

Forum:[Hack Forums](#)

Thread: [\[HELP\] HTTP bot net vs IRC bot net](#)

DOWN3D - May 3, 2016, 6:30 am

So...Im new to Bot Net and Zombies. What is the difference between IRC and HTTP bot net? I did a search on GOOGLE but I couldn't find anything usefull. I think that HTTP bot net is an free website where you host a panel and then u upload shells to other websites and DDoS with them. IRC I think is about making an simple .exe file that an user executes and it becomes an zombie that is directly linked with the control panel program in your PC. So could someone give me some details? Also what are the best HTTP bot nets files and how to set them up? (I need them for DDoS especially) ~ Sorry for bad english

13795847 - May 3, 2016, 6:32 am

Ironical that you know almost nothing about nets,
Yet your name is "DOWN3D".
Just seems cocky.

If you need access contact me via. Skype
rushdecieveabsorbingbat57

DOWN3D - May 3, 2016, 6:35 am

Well, Im new to nets :(So dont flame me...

SIM-2198759 - May 3, 2016, 8:51 am

Before i start anything, you WILL need money for this, and if you plan on trying to do it for free, theres no chance, but anyway, ill try give you a quick idea.

A HTTP Botnet is mainly used for things like data farming (Passwords, emails, ect..), bot selling/botshops, hoarding bots, and more.

An IRC Botnet is better for fast response time, so it's mainly used for things like DDoS, Where the command will be executed almost instantly.

HTTP uses something called a "knock timer" (Im sure some people will have other names), Where as IRC holds a constant connection between the bot and server. The knock timer is basically a time interval between the bots connections, so lets say i set it to 30 seconds, Once every 30 seconds, the bots will check in, say "Im here, anything i need to do?" and so on, they will execute commands you issue, and it will help the panel keep count on what bots are online, and which bots are offline.

Now, for spreading, both IRC and HTTP bots can use an exe to get bots, just like a RAT, You have to spread your binary to your victims, and get them to execute it, You will also come across things like Kaiten, an IRC Bot coded in C, Most bots that are coded in C, will be directed at you infecting linux machines and servers, where as an exe is aimed at windows machines.

What you asked for in the OP, is a Botnet for DDoS, so id recommend an IRC Bot, You can either purchase one that targets windows systems, or get something that targets linux systems as this will probably be better for your DDoS Attacks.

P.S I did miss some info out, i tried to make it short but give you a general idea, try googling again.

(What is an IRC Botnet, What is a HTTP Botnet, ect..)

nomnomq - May 3, 2016, 4:59 pm

i'm still using my ircbot and always will, not keep listen to all the l33t h4x0rz who think they are something special and better than you now just cos using some HTTP bot.

DNSHACKING - May 3, 2016, 6:38 pm

(May 3, 2016 06:30 AM)DOWN3D Wrote: [\[CITE\]](#) So...Im new to Bot Net and Zombies. What is the difference between IRC and HTTP bot net? I did a search on GOOGLE but I couldn't find anything usefull. I think that HTTP bot net is an free website where you host a panel and then u upload shells to other websites and DDoS with them. IRC I think is about making an simple .exe file that an user executes and it becomes an zombie that is directly linked with the control panel program in your PC. So could someone give me some details? Also what are the best HTTP bot nets files and how to set them up? (I need them for DDoS especially) ~ Sorry for bad english

Join our team, and we will work with you and spread the bot. We know some great spreading methods. We are looking to start a botnet as well.

youtube.com/watch?v=PNU1qnL7btc

I'm thinking if we work together, we will have a large botnet server.

SIM-2198759 - May 3, 2016, 8:02 pm

(May 3, 2016 06:38 PM)DNSHACKING Wrote: [\[CITE\]](#) Join our team, and we will work with you and spread the bot. We know some great spreading methods. We are looking to start a botnet as well.

youtube.com/watch?v=PNU1qnL7btc

I'm thinking if we work together, we will have a large botnet server.

Oh boy, that video was cringe.

Nuclear3mbargo - May 4, 2016, 7:51 am

Quote:Also, HTTP botnets are harder to detect, because they generally blend in with network traffic.

While IRC botnets tend to be detected more often because they aren't used as much anymore.

BULLSHIT, it depends on how the bot is written! And how does the fact that IRC botnets are used less nowadays make their detection ratio different? The fact that the HTTP botnet "blends" with other traffic wouldn't make any difference at the end nobody will inspect every package on hand.

