

Forum:[Hack Forums](#)

Thread: [Botnets 101](#)

Juggernaut - January 10, 2012, 3:58 am

Hello im going to talk about botnets and i will also go through the pros and cons on each type (http,p2p,irc). Sooo without further redue, lets begin.

And yeah, i do not take any responsebility for what you do, this is just a tutorial.

1.1 Introduction.

Botnets are a type of malware that allows the master to somewhat controll the slaves, more likely send packets via the ip protocol.

There are allot of diffrent botnet sources, some costs money and some are free, if you are looking for a free botnet source i recomend you to use the search function, or use google.

Diffrent botnet sources have diffrent fetures, but the most common ones are:UDP* Attack of some sort.

SYN* flood, or if its a simpler it will use SSYN*

HTTP flood

UDP (User Datagram Protocol) http://en.wikipedia.org/wiki/User_Datagram_Protocol

is the most basic protocol, if you compare it with TCP. it does not open a stream but instead just sends its data and then its done with it, udp is good for just flooding the victim and using up all his bandwith so no one else can use the service and so causing a Denial Of Service.

SYN is more or less the synonym for TCP, becouse when spamming with TCP (Transmission control protocol), Is opening a stream to the server and then disconnecting after a response like this: Attacker-> Victim and when the victim is trying to send a ack back, the

Attacker aborts and starts a new one, but the server still waits for the ack until the timout is reached and the packet is dropped. But the attacker does this so fast so in the end the victim is going to have the maximum connections it can handle and then a denial of service will ocur.

1.2 Diffrent types of botnets:Http botnets

p2p botnets

IRC botnets

1.3 Http botnets:

A http botnet is a botnet that is running on a webserver, wich then recives connections from the slaves.

The pros with the http version is that you only need a webhost supporting php and some sort of SQL.

The Cons of the http version is that its often rather unstable, its relying on that the slaves can comunicate on port 80.

1.4 p2p botnets

A p2p botnet (Peer-to-peer botnet) is the simplest version of botnets, they rely on your home

connection, so all slaves connects to you.

Even though they are so simple they have a few downsides: Requires a highspeed internet connection.

Unsafe*

Its generally allot of buggs in them.

Unsafe*: Becouse every slave connects to you, witch in it self can cause a denial of service attack (kinda ironic) but also that every bot get your ip.

Now some one is going to comment "But i use a vpn, they wont be able to track me!" and that is actualy not acurate. Lets sit down and think for a while. This is you: (im going to pretend that everyone uses a router)

your local address (192.168.1.100) -> 192.168.1.1 -> xxx.xxx.xxx.xxx -> VPN -> Internet. And now your thinking yeah, they will get my VPNs ip address not mine. wich is correct, but what do you think happens with a packet that comes to you? it will do the same but backwards:

Slave -> VPN -> xxx.xxx.xxx.xxx -> 192.168.1.1 -> 192.168.1.100.

You see now that all packets that come to the vpn is being forwarded to you. So how about if someone traces the vpns ip address? the packets will be forwarded to you! wich means that they will have your ip. result, YOUR DOOOOOMED. or something simulaire.

1.5 IRC botnets

Ah, my favorite. IRC botnets, they are acording to me the most stable type of botnet.

i will first go over the pros: Not hosted on your ip.

Stable.

No need for UPNP in the bot.

Cons:

Requires a offshore vps.

The Botnet sources often costs more.

A irc botnet works like this.

Slave -> IRC server -> channel

simple and relieble.

then you connect and give the irc commands.

you -> Irc -> channel -> .dos xxx.xxx.xxx.xxx 80

1.6 How to stay safe.

This is a very important step. first of all you want to: STAY AWAY FROM P2P BOTNETS!

Use a Proxy/VPN everytime you log on the webserver.

Use a Proxy/VPN everytime you log on the IRC.

1.7 Outro:

Well i guess that this is the end. You really hope that you can forgive me for my horrible spelling, ive tried to keep it as correct as possible but im not from an english speaking country.

If you want something added or changed you send me a pm.

If you have ANY questions About ANYTHING in this tutorial you can send me a pm, if you have a hard time learning protocols, send me a pm.

if you cant tell the difference between http and irc botnets, pm me!

This is all i had for today. God night/God evening / god something
PEACE!

Transpositional?Thinking - January 10, 2012, 10:32 am

Nice tutorial! Though I typically think of a peer-to-peer botnet a little differently. You can set them up to be self hosting, like a torrent network. Everyone connects to each other and that's how they stay active, then you just connect in and send out a command. This is the safest way to do a botnet but unless you code it yourself you will be spending thousands to get one of those suckers. They typically hold ridiculous amounts of bots and almost rely on the numbers to keep the network online.

Juggernaut - January 10, 2012, 11:18 am

Thank you! i actually havnt heard about that sort of botnet. If you have any sources id like to see them.

Transpositional?Thinking - January 10, 2012, 3:12 pm

Here is a very interesting case study focusing on p2p botnets if you're really interested.

http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard_html/

blady20 - January 10, 2012, 6:29 pm

SYN is not a synonym to TCP. SYN refers to the 3 step handshake of TCP connections.

Consider this. Host A & B are connecting.

A -> SYNchronize -> B

A <- SYN-ACKnowledge <- B

A -> ACK -> B

While most of this information is somewhat accurate, a portion is completely incorrect. Please don't make tutorials if you don't know what you're doing.

A SSYN flood is a Spoofed SYN Flood. SYN packets are spoofed, causing a half-connected TCP stream. A TCP flood is never referred to as a SYN flood.

For instance,

Consider this. A is SSYN flooding B. A spoofs it's address to C.

A -> SYN -> B

C <- SYN-ACK <- B

C -> Nothing (It never sent a SYN, so it doesn't reply to a SYN-ACK) -> B

Juggernaut - January 11, 2012, 7:15 am

Thank you for the correction blady, Please dont be a dick tho.

The Ethical Hacker - June 3, 2012, 11:14 am

OP LOL @ "IRC > HTTP" when it's a known fact that all of the biggest botnets use HTTP now days.

Juggernaut - June 3, 2012, 12:08 pm

(Jun 3, 2012 11:14 AM)The Ethical Hacker Wrote: [\[CITE\]](#) OP LOL @ "IRC > HTTP" when it's a known fact that all of the biggest botnets use HTTP now days.

No, the biggest botnets are still using IRCs for commands.

The Ethical Hacker - June 4, 2012, 10:24 am

(Jun 3, 2012 12:08 PM)Juggernaut Wrote: [\[CITE\]](#) No, the biggest botnets are still using IRCs for commands.

Mind proving that?

STUXNET etc... all seem to use HTTP as hosts can take more traffic, and when you post or whatever the packets are smaller, if that makes sense?

Juggernaut - March 2, 2013, 6:29 am

(Jun 4, 2012 10:24 AM)The Ethical Hacker Wrote: [\[CITE\]](#) Mind proving that?

STUXNET etc... all seem to use HTTP as hosts can take more traffic, and when you post or whatever the packets are smaller, if that makes sense?

HTTP is not better, sure it's easier but it can get compromised very easily.

And what the fuck are you smoking? bigger packets? No, the packets are still the same size.