

Forum:[Hack Forums](#)

Thread: [Advanced Linux Botkiller](#)

Shisho - December 17, 2019, 10:15 pm

I've been developing a botkiller that specifically targets malware running on Linux servers. Ideally it runs on 32 bit and 64 bit architectures and uses the C99 header `stdint.h` to define architecture independent unsigned integers with fixed widths. This should allow it to be portable across any 32/64 bit system.

The code can be found below:

<https://github.com/shishohf/advanced-botkiller>

The code uses the kernel PID max file to get the maximum PID and uses a zero signal kill that iterates from 1 to the PID max and stores it in an array. It then uses the `/proc` filesystem to find the binary file that started the process by reading the symlink found under `/proc/PID/exe` and stores the real path. It checks if the file has been removed by searching the real path for the string "(deleted)" and kills the process if it has. If it has not been deleted it then proceeds to store the binary file in a buffer and iterates over it byte by byte to match any sequence of characters located within the binary provided in the `STRINGS[]` array. If it matches any sequence it kills the process and removes the binary.

I am looking for suggestions that will improve this botkiller.

I was considering adding functions like a `ptrace` if you are root to access process memory and scan heap and stack for strings since bots like Mirai use encrypted strings loaded into a linked list and reverse the encryption at runtime.

Anything you think is useful will be considered as I am actively developing this code.

Thanks in advance.

CyberStrike - December 18, 2019, 12:15 pm

This is interesting certainly a good edition, I will look at it more in depth.

Shisho - December 18, 2019, 4:03 pm

(Dec 18, 2019 01:15 PM)CyberStrike Wrote: [\[CITE\]](#) This is interesting certainly a good edition, I will look at it more in depth.

Whenever you get the chance: please do suggest any functions that can be implemented to improve the detection of Linux malware so that it can be adequately killed.

G0dzSoldiers - December 19, 2019, 1:46 pm

Nice share maybe add more known strings ?

Shisho - December 19, 2019, 3:33 pm

(Dec 19, 2019 02:46 PM)G0dzSoldiers Wrote: [\[CITE\]](#) Nice share maybe add more known strings ?

This is still in the phase of proof of concept. When it is ready to be run on production environments the array of known strings can be expanded. You can change the size of the array and add any known strings if you currently would like to expand them. The string detection function works for

strings of any size.

(Dec 19, 2019 02:51 PM)xtraemint440 Wrote: [\[CITE\]](#) You could try and address rootkit detection as well.

There's plenty of resources on Linux rootkit research so you could read that kind of material to get a grip on what you can start to do regarding detection features.

I will go ahead and look into this. It seems like a good suggestion.

Senpai™ - December 19, 2019, 3:37 pm

I will check this and review

Dhoroty - December 19, 2019, 11:35 pm

There could be random apps, that could be valid, but still it can contains any of the strings.

You should implement some kind of whitelist, to keep that apps.

For example your app will contain all the bad words, and that will be running, but, you should not kill and delete it.