Pick3 - May 4, 2016, 8:34 am

I think IRC is better for ddos.

qwertyblah - May 4, 2016, 9:04 am

(May 4, 2016 07:51 AM)Nuclear3mbargo Wrote: [\[CITE\]](#) BULLSHIT, it depends on how the bot is written! And how does the fact that IRC botnets are used less nowadays make their detection ratio different? The fact that the HTTP botnet "blends" with other traffic wouldn't make any difference at the end nobody will inspect every package on hand.

Its not bullshit. Nowadays 99% IRC traffic is malicious because almost no one is using IRC for communication. You can't say the same for HTTP.

The only reason you should be using IRC over HTTP is if you REALLY REALLY REALLY need almost instant responses. If you can afford to wait 10-20 minutes for your DDOS to start then HTTP will be better.

Nuclear3mbargo - May 4, 2016, 9:34 am

(May 4, 2016 09:04 AM)qwertyblah Wrote: [\[CITE\]](#) Its not bullshit. Nowadays 99% IRC traffic is malicious because almost no one is using IRC for communication. You can't say the same for HTTP.

The only reason you should be using IRC over HTTP is if you REALLY REALLY REALLY need almost instant responses. If you can afford to wait 10-20 minutes for your DDOS to start then HTTP will be better.

You can't make this assumption just like this. But then again, if somebody is analyzing the system for malware, the fact that the malware uses HTTP instead of IRC wouldn't matter at all.

Note: I'm not stating that IRC is better than HTTP botnet, I'm stating that their difficulty for analysis is the same(as long as only the protocol is concerned)

qwertyblah - May 4, 2016, 9:36 am

(May 4, 2016 09:34 AM)Nuclear3mbargo Wrote: [\[CITE\]](#) You can't make this assumption just like this. But then again, if somebody is analyzing the system for malware, the fact that the malware uses HTTP instead of IRC wouldn't matter at all.

It does indeed matter. There are networks where only HTTP and HTTPS is allowed. If you use a disallowed protocol your connection simply does not get through.

?cary - May 4, 2016, 10:15 am

IRC : Stable connection , Used mostly for DDOS .

HTTP : It gives you complete control over your victim PC. (can be used for DDOS ,power depends on number of slaves you have on your panel)

For brief explanation , refer DeathStroke ?

Nuclear3mbargo - May 4, 2016, 12:16 pm

(May 4, 2016 09:36 AM)qwertyblah Wrote: [\[CITE\]](#) It does indeed matter. There are networks where only HTTP and HTTPS is allowed. If you use a disallowed protocol your connection simply does not get through.

That's a fact, however those networks are mainly corporate, and usually the devices from this network connect to short range of servers, in which case the fact that you use HTTP/s will likely bring your botnet down faster.

Also if you look in general, if you don't target a specific network, the number of networks which allow only HTTP/S will probably be irrelevant.

refocus - May 5, 2016, 5:07 pm

(May 3, 2016 06:22 PM)Nukes Wrote: [\[CITE\]](#) Just want to point out that if you were to use an HTTP botnet you could set it up in a way that every client knocks the server at the same time (assuming the server can handle all of the simultaneous requests). This can be done by getting the time from a site (like google) and then every hour it can knock the web server and you can just upload the ddos script 10 min. before the hour and have all the bots ddos simultaneously.

Also, HTTP botnets are harder to detect, because they generally blend in with network traffic. While IRC botnets tend to be detected more often because they aren't used as much anymore.

What to take from this, HTTP botnets are in general better than IRC ones.
Do you like bots because you can't root in 2016? :P

__SIP - May 5, 2016, 6:03 pm

(May 4, 2016 07:51 AM)Nuclear3mbargo Wrote: [\[CITE\]](#) BULLSHIT, it depends on how the bot is

written! And how does the fact that IRC botnets are used less nowadays make their detection ratio different? The fact that the HTTP botnet "blends" with other traffic wouldn't make any difference at the end nobody will inspect every package on hand.

Aside from the fact IRC is a dated protocol that is hardly use, it is extremely easy to detect simply because of the IRC traffic. Not only is it continuous but it extremely easy to check on a network.

tl;dr you are an idiot.

(May 5, 2016 05:07 PM)refocus Wrote: [\[CITE\]](#) Do you like bots because you can't root in 2016? :P Rooting has nothing to do with using IRC as means for communication. In fact, it is deprecated.

Nuclear3mbargo - May 5, 2016, 11:55 pm

(May 5, 2016 06:03 PM)___SIP Wrote: [\[CITE\]](#) Aside from the fact IRC is a dated protocol that is hardly use, it is extremely easy to detect simply because of the IRC traffic. Not only is it continuous but it extremely easy to check on a network.

tl;dr you are an idiot.

