

Re: How did they get behind my NAT?

Re: How did they get behind my NAT?

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2007-10/msg00012.html>

- *From:* Maniaque <maniaque27@xxxxxxxxxx>
 - *Date:* Thu, 11 Oct 2007 08:50:42 -0700
-

On Oct 11, 6:25 am, Leythos <v...@xxxxxxxxxxxxx> wrote:

– 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.

Not having experience with that router, I can't be sure what limits it has or what quality of NAT and forwarding it has. The key thing is that the device does not provide a PUBLIC IP inside the LAN area and that you have control over what is forwarded inbound.

It does not.

I've seen a number of DSL routers that are PPPOE (no experience with oA) that use NAT to 1 IP, but they forward ALL ports inbound to that IP – so the users might as well be on a public IP.

regardless of the inbound transport type (PPPoE, PPPoA, RFC1483, etc), most NAT router devices (that I have seen) do not by default use a "default forwarding IP", although it is an option on many. Not this one, as it turns out.

Double NAT'ing only has an advantage if you have one of those devices that forwards ALL PORTS to the single internal IP provided by the device.

Re: How did they get behind my NAT?

ok... and what is the advantage then? The only reason I'm considering it is because then I can use a regular/standard device like the linksys wrt54G that is well-known and supported on the internet, turn on the firewall on that device (which I had to disable on the router I use now), and keep the services that I need up.

Because if you don't know enough that you have to ask here, it means you don't know enough to be securely exposed to the internet.

Oh come on – this sounds a lot like "I don't know exactly, but I know it's a bad idea, so I'm going to make fun of you instead of answering the question". I understand that exposing a port exposes any service that listens on that port. I also understand that that then means any vulnerability in that service then becomes a vulnerability for the entire server, and potentially (in my case, without DMZ etc) the entire network. I understand that, and it's a risk I'm OK with. My question is whether anyone can tell me whether there are any circumstances under which port forwarding is "bad" in and of itself, rather than because of any vulnerabilities in the services that it purposefully exposes.

uTorrent doesn't expose your VNC, but, there is any number of unknowns where as to what you've done in addition. The issue is that I've not seen anyone that needs to run a file-sharing program on their computer unless they were pirating files of some type. Yea, not always true, but it's a good assumption since there are legal means and methods without using file sharing methods.

OK, now there's a sensible suggestion – you're saying (unless I got it wrong) that the infection probably had nothing to do with the port forwarding at all, but rather was because of some something I picked up while downloading all those pirated "w4r3z" that I keep hidden under the kitchen sink, and that said malware has escaped detection either through compromising my detection tools or because they're just too specific, not known widespread infections. To be fair, that is a possibility. I do take more risks than I probably should, I could well at some point have run something I shouldn't have... but I don't think so.

No, it's the start of trying to determine what happened while you are

Re: How did they get behind my NAT?

Re: How did they get behind my NAT?

also secure to do it. NAT only blocks inbound, so you could learn if what's on your machine also phones home or creates a connection to a remote location to allow control. First thing is block inbound connections, second is monitor outbound connections or block them entirely while you look.

Ah, now there's a sensible suggestion, again – running a software firewall or carefully monitoring all outgoing traffic on the router (a monster task, i
it's accumulated 20 megs of data in 1 day) would certainly help identify any unpleasant low-key trojan I may have running.

AVG is crap – I've seen hundreds of computers with AVG compromised. I use Symantec Corporate software, it's not a resource hog like Norton is and it's stopped all that I've been exposed to.

If you want to know what AV products to trust, I've always found this site to have unbiased reviews and test results:

<http://www.av-comparatives.org/>

Nice to know, thanks!

Here are a few tools that I use and trust:

Always remember – only download files from Trusted Sites.

The following links will take you to vendors sites for Spy Ware / Ad ware removal tools and also for Antivirus tools. After you install any of these applications and update them, run them in SAFE MODE to allow them to properly clean your system.

