

Forum:[Hack Forums](#)

Thread: [Bot Killer Source code?](#)

SIM-5102439 - April 25, 2022, 1:07 pm

Been looking around HF and I can't seem to find any bot killer or source code for one, not even on Git

Can anyone point me in the right direction to find one?

SIM-3602340 - April 25, 2022, 1:37 pm

A simple idea that comes to mind in order to disable malware on a system is to disable startup programs, by removing malicious startup keys in the registry or schtasks and then rebooting the system. A more "aggressive" approach would be something like https://github.com/hasherezade/hollows_hunter or <https://github.com/hasherezade/pe-sieve> to identify injected implants that are running in the system.

Ofcourse there are more ways a software could achive startup
<https://www.ired.team/offensive-security/persistence>

ManWithNoFear - April 25, 2022, 1:41 pm

Good idea very nice.....

SIM-5102439 - April 25, 2022, 3:11 pm

(Apr 25, 2022 01:37 PM)Cereal000 Wrote: [\[CITE\]](#) A simple idea that comes to mind in order to disable malware on a system is to disable startup programs, by removing malicious startup keys in the registry or schtasks and then rebooting the system. A more "aggressive" approach would be something like https://github.com/hasherezade/hollows_hunter or <https://github.com/hasherezade/pe-sieve> to identify injected implants that are running in the system.

Ofcourse there are more ways a software could achive startup
<https://www.ired.team/offensive-security/persistence>

You are missing the point. The main reason you would want to run a botkiller is to kill every other bot on your victim, while still maintaining yours. Your suggestion will kill every bot on the victim's machine, including yours

SIM-3602340 - April 25, 2022, 3:51 pm

(Apr 25, 2022 03:11 PM)DawgyDawg Wrote: [\[CITE\]](#) You are missing the point. The main reason you would want to run a botkiller is to kill every other bot on your victim, while still maintaining yours. Your suggestion will kill every bot on the victim's machine, including yours

I didn't suggest anything sir, I just shared an idea on how one could remove or disable basic malicious software running on his own system without using software like anti viruses or EDRs(which of course should be the first choices), and linked two good open source projects that were programmed after a good research.

Also in many states its against the law to run software on systems without the owner permission.

Originally you asked about anti-malware source code and then started talking about "victim"? I don't partecipate in illegal actions. I misinterpreted your question, sorry about that.

Anyway I am done with this thread... and probably section.

RobStark - June 9, 2022, 6:20 am

Do you think it is possible to create such a killer bot, which would remove other people's miners from the computer? It constantly comes out that my hash rate drops because we always interfere with each other's mining.

AnonTri - June 9, 2022, 4:41 pm

(Apr 25, 2022 01:07 PM)DawgyDawg Wrote: [\[CITE\]](#) Been looking around HF and I can't seem to find any bot killer or source code for one, not even on Git

Can anyone point me in the right direction to find one?

There probably will not be many. The best ones work for specific pieces of malware and remove them based on how they achieve persistence. Like all the botnets on github that have a remover. You would just build the same kind of thing for each malware you want to kill. You could try to kill them all by removing any suspicious auto starts but those could be programs setup by the owner of the device and it may tip them off something is wrong. IOT botnets usually come with a bot kill function, you could see if anything they do is helpful to you.

A lot of older nets advertised bot killers and I am sure most private nets will have them for public malware. If not you might want to see if you can get your hands on it to test it or find a piece in the wild and try to understand it by executing or reversing it (in terms of building your own botkiller based on specific pieces of malware).

Ph4n70M Phr34K - June 10, 2022, 2:05 pm

betabot had a pretty strong botkiller but i dont think you can find its source.

__Digital__ - June 11, 2022, 12:48 pm

Honestly the best way would be to build as i have a killer which once infected with my malware, it takes snapshot of registry and monitors for dropped files. Once you know how to do that then you can mark them for deletion upon reboot or even to be a complete @\$\$ would be to replace their malware with yours thus preventing removal. As long as your malware is coded correctly it would only allow one instance of it self anyways. Just so you all think outside the box. It is really easy not hard at all to have a good killer.. Anyways enough about that you all have a good day.