force attack. Is there anything else I can do to investigate this or help prevent future issues? Does anyone have any experience with the Xavi router or GlobespanVirata chipset that could help me get it set up to prevent this from happening again? For now I will probably install a local firewall on the desktop allowing only the servers I need to work, but that of course makes all sorts of things more complicated – file and printer sharing, VPN client software setup, HTTP proxy setup, etc etc. I just wish I could feel safe in my own network again!

Sorry about the monster first post, I would appreciate any and all feedback.

Thanks,
Tao