First, make sure that your Java is updated to the latest version:<http://www.java.com/en/download/index.jsp>

These sites are for downloading Anti-Malware and Anti-Spyware tools, in order that I would use them myself:

Dave Lipman's tools:

Download MULTI_AV.EXE from the URL
--http://www.pctipp.ch/ds/28400/28470/Multi_AV.exe

AdAwareSE can be found here:http://www.lavasoft.com/products/ad_aware_free.php

SpyBot Search and Destroy can be found

Re: How did they get behind my NAT?

here:<http://www.safer-networking.org/en/download/index.html>

Thanks, never heard of multi-AV

err – how does safe mode help? you mean so I don't have any additional programs running?

Because many malware can't run in safe mode – it's not just "you having any additional programs running". In the case of Multi-av, download it, run it in normal mode to get the updates, but don't run the scans, then reboot in safe mode, run it again, since safe mode disables the network, you've already downloaded them, now run the scans, full drive, run each of the 4 scanners and run them until nothing is found.

Fair enough, I didn't realize the idea was to more thoroughly scan for malware, but with the suggestions above I think I'm well equipped to do that :)

I'm well aware of torrent software, but I don't use it either and never have a problem getting distro's downloaded. I don't subject my networks to unknowns.

ok, but calling the entire family of bittorrent programs a general "unknown" is exaggerating a little, no? The protocol is well-specified and well-understood, there are the same security measures built in as for a direct download from a distributor via HTTP or FTP (i.e MD5 hash). If you're referring specifically to uTorrent, fair enough. Not open-source, already had one known vulnerability – I'd say it's more risky than I planned.

I also don't download apps I've not paid for or music or anything that is questionable – not saying you do, as you've side stepped that issue – but the quickest way to get compromised is to start downloading pirate wares.

Yep, that's fair.

Re: How did they get behind my NAT?

Re: How did they get behind my NAT?

5) Put your website on a proper web server, one protected by a real firewall and on a locked down OS following the OS Vendors FULL SUGGESTIONS ON HOW TO SECURE IT.

ok, so what you're saying is that there is no way to safely run a simple website without paying out either professional hosting fees or buying all the equipment that hosting vendors require. A safe, but uninspiring, answer.

No, what I'm saying is that there is little chance that a non-OS guru, that a non-technical type, is going to run a website without being compromised or exploited – notice why you are here.

Yep, but that's how you learn. I'm a little bit irked by your condescending tone, but I really do appreciate the time and help – while I have worked with professional windows-based webserver development and hosting for several years and have a pretty good idea of "best practices" are at a corporate level, I'm trying to work on a shoe-string budget here, get a taste for doing things for free or cheap. As I get burned, I'm trying to understand exactly why and how.

UPnP is disabled, but I would love to understand what the problem / risk with port forwarding is – can you provide any information, links, resources to help me understand?

IF you allow anyone in you risk being connected too, simple enough to understand.

But more than a little simplistic, no? The ONLY argument against port-forwarding that I have seen from you so far, and that I was well aware of before, is that it limits the security of your server, and in my case network, to the security of the service running on the forwarded port. On the other thread (sorry about the messed up cross-post, like I said I am new here), someone suggested that there are ways and means to gain access to a port OTHER than the one being forwarded – but if I understand correctly that argument applies equally if you don't forward ports at all!

Re: How did they get behind my NAT?

Re: How did they get behind my NAT?

If you run a website then you really need to step back and start learning about security and how to setup a DMZ and how to lock down your services, BEFORE YOU PUT THEM ONLINE.

Well, I was pretty sure I had :)

Which is why I'm trying to understand where I went wrong. As you've noted, I have probably not searched extensively enough for malware – I will keep at it. Other than that, I run an updated version of Apache, there are no known vulnerabilities for other services I expose, uTorrent seems the most risky, and the jury's still out on what actually caused the problem:

- malware that I somehow acquired?
- unknown uTorrent vulnerability?
- misunderstanding of how NAT works, leading to attacker's ability to access a port that was NOT forwarded?

Port Forwarding – means you are allowing the WORLD ACCESS TO THE PC YOU ARE PORT FORWARDING TO, FOR THAT PORT/SERIES OF PORTS. If you don't have the service answering that port(s) secured then you've exposed your network.

Yes, that's pretty obvious. But that's not a problem with port forwarding, it's a problem with the services you are exposing. Obviously if they are not secure, and they are public, nothing is secure.

Thanks again,
Tao

.