Hey moron, read the previous posts, I stated that the fact that a bot uses HTTP doesn't make the analysis harder.

qwertyblah - May 6, 2016, 2:08 am

(May 5, 2016 11:55 PM)Nuclear3mbargo Wrote: [\[CITE\]](#) Hey moron, read the previous posts, I stated that the fact that a bot uses HTTP doesn't make the analysis harder.

DPI will rape all your IRC bots.

___SIP - May 6, 2016, 8:21 am

(May 5, 2016 11:55 PM)Nuclear3mbargo Wrote: [\[CITE\]](#) Hey moron, read the previous posts, I stated that the fact that a bot uses HTTP doesn't make the analysis harder.

That is simply wrong. Any unskilled person can figure out if they are infected with malware using IRC as CNC.

Stop posting, thank you.

Nuclear3mbargo - May 7, 2016, 2:22 am

(May 6, 2016 08:21 AM)___SIP Wrote: [\[CITE\]](#) That is simply wrong. Any unskilled person can figure out if they are infected with malware using IRC as CNC.

Stop posting, thank you. How does this make the analysis of HTTP harder, than IRC ? Do you even know what this argument is about?

___SIP - May 7, 2016, 10:20 am

(May 7, 2016 02:22 AM)Nuclear3mbargo Wrote: [\[CITE\]](#) How does this make the analysis of HTTP harder, than IRC ? Do you even know what this argument is about?

I already told you why.

The issue is you are simply too unskilled and unknowledgeable to follow up with a proper response stating why analysis would not be harder.

Stop posting and drink bleach, retard.

qwertyblah - May 7, 2016, 10:51 am

(May 7, 2016 02:22 AM)Nuclear3mbargo Wrote: [\[CITE\]](#) How does this make the analysis of HTTP harder, than IRC ? Do you even know what this argument is about?

lol.

Getting number of infections for HTTP is much more harder than IRC.

For IRC is pretty straight forward - just join the channel lmfao.

__SIP - May 7, 2016, 11:05 am

(May 7, 2016 10:51 AM)qwertyblah Wrote: [\[CITE\]](#) Getting number of infections for HTTP is much more harder than IRC.

The majority of botnet web panels have exploits in them which are publicly available. So you can certainly get way more information than an IRC server.

(May 7, 2016 10:51 AM)qwertyblah Wrote: [\[CITE\]](#) For IRC is pretty straight forward - just join the channel lmfao.

Unless the IRC server is configured correctly.

TERRORISST----- - May 7, 2016, 12:52 pm

(May 7, 2016 11:05 AM)__SIP Wrote: [\[CITE\]](#) The majority of botnet web panels have exploits in them which are publicly available. So you can certainly get way more information than an IRC server.

Unless the IRC server is configured correctly.

You're defining the security and authenticity of a protocol on what HF skids manage to write? That's like saying IRC is insecure because you gave everyone OP.

qwertyblah - May 7, 2016, 12:55 pm

(May 7, 2016 11:05 AM)__SIP Wrote: [\[CITE\]](#) Unless the IRC server is configured correctly. If bots can join the IRC channel then anyone can.

You talk about password? Anyone can reverse it.

__SIP - May 7, 2016, 1:08 pm

(May 7, 2016 12:55 PM)qwertyblah Wrote: [\[CITE\]](#) If bots can join the IRC channel then anyone can.

You talk about password? Anyone can reverse it.

Does not mean bots can see everyone else in the channel.

(May 7, 2016 12:52 PM)TERRORISST----- Wrote: [\[CITE\]](#) You're defining the security and authenticity of a protocol on what HF skids manage to write? That's like saying IRC is insecure because you gave everyone OP.

What makes you think I was referring to what HF kiddies write? It is well known panels from bots off this board get pwn'd every version due to the lack of competency from developers.

I mean, one could say it boils down to how the setup is being operated. It does not necessarily define the security and authenticity of a protocol but it does define the risk and vulnerabilities you take when using <insert protocol here>.

Nuclear3mbargo - May 7, 2016, 1:30 pm

(May 7, 2016 10:20 AM)__SIP Wrote: [\[CITE\]](#) I already told you why.

The issue is you are simply too unskilled and unknowledgeable to follow up with a proper response stating why analysis would not be harder.

Stop posting and drink bleach, retard.

Then why don't you tell me how, exactly ? I mean, does HTTP have some hidden feature, which will

make the analysis of the executable harder? Or you're going to tell me that the server executable will hide its self into the traffic(if it's the second - go and kill your self)

The fact that the a botnet uses HTTP instead of ANY other protocol for communication, doesn't make the analysis nor the detection harder.

