

RE: Networking and DOS attacks

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-05/msg00088.html>

- *From:* "Jim Serino" <jim.serino@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 3 May 2006 22:37:06 -0400
-

Well Since I have done extensive work on these UDP Port hits and have recorded them for over 7 months and I can assure you that the address are not being spoofed as many think. As you say they are since I have done serious detailed analysis of the data that is sent in those packets. They are nothing more than ADVERTISEMENTS. I have sent all my information to those companies and countries involved with this scam. As such I have been at times blacklisted thru SORBS as a spammer because I have sent legitimate information about these scams. Most of these IP address show up on the SANS top 10 listing every night.

I have all the known sending IP address since they continue to be the same. It took me a full week of just going thru One Hours worth of DETAILED packet information from my firewall rawlogs. That spreadsheet is 5 MEG in size where as the log file is only 2 meg ins size. The difference is because I not only have the sending IP address and who is controlling it and the Advertised website name and its IP address and the Company that is maintaining it for them and the final destination address.

This is not a joke these are nothing more than scammers. I have kept quiet about this and have written to Craig Wright about this and the scam. Craig's Law knowledge impressed me and sent him only a little of the information I get.

Here is only a brief listing of the scammers:

Sending IP Address Country Advertised Website which is only a jump thru site IP Address of the website Owner of IP Address Final Destination website IP Address of final OWNER /country
202.111.173.84 CHINA www.helpfixpc.com 64.214.203.136 Global Crossing
<http://www.registryupdate.com/> 200.105.36.166 OPTYNEX TELECOM of Panama
202.111.173.84 CHINA www.helpfixpc.com 64.214.203.136 Global Crossing
<http://www.registryupdate.com/> 200.105.36.166 OPTYNEX TELECOM[PARA]of Panama
221.5.251.242 CHINA <http://theregfixer.com> 63.251.92.195 eNom thru Internap
<http://winregcleaner.com/?hop=xiulipc1> 68.178.172.84 Go Daddy Software,
Inc[PARA]USA
202.99.172.130 CHINA www.cleanthispc.com 67.19.13.19 ThePlanet.com Internet
Services, Inc. <http://www.registrycleaner32.com/?hop=cleanthepc>
64.111.198.131 ISPrime, Inc.[PARA]USA