

## Re: Port scanned by these strange IPs...

**Source:** <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-11/1486.html>

---

**From:** Moe Trin (*ibuprofin\_at\_painkiller.example.tld*)

**Date:** 11/23/05

Date: Wed, 23 Nov 2005 13:49:16 -0600

On 22 Nov 2005, in the Usenet newsgroup alt.computer.security, in article <1132708062.890858.220370@g47g2000cwa.googlegroups.com>, someone wrote:

>Hi, thanks for your helpful insight. I've been port scanned more today,  
>and they seem to be going for ports 1025, 1027, 1028, 1029 and 135.

135 is a different service – they're looking to gain clues. The ports 1025 to 1029 (in your case, though I've seen slightly higher) is just messenger spam. They aren't attacking you. They are looking for fools who have windoze messenger service open, so they can deliver advertising. Block it and ignore.

>What tool do you use for your WHOIS lookups? I use [www.dnsstuff.com](http://www.dnsstuff.com),  
>which obviously isn't 100% complete!

```
[compton ~]$ which whois  
/usr/bin/whois  
[compton ~]$
```

That might be a hint that I'm not using windoze. That's actually the whois3 tool from RIPE. I don't know if they have a version for windoze.

>BTW, why would anyone want to do a UDP port scan if it is  
>connectionless? Obviously the point of a port scan is to find open &  
>vulnerable port numbers to establish an illicit connection...

It's not a scan. Depending on what else you have running on your system, and what starts first, messenger is listening on one of those ports. In normal use, a peer would query your system to find out which port your system is listening on – but spammers just send the garbage blindly and hope that one of those ports is open. If it is, the spam is delivered. If it's not open – it didn't cost the spammer anything, it's no big deal. It's like the spammers are flying overhead in a big plane, and dumping millions of sheets of paper – if one lands on you, they have a possible success (you still have to read it, and buy whatever crap they are trying to sell). If the paper misses you – no problem, because they don't have to pay for it and they can get tons more. Look out, here comes another plane!

When microsoft invented this Interweb thingy for windoze95, they copied some of the tools we've had for ten or more years earlier. Because they didn't understand all of the background (and because the users are untrained), they eliminated the security features that had existed. In the case of this 'messenger service' they took the old UNIX 'talk' service and enabled it by default (it's almost never used in UNIX) and changed it to UDP (with a TCP connection, if the peer does not agree to a connection, one does not exist – no messenger spam), so that it's easy to use (and abuse – but that's your problem, not microsoft's).

*>UDP keeps track of the contacts using port numbers, just like TCP.*

UDP is usually used for 'one-shot' connections. A primary example is DNS. Your system sends a single packet to a DNS server asking (for example) "what is the IP Address of www.foo.example.com?". The server replies with a single packet – and from the network standpoint, there is no connection, just two one-way packets. Your client (and the server) know it's question/answer but no one else cares. If your client doesn't receive an answer in a reasonable time (seconds), it merely sends a new question. DNS conversations are very simple, and can be abbreviated down to a few bytes, so it makes no sense to go through all of the work of setting up a TCP connection which would take a total of seven packets, when UDP can do it in two.

Old guy