__SIP - May 7, 2016, 1:42 pm

(May 7, 2016 01:30 PM)Nuclear3mbargo Wrote: [\[CITE\]](#) Then why don't you tell me how, exactly ? I mean, does HTTP have some hidden feature, which will make the analysis of the executable harder? Or you're going to tell me that the server executable will hide its self into the traffic(if it's the second - go and kill your self)

The fact that the a botnet uses HTTP instead of ANY other protocol for communication, doesn't make the analysis nor the detection harder.

So you go from making shitty posts regarding protocol to bins? Your unclear and lack of concise posts reflects your knowledge.

Please, stop posting. You are upset the fact any bot using IRC as a CNC can be detected by any unskilled person.

The protocol a bot uses has a lot to do with "detection." Any shitty AV will flag a program or connection to a IRC server. It is a simple fact. IRC is deprecated, especially for windows, in regards of being a CNC for bots. The only decent or acceptable use now is for DDoS when you are looking for near instant responses.

Nuclear3mbargo - May 7, 2016, 1:48 pm

(May 7, 2016 01:42 PM)__SIP Wrote: [\[CITE\]](#) So you go from making shitty posts regarding protocol to bins? Your unclear and lack of concise posts reflects your knowledge.

Please, stop posting. You are upset the fact any bot using IRC as a CNC can be detected by any unskilled person.

The protocol a bot uses has a lot to do with "detection." Any shitty AV will flag a program or connection to a IRC server. It is a simple fact. IRC is deprecated, especially for windows, in regards of being a CNC for bots. The only decent or acceptable use now is for DDoS when you are looking for near instant responses.

HEY MORON, who is talking about detection ration of AV?

I was arguing about analysis of unknown malware, one which isn't yet known to AV vendors and humans must analyze it. YOU CAN'T ASSUME THAT PROGRAM IS MALICIOUS ONLY BECAUSE IT USES IRC PROTOCOL WHEN YOU ARE CONDUCTING ANALYSIS OF UNKNOWN PIECE OF PROGRAM.

TERRORISST----- - May 7, 2016, 1:55 pm

(May 7, 2016 01:08 PM)__SIP Wrote: [\[CITE\]](#) Does not mean bots can see everyone else in the channel.

What makes you think I was referring to what HF kiddies write? It is well known panels from bots off this board get pwn'd every version due to the lack of competency from developers.

I mean, one could say it boils down to how the setup is being operated. It does not necessarily define the security and authenticity of a protocol but it does define the risk and vulnerabilities you take when using <insert protocol here>.

The point i'm trying to make here is that a protocol is just a means of communication. Security is

merely dependent on the developer. You can't justify using an alternate protocol because of developer incompetence.

__SIP - May 7, 2016, 1:55 pm

(May 7, 2016 01:48 PM)Nuclear3mbargo Wrote: [\[CITE\]](#) HEY MORON, who is talking about detection ration of AV?

I was arguing about analysis of unknown malware, one which isn't yet known to AV vendors and humans must analyze it."Unknown malware." God please stop posting if you do not know anything about heuristics or any behavior analysis techniques AV's utilize.

(May 7, 2016 01:48 PM)Nuclear3mbargo Wrote: [\[CITE\]](#) YOU CAN'T ASSUME THAT PROGRAM IN MALICIOUS ONLY BECAUSE IT USES IRC PROTOCOL WHEN YOU ARE CONDUCTING ANALYSIS OF UNKNOWN PIECE OF PROGRAM.

Of course you can, what legitimate programs use IRC these days?

(May 7, 2016 01:55 PM)TERRORISST----- Wrote: [\[CITE\]](#) The point i'm trying to make here is that a protocol is just a means of communication. Security is merely dependent on the developer. You can't justify using an alternate protocol because of developer incompetence.

Good thing I was replying to a post attempting to berate a protocol based on flaws of the operator.

Nuclear3mbargo - May 7, 2016, 2:04 pm

(May 7, 2016 01:55 PM)__SIP Wrote: [\[CITE\]](#) "Unknown malware." God please stop posting if your do not know anything about heuristics or any behavior analysis techniques AV's utilize.

Of course you can, what legitimate programs use IRC these days?

1. Name me a AV which heuristic engine will mark a program as malicious so that I don't buy it (I'm pretty sure that there is vendor which will mark an program for dangerous only because it uses IRC protocol, however it's not one of the popular vendors).

2. On one hand you're right, on the other you don't know who has developed it, and there may be some legit reason to use it, but you just can't flag a program as malware only because it uses IRC (well you can on your systems of course, but it will be irresponsible to add it as potential harmful software on others).

P.S Sorry for calling you moron, it was childish from my side. You have my apologies.

libc - May 8, 2016, 9:05 am

IRC is an awful protocol for C&C. Period. That's a fact.

If you're so damn concerned about instant response time then write your own scalable TCP/IP server.