

Re: TCP Scan by Google machine?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-01/0351.html>

From: Michael Fuhr (mfuhr_at_fuhr.org)

Date: 01/07/05

Date: 7 Jan 2005 13:26:39 -0700

"Documatrix" <florrie@casualsailor.com> writes:

- > *I've been playing around with OnlineEye Pro today and its Network*
- > *Traffic Monitor has been logging attempts by a Google machine (verified*
- > *by WhoIs) to access TCP ports on my home Windows XP laptop. (It's up to*
- > *the 4100's now.)*

What are the source ports on Google's side? If the connections have a source port of 80 then the "attempts" might simply be packets that belong to old HTTP connections you made to Google. Does the monitor log TCP flags like SYN, ACK, FIN, RST, etc.? If so, what are they?

Another possibility is that somebody's running a port scan by exploiting a Google service that proxies connections. Hopefully Google has taken steps to prevent such abuse, but somebody might have found a way. Their translation service, for example, appears to allow only certain ports in the URLs it accepts.

- > *Why would a Google machine do this? I'm running Google Desktop Search*
- > *and the Google Toolbar, but this hardly seems provocative.*

I don't know how these work so I don't know if they could be responsible. If the "attempts" your monitor logs are just packets that are part of an old connection, then I suppose these services could have initiated those connections.

--

Michael Fuhr

<http://www.fuhr.org/~mfuhr/>