

Forum:[Hack Forums](#)

Thread: [Botkill Script](#)

?Golden Freddy - January 10, 2015, 8:20 am

Hello HF,

I need a bot kill script for a program I am making. If someone would be so kind to make one for me it would be greatly appreciated. If you would not like it to be public you could PM me the script.

~Creatiionz ?

stackoverflowin - January 10, 2015, 8:25 am

Hi,

You could go through each process, read the bytes of the file and see if it matches up any type of keyword.

?Golden Freddy - January 10, 2015, 8:33 am

(Jan 10, 2015 09:25 AM)StackOverlowin Wrote: [\[CITE\]](#) Hi,

You could go through each process, read the bytes of the file and see if it matches up any type of keyword.

Yes I might try that, but I believe there are better methods.

He B TeMy - January 10, 2015, 8:39 am

(Jan 10, 2015 09:33 AM)Creatiionz Wrote: [\[CITE\]](#) Yes I might try that, but I believe there are better methods.

What do you mean by better methods?

?Golden Freddy - January 10, 2015, 8:40 am

(Jan 10, 2015 09:39 AM)He B TeMy Wrote: [\[CITE\]](#) What do you mean by better methods?

Better ways to detect the bots, and stop them

He B TeMy - January 10, 2015, 8:44 am

And what do you mean by bots?

Sure they start with windows, you can start there.

?Golden Freddy - January 10, 2015, 8:46 am

(Jan 10, 2015 09:44 AM)He B TeMy Wrote: [\[CITE\]](#) And what do you mean by bots?

Sure they start with windows, you can start there.

Bots like RATs, keyloggers, etc.

It can be used for both white hat, and black hat use.

+Haze - January 10, 2015, 9:46 am

(Jan 10, 2015 09:46 AM)Creatiionz Wrote: [\[CITE\]](#) Bots like RATs, keyloggers, etc.

It can be used for both white hat, and black hat use.

Don't quote me on this, but you could mimic what antiviruses do. In terms of going through each process, and scanning the HASH of the file for viruses. If it contains a virus or whatnot, then you kill

the process. Much like what VirusTotal.Com does.

I'm not a malware developer so I wouldn't know but it's just an idea that you could try.

Odus - January 10, 2015, 9:56 am

(Jan 10, 2015 10:46 AM)+Haze Wrote: [\[CITE\]](#) Don't quote me on this, but you could mimic what antiviruses do. In terms of going through each process, and scanning the HASH of the file for viruses. If it contains a virus or whatnot, then you kill the process. Much like what VirusTotal.Com does.

Wait what?

VirusTotal's antivirus engines are command line versions, so depending on the product, they will not behave exactly the same as the desktop versions: for instance, desktop solutions may use techniques based on behavioural analysis and count with personal firewalls that may decrease entry points and mitigate propagation, etc.

Citation: <https://www.virustotal.com/en/about/about/>

+Haze - January 10, 2015, 10:02 am

(Jan 10, 2015 10:56 AM)Odus Wrote: [\[CITE\]](#) Wait what?

VirusTotal's antivirus engines are command line versions, so depending on the product, they will not behave exactly the same as the desktop versions: for instance, desktop solutions may use techniques based on behavioural analysis and count with personal firewalls that may decrease entry points and mitigate propagation, etc.

Citation: <https://www.virustotal.com/en/about/about/>

Isn't that how desktop antiviruses work? In terms of, they scan the hash of the file right? Because that's what I've heard around here. If not then I'm wrong, and disregard my last two posts.

Hmmm, well what I meant to say was. To kill "bots", you could scan the file of the process. And if It contains a suspicious hash file then maybe you check the file for other things, and if it's suspicious enough you kill it.

iamskid - January 10, 2015, 10:53 am

(Jan 10, 2015 11:02 AM)+Haze Wrote: [\[CITE\]](#) Isn't that how desktop antiviruses work? In terms of, they scan the hash of the file right? Because that's what I've heard around here. If not then I'm wrong, and disregard my last two posts.

Hmmm, well what I meant to say was. To kill "bots", you could scan the file of the process. And if It contains a suspicious hash file then maybe you check the file for other things, and if it's suspicious enough you kill it.

No antivirus software check for known HASHes sir. Its quite easy to make your file change hash on each run(by appending 0x00 lol).

In fact, scantime detection by anti-virus software is useless(as proved by our beloved script kiddies capable of copy+pasting AutoIT/.NET crypters and get them FUD) what is important is the runtime detection(HIPS/Proactive defense) (which these script kiddies fail to defeat due to use of RunPE(VirtualAllocEx+WriteProcessMemory) which is impossible to reproduce in any .NET framework language because a efficient HIPS runs from kernel-mode(Betamonkey attempted this from ring3 and it was quite successful however still trash when fighting against malware which hide their presence from kernel-mode).

TL;DR Stop using .NET trash for anything, its slow as shit and nothing decent can be made in it. Look at Visual Studio, coded in C# yet cannot handle ANY(due to how slow .NET is. Java is too btw) large projects so companys just look for other IDE.