

Forum:[Hack Forums](#)

Thread: [How to avoid getting your botnet shutdown](#)

aquabats - September 8, 2009, 12:18 pm

I hear that most Botnets that are shutdown have over 10k bots

But I was wondering how exactly do these Botnets get shut down?

What can you do to avoid getting your botnet down and what precautions should you take?

There's people will far more than 10k bots in their botnet and are still running fine so what are they doing differently than those who do get shut down?

When DDoSing, are there things you should avoid? or are there extra things you should do to make sure your botnet isn't found?

Would you suggest having multiple botnets with multiple IRC servers?

?Analog? - September 9, 2009, 1:40 pm

Bump cause im also curious

B-B-B-Brandon - September 9, 2009, 1:47 pm

It depends on the hosting you have and how secure your bot/server is.

Soiz - September 9, 2009, 2:49 pm

The victim needs a warrant to get the ip info from the ISP Which can only be obtained if alot of damage is caused.

Please correct me if Im wrong

marq14 - September 9, 2009, 2:55 pm

Someone can also take them over, IDK how though.

aquabats - September 11, 2009, 4:07 am

(Sep 9, 2009 02:49 PM)Soiz Wrote: [CITE](#) The victim needs a warrant to get the ip info from the ISP Which can only be obtained if alot of damage is caused.

Please correct me if Im wrong

yeah but the IPs are IPs of your zombies

How exactly do the authorities shut down botnets?

I'm thinking they get in contact with a zombie and somehow see to which IRC server it is connecting to and find you from there

Kewlhotrod - September 11, 2009, 4:37 am

Basically. They can commandeer the PC, find your .EXE, decompile it and gain all the info to your server... Or they can packet sniff the IP and port on multiple of these computers, find a connection/similarity if they're all sending to the same IP with the same port.

Grab a VPN.

aquabats - September 11, 2009, 4:48 am

(Sep 11, 2009 04:37 AM)kewlhotrod Wrote: [CITE](#) Basically. They can commandeer the PC, find your .EXE, decompile it and gain all the info to your server... Or they can packet sniff the IP and port on multiple of these computers, find a connection/similarity if they're all sending to the same IP with the same port.

Grab a VPN.

Can the FBI/Authorities get warrents for all VPNs?

Can you suggest any VPNs that some how don't have to give into warrents?

Free/Paid doesn't matter