Subject: Re: Renguard Crash or something.
Posted by 0x90 on Thu, 04 Jan 2007 07:14:07 GMT
View Forum Message <> Reply to Message

> Creed3020 wrote on Wed, 03 January 2007 23:48
> I was doing some of my own reconaissence of Renguard and while it boots up new HTTP connections open up to members.tmm.lyceu.net
>
> Could that site be another depot for the index.bin file? It queries my PC from a different port each time so opening up a port for it would mean opening up a huge range.

members.tmm.lyceu.net is the first host "members.lycos.co.uk". renguard connects to lycos.co.uk but i guess you looked it up with some external tool which only gets the IP and does a reverse dns resolution. if you ping members.lycos.co.uk and this lyceu.net address you will notice they have both the same IP. and if you do a reverse dns (cmd: "ping -a THEIP") you will only get the lyceu.net.
so this is all ok and just like it should!

but first again.. please forget all those port opening / port forwarding things theyre all talking about here. im always behind a router with hardware firewall plus my desktop firewall and i got no problems (and i dont have any ports forwarded).
its just a web-request and an outgoing connection to renguard! you dont need _any_ incoming ports for this.

so i would ask you now to try this other thing i said and use "ethereal" or some other network-analyzer to see whats happening!
get the latest binary from www.ethereal.com (direct download link:
http://www.ethereal.com/distribution/win32/ethereal-setup-0.99.0.exe
after its installed and running try to capture and analyze the http traffic.
we should see very fast then where it stops working!

if you need help with this just reply back.

regards
0x90