

Forum:[Hack Forums](#)

Thread: [How bots are stable.](#)

L C K - November 3, 2018, 9:26 pm

Hello, I'm here from the pen testing community and i always see people complain about losing bots? Please inform me on why that's bad and how do people hold bots so well compared to others. I'm asking because I'm not too educated in this field.

F.B.I - November 3, 2018, 9:41 pm

(Nov 3, 2018 09:26 PM)Fitzkiss Wrote: [\[CITE\]](#) Hello, I'm here from the pen testing community and i always see people complain about losing bots? Please inform me on why that's bad and how do people hold bots so well compared to others. I'm asking because I'm not too educated in this field. Not too educated either but its obviously bad to lose bots because you lose money. The bigger the botnet the more money you make.

L C K - November 3, 2018, 9:42 pm

(Nov 3, 2018 09:41 PM)DotComs Wrote: [\[CITE\]](#) Not too educated either but its obviously bad to lose bots because you lose money. The bigger the botnet the more money you make. I'm more interested in the code side. Like what makes different botnets more stable then others?

user9b - November 3, 2018, 10:17 pm

Stable refers to two things. How well the bot can communicate and stay undetected with the host and how well the server on the php side can handle traffic. For instance, if you can't code worth a shit or your server cannot handle 1K plus connections at one time your bots will start to drop. On the host side of it, you need to stay under the radar or AV and not be noticed by the user. The big-time malware families do an excellent job of this because I mean let's be real it's their full-time job. They spend hours researching AV and exploits, and new CVE. The reason anyone on this forum has a CVE in their project is most likely some security researcher reverse engineered one of the prominent malware families new techniques and showed it to the world so the good guys can look out for it. It will take months for the companies actually to patch it so on the meanwhile all the low-level coders implement this into their new programs and sell them on here for several hundred bucks pretending to be 1337 hax0rs. I got a little off topic, but basically, that's how bots/botnets are referred to as stable in a general sense. I could get more technical but its no point I'm too buzzed.

Sillee - November 4, 2018, 1:07 am

Keeping your builds updated periodically (FUD Crypt) as well as making sure run-time works.

Your hosting servers network also has some play in it; especially when holding mass amounts of bots.

L C K - November 4, 2018, 6:30 am

(Nov 3, 2018 10:17 PM)user9b Wrote: [\[CITE\]](#) Stable refers to two things. How well the bot can communicate and stay undetected with the host and how well the server on the php side can handle traffic. For instance, if you can't code worth a shit or your server cannot handle 1K plus connections at one time your bots will start to drop. On the host side of it, you need to stay under the radar or AV and not be noticed by the user. The big-time malware families do an excellent job of this because I mean let's be real it's their full-time job. They spend hours researching AV and exploits, and new CVE. The reason anyone on this forum has a CVE in their project is most likely some security researcher reverse engineered one of the prominent malware families new techniques and showed

it to the world so the good guys can look out for it. It will take months for the companies actually to patch it so on the meanwhile all the low-level coders implement this into their new programs and sell them on here for several hundred bucks pretending to be 1337 hax0rs. I got a little off topic, but basically, that's how bots/botnets are referred to as stable in a general sense. I could get more technical but its no point I'm too buzzed.

Been doing research on iot mirai specifically. I asked around and people said that for it to be considered a bot that hold good. That you need to pack the bins. What does this mean.

user9b - November 4, 2018, 11:35 am

(Nov 4, 2018 07:30 AM)Fitzkiss Wrote: [\[CITE\]](#) Been doing research on iot mirai specifically. I asked around and people said that for it to be considered a bot that hold good. That you need to pack the bins. What does this mean.

A packer is like a technique where it hides your actual payload from the host. It is used to bypass AV's and to make the malware harder to detect. It is like persistence. In simple terms, it packs/encrypts and changes around the file format. Packers make it harder for security researchers to reverse engineer the malware. Yet in the end, it might take them a while but they usually end up getting around the packers.

R4A1 - November 4, 2018, 12:10 pm

There are many things that make a botnet "stable" if you're talking about stable as in ability to hold bots then here are some key factors:

- Your botnet must have good persistence

- It must be undetected by antiviruses at scantime AND runtime or else the antiviruses will remove the file from their machine.

The_Wise_Saviour - November 4, 2018, 4:59 pm

(Nov 4, 2018 01:07 AM)JumpmanJay Wrote: [\[CITE\]](#) Keeping your builds updated periodically (FUD Crypt) as well as making sure run-time works.

Your hosting servers network also has some play in it; especially when holding mass amounts of bots.

- hello friend please tell

- how to update build

- how to make FUD Crypt

- how to make sure runtime work

- how to play network servers

Elvira - November 4, 2018, 8:01 pm

well its bad if you lose bots because youre losing power. holding bots comes to the quality of the malware.

Legion - November 5, 2018, 7:13 am

(Nov 4, 2018 09:01 PM)Elvira Wrote: [\[CITE\]](#) well its bad if you lose bots because youre losing power. holding bots comes to the quality of the malware.

Kinda right there. The quality of how the malware injects itself and keeps itself running matters. So does the encryption and spreading method

It's also been mentioned here before but if you're running an HTTP botnet, you want a good webserver. If not then you can't say for sure than you can hold all the bots.

Junx - November 6, 2018, 12:21 am

One of the most important things in your malware is the startup method implemented in your crypter or payload.

Zettabit - November 7, 2018, 6:45 am

Another key thing is proper error handling. If you don't handle exceptions or just catch them and ignore them, then chances are your bot is going to crash.